

А. С. Холево

Квантовые системы, каналы, информация

Электронное издание

Москва
Издательство МЦНМО
2014

УДК 519.72, 530.145
ББК 22.18, 22.311, 22.314
X71

Холево А. С.
Квантовые системы, каналы, информация.
Электронное издание.
М.: МЦНМО, 2014.
327 с.
ISBN 978-5-4439-2092-4

Квантовая теория информации — новая быстро развивающаяся научная дисциплина, которая изучает общие закономерности передачи, хранения и преобразования информации в системах, подчиняющихся законам квантовой механики. Квантовая теория информации активно использует аналитический аппарат теории матриц и операторов в гильбертовом пространстве для исследования потенциальных возможностей таких систем и разработки принципов их рационального синтеза. Попутным результатом развития идей квантовой теории информации является существенное прояснение логической структуры квантовой механики, ее оснований и соотношения с реальностью.

Настоящая монография посвящена математической теории квантовых систем, каналов связи, их энтропийных и информационных характеристик и является продолжением и существенным развитием ранее вышедшей книги автора «Введение в квантовую теорию информации» (МЦНМО, 2002). В ней нашел отражение ряд новейших результатов, таких как доказательство теоремы о квантовой пропускной способности, основанное на тесной связи с криптографическими свойствами канала; вычисление информационных характеристик квантовых гауссовских систем; достижения в проблеме аддитивности энтропийных характеристик каналов и пр.

В настоящем издании исправлены опечатки.

Для студентов, аспирантов и научных работников, специализирующихся в областях современной математической физики, теории информации, теории вероятностей и математической статистики.

Подготовлено (с исправлениями) на основе книги:

Холево А. С. Квантовые системы, каналы, информация. — М.: МЦНМО, 2010. — 328 с. — ISBN 978-5-94057-574-0

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11,
тел. (499)241-08-04.
<http://www.mccme.ru>

ISBN 978-5-4439-2092-4

© Холево А. С., 2014.
© МЦНМО, 2014.

Оглавление

Предисловие	8
-----------------------	---

Часть I

Глава 1. Векторы и операторы	13
§ 1.1. Гильбертово пространство	13
§ 1.2. Операторы	14
§ 1.3. Положительность	16
§ 1.4. След и двойственность	16
§ 1.5. Выпуклость	18
§ 1.6. Комментарии	20
Глава 2. Состояния, наблюдаемые, статистика	21
§ 2.1. Структура статистических теорий	21
2.1.1. Классические системы	21
2.1.2. Аксиомы статистического описания	22
2.1.3. Квантовые состояния	25
§ 2.2. Квантовые наблюдаемые	28
2.2.1. Квантовые наблюдаемые: построение из аксиом	28
2.2.2. Совместимость и дополнительность	30
2.2.3. Соотношение неопределенностей	33
2.2.4. Выпуклая структура множества наблюдаемых	34
§ 2.3. Оптимальное различение квантовых состояний	37
2.3.1. Постановка задачи	37
2.3.2. Оптимальные наблюдаемые	38
§ 2.4. Комментарии	44
Глава 3. Составные квантовые системы и сцепленность	46
§ 3.1. Составные системы	46
3.1.1. Тензорное произведение	46
3.1.2. Расширение Наймарка	48
3.1.3. Разложение Шмидта и очищение	50
3.1.4. Парадокс Эйнштейна—Подольского—Розена. Неравенство Белла	52
§ 3.2. Квантовая система как носитель информации	57
3.2.1. Передача классической информации	57
3.2.2. Сцепленность и локальные операции	58
3.2.3. Сверхплотное кодирование	60

3.2.4. Телепортация квантовых состояний	61
§ 3.3. Комментарии	63

Часть II

Глава 4. Классическая энтропия и информация	67
§ 4.1. Энтропия случайной величины и сжатие данных	67
§ 4.2. Условная энтропия, относительная энтропия и информация Шеннона	70
§ 4.3. Шенноновская пропускная способность канала с шумом	72
§ 4.4. Теорема кодирования для канала с шумом	74
§ 4.5. Канал с перехватом	80
§ 4.6. Гауссовский канал	82
§ 4.7. Комментарии	83
Глава 5. Квантовая теорема кодирования	84
§ 5.1. Пропускная способность классически-квантового канала связи	84
§ 5.2. Формулировка теоремы кодирования	85
§ 5.3. Верхняя граница	88
§ 5.4. Доказательство слабого обращения	92
§ 5.5. Типичные проекторы	97
§ 5.6. Доказательство прямого утверждения теоремы кодирования	102
§ 5.7. Функция надежности для канала с чистыми состояниями	105
§ 5.8. Комментарии	107

Часть III

Глава 6. Квантовые эволюции и каналы	113
§ 6.1. Эволюции квантовой системы	113
§ 6.2. Вполне положительные отображения	116
§ 6.3. Определение канала	121
§ 6.4. Каналы, разрушающие сцепленность	123
§ 6.5. Процессы квантовых измерений	124
§ 6.6. Комплементарные каналы	127
§ 6.7. Ковариантные каналы	131
§ 6.8. Q-битные каналы	133
§ 6.9. Комментарии	135

Глава 7. Квантовая энтропия и информация	137
§ 7.1. Квантовая относительная энтропия	137
§ 7.2. Монотонность относительной энтропии	138
§ 7.3. Свойства непрерывности	144
§ 7.4. Информационная корреляция, сцепленность формирования и условная энтропия	146
§ 7.5. Обменная энтропия	151
§ 7.6. Квантовая взаимная информация	153
§ 7.7. Комментарии	155
Глава 8. Классическая пропускная способность квантового канала связи	158
§ 8.1. Теорема кодирования	158
§ 8.2. χ -пропускная способность	160
§ 8.3. Проблема аддитивности	163
8.3.1. Эффект сцепленности в кодировании и декодировании	163
8.3.2. Иерархия свойств аддитивности	167
8.3.3. Некоторые энтропийные неравенства	170
§ 8.4. Передача классической информации с помощью сцепленного состояния	173
8.4.1. Выигрыш благодаря сцепленности	173
8.4.2. Доказательство обращения теоремы кодирования	177
8.4.3. Доказательство прямого утверждения теоремы кодирования	179
§ 8.5. Комментарии	183
Глава 9. Передача квантовой информации	185
§ 9.1. Квантовые коды, исправляющие ошибки	185
9.1.1. Постановка вопроса	185
9.1.2. Общая формулировка	187
9.1.3. Необходимые и достаточные условия исправления ошибок	188
9.1.4. Когерентная информация и точное исправление ошибок	190
§ 9.2. Точность воспроизведения квантовой информации	194
9.2.1. Точность воспроизведения чистых состояний	194
9.2.2. Соотношения между мерами точности воспроизведения	196
9.2.3. Точность воспроизведения и расстояние Бюреса	198
§ 9.3. Квантовая пропускная способность	201
9.3.1. Достижимые скорости	201

9.3.2. Квантовая пропускная способность и когерентная информация	204
9.3.3. Дegrадируемые каналы	206
§ 9.4. Секретная классическая пропускная способность и квантовая пропускная способность	210
9.4.1. Квантовый канал с перехватом	210
9.4.2. Доказательство теоремы о секретной пропускной способности	212
9.4.3. Большие отклонения для случайных операторов	219
9.4.4. Прямая теорема кодирования для квантовой пропускной способности	222
§ 9.5. Комментарии	227
Глава 10. Каналы с ограничениями на входе	230
§ 10.1. О сходимости квантовых состояний	230
§ 10.2. Квантовая энтропия и относительная энтропия	234
§ 10.3. С-q-канал с бесконечным алфавитом	236
§ 10.4. С-q-канал с непрерывным алфавитом	239
§ 10.5. Квантовый канал с ограничением	242
§ 10.6. Передача классической информации с помощью сцепленного состояния через канал с ограничениями	245
§ 10.7. Каналы, разрушающие сцепленность	246
§ 10.8. Приложение: спектральное разложение	251
§ 10.9. Комментарии	254
Глава 11. Гауссовские системы	256
§ 11.1. Операторы, ассоциированные с коммутационным соотношением Гейзенберга	257
§ 11.2. Канонические коммутационные соотношения	262
§ 11.3. Динамика, квадратичные операторы и комплексные структуры	266
§ 11.4. Гауссовские состояния	270
11.4.1. Характеристическая функция	270
11.4.2. Определение и свойства гауссовских состояний	271
11.4.3. Оператор плотности гауссовского состояния	274
11.4.4. Энтропия гауссовского состояния	276
11.4.5. Очищение гауссовского состояния	279
§ 11.5. Гауссовские каналы	280
11.5.1. Классически-квантовый гауссовский канал	280

11.5.2. Открытые бозонные системы	282
11.5.3. Основные свойства гауссовских каналов	286
11.5.4. Гауссовские наблюдаемые	287
11.5.5. Гауссовские каналы, разрушающие сцепленность	289
§ 11.6. Пропускные способности гауссовских каналов	292
11.6.1. Максимизация квантовой взаимной информации	292
11.6.2. Калибровочно ковариантные каналы	294
11.6.3. Максимизация когерентной информации	296
11.6.4. Классическая пропускная способность	297
§ 11.7. Случай одной моды	299
11.7.1. Классификация гауссовских каналов	299
11.7.2. Каналы, разрушающие сцепленность	304
11.7.3. Аттенюатор/усилитель	305
11.7.4. Квантовая пропускная способность	309
§ 11.8. Комментарии	312
Литература	316
Предметный указатель	325

Предисловие

Квантовая теория информации, изучающая общие закономерности передачи, хранения и преобразования информации в системах, подчиняющихся законам квантовой механики, сформировалась как самостоятельная область исследований в 1990-е гг., однако ее зарождение относится к 1950-м гг. Она возникла вслед за появлением основ теории информации и помехоустойчивой связи в трудах В. А. Котельникова и К. Шеннона. На начальном этапе, который охватывает период 1950—80 гг., основным вопросом было выяснение фундаментальных ограничений на возможности передачи и обработки информации, обусловленных квантовомеханической природой ее носителя. Развитие информационных технологий в направлении микроминиатюризации, использования достижений квантовой оптики и электроники заставляет предположить, что в обозримой перспективе такие ограничения могут стать главным препятствием для дальнейшей экстраполяции существующих технологий и принципов обработки информации.

С другой стороны, появление в 1980—90 гг. идей квантового компьютеринга, квантовой криптографии и новых коммуникационных протоколов позволило говорить не только об ограничениях, но и о новых возможностях, заключенных в использовании специфически квантовых ресурсов, таких как *сцепленность* квантовых состояний (entanglement), *квантовый параллелизм* и *дополнительность* между измерением и возмущением¹. Квантовая теория информации дает ключ к пониманию фундаментальных закономерностей, до недавних пор остававшихся вне поля зрения исследователей, а также стимулирует развитие экспериментальной физики, значительно расширяющее возможности манипулирования состояниями микросистем и потенциально важное для новых эффективных приложений. В настоящее время работы в области *квантовой информатики*, включающей квантовую теорию информации, ее экспериментальные основы и технологические разработки, ведутся во многих научно-исследовательских центрах развитых стран.

В теории информации центральную роль играют понятия канала связи и его пропускной способности, дающей предельную скорость безошибочной передачи данных. Математический подход придает этим понятиям универсальную значимость: например, память компьютера (классического или квантового) может рассматриваться как канал из прошлого в будущее, тогда пропускная способность дает количественное выражение для предельной емкости памяти при исправлении ошибок. Важность рассмот-

¹ Обсуждение физических аспектов см. в книгах Нильсена и Чанга [22], К. А. Валиева и А. А. Кокина [2], Б. Б. Кадомцева [9].

рения квантовых каналов связи обусловливается тем, что всякий физический канал в конечном счете является квантовым, и такой подход позволяет учесть фундаментальные квантовомеханические закономерности. Отметим, что в квантовом случае понятие пропускной способности разветвляется, порождая целый спектр информационных характеристик канала, зависящих от вида передаваемой информации (квантовой или классической) и от дополнительных ресурсов, используемых при передаче.

Математическая традиция в теории информации восходит к А. Н. Колмогорову и А. Я. Хинчину. Для математика, которому безразлична естественнонаучная сторона его исследований, теория информации является источником глубоких идей и новых трудных задач, имеющих достойную мотивацию. В равной, если не в большей мере это относится и к квантовой теории информации, проблематика которой оказывается тесно связанной с некоммутативным анализом, асимптотической теорией конечномерных нормированных операторных пространств и алгебр, тонкими свойствами структур положительности и тензорного произведения, а также с методами случайных матриц. В 2002 г. в издательстве МЦНМО вышла книга автора [38], посвященная математическому изложению основ квантовой теории информации. В ней, в частности, были затронуты две открытые проблемы: А) аддитивность энтропийных характеристик квантового канала, связанных с его классической пропускной способностью; Б) теорема кодирования для квантовой пропускной способности. Прошедшие годы ознаменовались быстрым прогрессом, в частности, усилиями разных исследователей было получено полное решение проблемы Б. Квантовая пропускная способность оказалась тесно связанной с криптографическими характеристиками канала, такими как пропускная способность для секретной передачи классической информации и скорость распределения случайного ключа. Был выделен важный класс деградируемых каналов, для которых эти две характеристики совпадают и зачастую могут быть вычислены в явном виде. Значительный прогресс был достигнут и в решении проблемы аддитивности (в которой, однако, по-прежнему остается много неисследованных вопросов): неожиданный результат П. Шора показал глобальную эквивалентность ряда ранее разрозненных формулировок². Проблема аддитивности обсуждалась на Международном математическом конгрессе 2006 г., а квантовая теория информации вошла в список основных тем на V Европейском конгрессе математиков 2008 г.

Все это показывает, что назрела необходимость в появлении книги, которая не только вводила бы в круг основных понятий квантовой теории

²Недавно был анонсирован контрпример к аддитивности минимальной выходной энтропии, см. Hastings M. B., e-print arXiv:0809.3972

информации, но и отражала бы по крайней мере некоторые из новейших ее достижений. Такую цель и преследует настоящая монография, основное содержание которой составляет математическая теория квантовых каналов. Ее материал разбит на три части.

Часть I содержит введение в статистическую структуру квантовой теории, а также первые применения информационных идей в квантовой статистике. Значительное внимание уделено обсуждению ключевого понятия сцепленных состояний составных квантовых систем. В части II дается обзор основных понятий и некоторых результатов классической теории информации, квантовые аналоги которых составляют основной предмет настоящей книги, а также прямое доказательство основной теоремы кодирования для классически-квантового канала.

Часть III посвящена изучению квантовых каналов общего вида и их информационных характеристик. В главе 6 подробно обсуждается абстрактное понятие канала, которое является основным для всего рассматриваемого круга вопросов. С точки зрения теории операторов это вполне положительное отображение соответствующей алгебры, аналог марковского отображения в некоммутативной теории вероятностей. С точки зрения статистической механики канал дает общее конечное описание эволюции открытой квантовой системы, взаимодействующей с окружением. Разнообразные энтропийные характеристики каналов и их свойства исследуются в главе 7. Глава 8 посвящена классической пропускной способности квантового канала и уже упоминавшейся проблеме аддитивности энтропийных характеристик каналов относительно операции тензорного произведения. В главе 9 рассматривается круг вопросов, связанных с исправлением ошибок при хранении и передаче квантовой информации и с соответствующей квантовой пропускной способностью. В главах 10, 11 действие переносится из конечномерного в сепарабельное гильбертово пространство, которое, в частности, является ареной для квантовых гауссовских систем. Многие эксперименты по квантовой обработке информации реализованы именно в таких системах с «непрерывными переменными», основанных на принципах квантовой оптики. С другой стороны, математическая сторона вопроса связана здесь с интересными и ранее не изучавшимися аспектами канонических коммутационных соотношений. Здесь возникает еще одна глубокая аналитическая проблема — «гипотеза об оптимальных гауссовских ансамблях», сопоставимая по сложности с проблемой аддитивности и, видимо, глубоко связанная с ней.

В основу книги легли лекции, прочитанные автором в Московском государственном университете и Московском физико-техническом институте. Автор благодарит М. Е. Широкова, А. А. Кузнецову и В. А. Панова за помощь при подготовке рукописи.

ЧАСТЬ I

ГЛАВА 1

Векторы и операторы

Мы будем иметь дело с квантовомеханическими системами, которые описываются конечномерными комплексными гильбертовыми пространствами. С одной стороны, уже в этом случае, причем наиболее наглядно, проявляются радикальные отличия квантовой статистики. С другой стороны, системы с конечным числом уровней представляют основной интерес для таких приложений, как передача информации, квантовые вычисления и квантовая криптография (хотя в последнее время все чаще используются системы с непрерывными переменными, которые описываются бесконечномерными пространствами, см. гл. 10, 11).

§ 1.1. Гильбертово пространство

Пусть $\mathcal{H}$ — d -мерное комплексное векторное пространство размерности $\dim \mathcal{H} = d < \infty$ со скалярным произведением $\langle \varphi | \psi \rangle$, $\varphi, \psi \in \mathcal{H}$, удовлетворяющее аксиомам унитарного пространства; следуя скорее физической, нежели математической традиции, мы считаем, что $\langle \varphi | \psi \rangle$ линейно по второму аргументу ψ и антилинейно по первому аргументу φ . Также следуя физической литературе, мы называем такое пространство гильбертовым (хотя в математике в конечномерном случае обычно используется термин «унитарное пространство», а термин «гильбертово» применяют лишь к бесконечномерным пространствам).

Мы будем использовать обозначения Дирака: вектор $\psi \in \mathcal{H}$ (который следует представлять себе как вектор-столбец) будет обозначаться $|\psi\rangle$; соответственно $\langle \varphi |$ определяет линейную функцию на $\mathcal{H}$, задаваемую скалярным произведением:

$$\langle \varphi | : \psi \rightarrow \langle \varphi | \psi \rangle, \quad \psi \in \mathcal{H}.$$

Такие линейные функции также образуют гильбертово пространство — двойственное пространство $\mathcal{H}^*$ (его элементы следует представлять себе как вектор-строки $|\varphi\rangle^*$, эрмитово сопряженные к $|\varphi\rangle$). Пространство $\mathcal{H}^*$ антиизоморфно $\mathcal{H}$ в силу отображения $|\psi\rangle \leftrightarrow \langle \psi |$; скалярное произведение $\langle \varphi | \psi \rangle$ удобно представлять себе как произведение «bra»- и «ket»-векторов $\langle \varphi |$ и $|\psi\rangle$. Квадрат нормы как в $\mathcal{H}$, так и в $\mathcal{H}^*$ равен $\langle \psi | \psi \rangle = \|\psi\|^2$.

Такой способ записи векторов позволяет удобно задавать действие операторов. Например, «внешнее произведение» «ket»- и «bra»-векторов $A = |\psi\rangle\langle\varphi|$ есть оператор ранга один, который действует на вектор $|\chi\rangle$ в соответствии с формулой $A|\chi\rangle = |\psi\rangle\langle\varphi|\chi\rangle$.

Пусть $\{e_i\}_{i=1,d}$ — ортонормированный базис (о.н.б.) в $\mathcal{H}$. Произвольный вектор $\psi \in \mathcal{H}$ может быть представлен в виде

$$|\psi\rangle = \sum_{i=1}^d |e_i\rangle\langle e_i|\psi\rangle, \quad (1.1)$$

что эквивалентно равенству

$$\sum_{i=1}^d |e_i\rangle\langle e_i| = I, \quad (1.2)$$

где I — единичный оператор в $\mathcal{H}$.

Задача 1.1.1. Запишите матричное представление для операторов в $\mathcal{H}$, аналогичное представлению векторов (1.1).

Дополнительным преимуществом обозначений Дирака является возможность записи вместо векторов их меток, например, можно писать просто $|i\rangle$ вместо $|e_i\rangle$.

Иногда мы будем рассматривать *вещественное* гильбертово (т. е. евклидово) пространство. Фундаментальное отличие комплексного случая проявляется в существовании *поляризационного тождества*

$$\beta(\varphi, \psi) = \frac{1}{4} \sum_{k=0}^3 (-i)^k \beta(\varphi + i^k \psi, \varphi + i^k \psi), \quad (1.3)$$

позволяющего восстановить все значения формы $\beta(\varphi, \psi)$, линейной по второму аргументу и антилинейной по первому, по ее диагональным значениям $\beta(\psi, \psi)$, $\psi \in \mathcal{H}$ (в вещественном случае подобное восстановление возможно лишь для симметричных форм). Благодаря этому, например, для доказательства операторного равенства $A = B$ достаточно установить равенство всех диагональных матричных элементов $\langle\psi|A\psi\rangle = \langle\psi|B\psi\rangle$, $\psi \in \mathcal{H}$.

§ 1.2. Операторы

Если A — оператор в $\mathcal{H}$, то A^* обозначает оператор, *сопряженный* к A , который определяется равенством

$$\langle\varphi|A^*\psi\rangle = \langle A\varphi|\psi\rangle, \quad \varphi, \psi \in \mathcal{H}. \quad (1.4)$$

Оператор A называется *эрмитовым*, если $A = A^*$. (Ортогональным) *проектором* называется такой эрмитов оператор P , что $P^2 = P$. Областью значений проектора P является подпространство

$$\mathcal{L} = \{\psi: P|\psi\rangle = |\psi\rangle\}.$$

Если $\|\psi\| = 1$, то оператор $|\psi\rangle\langle\psi|$ является проектором на единичный вектор $|\psi\rangle$. Более общим образом, для любой ортонормированной системы $\{e_i\}_{i \in I}$ оператор $\sum_{i \in I} |e_i\rangle\langle e_i| = P$ является проектором на подпространство, порожденное системой $\{e_i\}_{i \in I}$.

Унитарным называется такой оператор U , что $U^*U = I$; в конечномерном случае из этого равенства следует, что $UU^* = I$. *Частичной изометрией* называется такой оператор U , что $U^*U = P$ является проектором; в этом случае $UU^* = Q$ также есть проектор. Оператор U отображает область значений оператора P на область значений оператора Q *изометрично*, т.е. сохраняя скалярное произведение и нормы векторов.

Теорема 1.2.1 (спектральное разложение). *Для любого эрмитова оператора A существует ортонормированный базис из собственных векторов, которым отвечают вещественные собственные значения a_i , так что*

$$A = \sum_{i=1}^d a_i |e_i\rangle\langle e_i|. \quad (1.5)$$

Другая полезная форма спектрального разложения получается, если рассмотреть *различные* собственные значения $\{a\}$ и соответствующие им спектральные проекторы

$$E_a = \sum_{i: a_i=a} |e_i\rangle\langle e_i|.$$

Набор различных собственных значений $\text{спес}(A) = \{a\}$ называется *спектром* оператора A . В этих обозначениях

$$A = \sum_{a \in \text{спес}(A)} a E_a. \quad (1.6)$$

Такое представление единственно с точностью до порядка перечисления собственных значений. Набор проекторов $\{E_a\}$ образует *ортогональное разложение единицы*:

$$E_a E_{a'} = \delta_{aa'} E_a, \quad \sum_{a \in \text{спес}(A)} E_a = I. \quad (1.7)$$

Гильбертово пространство $\mathcal{H}$ разлагается в прямую ортогональную сумму областей значений проекторов $\{E_a\}$, на которых A действует как умножение на число a .

§ 1.3. Положительность

Эрмитов оператор A называется *положительным*, $A \geq 0$, если $\langle \psi | A \psi \rangle \geq 0$ для любого $\psi \in \mathcal{H}$. Собственные значения положительного оператора неотрицательны: $a \geq 0$ для $a \in \text{спес}(A)$.

Оператор является положительным тогда и только тогда, когда он может быть представлен в виде $A = B^*B$ для некоторого оператора B . Для любого положительного оператора A существует единственный положительный квадратный корень $C = \sqrt{A} = A^{1/2}$ такой, что $C^2 = A$.

Для любого эрмитова оператора A имеет место разложение

$$A = A_+ - A_-, \quad (1.8)$$

где $A_+ = \sum_{a>0} aE_a$, $A_- = - \sum_{a<0} aE_a$ — положительные операторы, называемые *положительной* и *отрицательной* частями оператора A .

Теорема 1.3.1 (полярное разложение). *Любой оператор A в $\mathcal{H}$ может быть представлен в виде*

$$A = U|A| = |A^*|U, \quad (1.9)$$

где $|A| = \sqrt{A^*A}$ — *положительный оператор*, а U — *унитарный оператор*.

Носителем $\text{supp } A$ положительного оператора A называется его собственное подпространство, соответствующее положительным собственным значениям. Унитарный оператор в полярном разложении определяется единственным образом только на $\text{supp } |A|$.

В вещественном гильбертовом пространстве эрмитовы операторы заменяются на симметричные, а унитарные — на ортогональные, причем определения формально остаются теми же. Полярное разложение также имеет место, причем $|A|$ — симметричный положительный, а U — ортогональный оператор.

§ 1.4. След и двойственность

След оператора T определяется соотношением

$$\text{Tr } T = \sum_{i=1}^d \langle e_i | T e_i \rangle, \quad (1.10)$$

где $\{e_i\}$ — произвольный ортонормированный базис.

Задача 1.4.1. Покажите, что это определение не зависит от выбора базиса и что

$$\mathrm{Tr} A^* = \overline{\mathrm{Tr} A}, \quad \mathrm{Tr} AB = \mathrm{Tr} BA. \quad (1.11)$$

Покажите, что

$$\mathrm{Tr} |\psi\rangle\langle\varphi|A = \langle\varphi|A\psi\rangle. \quad (1.12)$$

Покажите, что для $A, B \geq 0$ выполнено неравенство

$$\mathrm{Tr} AB \geq 0 \quad (1.13)$$

и равенство имеет место тогда и только тогда, когда $AB = 0$.

Выражение

$$\|T\|_1 = \mathrm{Tr} |T| \quad (1.14)$$

определяет *следовую норму* на комплексном линейном векторном пространстве всех операторов, действующих в $\mathcal{H}$. Для эрмитова оператора T справедливо соотношение

$$\|T\|_1 = \mathrm{Tr} T_+ + \mathrm{Tr} T_- = \sum_{i=1}^d |t_i|, \quad (1.15)$$

где t_i — собственные значения оператора T . Другой важной нормой является *операторная норма*

$$\|A\| \equiv \|A\|_\infty = \max_{\psi: \|\psi\|=1} \|A\psi\|, \quad (1.16)$$

которая для эрмитова оператора A равна

$$\|A\| = \max_{a \in \mathrm{spec}(A)} |a|. \quad (1.17)$$

Имеет место неравенство

$$|\mathrm{Tr} TA| \leq \|T\|_1 \|A\|, \quad (1.18)$$

где равенство достижимо как для любого фиксированного T , так и для любого фиксированного A . А именно, для фиксированного T следует положить $A = U^*$, где U — унитарный оператор из полярного разложения $T = |T|U$. Тогда

$$\|T\|_1 = \max_U |\mathrm{Tr} TU| = \max_{\|A\|=1} |\mathrm{Tr} TA|. \quad (1.19)$$

Аналогично для заданного оператора A равенство достигается при $T = |\psi\rangle\langle\psi|U^*$, где U — унитарный оператор из полярного разложения

$A = U|A|$, а ψ — нормированный собственный вектор оператора $|A|$ с наибольшим собственным значением. Отсюда следует, что

$$\|A\| = \max_{\|T\|_1=1} |\operatorname{Tr} TA|. \quad (1.20)$$

Эти факты лежат в основе важного соотношения двойственности. Пространство всех операторов в $\mathcal{H}$, снабженное следовой нормой, превращается в комплексное банахово пространство $\mathfrak{I}(\mathcal{H})$. Это же пространство, снабженное операторной нормой, является банаховой алгеброй $\mathfrak{B}(\mathcal{H})$. Эти пространства являются двойственными; это означает, что любая линейная функция на $\mathfrak{I}(\mathcal{H})$ представима в виде $T \rightarrow \operatorname{Tr} TA$ для некоторого оператора $A \in \mathfrak{B}(\mathcal{H})$ и имеет норму (1.20) и, наоборот, любая линейная функция на $\mathfrak{B}(\mathcal{H})$ представима в виде $A \rightarrow \operatorname{Tr} TA$ для некоторого оператора $T \in \mathfrak{I}(\mathcal{H})$ и имеет норму (1.19).

Индекс h в обозначениях пространств операторов будет использоваться для обозначения соответствующих вещественных банаховых пространств эрмитовых операторов. Вещественные банаховы пространства $\mathfrak{I}_h(\mathcal{H})$ и $\mathfrak{B}_h(\mathcal{H})$ также находятся в двойственности, задаваемой билинейной формой $T, A \rightarrow \operatorname{Tr} TA$. Тот факт, что эта форма принимает вещественные значения для эрмитовых операторов T, A , следует из соотношений (1.11).

В конечномерном случае пространства $\mathfrak{I}(\mathcal{H})$ и $\mathfrak{B}(\mathcal{H})$ совпадают с множеством всех операторов в $\mathcal{H}$ и различаются только нормами. Однако в бесконечномерном случае они существенно различаются (так же как пространства последовательностей l^1 и l^∞ над конечным и бесконечным множествами индексов).

Задача 1.4.2. Покажите, что (комплексная) размерность пространства всех операторов в $\mathcal{H}$ равна d^2 , тогда как (вещественная) размерность пространства всех эрмитовых операторов в $\mathcal{H}$ также равна d^2 . Если $\mathcal{H}$ — вещественное d -мерное гильбертово пространство, то размерность пространства всех операторов в $\mathcal{H}$ равна d^2 , а размерность подпространства всех симметрических операторов в $\mathcal{H}$ равна $d(d+1)/2$.

§ 1.5. Выпуклость

Подмножество $\mathfrak{S}$ вещественного линейного пространства называется *выпуклым*, если для любого конечного набора точек $\{S_j\} \subset \mathfrak{S}$ и любого распределения вероятностей $\{p_j\}$ *выпуклая комбинация* $S = \sum_j p_j S_j$ принадлежит $\mathfrak{S}$ (достаточно потребовать, чтобы указанное условие вы-

полнялось только для наборов из двух точек, т. е. чтобы множество $\mathfrak{S}$ вместе с любыми двумя точками содержало и соединяющий их отрезок). В выпуклых множествах особо важны *крайние точки*, не представимые в виде нетривиальной выпуклой комбинации других точек. Это эквивалентно утверждению, что из условия $S = pS_1 + (1 - p)S_2$, $0 < p < 1$, следует, что $S = S_1 = S_2$, т. е. что ни один отрезок в $\mathfrak{S}$ не содержит S в качестве своей внутренней точки. Мы обозначаем через $\text{extr}(\mathfrak{S})$ множество всех крайних точек выпуклого множества $\mathfrak{S}$. Имеет место следующий общий результат.

Теорема 1.5.1 (Каратеодори). *Пусть $\mathfrak{S}$ — компактное выпуклое подмножество пространства $\mathbb{R}^n$. Тогда любая точка $S \in \mathfrak{S}$ может быть представлена в виде выпуклой комбинации не более чем $n + 1$ крайних точек $S_j \in \text{extr}(\mathfrak{S})$:*

$$S = \sum_{j=1}^{n+1} p_j S_j, \quad S_j \in \text{extr}(\mathfrak{S}). \quad (1.21)$$

В качестве примера рассмотрим выпуклое множество $\mathfrak{P}_n$ всех распределений вероятностей $P = \{p_1, \dots, p_{n+1}\}$ на множестве из $n + 1$ элементов. В силу условия $\sum_j p_j = 1$ множество $\mathfrak{P}_n$ может быть погружено в $\mathbb{R}^n$. Его крайними точками являются вырожденные распределения, для которых все вероятности p_j равны нулю, за исключением одной, равной 1. Всего имеется $n + 1$ таких точек, и любое распределение из $\mathfrak{P}_n$ единственным образом представляется в виде их выпуклой комбинации с коэффициентами p_j . Такое множество называется *симплексом*, и единственность представления является характеристическим свойством этого выпуклого множества.

Вещественная функция $\mathcal{F}$, определенная на выпуклом подмножестве $\mathfrak{S}$ конечномерного линейного пространства, называется *выпуклой* (*вогнутой*), если

$$\mathcal{F}\left(\sum_j p_j S_j\right) \leq (\geq) \sum_j p_j \mathcal{F}(S_j)$$

для любой выпуклой комбинации точек $S_j \in \mathfrak{S}$. Функция называется *аффинной*, если она как выпукла, так и вогнута, т. е. в приведенном выше соотношении имеет место знак равенства.

Задача 1.5.1. Докажите, что непрерывная выпуклая (в частности, аффинная) функция на компактном выпуклом множестве $\mathfrak{S}$ достигает своего максимума в крайней точке этого множества.

§ 1.6. Комментарии

Основы операторного формализма квантовой механики были заложены в классическом труде Дирака [8]. Из множества учебников по линейной алгебре отметим современный курс А. И. Кострикина и Ю. И. Манина [13], в котором учтены потребности квантовой механики, а также книгу И. М. Глазмана и Ю. И. Любича [6], нацеленную на активное освоение некоммутативного конечномерного функционального анализа через решение задач. Основные понятия и факты выпуклого анализа изложены в книгах Г. Г. Магарил-Ильяева и В. М. Тихомирова [17], а также Рокафеллара [25].

ГЛАВА 2

Состояния, наблюдаемые, статистика

§ 2.1. Структура статистических теорий

2.1.1. Классические системы

Классическая система характеризуется наличием *фазового пространства* Ω , точки которого ω описывают детерминированные состояния системы. Для простоты далее рассматривается случай конечного множества Ω . (Статистическим) *состоянием* называется распределение вероятностей $P = \{p_\omega\}$ на Ω . Совокупность всех распределений вероятностей представляет собой симплекс $\mathfrak{P}(\Omega)$, в котором каждая точка однозначно представляется в виде выпуклой комбинации крайних точек — *чистых состояний*, задаваемых вырожденными распределениями вероятностей. Простейшей системой является *бит* — система с двумя чистыми состояниями 0, 1, для которой множество статистических состояний изоморфно единичному отрезку.

Всякая детерминированная наблюдаемая величина есть функция $X = \{x_\omega\}$ на фазовом пространстве Ω , задающая разбиение Ω на непересекающиеся подмножества Ω_x , в которых X принимает какое-то значение x . Индикаторы $E_x(\omega)$ этих подмножеств удовлетворяют условиям

$$E_x(\omega)E_y(\omega) = \delta_{x,y}E_x(\omega), \quad \sum_x E_x(\omega) = 1.$$

Помимо детерминированных наблюдаемых, которые далее будут называться *четкими*, возможны *нечеткие* наблюдаемые, которые принимают значение x с вероятностями $M(x|\omega)$ (наблюдения с ошибкой либо рандомизованные). Набор условных вероятностей $M = \{M(x|\omega)\}$ характеризуется свойствами

$$M(x|\omega) \geq 0, \quad \sum_x M(x|\omega) = 1.$$

Для четких наблюдаемых вероятности $M(x|\omega) = E_x(\omega)$ равны 0 или 1, т. е. $M(x|\omega)^2 = M(x|\omega)$.

Распределение вероятностей произвольной наблюдаемой M в состоянии P дается формулой

$$\mu_P^M(x) = \sum_\omega p_\omega M(x|\omega). \quad (2.1)$$

Для плавного перехода к квантовым системам полезно ввести матричное представление классических величин. Рассмотрим гильбертово пространство, в котором фиксирован ортонормированный базис $\{|\omega\rangle; \omega \in \Omega\}$. Всякой числовой функции f_ω на Ω сопоставим оператор

$$f = \sum_{\omega} f_{\omega} |\omega\rangle \langle \omega|,$$

диагональный в этом базисе. Тогда состоянию сопоставляется оператор $P = \sum_{\omega} p_{\omega} |\omega\rangle \langle \omega|$, характеризующийся свойствами

$$P \geq 0, \quad \text{Tr } P = 1. \quad (2.2)$$

Наблюдаемая задается разложением единицы, т. е. набором операторов $M = \{M_x\}$, где

$$M_x = \sum_{\omega} M(x|\omega) |\omega\rangle \langle \omega|,$$

удовлетворяющих условиям

$$M_x \geq 0, \quad \sum_x M_x = I. \quad (2.3)$$

При этом для четкой наблюдаемой операторы M_x являются попарно ортогональными проекторами.

Формула (2.1) для распределения вероятностей наблюдаемой принимает вид

$$\mu_P^M(x) = \text{Tr } P M_x. \quad (2.4)$$

2.1.2. Аксиомы статистического описания

В основе математической структуры квантовой теории лежит разделение статистического эксперимента на стадии приготовления и измерения, которое порождает двойственность между квантовыми состояниями и наблюдаемыми. Следующий набор аксиом суммирует общие черты статистического описания и применим как к классическим, так и к квантовым системам.

Аксиома 1. Пусть задано множество $\mathfrak{S}$, элементы которого называют состояниями, и множество $\mathfrak{M}$, элементы которого называют (конечнозначными) наблюдаемыми. Для произвольного $M \in \mathfrak{M}$ определено конечное множество $\mathcal{X}^M$ возможных исходов измерения наблюдаемой. Для любых $S \in \mathfrak{S}$ и $M \in \mathfrak{M}$ определено распределение вероятностей μ_S^M на $\mathcal{X}^M$, называемое распределением вероятностей наблюдаемой M в состоянии S .



Рис. 2.1. Квантовое состояние, описываемое оператором плотности S , характеризует приготовление системы, тогда как статистика измерений описывается вероятностной мерой $\mu_S^M(x)$, где x обозначает возможные исходы измерения M

Состояние S интерпретируется как более или менее подробное описание приготовления *статистического ансамбля* независимых индивидуальных экземпляров рассматриваемой системы, а наблюдаемая M — как величина, которая может быть измерена определенным прибором для каждого экземпляра системы. Таким образом, аксиома 1 предполагает *воспроизводимость* экспериментов и *устойчивость частот* при независимых повторениях эксперимента. Если эти предположения не выполнены для некоторой ситуации (например, по причине ее уникальности), то говорить о статистическом описании вообще не имеет смысла.

Вторая аксиома выражает возможность *смешивания* ансамблей.

Аксиома 2. Для любых $S_1, S_2 \in \mathfrak{S}$ и любого числа $p, 0 < p < 1$, найдется такое $S \in \mathfrak{S}$, что

$$\mu_S^M = p\mu_{S_1}^M + (1-p)\mu_{S_2}^M \quad \text{для всех } M \in \mathfrak{M}.$$

Состояние S называется *смесью состояний* S_1 и S_2 с весами $p, 1-p$.

Следующая аксиома описывает возможность обработки информации, полученной при измерении наблюдаемой. Пусть $M_1, M_2 \in \mathfrak{M}$, а f — такая функция из $\mathcal{X}^{M_1}$ в $\mathcal{X}^{M_2}$, что для всех $S \in \mathfrak{S}$ выполняется равенство

$$\mu_S^{M_2}(y) = \sum_{x: f(x)=y} \mu_S^{M_1}(x).$$

Тогда наблюдаемая M_2 называется *укрупнением* наблюдаемой M_1 . В этом случае мы будем писать $M_2 = f \circ M_1$.

Аксиома 3. Для всякой наблюдаемой $M_1 \in \mathfrak{M}$ и (с необходимостью конечнозначной) функции f на $\mathcal{X}^{M_1}$ найдется такая наблюдаемая $M_2 \in \mathfrak{M}$, что $M_2 = f \circ M_1$.

Пара непустых множеств $(\mathfrak{S}, \mathfrak{M})$, удовлетворяющих аксиомам 1—3, называется *статистической моделью* системы. Статистическая модель называется *отделимой*, если выполняется следующее условие.

Аксиома 4. Из того, что $\mu_{S_1}^M = \mu_{S_2}^M$ для всех $M \in \mathfrak{M}$, следует, что $S_1 = S_2$, а из того, что $\mu_S^{M_1} = \mu_S^{M_2}$ для всех $S \in \mathfrak{S}$, следует, что $M_1 = M_2$.

Для отделимых моделей как смешивание в $\mathfrak{S}$, так и укрупнение в $\mathfrak{M}$ определены однозначно. Таким образом, множество состояний $\mathfrak{S}$ приобретает выпуклую структуру, а множество наблюдаемых $\mathfrak{M}$ — структуру частичного порядка.

Наблюдаемые $M_1, \dots, M_m$ называются *совместимыми*, если они являются укрупнениями некоторой наблюдаемой M , т. е. $M_j = f_j \circ M$ для $j = 1, \dots, m$. Результаты измерений совместимых наблюдаемых могут быть получены посредством обработки данных эксперимента с одним измерением. Статистические модели, в которых все наблюдаемые совместимы, являются по существу классическими.

Предложение 2.1.1. Пусть $(\mathfrak{S}, \mathfrak{M})$ — отделимая статистическая модель, в которой существует такая максимальная наблюдаемая M^* , что все остальные наблюдаемые являются ее укрупнениями. Тогда найдутся конечное множество Ω , взаимно однозначное аффинное отображение $S \rightarrow P_S$ множества состояний $\mathfrak{S}$ на выпуклое подмножество распределений вероятностей на Ω и взаимно однозначное отображение $M \rightarrow f_M$ множества наблюдаемых $\mathfrak{M}$ на подмножество случайных величин на Ω , сохраняющее отношение укрупнения, такие, что

$$\mu_S^M(x) = \sum_{\omega: f_M(\omega)=x} P_S(\omega). \quad (2.5)$$

Доказательство. Возьмем за Ω множество исходов максимальной наблюдаемой M^* , и пусть $P_S(\omega)$ — ее распределение в состоянии S . Согласно предположению для любой наблюдаемой M найдется такая функция f_M , что выполняется соотношение (2.5). Взаимная однозначность соответствий $S \rightarrow P_S$ и $M \rightarrow f_M$ вытекает из отделимости. Проверка их свойств оставляется в качестве задачи. $\square$

Таким образом, возможные значения «максимальной наблюдаемой» составляют фазовое пространство Ω , и состояния представляются распределениями вероятностей P на пространстве Ω . В базовой классической модели, которую естественно назвать *моделью Колмогорова*, множеством состояний является симплекс всех распределений вероятностей $\mathfrak{P}(\Omega)$, а наблюдаемые описываются случайными величинами, т. е. (измеримыми) функциями на пространстве Ω . Доказанное предложение означает, что статистическая модель, в которой все наблюдаемые совместимы, вкладывается в модель Колмогорова.

Другой важной классической моделью является *модель Вальда*, отличающаяся от модели Колмогорова включением «нечетких» или «рандомизованных» наблюдаемых¹ (см. п. 2.1.1). Чтобы получить для нее результат, аналогичный предложению 2.1.1, следует ввести стохастические варианты понятий укрупнения и совместимости. Пусть $M_1, M_2 \in \mathfrak{M}$ и Π — такая переходная вероятность из $\mathcal{X}^{M_1}$ в $\mathcal{X}^{M_2}$, что для всех $S \in \mathfrak{S}$ выполняется равенство

$$\mu_S^{M_2}(y) = \sum_x \Pi(y|x) \mu_S^{M_1}(x).$$

Тогда наблюдаемая M_2 называется *стохастическим укрупнением* наблюдаемой M_1 . Наблюдаемые $M_1, \dots, M_m$ называются *стохастически совместимыми*, если все они являются стохастическими укрупнениями некоторой наблюдаемой M . В модели Вальда все наблюдаемые стохастически совместимы, и всякая отделимая модель, обладающая этим свойством, вкладывается в модель Вальда.

В статистической модели квантовой механики состояния и наблюдаемые описываются операторами в гильбертовом пространстве. Было предпринято много попыток построения аксиоматических схем, приводящих к формализму гильбертова пространства в квантовой механике. Однако это не является нашей целью, и мы пойдем по другому пути: возьмем за отправной пункт описание квантовых состояний как операторов плотности и, следуя аксиомам статистической модели, выведем из этого наиболее общую концепцию квантовой наблюдаемой (включающую как «четкие», так и «нечеткие» наблюдаемые).

2.1.3. Квантовые состояния

Состояние квантовомеханической системы описывает статистический ансамбль независимых одинаково приготовленных экземпляров системы.

Определение 2.1.1. *Квантовое состояние* задается оператором плотности, т. е. эрмитовым оператором S в гильбертовом пространстве системы $\mathcal{H}$, удовлетворяющим условиям

$$S \geq 0, \quad \text{Tr } S = 1.$$

Пусть $\mathfrak{S}(\mathcal{H})$ — множество всех операторов плотности. Это выпуклое подмножество вещественного линейного пространства всех эрмитовых операторов в $\mathcal{H}$. Выпуклая комбинация $S = \sum_j p_j S_j$ операторов плотности

¹Рандомизация была введена Вальдом в теории статистических решений, а также фон Нейманом в теории игр.

описывает *смесь* с весами p_j соответствующих статистических ансамблей, приготовленных в состояниях S_j . В квантовом статистическом ансамбле есть два вида стохастичности: во-первых, устранимая в принципе стохастичность, обусловленная флуктуациями классических параметров процедуры приготовления, и во-вторых, не уничтожимая никакими усилиями квантовая стохастичность, присутствующая в любом состоянии. Следующая теорема характеризует такие состояния без классической случайности.

Теорема 2.1.1. *Крайние точки множества квантовых состояний $\mathfrak{S}(\mathcal{H})$, называемые чистыми состояниями, суть одномерные проекторы и только они.*

Доказательство. Рассмотрим спектральное разложение эрмитова оператора S :

$$S = \sum_{i=1}^d s_i |e_i\rangle\langle e_i|, \quad s_j \geq 0, \quad \sum s_j = 1, \quad (2.6)$$

где s_i — собственные значения, $|e_i\rangle$ — собственные векторы оператора S , $d = \dim \mathcal{H}$. Если S — крайняя точка, то эта сумма содержит только одно ненулевое слагаемое, следовательно, S есть одномерный проектор. Обратно, пусть S — одномерный проектор и $S = pS_1 + (1-p)S_2$, где $0 < p < 1$. Возведем это выражение в квадрат и рассмотрим разность операторов S и S^2 :

$$pS_1(I - S_1) + (1-p)S_2(I - S_2) + p(1-p)(S_1 - S_2)^2 = S - S^2 = 0. \quad (2.7)$$

Сумма трех положительных операторов равна нулю, следовательно, каждое слагаемое должно равняться нулю. Но это означает, что $S_1 = S_2 = S$, т. е. S — крайняя точка. $\square$

С точки зрения теории вероятностей, одномерные проекторы являются некоммутативным аналогом вырожденных распределений, тогда как роль равномерного распределения играет *хаотическое состояние* с оператором плотности $S = \frac{1}{d}I$.

Задача 2.1.1. Покажите, что если $\dim \mathcal{H} = d$, то $\mathfrak{S}(\mathcal{H})$ погружается в вещественное пространство размерности $n = d^2 - 1$. Если $\mathcal{H}$ — евклидово (вещественное гильбертово) пространство, то $n = d(d+1)/2 - 1$.

Спектральное разложение (2.6) показывает, что любое квантовое состояние представимо в виде смеси не более чем d чистых состояний, где $d = \dim \mathcal{H}$; таким образом, для множества квантовых состояний теорема Каратеодори дает завышенное значение количества крайних точек, в действительности присутствующих в смеси (1.21). С другой стороны,

эта теорема дает точное значение для симплекса распределений вероятностей на «фазовом пространстве» $\Omega = \{1, \dots, n+1\}$, представляющем статистические состояния в классической системе. Это наводит на мысль интерпретировать квантовую теорию как классическую вероятностную модель, в статистической структуре которой зашифрованы некие неклассические ограничения (теорию со скрытыми параметрами). Для одиночной квантовой системы такая точка зрения возможна, но до сих пор она не оказалась плодотворной. При переходе же к составным системам она приводит к неустранимым противоречиям с физическими принципами локальности и причинности (см. п. 3.1.4).

Простейшим и в то же время фундаментальным примером является *q-бит* — двухуровневая квантовая система, $\dim \mathcal{H} = 2$. Будем использовать канонический базис: $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. В вещественном пространстве эрмитовых (2×2) -матриц удобно ввести *базис Паули*:

$$I \equiv \sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

В частности, оператор плотности $S \in \mathfrak{S}(\mathcal{H})$ представляется как

$$S = \frac{1}{2}(I + a_x \sigma_x + a_y \sigma_y + a_z \sigma_z) = \frac{1}{2} \begin{bmatrix} 1 + a_z & a_x - ia_y \\ a_x + ia_y & 1 - a_z \end{bmatrix}. \quad (2.8)$$

Условие $\det S \geq 0$ накладывает следующее ограничение на *параметры Стокса* $\mathbf{a} = (a_x, a_y, a_z)$:

$$|\mathbf{a}|^2 \equiv a_x^2 + a_y^2 + a_z^2 \leq 1.$$

Таким образом, $\mathfrak{S}(\mathcal{H})$ как выпуклое множество изоморфно единичному шару в $\mathbb{R}^3$, который мы будем называть *шаром Блоха*.

Задача 2.1.2. Покажите, что оператор плотности (2.8) имеет собственные значения $\frac{1 \pm |\mathbf{a}|}{2}$.

Чистые состояния характеризуются условием $a_x^2 + a_y^2 + a_z^2 = 1$ и составляют *сферу Блоха*. Вводя углы Эйлера θ, φ так, чтобы выполнялись равенства $a_z = \cos \theta, a_x + ia_y = \sin \theta e^{i\varphi}$, получаем $S = |\mathbf{a}\rangle\langle\mathbf{a}|$, где

$$|\mathbf{a}\rangle = \begin{bmatrix} \cos \frac{\theta}{2} e^{-i\varphi/2} \\ \sin \frac{\theta}{2} e^{i\varphi/2} \end{bmatrix}. \quad (2.9)$$

Для электрона, являющегося частицей со спином $1/2$, вектор $\mathbf{a}$ описывает ансамбль (пучок частиц) со спином в направлении $\mathbf{a}$, приготовленный при помощи фильтра Штерна—Герлаха в направлении градиента

магнитного поля. Смешанное состояние с $a_x = a_y = a_z = 0$, для которого все направления спина равновероятны, описывается оператором плотности $S = \frac{1}{2}I$, т. е. является хаотическим.

Другим важным примером двухуровневой системы является поляризация монохроматического фотона, визуализируемая в классических оптических экспериментах. В этом случае параметр $\theta/2$ есть угол линейной поляризации, в то время как $\varphi/2$ характеризует круговую поляризацию. Для линейно поляризованного фотона $\varphi = 0$, в частности, для вертикально поляризованного фотона $\theta = 0$, а для горизонтально поляризованного — $\theta = \pi$.

§ 2.2. Квантовые наблюдаемые

2.2.1. Квантовые наблюдаемые: построение из аксиом

Рассмотрим статистическую модель, в которой пространство состояний есть выпуклое множество $\mathfrak{S}(\mathcal{H})$ всех операторов плотности в гильбертовом пространстве $\mathcal{H}$. Пусть M — некоторая наблюдаемая, тогда согласно аксиоме 2 вероятности исходов измерения $\mu_S^M(x)$ должны быть *аффинными* функциями состояния.

Теорема 2.2.1. *Предположим, что отображение $S \rightarrow \mu_S$ является аффинной функцией на $\mathfrak{S}(\mathcal{H})$, причем $0 \leq \mu_S \leq 1$. Тогда существует единственный оператор M в $\mathcal{H}$, $0 \leq M \leq I$, такой, что для любого $S \in \mathfrak{S}(\mathcal{H})$ выполняется равенство*

$$\mu_S = \text{Tr } SM. \quad (2.10)$$

Набросок доказательства. Покажем, как можно расширить отображение $S \rightarrow \mu_S$ до линейной функции на пространстве $\mathfrak{T}(\mathcal{H})$ всех эрмитовых операторов в $\mathcal{H}$.

Прежде всего отметим, что любой эрмитов оператор A можно представить как разность двух положительных операторов, $A = A'_+ - A'_-$, например в силу разложения (1.8). Нормируя на величины следов $t_{\pm} = \text{Tr } A'_{\pm}$, мы всегда можем записать

$$A = t_+ S_+ - t_- S_-, \quad t_{\pm} \geq 0, \quad S_{\pm} \in \mathfrak{S}(\mathcal{H}). \quad (2.11)$$

Представление оператора A в виде линейной комбинации операторов плотности (2.11), конечно, не является единственным.

Задача 2.2.1. Используя аффинность отображения $S \rightarrow \mu_S$, покажите, что значение $\mu_A = t_+ \mu_{S_+} - t_- \mu_{S_-}$ определено единственным образом (т. е. зависит только от оператора A , но не от конкретного разложения $A = A'_+ - A'_-$), а функция $A \rightarrow \mu_A$ является вещественной и линейной.

Далее, любой оператор A может быть представлен в виде $A = A_1 + iA_2$, где $A_1 = \frac{1}{2}(A + A^*)$, $A_2 = \frac{1}{2i}(A - A^*)$ — эрмитовы операторы. Это представление единственно, и, положив $\mu_A = \mu_{A_1} + i\mu_{A_2}$, мы получаем единственное комплексно-линейное расширение функции μ_A на пространство всех линейных операторов в $\mathcal{H}$. Как отмечено в § 1.4, любая такая функция имеет вид

$$\mu_A = \text{Tr } AM, \quad (2.12)$$

где M — (единственный) оператор в $\mathcal{H}$. Взяв $A = |\psi\rangle\langle\psi|$, где ψ — единичный вектор, и используя соотношение (1.12), по предположению получим $0 \leq \langle\psi|M\psi\rangle \leq 1$, следовательно, $0 \leq M \leq I$. $\square$

Следствие 2.2.1. Пусть $S \rightarrow \{\mu_S(x), x \in \mathcal{X}\}$ — аффинное отображения выпуклого множества состояний $\mathfrak{S}(\mathcal{H})$ в множество распределений вероятностей на конечном множестве $\mathcal{X}$. Тогда существует единственный набор эрмитовых операторов $\{M_x, x \in \mathcal{X}\}$ в $\mathcal{H}$ такой, что $\sum_x M_x = I$ и

$$\mu_S(x) = \text{Tr } SM_x, \quad x \in \mathcal{X}. \quad (2.13)$$

Доказательство этого следствия предоставляется читателю в качестве задачи.

Набор операторов $\{M_x\}$ называется *разложением единицы* или *вероятностной операторнозначной мерой* на $\mathcal{X}$. Следствие 2.2.1 приводит к следующему определению.

Определение 2.2.1. Квантовая наблюдаемая со значениями в множестве $\mathcal{X}$ описывается разложением единицы $\{M_x, x \in \mathcal{X}\}$. Вероятностное распределение μ_S^M наблюдаемой $M = \{M_x\}$ в состоянии S задается формулой (2.13).

Принимая такое определение квантовой наблюдаемой, мы вводим *максимальную* статистическую модель, множество состояний которой совпадает с множеством всех операторов плотности в $\mathcal{H}$. В стандартных текстах по квантовой механике используется более узкое понятие квантовой наблюдаемой.

Определение 2.2.2. Наблюдаемая называется *четкой*, если все операторы $M_x = E_x$ являются проекторами: $E_x^2 = E_x$.

Задача 2.2.2. Покажите, что условие $E_x^2 = E_x$ для всех исходов x эквивалентно тому, что $E_x E_y = \delta_{xy} E_x$ для всех x, y .

Соответствующие разложения единицы называются *ортогональными*. Итак, четкие наблюдаемые описываются ортогональными разложениями единицы в $\mathcal{H}$. Наблюдаемые, значения которых являются веще-

ственными числами, т. е. $\mathcal{X} \subset \mathbb{R}$, называются *вещественными*. Спектральное разложение

$$X = \sum_{x \in \mathcal{X}} x E_x$$

задает взаимно однозначное соответствие между четкими вещественными наблюдаемыми $E = \{E_x\}$ и эрмитовыми операторами X в $\mathcal{H}$. Укрупнение для таких наблюдаемых принимает форму функционального исчисления, так что для любой функции $f: \mathbb{R} \rightarrow \mathbb{R}$ наблюдаемая $f \circ E$ описывается эрмитовым оператором $f(X)$ (**задача**). Математическое ожидание (среднее значение) наблюдаемой X в состоянии S задается *статистической формулой Борна—фон Неймана*

$$E_S(X) = \sum x \mu_S^E(x) = \text{Tr} SX.$$

Соотношение (2.13) можно рассматривать как обобщение этой формулы.

Статистическая модель, в которой состояния описываются операторами плотности, а наблюдаемые — эрмитовыми (самосопряженными) операторами, была детально рассмотрена фон Нейманом.

2.2.2. Совместимость и дополнительность

Определение 2.2.3. Коммутатором операторов X, Y называется оператор $[X, Y] = XY - YX$. Операторы X, Y коммутируют, если $[X, Y] = 0$.

Теорема 2.2.2. Пусть $E = \{E_x\}$ и $F = \{F_y\}$ — четкие наблюдаемые. Тогда следующие утверждения эквивалентны:

1) E, F совместимы;

2) проекторы E_x и F_y коммутируют для всех x, y .

Если E, F — вещественные наблюдаемые, то эти условия эквивалентны следующему условию:

3) соответствующие эрмитовы операторы $X = \sum_x x E_x, Y = \sum_y y F_y$ коммутируют.

Доказательство. 2) $\Rightarrow$ 1). Положим $M_{x,y} = E_x F_y = F_y E_x$. Так как произведение коммутирующих проекторов является проектором, $M = \{M_{x,y}\}$ — (четкая) наблюдаемая. Кроме того, $E = f \circ M, F = g \circ M$, где $f(x, y) = x, g(x, y) = y$. Таким образом, наблюдаемые E, F совместимы.

1) $\Rightarrow$ 2). Если наблюдаемые E, F совместимы, то найдется такая наблюдаемая $M = \{M_z\}$, что

$$E_x = \sum_{z: f(z)=x} M_z, \quad F_y = \sum_{z: g(z)=y} M_z$$

для некоторых функций f, g (условимся считать, что $M_z = 0$, если значений z , удовлетворяющих условию в суммах, не существует).

Лемма 2.2.1. Пусть $0 \leq A \leq P$, где P — проектор. Тогда $AP = A$ и, следовательно, $[A, P] = 0$.

Доказательство. Имеем $(I - P)A(I - P) = 0$, откуда последовательно получаем $\sqrt{A}(I - P) = 0$, $A(I - P) = 0$, $A = AP$ и $PA = (AP)^* = AP$. $\square$

Пусть теперь $f(z) = x$, тогда $E_x \geq M_z$; согласно лемме $[E_x, M_z] = 0$. Если $f(z) \neq x$, то $I - E_x \geq M_z$ и вновь $[E_x, M_z] = 0$. Итак, E_x коммутирует со всеми наблюдаемыми M_z и, значит, с $F_y = \sum_{z: g(z)=y} M_z$.

Импликация $2) \Rightarrow 3)$ очевидна. Обратно, пусть $[X, Y] = 0$, тогда $[f(X), g(Y)] = 0$ для произвольных многочленов f, g . Рассматривая многочлены, которые обращаются в нуль во всех точках соответствующего спектра, за исключением x (соответственно y), получаем $[E_x, F_y] = 0$. $\square$

Если E, F совместимы, то, обозначая $\hat{M}_{xy} = \sum_{z: f(z)=x, g(z)=y} M_z$, получаем

$$E_x = \sum_y \hat{M}_{xy}, \quad F_y = \sum_x \hat{M}_{xy}.$$

Наблюдаемая $\hat{M}$ описывает статистику совместного измерения наблюдаемых E, F ; их совместное распределение вероятностей в состоянии S определяется формулой

$$\mu_S^{EF}(x, y) = \text{Tr } S \hat{M}_{xy}.$$

Подобным образом можно определить совместное измерение и распределение вероятностей для любого конечного набора совместимых наблюдаемых.

Задача 2.2.3. Покажите, что единственной вещественной наблюдаемой, совместимой со всеми квантовыми наблюдаемыми, является постоянная, т. е. наблюдаемая, кратная единичному оператору.

Существование несовместимых наблюдаемых — это проявление квантового свойства *дополнительности*. Физические измерения над микрообъектами производятся при помощи макроскопических экспериментальных устройств (как, например, фильтр Штерна—Герлаха), предполагающих сложную и специфичную пространственно-временную организацию окружающей среды. Различные способы такой организации, соответствующие измерениям различных наблюдаемых, могут быть взаимно исключаящими (несмотря на то что относятся к одинаково приготовленному микрообъекту), т. е. дополнительными. Дополнительность — это первое

фундаментальное различие между квантовой и классической статистическими моделями.

Пример 2.2.1. Рассмотрим математическую модель частицы со спином $1/2$. Спин является векторной величиной, компоненты которой вдоль осей x, y, z описываются эрмитовыми операторами $\sigma_x, \sigma_y, \sigma_z$. Пусть единичный вектор $\mathbf{a} = (a_x, a_y, a_z)$ задает направление в $\mathbb{R}^3$, тогда эрмитов оператор

$$\sigma(\mathbf{a}) = a_x \sigma_x + a_y \sigma_y + a_z \sigma_z = \begin{bmatrix} a_z & a_x - ia_y \\ a_x + ia_y & -a_z \end{bmatrix} \quad (2.14)$$

задает наблюдаемую «проекция спина на направление $\mathbf{a}$ ». Оператор $\sigma(\mathbf{a})$ имеет собственные значения ± 1 (спин вдоль и против направления $\mathbf{a}$) и спектральное разложение

$$\sigma(\mathbf{a}) = |\mathbf{a}\rangle\langle\mathbf{a}| - |-\mathbf{a}\rangle\langle-\mathbf{a}|. \quad (2.15)$$

Напомним, что направление $\mathbf{a}$ имеет углы Эйлера (θ, φ) , а вектор $\mathbf{a}$, задаваемый соотношением (2.9), есть вектор чистого состояния в $\mathcal{H}$ с направлением спина $\mathbf{a}$. Соответствующий оператор плотности, являющийся проектором на вектор $|\mathbf{a}\rangle$, имеет вид

$$S(\mathbf{a}) = |\mathbf{a}\rangle\langle\mathbf{a}| = \frac{I + \sigma(\mathbf{a})}{2}.$$

Задача 2.2.4. Докажите формулу

$$\sigma(\mathbf{a}_1) \sigma(\mathbf{a}_2) = (\mathbf{a}_1 \cdot \mathbf{a}_2) I + i \sigma(\mathbf{a}_1 \times \mathbf{a}_2). \quad (2.16)$$

Это равенство, записанное для базисных векторов, приводит к соотношениям

$$\begin{aligned} \sigma_x^2 &= I, & \sigma_y^2 &= I, & \sigma_z^2 &= I, \\ \sigma_x \sigma_y &= i \sigma_z, & \sigma_y \sigma_z &= i \sigma_x, & \sigma_z \sigma_x &= i \sigma_y. \end{aligned} \quad (2.17)$$

Принимая во внимание, что $\text{Tr} \sigma(\mathbf{a}) = 0$, из соотношения (2.16) получаем формулу для среднего значения $\sigma(\mathbf{b})$:

$$\text{Tr} S(\mathbf{a}) \sigma(\mathbf{b}) = \mathbf{a} \cdot \mathbf{b}.$$

Другим следствием формулы (2.16) является равенство

$$[\sigma(\mathbf{a}_1), \sigma(\mathbf{a}_2)] = 2i \sigma(\mathbf{a}_1 \times \mathbf{a}_2), \quad (2.18)$$

которое означает, что наблюдаемые $\sigma(\mathbf{a}_1), \sigma(\mathbf{a}_2)$ совместимы тогда и только тогда, когда $\mathbf{a}_1 = \pm \mathbf{a}_2$. В частности, компоненты спина $\sigma_x, \sigma_y, \sigma_z$ являются несовместимыми наблюдаемыми.

2.2.3. Соотношение неопределенностей

Пусть X, Y — два оператора. Тогда

$$XY = X \circ Y + \frac{1}{2}[X, Y],$$

где $X \circ Y = \frac{1}{2}(XY + YX)$ — симметризованное или *йорданово* произведение операторов X, Y .

Пусть S — некоторое состояние. Для произвольного набора $X = [X_1, \dots, X_n]$ четких вещественных наблюдаемых положим $X_j^0 = X_j - I E_S X_j$ и введем две вещественные матрицы: симметричную *матрицу ковариаций*

$$B_S(X) = [\text{Tr} S X_j^0 \circ X_k^0]_{j,k=1,\dots,n} \quad (2.19)$$

и кососимметричную *коммутационную матрицу*

$$C_S(X) = [i \text{Tr} S [X_j, X_k]]_{j,k=1,\dots,n} = [i \text{Tr} S [X_j^0, X_k^0]]_{j,k=1,\dots,n}. \quad (2.20)$$

Имеем

$$B_S(X) \geq \frac{i}{2} C_S(X) \quad (2.21)$$

в смысле неравенства между комплексными эрмитовыми матрицами. Действительно, эрмитова матрица

$$B_S(X) - \frac{i}{2} C_S(X) = [\text{Tr} S X_j^0 X_k^0]_{j,k=1,\dots,n}$$

положительно определена, поскольку для произвольных $c_j \in \mathbb{C}$ выполняется неравенство

$$\sum_{j,k=1}^n \bar{c}_j c_k \text{Tr} S X_j^0 X_k^0 = \text{Tr} S Z^* Z \geq 0,$$

где $Z = \sum_{j=1}^n c_j X_j$.

Для двух наблюдаемых $X_1 = X$ и $X_2 = Y$ неравенство (2.21) эквивалентно соотношению неопределенностей Шрёдингера—Робертсона

$$D_S(X) D_S(Y) \geq \{E_S(X - I E_S(X)) \circ (Y - I E_S(Y))\}^2 + \frac{1}{4} |E_S[X, Y]|^2, \quad (2.22)$$

где

$$D_S(X) = \text{Tr} S (X - I E_S(X))^2 \quad (2.23)$$

— *дисперсия* четкой вещественной наблюдаемой X в состоянии S . Если X, Y — совместимые наблюдаемые, то величина

$$E_S(X - I E_S(X)) \circ (Y - I E_S(Y)) \quad (2.24)$$

представляет собой *ковариацию* этих наблюдаемых в состоянии S ; в этом случае $[X, Y] = 0$ и неравенство (2.22) превращается в неравенство Коши—Буняковского для ковариации случайных величин. Если же X, Y несовместимы, то они неизмеримы в одном эксперименте и дисперсии $D_S(X), D_S(Y)$ в соотношении неопределенностей относятся к двум различным измерениям, произведенным над разными представителями одного статистического ансамбля.

Задача 2.2.5. Докажите некоммутативное неравенство Коши—Буняковского

$$|\mathrm{Tr} SX^*Y|^2 \leq \mathrm{Tr} SX^*X \mathrm{Tr} SY^*Y \quad (2.25)$$

для произвольного состояния S и операторов X, Y в $\mathcal{H}$.

2.2.4. Выпуклая структура множества наблюдаемых

Множество всех (конечнозначных) квантовых наблюдаемых в гильбертовом пространстве $\mathcal{H}$ обозначим $\mathfrak{M}(\mathcal{H})$. Для данного гильбертова пространства $\mathcal{H}$ множество $\mathfrak{S}(\mathcal{H})$ квантовых состояний и множество $\mathfrak{M}(\mathcal{H})$ квантовых наблюдаемых вместе с обобщенным статистическим правилом Борна—фон Неймана (2.13) по построению удовлетворяют аксиомам отделимой статистической модели. Кроме того, эта модель имеет дополнительную структуру в множестве наблюдаемых $\mathfrak{M}(\mathcal{H})$, аналогичную выпуклой структуре множества $\mathfrak{S}(\mathcal{H})$.

Пусть $\{M^i\}$ — конечный набор наблюдаемых с одним и тем же пространством исходов $\mathcal{X}$. Для данного распределения вероятностей $\{p_j\}$ можно естественным образом определить *смесь* $M = \{M_x; x \in \mathcal{X}\}$ этих наблюдаемых по формуле

$$M_x = \sum_j p_j M_x^i, \quad x \in \mathcal{X}. \quad (2.26)$$

Таким образом, множество $\mathfrak{M}_{\mathcal{X}}$ всех наблюдаемых с заданным пространством исходов $\mathcal{X}$ становится выпуклым множеством. Аналогично смесям состояний смеси наблюдаемых описывают измерения с флуктуирующими классическими параметрами.

Следующий результат описывает нетривиальное соотношение между наблюдаемыми без классической стохастичности и четкими наблюдаемыми.

Теорема 2.2.3. *Всякая четкая наблюдаемая $M \in \mathfrak{M}_{\mathcal{X}}$ есть крайняя точка выпуклого множества $\mathfrak{M}_{\mathcal{X}}$. Обратно, всякая крайняя точка множества $M \in \mathfrak{M}_{\mathcal{X}}$ с коммутирующими компонентами, $[M_x, M_{x'}] \equiv 0$, является четкой наблюдаемой.*

Доказательство. Пусть M — четкая наблюдаемая. Предположим, что $M = pM^1 + (1 - p)M^2$, $0 < p < 1$. Тогда аналогично соотношению (2.7) получаем

$$pM_x^1(I - M_x^1) + (1 - p)M_x^2(I - M_x^2) + p(1 - p)(M_x^1 - M_x^2)^2 = 0, \quad (2.27)$$

откуда следует, что $M_x^1 \equiv M_x^2 \equiv M_x$ и M — крайняя точка.

Теперь заметим, что всегда $M_x \leq I$ и, значит, $M_x^2 \leq M_x$. Зафиксировав некоторый исход $x \in \mathcal{X}$, получим

$$M_x = \frac{1}{2}M_x^2 + \frac{1}{2}(2M_x - M_x^2), \quad (2.28)$$

$$M_{x'} = \frac{1}{2}M_{x'}(I + M_x) + \frac{1}{2}M_{x'}(I - M_x), \quad x' \neq x. \quad (2.29)$$

Если $[M_x, M_{x'}] \equiv 0$, то эти соотношения представляет M как выпуклую комбинацию (с равными весами) двух других наблюдаемых. Если M — крайняя точка, то они должны совпасть с M , в частности, $M_x^2 = M_x$, значит, M — четкая наблюдаемая. $\square$

Крайние точки множества наблюдаемых будем называть *экстремальными* наблюдаемыми. Из теоремы 2.2.3 следует, что в классическом случае экстремальные наблюдаемые совпадают с четкими, а из этого следует их очень понятная характеристика как наблюдаемых без стохастичности в процедуре измерения. В квантовой статистической модели все не так просто (и поэтому более интересно). Множество крайних точек квантовых наблюдаемых исчерпывается четкими наблюдаемыми только в случае двух исходов измерения (они играют особую роль в различных аксиоматических подходах; разные авторы называют такие наблюдаемые *предложениями*, *вопросами*, *эффектами*; мы будем называть их *тестами*). Это следует из теоремы, так как любой тест имеет коммутирующие компоненты $\{M_0, M_1 = I - M_0\}$. Таким образом, любой экстремальный тест вполне определяется проектором $P = M_0$. Переходя к наблюдаемым с более чем двумя значениями, рассмотрим следующую конструкцию.

Определение 2.2.4. Пусть $\{|\psi_x\rangle\}$ — произвольный набор векторов (которые могут быть ненормированными) в $\mathcal{H}$, удовлетворяющий условию $\sum_x |\psi_x\rangle\langle\psi_x| = I$. Такой набор называется *переполненной системой*.

Если $\{|\psi_x\rangle\}$ — переполненная система, то произвольный вектор $|\psi\rangle \in \mathcal{H}$ может быть представлен в виде

$$|\psi\rangle = \sum_x c_x |\psi_x\rangle, \quad \text{где } c_x = \langle\psi_x|\psi\rangle, \quad (2.30)$$

причем коэффициенты $\{c_x\}$ могут определяться не единственным образом, так как векторы $|\psi_x\rangle$ могут быть линейно зависимыми. Для операторов

имеет место аналогичное матричное представление. В d -мерном комплексном пространстве переполненная система с более чем d векторами всегда существует и может быть построена из любой полной (возможно, линейно зависимой) системы следующим образом. Пусть $\{|\varphi_x\rangle\}$ — полная система векторов в $\mathcal{H}$. Соответствующий *оператор Грама* определяется как

$$G = \sum_x |\varphi_x\rangle\langle\varphi_x|. \quad (2.31)$$

Полнота означает, что оператор G невырожден. Система векторов $|\psi_x\rangle = G^{-1/2}|\varphi_x\rangle$ является переполненной, так как

$$\sum_x |\psi_x\rangle\langle\psi_x| = G^{-1/2} \underbrace{\sum_x |\varphi_x\rangle\langle\varphi_x|}_{=G} G^{-1/2} = I. \quad (2.32)$$

Переполненная система определяет квантовую наблюдаемую M с компонентами

$$M_x = |\psi_x\rangle\langle\psi_x|, \quad x \in \mathcal{X}. \quad (2.33)$$

В частности, для любого ортонормированного базиса $\{e_x\}$ наблюдаемая $M = \{|e_x\rangle\langle e_x|\}$ является четкой и, следовательно, экстремальной.

Теорема 2.2.4. *Наблюдаемая (2.33) является экстремальной тогда и только тогда, когда операторы M_x линейно независимы.*

Доказательство. Пусть M — крайняя точка, и предположим, что

$$\sum_x c_x |\psi_x\rangle\langle\psi_x| = 0. \quad (2.34)$$

Взяв достаточно малое $\varepsilon > 0$, определим

$$M_x^\pm = (1 \pm \varepsilon c_x) M_x \geq 0, \quad x \in \mathcal{X}.$$

Тогда $M^\pm$ являются наблюдаемыми, и по построению $M = \frac{1}{2}M^+ + \frac{1}{2}M^-$. Но M — крайняя точка, значит, $M_x^+ = M_x^- = M_x$. Итак, из соотношения (2.34) следует, что $c_x = 0$, т.е. компоненты наблюдаемой M линейно независимы.

Обратно, пусть

$$|\psi_x\rangle\langle\psi_x| = pM_x^1 + (1-p)M_x^2$$

— разложение наблюдаемой M , тогда $0 \leq pM_x^1 \leq |\psi_x\rangle\langle\psi_x|$. Используя лемму 2.2.1, получаем

$$M_x^1 |\psi_x\rangle\langle\psi_x| = |\psi_x\rangle\langle\psi_x| M_x^1 = \langle\psi_x|\psi_x\rangle M_x^1,$$

откуда следует, что

$$M_x^1 = \lambda_x |\psi_x\rangle\langle\psi_x|, \quad \text{где } \lambda_x = \langle\psi_x|M_x^1|\psi_x\rangle/\langle\psi_x|\psi_x\rangle^2.$$

Тогда $\sum_x \lambda_x |\psi_x\rangle\langle\psi_x| = I$, т. е.

$$\sum_x (\lambda_x - 1) |\psi_x\rangle\langle\psi_x| = 0.$$

В силу линейной независимости $\lambda_x = 1$ и $M_x^1 = M_x$ для всех x , следовательно, M — крайняя точка. $\square$

В силу результата задачи 1.4.2 размерность вещественного пространства эрмитовых операторов равна d^2 . Итак, все переполненные системы с n линейно независимыми компонентами, $d < n \leq d^2$, являются нечеткими экстремальными наблюдаемыми. Конкретный пример такой наблюдаемой при $n = 3$, $d = 2$ будет рассмотрен в следующем параграфе.

§ 2.3. Оптимальное различение квантовых состояний

2.3.1. Постановка задачи

В этом параграфе мы рассмотрим статистическую задачу, которая позволит в дальнейшем перейти к изучению квантовых каналов связи.

Пусть квантовая система готовится в одном из состояний S_x , $x = 1, \dots, n$. Над системой можно производить произвольное измерение. Требуется найти оптимальную наблюдаемую, позволяющую наилучшим образом выяснить, в каком из этих априорно данных состояний находится система. Такая постановка задачи характерна для математической статистики и ее применений в теории связи (см. п. 3.2.1). В высокоточных экспериментах и в квантовой оптике исследователи уже способны оперировать элементарными квантовыми системами, такими как одиночные ионы, атомы и фотоны. В обсуждаемых предложениях квантовых вычислений информация записывается в состояния элементарных квантовых ячеек — q -битов, а считывается при помощи квантовых измерений. Со статистической точки зрения, измерение дает оценку квантового состояния — либо всего состояния целиком, либо некоторых его параметров, и при этом возникает вопрос наиболее точного оценивания.

Статистика измерения описывается квантовой наблюдаемой, т. е. разложением единицы $M = \{M_x\}$ в пространстве системы $\mathcal{H}$. Вероятность принять решение y при условии, что система находилась в состоянии S_x , равна $p_M(y|x) = \text{Tr } S_x M_y$. При этом вероятность того, что будет принято правильное решение, равна $p_M(x|x)$. Примем дополнительное предположение, что состояния S_x появляются с вероятностями π_x (например,

в случае равновероятных состояний $\pi_x = 1/n$). Тогда средняя вероятность правильного решения вычисляется по формуле

$$\mathcal{P}\{M\} = \sum_{x=1}^n \pi_x p_M(x|x),$$

и задача состоит в ее максимизации.

2.3.2. Оптимальные наблюдаемые

Вероятность правильного решения

$$\mathcal{P}\{M\} = \sum_{x=1}^n \text{Tr } W_x M_x,$$

где $W_x = \pi_x S_x \geq 0$, является аффинной функцией,

$$\mathcal{P}\left\{\sum p_\lambda M^\lambda\right\} = \sum p_\lambda \mathcal{P}\{M^\lambda\},$$

определенной на выпуклом множестве наблюдаемых

$$\mathfrak{M}_n = \left\{ M = \{M_y\}_{y=1, \dots, n} : M_y \geq 0, \sum_{y=1}^n M_y = I \right\}.$$

Максимизация аффинной функции, заданной на выпуклом множестве, — это типичная задача линейного программирования.

Теорема 2.3.1. *Средняя вероятность правильного решения $\mathcal{P}\{M\}$ достигает максимума в крайней точке множества $\mathfrak{M}_n$. Наблюдаемая M^0 оптимальна тогда и только тогда, когда найдется такой эрмитов оператор Λ^0 , что*

$$1) (\Lambda^0 - W_y)M_y^0 = 0;$$

$$2) \Lambda^0 \geq W_y.$$

При этом имеет место соотношение двойственности

$$\max\{\mathcal{P}\{M\} : M \in \mathfrak{M}_n\} = \min\{\text{Tr } \Lambda : \Lambda \geq W_y, y = 1, \dots, n\}. \quad (2.35)$$

Доказательство. Поскольку $\mathcal{P}\{M\}$ является непрерывной аффинной функцией на компактном выпуклом множестве $\mathfrak{M}_n$, первое утверждение вытекает из результата задачи 1.5.1.

Докажем достаточность условий 1, 2. Пусть Λ^0 — эрмитов оператор, удовлетворяющий условиям 1, 2. Используя условие 1 и свойство (1.13), получаем

$$\mathcal{P}\{M\} = \text{Tr} \sum_x W_x M_x \leq \text{Tr} \sum_x \Lambda^0 M_x = \text{Tr} \Lambda^0. \quad (2.36)$$

Из условия 2 получаем $\Lambda^0 M_x^0 = W_x M_x^0$. Просуммировав по x и взяв след, получаем

$$\mathrm{Tr} \Lambda^0 = \mathrm{Tr} \Lambda^0 \sum_x M_x^0 = \mathrm{Tr} \sum_x W_x M_x^0 = \mathcal{P}\{M^0\}. \quad (2.37)$$

Итак,

$$\mathcal{P}\{M\} \leq \mathcal{P}\{M^0\} \quad \text{для всех } M. \quad (2.38)$$

Отметим, что

$$\Lambda^0 = \sum_x W_x M_x^0 = \sum_x M_x^0 W_x.$$

Докажем необходимость. Положим $M_y = X_y^2$, где X_y — эрмитовы операторы, удовлетворяющие условию $\sum_y X_y^2 = I$. Применяя метод Лагранжа, сведем задачу максимизации функции $\mathcal{P}\{M\}$ на множестве $\mathfrak{M}_n$ к нахождению максимума функции

$$\mathrm{Tr} \sum_y W_y X_y^2 - \mathrm{Tr} \Lambda \left(\sum_y X_y^2 - I \right), \quad (2.39)$$

где Λ — эрмитов оператор, по всевозможным наборам эрмитовых операторов X_y . Здесь оператор Λ представляет совокупность вещественных множителей Лагранжа для данной задачи. Пусть X_y^0 — оптимальный набор. Положим $X_y = X_y^0 + \varepsilon Y_y$ и рассмотрим (2.39) как функцию от ε . Рассматривая коэффициенты при ε и ε^2 , получаем условия

$$\begin{aligned} \mathrm{Tr} [(W_y - \Lambda) X_y^0 + X_y^0 (W_y - \Lambda)] Y_y &= 0, \\ \mathrm{Tr} (W_y - \Lambda) Y_y^2 &\leq 0 \end{aligned}$$

для произвольных эрмитовых операторов Y_y , т. е.

$$(W_y - \Lambda) X_y^0 + X_y^0 (W_y - \Lambda) = 0, \quad \Lambda - W_y \geq 0.$$

Второе неравенство есть условие 2 теоремы. Полагая $M_y^0 = (X_y^0)^2$, из первого соотношения получаем $\mathrm{Tr} (\Lambda - W_y) M_y^0 = 0$, а из этого соотношения и из второго неравенства следует условие 1. $\square$

Задача 2.3.1. Докажите, что операторный множитель Лагранжа Λ является единственным решением двойственной задачи в правой части равенства (2.35).

Проиллюстрируем значение и применение этих условий на примерах.

Пример 2.3.1. Рассмотрим классический случай, когда все операторы плотности S_x , а значит, и операторы W_x коммутируют и, следовательно, найдется общий ортонормированный базис, в котором все они диагональны,

$$W_x = \sum_{\omega} W_x(\omega) |\omega\rangle \langle \omega|.$$

Тогда двойственная задача имеет решение

$$\Lambda^0 = \sum_{\omega} \max_x W_x(\omega) |\omega\rangle \langle \omega|,$$

где $\max_x W_x(\omega)$ — верхняя огибающая функций $W_x(\omega)$, $x = 1, \dots, n$. Одно из решений исходной задачи дается формулой

$$M_x^0 = \sum_{\omega} \mathbf{1}_{\Omega_x}(\omega) |\omega\rangle \langle \omega|,$$

где $\mathbf{1}_{\Omega_x}$ обозначает индикатор подмножества Ω_x , причем непересекающиеся подмножества $\Omega_x \subset \{\omega: \Lambda^0(\omega) = W_x(\omega)\}$ образуют разбиение множества $\Omega = \{\omega\}$.

Это сводится к принципу *максимального правдоподобия* в классической статистике: решение x необходимо принимать для тех исходов ω , для которых апостериорный выигрыш $W_x(\omega)$ максимален. Таким образом, в классическом случае оптимальная наблюдаемая всегда может быть выбрана нерандомизованной. Это прямо связано с тем фактом, что в коммутативном случае крайние точки множества $\mathfrak{M}_n$ отвечают ортогональным разложениям единицы (см. теорему 2.2.3).

Пример 2.3.2 (различение двух квантовых состояний). Пусть S_0, S_1 — два оператора плотности, π_0, π_1 — их априорные вероятности. Наблюдаемая дается разложением единицы $\{M_0, M_1\}$, так что $M_0 + M_1 = I$. Этот случай можно свести к предыдущему примеру, полагая

$$W_0 = \pi_1 S_1 + W'_0, \quad W_1 = \pi_1 S_1 + W'_1,$$

где операторы $W'_0 = \pi_0 S_0 - \pi_1 S_1$, $W'_1 = 0$ коммутируют. Таким образом,

$$\mathcal{P}\{M\} = \pi_1 + \text{Tr}(W'_0 M_0 + W'_1 M_1), \quad (2.40)$$

и

$$\Lambda' = \max\{\pi_0 S_0 - \pi_1 S_1, 0\} = (\pi_0 S_0 - \pi_1 S_1)_+. \quad (2.41)$$

Всякий оптимальный оператор M_0^0 имеет вид

$$M_0^0 = \mathbf{1}_{(0, \infty)}(\pi_0 S_0 - \pi_1 S_1) + X_0, \quad (2.42)$$

где первое слагаемое является проектором на собственное подпространство оператора $\pi_0 S_0 - \pi_1 S_1$, отвечающее положительным собственным значениям, а второе слагаемое имеет носитель на нулевом подпространстве оператора $\pi_0 S_0 - \pi_1 S_1$, причем $0 \leq X_0 \leq I$. Максимальная вероятность правильного решения равна

$$\mathcal{P}\{M\} = \pi_1 + \text{Tr}(\pi_0 S_0 - \pi_1 S_1)_+. \quad (2.43)$$

Используя соотношение

$$(\pi_0 S_0 - \pi_1 S_1)_+ = \frac{1}{2}|\pi_0 S_0 - \pi_1 S_1| + \frac{1}{2}(\pi_0 S_0 - \pi_1 S_1),$$

получаем

$$\max \mathcal{P}\{M\} = \frac{1}{2}(1 + \|\pi_0 S_0 - \pi_1 S_1\|_1). \quad (2.44)$$

В частности, при $\pi_0 = \pi_1 = \frac{1}{2}$ различимость состояний S_0 и S_1 определяется величиной ядерной нормы разности соответствующих операторов плотности.

Предложение 2.3.1. Пусть $S_0 = |\psi_0\rangle\langle\psi_0|$, $S_1 = |\psi_1\rangle\langle\psi_1|$ — чистые состояния, тогда максимум величины $\mathcal{P}\{M\}$ равен

$$\max_M \mathcal{P}\{M\} = \frac{1}{2} \left(1 + \sqrt{1 - 4\pi_0\pi_1|\langle\psi_0|\psi_1\rangle|^2} \right). \quad (2.45)$$

В частности, при $\pi_0 = \pi_1 = \frac{1}{2}$ выполняется равенство

$$\max_M \mathcal{P}\{M\} = \frac{1}{2} \left(1 + \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2} \right). \quad (2.46)$$

Доказательство. Рассмотрим задачу на собственные значения для оператора $\pi_0|\psi_0\rangle\langle\psi_0| - \pi_1|\psi_1\rangle\langle\psi_1|$, имеющего ранг 2. Этот оператор может иметь нулевые собственные значения, отвечающие ортогональному дополнению к носителю $\mathcal{L}$, который натянут на векторы $|\psi_0\rangle$, $|\psi_1\rangle$. Существенная составляющая оптимальной наблюдаемой также сосредоточена на $\mathcal{L}$, поэтому можно ограничиться поиском собственных векторов вида

$$|\psi\rangle = c_0|\psi_0\rangle + c_1|\psi_1\rangle.$$

Подстановка в уравнение для собственных векторов приводит к равенствам

$$\pi_0(c_0 + \langle\psi_0|\psi_1\rangle c_1) = \lambda c_0, \quad (2.47)$$

$$-\pi_1(\langle\psi_1|\psi_0\rangle c_0 + c_1) = \lambda c_1, \quad (2.48)$$

откуда находим собственные значения

$$\lambda_{0,1} = \frac{1}{2} \left[\pi_0 - \pi_1 \pm \sqrt{1 - 4\pi_0\pi_1|\langle\psi_0|\psi_1\rangle|^2} \right]$$

с соответствующим базисом собственных векторов $|e_0\rangle, |e_1\rangle$. Следовательно,

$$\|\pi_0|\psi_0\rangle\langle\psi_0| - \pi_1|\psi_1\rangle\langle\psi_1|\|_1 = \lambda_0 - \lambda_1 = \sqrt{1 - 4\pi_0\pi_1|\langle\psi_0|\psi_1\rangle|^2},$$

откуда получаем равенство (2.45). $\square$

Оптимальная четкая наблюдаемая в подпространстве $\mathcal{L}$ имеет вид $\{|e_0\rangle\langle e_0|, |e_1\rangle\langle e_1|\}$. Если $\pi_0 = \pi_1 = 1/2$, то оптимальный базис расположен симметрично по отношению к $|\psi_0\rangle, |\psi_1\rangle$ (см. рис. 2.2).

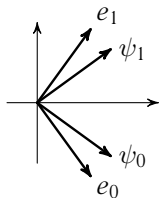


Рис. 2.2. Различение двух чистых состояний

Пример 2.3.3. На плоскости (рассматриваемой как вещественное подпространство двумерного комплексного пространства) рассмотрим «равноугольную» конфигурацию трех векторов (рис. 2.3)

$$|\psi_j\rangle = \begin{bmatrix} \cos \frac{2j\pi}{3} \\ \sin \frac{2j\pi}{3} \end{bmatrix}, \quad j = 0, 1, 2. \quad (2.49)$$

Соответствующие операторы плотности $S_j = |\psi_j\rangle\langle\psi_j|$ описывают состояния двухуровневой системы, например плоскополяризованного фотона или частицы со спином $1/2$.

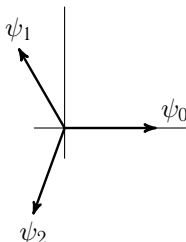


Рис. 2.3. Три равноугольных состояния

Имеем

$$S_j = \frac{1}{2} \left(I + \begin{bmatrix} \cos \frac{4j\pi}{3} & \sin \frac{4j\pi}{3} \\ \sin \frac{4j\pi}{3} & -\cos \frac{4j\pi}{3} \end{bmatrix} \right), \quad (2.50)$$

так что

$$\sum_{j=0}^2 S_j = \frac{3}{2}I,$$

в силу того что $\sum_{j=0}^2 e^{i\frac{4\pi j}{3}} = 0$.

Отсюда следует, что $M_k^0 = \frac{2}{3}S_k$, $k = 0, 1, 2$, является разложением единицы, отвечающим переполненной системе векторов $\sqrt{\frac{2}{3}}|\psi_k\rangle$, $k = 0, 1, 2$. Соответствующая наблюдаемая экстремальна, поскольку выполнено условие теоремы 2.2.4.

Покажем, что в случае равновероятных состояний ($\pi_j = \frac{1}{3}$) $\{M_k^0\}$ является оптимальной наблюдаемой. Проверим условия теоремы 2.3.1. Поскольку $S_j^2 = S_j$, мы имеем

$$\Lambda^0 = \sum_{j=0}^2 \frac{1}{3} S_j M_j^0 = \frac{2}{9} \sum_{j=0}^2 S_j = \frac{1}{3} I.$$

так что выполнено условие 2: $\frac{I}{3} = \Lambda^0 \geq \frac{S_j}{3}$. Условие 1 также выполнено, поскольку

$$\left(\Lambda^0 - \frac{1}{3} S_j \right) M_j^0 = \frac{1}{3} (I - S_j) S_j = 0.$$

Итак, $\max \mathcal{P}\{M\} = \text{Tr} \Lambda^0 = \frac{2}{3}$. Найдем теперь максимум по всевозможным четким наблюдаемым с тремя исходами. Нетривиальное ортогональное разложение единицы с тремя компонентами в двумерном пространстве имеет вид $M_0 = |e_0\rangle\langle e_0|$, $M_1 = |e_1\rangle\langle e_1|$, $M_2 = 0$, где $|e_0\rangle$, $|e_1\rangle$ — произвольный базис. Поэтому задача сводится к оптимальному различению двух равновероятных состояний S_0, S_1 . Применяя соотношение (2.46) для случая $\langle\psi_0|\psi_1\rangle = -\frac{1}{2}$, получаем

$$\max_{\substack{M-\text{четкие} \\ \text{наблюдаемые}}} \mathcal{P}\{M\} = \frac{2}{3} \frac{1 + \sqrt{3}/2}{2} < \frac{2}{3} = \max_{M \in \mathfrak{M}} \mathcal{P}\{M\}.$$

Таким образом, использование в квантовой статистике нечетких наблюдаемых может привести к выигрышу при различении состояний исходной системы по сравнению с четкими наблюдаемыми. Подчеркнем, что в ана-

логичном классическом случае никакая рандомизация не может улучшить качество процедуры различения состояний. С геометрической точки зрения причина, конечно, состоит в том, что в квантовом случае не все экстремальные наблюдаемые (среди которых и находится оптимальная) являются четкими.

§ 2.4. Комментарии

1. Из текстов, посвященных математическим основаниям квантовой механики, выделим монографии фон Неймана [21], Макки [16], Сигала [27], Л. Д. Фаддеева и О. А. Якубовского [29]. Обзор аксиоматических подходов имеется в статье Вайтмана [154], а также в замечаниях к гл. VIII книги Рида и Саймона [24]. Желанной целью любой аксиоматики является вывод формализма гильбертова пространства; такой вывод в рамках операционального подхода (см. ниже) в конечномерном варианте осуществлен в работе Араки [51]. Впрочем, это является отдельной темой; для наших целей достаточно просто постулировать множество состояний $\mathfrak{S} = \mathfrak{S}(\mathcal{H})$. Описание смешанных состояний операторами (матрицами) плотности было предложено независимо фон Нейманом, Вейлем и Л. Д. Ландау (см. примечание на с. 240 в книге [21]).

Аксиоматический подход, в основу которого положена двойственность между парой частично упорядоченных пространств, порождаемых выпуклым множеством квантовых состояний и порядковым интервалом 0-1-наблюдаемых (тестов), разрабатывался школой Людвига; см. работы [82, 127], а также книгу Дэвиса [73] (подобный подход часто называют *операциональным*). Подробное исследование статистической структуры квантовой теории на основе операционального подхода предпринято в книгах А. С. Холево [36, 37], где можно также найти подробную библиографию.

В предложении 2.1.1 нам пришлось предположить существование максимальной наблюдаемой только потому, что для простоты мы с самого начала ограничились конечными множествами исходов. При надлежащем обобщении существование максимальной наблюдаемой (вообще говоря, с бесконечным пространством Ω) может быть выведено из совместимости всех наблюдаемых модели. По существу, об этом говорит известная теорема Колмогорова о построении вероятностного пространства для случайного процесса, заданного системой согласованных (т. е. совместных) конечномерных распределений. Подробное исследование отношения стохастической совместимости, включающее доказательство того факта, что отделимая модель, все наблюдаемые которой стохастически совместимы, вкладывается в модель Вальда, имеется в работе А. С. Холево [97].

Изложение основных понятий для нужд квантовой теории информации имеется в книгах Нильсена и Чанга [22], а также Хайаши [90]. В работе Фукса [83] описана информационно-теоретическая точка зрения на основания квантовой теории.

2. Излагаемая здесь концепция квантовой наблюдаемой разрабатывалась в работах Людвига [127], Дэвиса и Льюиса [73], А. С. Холево [37]. Выпуклая структура множества наблюдаемых рассматривается в книге Крауса [116].

Спин квантовой частицы органически связан с представлениями группы вращений трехмерного пространства; см. [3, 16]. Результаты, связанные с теоремой 2.2.4, приведены в работе Дэвиса [72].

3. Задача различения двух чистых квантовых состояний была впервые рассмотрена в 1968 г. в работе П. А. Бакута и С. С. Щурова, см. книгу [14]. Подобные задачи естественно возникают при обнаружении слабых источников света, а также в квантовой оптике. Общая теория обнаружения и оценивания для квантовых состояний была разработана в 1970-е гг. в трудах Хелстрема, Юна, А. С. Холево, Р. Л. Стратоновича, В. П. Белавкина, см. монографии [30, 37]. Новый интерес к теории оценивания квантовых состояний появился в связи с идеями квантовых вычислений: всякое такое вычисление завершается измерением параметров конечного состояния квантового компьютера, которое должно быть максимально точным. Результаты современной теории оценивания квантовых состояний, включая асимптотический подход, излагаются в книгах Хайаши [90] и Петца [132]. Байесовская задача является задачей линейного программирования (см. [17], [25]), и теорема 2.3.1 может быть доказана на основе соответствующей теоремы двойственности. Пример 2.3.3 с тремя равноугольными состояниями предложен А. С. Холево в статье [33].

ГЛАВА 3

Составные квантовые системы и сцепленность

§ 3.1. Составные системы

3.1.1. Тензорное произведение

Своеобразие и новые возможности квантовой теории информации в значительной мере обусловлены свойствами составных квантовых систем. Пусть $\mathcal{H}_j$, $j = 1, 2$, — гильбертовы пространства двух квантовых систем со скалярными произведениями $\langle \cdot | \cdot \rangle_j$. Составная система описывается тензорным произведением гильбертовых пространств, которое может быть построено следующим образом.

Согласно § 1.1 элемент $\psi \in \mathcal{H}$ определяет антилинейную функцию $\psi(\varphi) = \langle \varphi | \psi \rangle$ аргумента $\varphi \in \mathcal{H}$; для двух элементов $\psi_j \in \mathcal{H}_j$, $j = 1, 2$, обозначим через $\psi_1 \otimes \psi_2$ биантилинейную функцию аргументов $\varphi_1 \in \mathcal{H}_1$, $\varphi_2 \in \mathcal{H}_2$, определенную соотношением

$$(\psi_1 \otimes \psi_2)(\varphi_1, \varphi_2) = \langle \varphi_1 | \psi_1 \rangle_1 \langle \varphi_2 | \psi_2 \rangle_2.$$

Рассмотрим векторное пространство $\mathcal{L}$ конечных линейных комбинаций таких функций $\sum_j c_j \psi_1^j \otimes \psi_2^j$. Введем скалярное произведение на $\mathcal{L}$, полагая

$$\langle \varphi_1 \otimes \varphi_2 | \psi_1 \otimes \psi_2 \rangle = \langle \varphi_1 | \psi_1 \rangle_1 \langle \varphi_2 | \psi_2 \rangle_2$$

на порождающих элементах и далее продолжая по линейности на $\mathcal{L}$.

Задача 3.1.1. Покажите, что такое линейное продолжение возможно, оно единственно и удовлетворяет всем свойствам скалярного произведения.

Пространство $\mathcal{L}$ с определенным выше скалярным произведением называется *тензорным произведением* $\mathcal{H}_1 \otimes \mathcal{H}_2$ гильбертовых пространств $\mathcal{H}_1$, $\mathcal{H}_2$.

Задача 3.1.2. Пусть $\{e_1^j\}$, $\{e_2^k\}$ — ортонормированные базисы в $\mathcal{H}_1$, $\mathcal{H}_2$. Докажите, что тогда $\{e_1^j \otimes e_2^k\}$ — ортонормированный базис в $\mathcal{H}_1 \otimes \mathcal{H}_2$ и $\dim \mathcal{H}_1 \otimes \mathcal{H}_2 = \dim \mathcal{H}_1 \times \dim \mathcal{H}_2$.

Отсюда вытекает, что всякий вектор $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ однозначно записывается в виде

$$|\psi\rangle = \sum_{j,k} c_{jk} |e_1^j\rangle \otimes |e_2^k\rangle.$$

Производя суммирование по j и вводя обозначение $|\psi_k\rangle = \sum_{j=1}^{d_1} c_{jk} |e_1^j\rangle \in \mathcal{H}_1$, получаем

$$|\psi\rangle = \sum_{k=1}^{d_2} |\psi_k\rangle \otimes |e_2^k\rangle,$$

так что в общем случае $\mathcal{H}_1 \otimes \mathcal{H}_2$ изоморфно прямой ортогональной сумме $d_2 = \dim \mathcal{H}_2$ слагаемых $\mathcal{H}_1 \oplus \dots \oplus \mathcal{H}_1$.

Для операторов X_j в пространствах $\mathcal{H}_j$ зададим их тензорное произведение, полагая

$$(X_1 \otimes X_2)(\psi_1 \otimes \psi_2) = X_1 \psi_1 \otimes X_2 \psi_2$$

и продолжая по линейности. Фиксируем базис в $\mathcal{H}_2$, так что $\mathcal{H}_1 \otimes \mathcal{H}_2$ представляется как $\mathcal{H}_1 \oplus \dots \oplus \mathcal{H}_1$. Тогда $X_1 \otimes X_2$ можно представить в виде блочной матрицы $[X_1 x_2^{jk}]$, где $[x_2^{jk}]$ — матрица оператора X_2 в базисе $\{e_2^k\}$. Произвольный оператор X в $\mathcal{H}_1 \otimes \mathcal{H}_2$ задается блочной матрицей $[X_{jk}]$, элементы которой суть операторы в $\mathcal{H}_1$.

Напомним, что в § 1.4 через $\mathfrak{B}_h(\mathcal{H})$ обозначалось вещественное линейное пространство всех эрмитовых операторов в $\mathcal{H}$, т. е. четких вещественных наблюдаемых. В силу результата задачи 1.4.2 в случае комплексных гильбертовых пространств $\mathcal{H}_1, \mathcal{H}_2$ мы имеем

$$\dim \mathfrak{B}_h(\mathcal{H}_1 \otimes \mathcal{H}_2) = \dim \mathfrak{B}_h(\mathcal{H}_1) \cdot \dim \mathfrak{B}_h(\mathcal{H}_2),$$

тогда как в случае вещественных $\mathcal{H}_1, \mathcal{H}_2$ для размерностей пространств симметричных операторов имеет место неравенство $>$.

Задача 3.1.3. Докажите, что если S_j — операторы плотности в $\mathcal{H}_j$, $j = 1, 2$, то $S_1 \otimes S_2$ — оператор плотности в $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Пусть T — оператор в $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. *Частичный след* оператора T (относительно $\mathcal{H}_2$), обозначаемый $\text{Tr}_{\mathcal{H}_2} T$, определяется как оператор в $\mathcal{H}_1$, ассоциированный с формой

$$\langle \varphi | (\text{Tr}_{\mathcal{H}_2} T) | \psi \rangle = \sum_k \langle \varphi \otimes e_2^k | T | \psi \otimes e_2^k \rangle, \quad \varphi, \psi \in \mathcal{H}_1.$$

Задача 3.1.4. Покажите, что определение корректно, т. е. не зависит от выбора ортонормированного базиса $\{e_2^k\}$. Если $T = T_1 \otimes T_2$, то $\text{Tr}_{\mathcal{H}_2}(T_1 \otimes T_2) = (\text{Tr } T_2) T_1$.

Пусть пространство $\mathcal{H}_1 \otimes \mathcal{H}_2$ реализовано как $\mathcal{H}_1 \oplus \dots \oplus \mathcal{H}_1$, так что $T = [T_{jk}]$. Докажите, что тогда $\text{Tr}_{\mathcal{H}_2} T = \sum_{j=1}^{d_2} T_{jj}$ и $\text{Tr}_{\mathcal{H}_1} T = [\text{Tr } T_{jk}]$.

3.1.2. Расширение Наймарка

Принципиальная связь между ортогональными и неортогональными разложениями единицы устанавливается следующей теоремой.

Теорема 3.1.1 (Наймарк). *Пусть $\{M_x\}$ — разложение единицы в $\mathcal{H}$ с t компонентами, $\dim \mathcal{H} = d$. Тогда существуют гильбертово пространство $\mathcal{K}$ размерности $\dim \mathcal{K} \leq td$, изометрическое отображение $V: \mathcal{H} \rightarrow \mathcal{K}$ и ортогональное разложение единицы $\{E_x\}$ в $\mathcal{K}$ такие, что*

$$M_x = V^* E_x V, \quad x \in \mathcal{X}. \quad (3.1)$$

Изометрическое отображение (изометрия) — это линейное отображение V , сохраняющее скалярное произведение векторов в гильбертовых пространствах. Для любых $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ выполняется равенство $\langle V\varphi | V\psi \rangle = \langle \varphi | \psi \rangle$, так что изометрия характеризуется равенством $V^*V = I$. Изометрическое вложение V позволяет отождествить $\mathcal{H}$ с подпространством $V\mathcal{H}$ пространства $\mathcal{K}$ и считать, что $\mathcal{H} \subset \mathcal{K}$. Тогда M_x можно рассматривать просто как ограничение E_x на $\mathcal{H}$:

$$E_x = \begin{bmatrix} M_x & \cdots \\ \cdots & \cdots \end{bmatrix}.$$

Доказательство. Построение пространства $\mathcal{K}$ будет осуществлено в два этапа. Сначала определим векторы $|\Psi\rangle \in \mathcal{H}_m$ формулой

$$|\Psi\rangle = \begin{bmatrix} |\psi_1\rangle \\ \vdots \\ |\psi_m\rangle \end{bmatrix}, \quad |\psi_i\rangle \in \mathcal{H}. \quad (3.2)$$

Определим также псевдоскалярное произведение, т. е. форму, удовлетворяющую всем свойствам скалярного произведения, кроме невырожденности, соотношением

$$\langle \Psi' | \Psi \rangle = \sum_x \langle \psi'_x | M_x | \psi_x \rangle. \quad (3.3)$$

Соответствующая квадратичная форма может быть вырожденна.

Для того чтобы обеспечить невырожденность, определим $\mathcal{K}$ как факторпространство $\mathcal{K} = \mathcal{H}_m / \mathcal{H}_0$, где $\mathcal{H}_0 = \{\Psi_0 \in \mathcal{H}_m : \langle \Psi_0 | \Psi_0 \rangle = 0\}$, т. е. объ-

единим векторы, разности которых имеют нулевую норму. Теперь отображение $V: \mathcal{H} \rightarrow \mathcal{H}_m$, определяемое как

$$V|\psi\rangle = \begin{bmatrix} |\psi\rangle \\ \vdots \\ |\psi\rangle \end{bmatrix}, \quad (3.4)$$

является изометрией, так как

$$\langle\psi|V^*V|\psi\rangle = \sum_{j=1}^m \langle\psi|M_x|\psi\rangle = \langle\psi|\psi\rangle. \quad (3.5)$$

В качестве ортогонального разложения единицы $\{E_x\}$ в $\mathcal{K}$ рассмотрим $E_x|\Psi\rangle = [0, \dots, |\psi_x\rangle, \dots, 0]^\top$, где единственная ненулевая компонента находится на x -м месте. Таким образом,

$$\langle V\varphi|E_x|V\psi\rangle = \langle\varphi|M_x|\psi\rangle, \quad \varphi, \psi \in \mathcal{H},$$

что завершает доказательство. $\square$

Рассмотрим теперь важное следствие из теоремы Наймарка, дающее статистическую интерпретацию произвольного разложения единицы и устанавливающее согласованность обобщенного и стандартного определений квантовой наблюдаемой.

Следствие 3.1.1. Пусть $\{M_x\}$ — наблюдаемая в $\mathcal{H}$, тогда найдутся гильбертово пространство $\mathcal{H}_0$, единичный вектор $\psi_0 \in \mathcal{H}_0$ и четкая наблюдаемая $\{E_x\}$ в $\mathcal{H} \otimes \mathcal{H}_0$ такие, что

$$M_x = \text{Tr}_{\mathcal{H}_0}(I \otimes |\psi_0\rangle\langle\psi_0|)E_x. \quad (3.6)$$

Доказательство. В соответствии с теоремой Наймарка $M_x = V^*E_xV$, где $V: \mathcal{H} \rightarrow \mathcal{K}$ — изометрическое вложение. отождествим $\mathcal{H}$ с подпространством $\mathcal{K}$. Расширяя, если необходимо, пространство $\mathcal{K}$, можно считать, что $\dim \mathcal{K} = \dim \mathcal{H} \cdot d_0$ и, значит

$$\mathcal{K} \simeq \mathcal{H} \oplus \dots \oplus \mathcal{H} \simeq \mathcal{H} \otimes \mathcal{H}_0,$$

где $\mathcal{H}_0 = \ell_{d_0}^2$ — координатное гильбертово пространство размерности d_0 , причем $\mathcal{H}$ отождествляется с первым слагаемым в прямой сумме, или с подпространством $\mathcal{H} \otimes |\psi_0\rangle$, где $|\psi_0\rangle = [1, 0, \dots, 0]^\top$. Тогда

$$(I \otimes |\psi_0\rangle\langle\psi_0|)E_x = \begin{bmatrix} M_x & \dots \\ 0 & 0 \end{bmatrix},$$

так что соотношение (3.6) действительно выполнено. $\square$

Итак, всякую наблюдаемую можно реализовать в виде четкой наблюдаемой составной системы за счет добавления вспомогательной системы, находящейся в фиксированном состоянии $S_0 = |\psi_0\rangle\langle\psi_0|$. Такой способ реализации естественно назвать *квантовой рандомизацией*.

В классической статистике рандомизация, т. е. добавление «рулетки», хотя и может оказаться полезным приемом (например, в теории игр), не увеличивает информации о состоянии наблюдаемой системы. Из результатов п. 2.3.2 следует, что в квантовой статистике это не всегда верно: парадоксальным образом, квантовая рандомизация позволяет извлечь больше информации о состояниях наблюдаемой системы, нежели содержится в четких наблюдаемых, не использующих независимой вспомогательной системы.

3.1.3. Разложение Шмидта и очищение

Рассмотрим состояние S_{12} составной системы в гильбертовом пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Определение 3.1.1. Чистое состояние S_{12} называется *сцепленным*, если оно не представимо в виде тензорного произведения $S_1 \otimes S_2$.

Таким образом, всякий единичный вектор $\psi_{12} \in \mathcal{H}_1 \otimes \mathcal{H}_2$, который является нетривиальной суперпозицией векторов-произведений, порождает чистое сцепленное состояние. Примером является *максимально сцепленное состояние*, которое порождается вектором

$$|\psi_{12}\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d |e_j^1\rangle \otimes |e_j^2\rangle \quad (3.7)$$

в пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$, где $d = \dim \mathcal{H}_1 = \dim \mathcal{H}_2$, а $\{e_j^{1,2}\}$ — ортонормированные базисы в $\mathcal{H}_{1,2}$. Смысл этого термина будет разъяснен позднее, в § 7.4, где понятие сцепленности будет также обобщено на произвольные состояния составной системы.

Мы будем часто использовать следующий результат.

Теорема 3.1.2 (разложение Шмидта). Пусть $S_{12} = |\psi\rangle\langle\psi|$ — чистое состояние в гильбертовом пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$, и пусть $S_1 = \text{Tr}_{\mathcal{H}_2} S_{12}$, $S_2 = \text{Tr}_{\mathcal{H}_1} S_{12}$ — частичные состояния. Тогда S_1 и S_2 имеют одни и те же ненулевые собственные значения λ_j . Более того,

$$|\psi\rangle = \sum_j \sqrt{\lambda_j} |e_j^1\rangle \otimes |e_j^2\rangle, \quad (3.8)$$

где $\{e_j^{1,2}\}$ — ортонормированные собственные векторы операторов S_1 и S_2 соответственно.

Доказательство. Пусть $\{e_j^1\}$ — ортонормированный базис в $\mathcal{H}_1$ из собственных векторов оператора S_1 , тогда имеет место разложение

$$|\psi\rangle = \sum_j |e_j^1\rangle \otimes |h_j^2\rangle \quad (3.9)$$

с некоторыми векторами $|h_j^2\rangle \in \mathcal{H}_2$. Вычисление частичного следа оператора $|\psi\rangle\langle\psi|$ по $\mathcal{H}_2$ дает

$$\sum_{j,k} \langle h_j^2 | h_k^2 \rangle |e_k^1\rangle \langle e_j^1| = \sum_j \lambda_j |e_j^1\rangle \langle e_j^1| \equiv S_1, \quad (3.10)$$

и поэтому $\langle h_j^2 | h_k^2 \rangle = \lambda_j \delta_{jk}$. Таким образом, полагая $|e_j^2\rangle = \frac{1}{\sqrt{\lambda_j}} |h_j^2\rangle$ при $\lambda_j > 0$, получаем ортонормированную систему, которую можно дополнить до базиса в $\mathcal{H}_2$, состоящего из собственных векторов оператора S_2 . $\square$

Имеет место следующее обращение предыдущего утверждения.

Теорема 3.1.3 (очищение состояний). Пусть S_1 — состояние в $\mathcal{H}_1$, тогда найдутся гильбертово пространство $\mathcal{H}_2$ той же размерности, что и $\mathcal{H}_1$, и чистое состояние $|\psi\rangle\langle\psi| \in \mathcal{H}_1 \otimes \mathcal{H}_2$ такие, что $S_1 = \text{Tr}_{\mathcal{H}_2} |\psi\rangle\langle\psi|$.

Для любого чистого состояния $|\psi'\rangle\langle\psi'| \in \mathcal{H}_1 \otimes \mathcal{H}_2$, обладающего этим же свойством, найдется унитарный оператор U_2 в $\mathcal{H}_2$ такой, что $|\psi'\rangle = (I_1 \otimes U_2)|\psi\rangle$.

Доказательство. Диагонализуем S_1 и определим $|\psi\rangle$ по формуле (3.8) с произвольным базисом $\{e_j^2\}$ в гильбертовом пространстве $\mathcal{H}_2$, изоморфном $\mathcal{H}_1$. Любой другой вектор $|\psi'\rangle$ имеет разложение (3.8) с другим базисом в $\mathcal{H}_2$. Остается заметить, что любые два базиса в гильбертовом пространстве связаны унитарным преобразованием. $\square$

Следствие 3.1.2. Пусть S_{12} — такое состояние в $\mathcal{H}_1 \otimes \mathcal{H}_2$, что частичное состояние S_1 является чистым. Тогда $S_{12} = S_1 \otimes S_2$.

Доказательство. Для чистого состояния S_{12} утверждение очевидным образом следует из теоремы 3.1.2; для произвольного состояния S_{12} мы можем применить аналогичное рассуждение к его очищению. $\square$

Из теоремы 3.1.2 следует, что очищение в существенном единственно: любые два очищения с пространствами $\mathcal{H}_2, \mathcal{H}_2'$ такими, что $\dim \mathcal{H}_2 \leq \dim \mathcal{H}_2'$, связаны изометрическим вложением $\mathcal{H}_2$ в $\mathcal{H}_2'$.

Замечательно, что существует одно универсальное гильбертово пространство, содержащее очищения всех состояний в $\mathcal{H}$. Рассмотрим гильбертово пространство $L^2(\mathcal{H})$ всех операторов $X, Y, \dots$ в $\mathcal{H}$, снабженное скалярным произведением

$$(X, Y) = \text{Tr } X^* Y.$$

Тогда линейное соответствие

$$|\psi\rangle\langle\varphi| \leftrightarrow |\psi\rangle \otimes \langle\varphi|, \quad (3.11)$$

где $\langle\varphi| \in \mathcal{H}^*$ (двойственное пространство линейных функций на $\mathcal{H}$), единственным образом продолжается до изометрии между гильбертовыми пространствами $L^2(\mathcal{H})$ и $\mathcal{H} \otimes \mathcal{H}^*$. Обозначая через L_A (соответственно R_B) оператор левого умножения на A (соответственно правого умножения на B), мы получим

$$L_A R_B X \equiv A X B \leftrightarrow |A\psi\rangle \otimes \langle B^*\varphi|$$

для $X = |\psi\rangle\langle\varphi|$. Для произвольного оператора плотности S в $\mathcal{H}$ рассмотрим единичный вектор $\sqrt{S}W \in L^2(\mathcal{H})$, где W — произвольный унитарный оператор в $\mathcal{H}$. Тогда

$$(\sqrt{S}W, L_A R_B \sqrt{S}W) = \text{Tr} \sqrt{S} A \sqrt{S} W B W^*.$$

Следовательно, полагая $B = I$, получаем

$$\text{Tr} SA = (\sqrt{S}W, (A \otimes I_{\mathcal{H}^*}) \sqrt{S}W).$$

Поэтому $\sqrt{S}W$ есть очищение оператора S в пространстве $L^2(\mathcal{H})$, отождествленном с $\mathcal{H} \otimes \mathcal{H}^*$ с помощью соответствия (3.11); более того, все очищения оператора S получаются таким образом.

3.1.4. Парадокс Эйнштейна—Подольского—Розена.

Неравенство Белла

Существование сцепленности, наряду с дополнительностью, является принципиальным структурным различием между классическим и квантовым описаниями систем.

Чистое состояние классической системы задается точкой фазового пространства (практически набором конкретных значений параметров, описывающих «внутренние свойства» системы). Если рассматриваемая классическая система состоит из нескольких подсистем, то всякое ее чистое состояние с необходимостью является произведением чистых состояний подсистем. Фиксируя значения параметров составной системы, мы тем самым фиксируем значения параметров всех ее подсистем. При этом нет необходимости прибегать к статистическому описанию.

В случае квантовых систем дело обстоит иначе. Как показывает следствие 3.1.2, для любого чистого сцепленного состояния S_{12} составной системы частичные состояния $S_{1,2}$ с необходимостью являются смешанными, т. е. требуют статистического описания.

Такой тип поведения составных систем совершенно необычен с классической точки зрения и, как будет показано далее в этом пункте, вообще

несовместим с классическим способом описания (который в зарубежной литературе часто называется «реализмом»).

Ключевой пример необычного (с классической точки зрения) поведения составной квантовой системы рассмотрели Эйнштейн, Подольский и Розен (ЭПР) в 1935 г. В 50-х годах XX века Бом представил пример в более рельефной форме, использующей спиновые степени свободы, а в 60-х годах Белл внес большую логическую ясность, предложив фундаментальное неравенство, которое выполняется для составных классических систем, удовлетворяющих естественному дополнительному условию «локальности» (разделимости), но нарушается для квантовых систем и в принципе может быть проверено экспериментально.

Рассмотрим две частицы со спином $1/2$, каждая из которых описывается гильбертовым пространством $\mathcal{H}$, $\dim \mathcal{H} = 2$. В результате некоторого взаимодействия (или реакции распада) в начальный момент возникает совместное состояние их спинов, которое задается вектором

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle],$$

где базисные векторы

$$|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

описывают состояния каждой частицы со спином, направленным в положительном (соответственно отрицательном) направлении оси z . Обычно пишут

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle].$$

Каждое слагаемое здесь описывает состояние с разнонаправленными спинами, а $|\psi\rangle$ есть их суперпозиция, которую невозможно представить в виде тензорного произведения векторов состояний, относящихся к разным частицам. Такое состояние, называемое в физике «синглетом», является образцом сцепленного состояния двух квантовых систем.

Предположим, что частицы разлетаются на некоторое макроскопическое расстояние; при этом их спиновое состояние — синглет — сохраняется. Рассмотрим эксперимент, в котором в двух удаленных друг от друга лабораториях A и B над этими разлетевшимися частицами производятся одновременные измерения: наблюдаемой спина $\sigma(\mathbf{a})$ для одной частицы и наблюдаемой спина $\sigma(\mathbf{b})$ для другой (рис. 3.1). Операторы $X = \sigma(\mathbf{a}) \otimes I$, $Y = I \otimes \sigma(\mathbf{b})$ коммутируют, следовательно, соответствующие наблюдаемые совместимы, и их ковариация дается выражением (2.24).

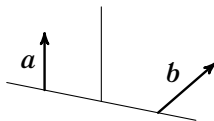


Рис. 3.1. Направления спинов

Задача 3.1.5. Используя выражения для матричных элементов

$$\langle \uparrow | \sigma(\mathbf{a}) | \uparrow \rangle = a_z, \quad \langle \downarrow | \sigma(\mathbf{a}) | \uparrow \rangle = a_x + ia_y, \quad \langle \downarrow | \sigma(\mathbf{a}) | \downarrow \rangle = -a_z, \quad (3.12)$$

вытекающие из соотношения (2.14), покажите, что в синглетном состоянии среднее значение и дисперсия каждой наблюдаемой равны

$$E\sigma(\mathbf{a}) = 0, \quad D\sigma(\mathbf{a}) = 1,$$

а ковариация между спинами задается формулой

$$\langle \psi | \sigma(\mathbf{a}) \otimes \sigma(\mathbf{b}) | \psi \rangle = -\mathbf{a} \cdot \mathbf{b}. \quad (3.13)$$

Отсюда следует, что если $\mathbf{b} = \mathbf{a}$, то коэффициент корреляции равен -1 и, следовательно, между исходами $\mathbf{a}$, $\mathbf{b}$ измерений имеется детерминированная связь: $\mathbf{a} = -\mathbf{b}$. Из формул (3.12) и соотношения $\sigma(\mathbf{a})^2 = I$ следует, что

$$\langle \psi | [\sigma(\mathbf{a}) \otimes I + I \otimes \sigma(\mathbf{a})]^2 | \psi \rangle = 0,$$

и, таким образом,

$$[\sigma(\mathbf{a}) \otimes I + I \otimes \sigma(\mathbf{a})] | \psi \rangle = 0.$$

Если бы спины описывались классическими векторными случайными величинами, то это означало бы, что при измерении спина первой частицы в произвольно выбранном направлении $\mathbf{a}$ спин второй частицы «моментально» принимает противоположное значение.

Таким образом, приходится выбирать между следующими альтернативами.

1. В квантовой механике, подобно классической, состояние описывает «реальные» внутренние свойства системы. При этом чтобы объяснить, как вторая частица «узнает» о выборе направления измеряемого спина для первой частицы, приходится допустить мгновенное дальнее действие, противоречащее физическому «принципу локальности».

2. Вектор состояния — это лишь выражение информационного содержания процедуры приготовления системы, включающее прошлое взаимодействие подсистем. В этом случае никакого противоречия с локальностью не возникает, но приходится отказаться от полноты механистического описания состояния как «совокупности внутренних свойств».

Задача 3.1.6. Докажите, что для любого направления $\mathbf{a}$ выполняется соотношение

$$|\psi\rangle = \frac{\varepsilon}{\sqrt{2}}[|\mathbf{a}\rangle \otimes |-\mathbf{a}\rangle - |-\mathbf{a}\rangle \otimes |\mathbf{a}\rangle], \quad (3.14)$$

где ε — несущественный множитель, по модулю равный единице.

Более основательное рассмотрение мысленного эксперимента с синглетным состоянием приводит к более конкретному и глубокому выводу: если попытаться описывать корреляции двух спинов классически и в соответствии с принципом локальности, то оказывается невозможным достичь такого характера и уровня коррелированности, который соответствует предсказаниям квантовой теории. «Локальный реализм» и предсказываемая квантовой статистикой корреляция (3.13) несовместимы.

Это доказывается с помощью **неравенства Белла—Клаузера—Хорна—Шимони—Хольта**.

Пусть $X_j, Y_k, j, k = 1, 2$, — случайные величины на произвольном вероятностном пространстве Ω такие, что $|X_j| \leq 1, |Y_k| \leq 1$. Тогда для любого распределения вероятностей P на Ω корреляция этих величин удовлетворяет неравенству

$$|EX_1Y_1 + EX_1Y_2 + EX_2Y_1 - EX_2Y_2| \leq 2, \quad (3.15)$$

где E — математическое ожидание, соответствующее распределению P .

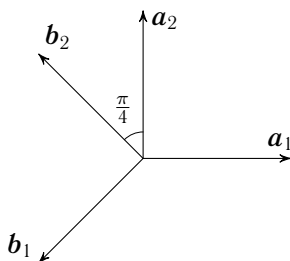
Доказательство получается усреднением по распределению P элементарного неравенства

$$-2 \leq X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2 \leq 2,$$

которое, в свою очередь, следует из неравенства

$$|X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2| \leq |Y_1 + Y_2| + |Y_1 - Y_2| \leq 2 \max\{|Y_1|, |Y_2|\}.$$

Вернемся теперь к системе из двух q -битов и рассмотрим четыре различных эксперимента, в которых наблюдаемые спина $\sigma(\mathbf{a}_j), j = 1, 2$, измеряются для первого q -бита, а $\sigma(\mathbf{b}_k), k = 1, 2$, — для второго; направления $\mathbf{a}_j, \mathbf{b}_k, j, k = 1, 2$, будут выбраны позже. Во всех четырех экспериментах система готовится в синглетном состоянии. Предположим, что существует «локальное» классическое представление для результатов всех этих четырех экспериментов. Это означает, что найдутся вероятностное пространство Ω , распределение вероятностей P на Ω , описывающее статистический ансамбль в синглетном состоянии, и случайные

Рис. 3.2. Выбор направлений a_j и b_k

величины X_j, Y_k , $j, k = 1, 2$, принимающие значения ± 1 , которые дают классическое описание наблюдаемых спина $\sigma(a_j), \sigma(b_k)$, $j, k = 1, 2$. Тогда квантовые корреляции (3.13) должны удовлетворять неравенству (3.15). Условие «локальности» (а лучше сказать, *разделимости* подсистем) выражается в том, что случайные величины, описывающие спин первой системы (X_1 в случае первых двух корреляций и X_2 в двух других случаях), предполагаются одними и теми же для экспериментов, различающихся выбором измеряемого направления спина (Y_1 или Y_2) во второй системе (и наоборот), что и позволяет применить неравенство (3.15). Отказ от этого означал бы, что данное классическое описание допускает влияние выбора измерения во второй системе на внутренние характеристики первой системы (термин «локальность» возникает в связи с тем, что системы предполагаются пространственно удаленными друг от друга).

Теперь выберем конкретные направления спинов, как показано на рис. 3.2. Подставляя корреляции, определяемые формулой (3.13), в левую часть неравенства (3.15), получаем значение $2\sqrt{2}$, нарушающее это неравенство. Следовательно, исходное предположение о возможности классического «локального» описания является неверным. Условие разделимости кажется настолько естественным, что оно даже трудно уловимо, однако именно оно запрещает мгновенное влияние измерения, проводящегося в одной системе, на результаты измерений в другой системе. Если же от него отказаться, то интересующие нас четыре физические корреляции могут быть любыми величинами из отрезка $[-1, 1]$ и левая часть неравенства (3.15) будет ограничена лишь величиной 4, что не входит в противоречие с квантовой теорией.

Таким образом, возникает дилемма: либо квантовая теория дает неверные предсказания для корреляций, либо составная система из двух q -битов не имеет классического «локального» описания. Был проделан целый ряд экспериментов начиная со знаменитых экспериментов Аспека

(1981—1982), результаты которых свидетельствуют в пользу квантовой теории.

§ 3.2. Квантовая система как носитель информации

3.2.1. Передача классической информации

Если носитель информации является классической системой с конечным числом состояний d , то максимальное количество двоичных единиц — бит, которое может быть записано либо передано с помощью такого носителя, равно, очевидно¹ $\log d$. Если передача происходит без ошибок, то говорят об идеальном канале связи. В общем случае классический канал описывается условными вероятностями $p(y|x)$ получить сообщение y на выходе, если на вход послано сообщение x . Для идеального канала $p(y|x) = \delta_{xy}$; антиподом идеального канала является канал, для которого вероятности $p(y|x) = p(y)$ не зависят от посланного сообщения x и, следовательно, информация вообще не передается. Более подробно о классических каналах будет рассказано в гл. 4.

Рассмотрим теперь, как происходит передача классической информации посредством квантового носителя, описываемого гильбертовым пространством $\mathcal{H}$. Состояние носителя S готовится некоторыми макроскопическими устройствами. Изменяя параметры этих устройств, экспериментатор изменяет состояние и таким образом получает возможность «записывать» классические сообщения, содержащиеся в значениях параметров, в квантовом состоянии. Пусть имеется n разных сообщений и S_x — квантовое состояние, отвечающее сообщению с номером x , $x = 1, \dots, n$. Отображение $x \rightarrow S_x$ описывает конечный результат физического процесса, порождающего состояние S_x . Подробное описание этого процесса не входит в задачу теории информации, которую интересуют лишь эти конечные состояния S_x .

Для того чтобы извлечь информацию о сообщении, содержащуюся в квантовом состоянии, необходимо произвести некоторое измерение. Если на выходе такого канала измеряется наблюдаемая $M = \{M_y\}$, то условная вероятность получить на выходе сообщение y , если на вход было послано сообщение x , равна

$$P_M(y|x) = \text{Tr } S_x M_y. \quad (3.16)$$

Таким образом, для фиксированного измерения получается обычный классический канал связи. Предположим, что приготовление состояний

¹Далее $\log = \log_2$ обозначает двоичный логарифм. Чтобы избежать несущественных оговорок, мы будем игнорировать тот факт, что $\log d$ не обязательно является целым числом.

и измерение удастся организовать так, что $S_x = |e_x\rangle\langle e_x|$, $M_y = |e_y\rangle\langle e_y|$, тогда $P_M(y|x) = \delta_{xy}$, т. е. возникает идеальный классический канал, способный передать $\log d$ бит, где $d = \dim \mathcal{H}$. Далее в гл. 5 будет установлено, что эта величина является верхней границей для количества классической информации, которое вообще может передано с помощью данного квантового носителя. Отсюда следуют важные выводы:

1) то обстоятельство, что гильбертово пространство содержит бесконечно много различных векторов чистых состояний, не помогает передать неограниченное количество информации; причина кроется в том, что чем больше состояний используется для передачи, тем они становятся более близкими друг к другу и, следовательно, более неразличимыми;

2) размерность гильбертова пространства является мерой максимального информационного ресурса квантовой системы.

3.2.2. Сцепленность и локальные операции

В этом пункте нам потребуются элементарные сведения об эволюциях квантовой системы. В дальнейшем, в гл. 6, этот вопрос будет рассмотрен углубленно и с общих позиций. Пока же достаточно знать, что обратимые эволюции квантовой системы описываются унитарными операторами U : в результате такой эволюции вектор исходного чистого состояния ψ преобразуется в вектор $U\psi$. Соответственно, оператор плотности (смешанное состояние) S преобразуется в USU^* .

Рассмотрим теперь следующий вопрос. Нелокальный, с классической точки зрения, характер ЭПР-корреляций наводит на мысль попытаться использовать их для мгновенной передачи сообщений. Покажем, что этого невозможно достичь, находясь в рамках квантовой механики (с точки зрения которой ЭПР-корреляции не противоречат локальности). Рассмотрим двух участников A и B , располагающих квантовыми системами в пространствах $\mathcal{H}_A$ и $\mathcal{H}_B$ соответственно, которые находятся в сцепленном состоянии S_{AB} . В случае, представляющем интерес, системы пространственно разделены, хотя формально это ни в чем не выражается. Участник A (передатчик) использует сообщения x , которые желательно передать участнику B (приемнику), для выполнения некоторых унитарных операций U_x (см. ниже) в своем пространстве $\mathcal{H}_A$ (такие операции называются *локальными*, т. е. действующими нетривиально только в одной из двух систем). При этом состояние системы AB переходит в $S_x = (U_x \otimes I_B)S_{AB}(U_x \otimes I_B)^*$, и, таким образом, классическая информация записывается в квантовом состоянии составной системы. В свою очередь, участник B может произвести локальное измерение произвольной наблюдаемой в $\mathcal{H}_B$, что соответствует разложению еди-

ницы вида $M = \{I_A \otimes M_y\}$ в пространстве составной системы $\mathcal{H}_A \otimes \mathcal{H}_B$. Результирующая переходная вероятность (3.16) имеет вид

$$P_M(y|x) = \text{Tr}(U_x \otimes I_B) S_{AB} (U_x \otimes I_B)^* (I_A \otimes M_y) = \text{Tr} S_B M_y,$$

где $S_B = \text{Tr}_{\mathcal{H}_A} S_{AB}$ — частичное состояние системы B , и не зависит от x . Это означает, что локальные операции участника A никак не влияют на состояние B , а значит, информация действительно не передается.

Рассмотрим теперь другую ситуацию, в которой участник A производит локальное измерение наблюдаемой M_x^A и посылает исход своего измерения участнику B . В этом случае *апостериорное состояние* $S_B(x)$ участника B будет зависеть от исхода x . Чтобы найти апостериорные состояния, предположим, что B производит свое локальное измерение M_y^B , и рассмотрим совместное распределение вероятностей исходов двух измерений

$$p_{x,y} = \text{Tr} S_{AB} (M_x^A \otimes M_y^B).$$

Вводя условные вероятности $p(y|x) = \frac{p_{x,y}}{p_x}$ (в предположении, что $p_x > 0$), получаем

$$p_x = \text{Tr} S_{AB} (M_x^A \otimes I_B) = \text{Tr} S_A M_x^A,$$

$$p(y|x) = \text{Tr} S_B(x) M_y^B,$$

где

$$S_B(x) = p_x^{-1} \text{Tr}_{\mathcal{H}_A} S_{AB} (M_x^A \otimes I_B)$$

— апостериорные состояния.

Изменение состояния участника B от S_B к $S_B(x)$ означает переход от полного статистического ансамбля, который имеется в распоряжении B , к подансамблю, который характеризуется значением x исхода измерения участника A . Если этот исход не учитывается (например, A вовсе не сообщает его B), то состояние B не изменяется:

$$S_B = \sum_x p_x S_B(x).$$

Задача 3.2.1. Пусть $S_{AB} = |\psi\rangle\langle\psi|$ — чистое сцепленное состояние,

$$|\psi\rangle = \sum_x |e_x^A\rangle \otimes |\psi_x^B\rangle,$$

где e_x^A — ортонормированный базис в $\mathcal{H}_A$, $\sum_x \|\psi_x^B\|^2 = 1$. Предположим, что участник A измеряет наблюдаемую $M_x^A = |e_x^A\rangle\langle e_x^A|$ и посылает исход x участнику B . Докажите, что тогда $p_x = \|\psi_x^B\|^2$ и апостериорные состояния участника B суть

$$S_B(x) = p_x^{-1} |\psi_x^B\rangle\langle\psi_x^B|. \quad (3.17)$$

Возвращаясь к эксперименту ЭПР, получаем из формулы (3.14), что если участник A измеряет наблюдаемую $\sigma(\mathbf{a})$ и посылает исход своего измерения ± 1 участнику B , то его апостериорным состоянием (т.е. состоянием соответствующего подансамбля) оказывается $|\mp \mathbf{a}\rangle\langle \mp \mathbf{a}|$. Если же связь между A и B отсутствует, то состояние участника B в результате измерения A не изменяется, оставаясь хаотическим. Таким образом, квантовая теория вполне согласуется с принципом локальности.

3.2.3. Сверхплотное кодирование

Хотя сцепленные состояния сами по себе не позволяют передавать информацию, оказывается, что наличие такого состояния позволяет увеличить максимальное количество классической информации, передаваемой от A к B , вдвое, если между системами имеется идеальный квантовый канал связи, позволяющий безошибочно передать любое квантовое состояние (например, посредством пересылки самого физического агента). Таким образом, сцепленное состояние выступает как «катализатор» при передаче классической информации через квантовый канал связи и с этой точки зрения также представляет собой особого рода информационный ресурс.

Для простоты рассмотрим системы A и B , каждая из которых представляет собой q -бит, причем между A и B имеется идеальный квантовый канал связи. Из обсуждения в предыдущем пункте вытекает, что максимальное количество классической информации, которое может быть передано от A к B , равно одному биту и получается при кодировании бита в два ортогональных вектора, например

$$0 \rightarrow |0\rangle, \quad 1 \rightarrow |1\rangle.$$

Протокол «сверхплотного кодирования», позволяющий удвоить количество передаваемой информации, имеет в своей основе простой математический факт: все векторы *базиса Белла*

$$\begin{aligned} |e_+\rangle &= |00\rangle + |11\rangle, & |e_-\rangle &= |00\rangle - |11\rangle, \\ |h_+\rangle &= |10\rangle + |01\rangle, & |h_-\rangle &= |10\rangle - |01\rangle \end{aligned}$$

в системе из двух q -битов AB (мы используем канонический базис $|0\rangle, |1\rangle$ в пространстве одного q -бита и опускаем нормировочный множитель $1/\sqrt{2}$) могут быть получены из любого из этих векторов действием «локальных» унитарных операторов, т.е. операторов, действующих нетривиально только в пространстве q -бита A (или B), например

$$|e_-\rangle = (\sigma_z \otimes I)|e_+\rangle, \quad |h_+\rangle = (\sigma_x \otimes I)|e_+\rangle, \quad |h_-\rangle = -i(\sigma_y \otimes I)|e_+\rangle.$$

Таким образом, если система AB изначально находится в сцепленном состоянии $|e_+\rangle$, то передатчик A может закодировать два бита классической информации в четыре состояния базиса Белла, производя только свои локальные операции, а затем переслать свой q -бит приемнику B по идеальному квантовому каналу. Тогда, производя измерение в базисе Белла, участник B получает 2 бита классической информации.

3.2.4. Телепортация квантовых состояний

До сих пор говорилось о передаче классической информации через квантовый канал связи. Такая информация может быть «записана» в квантовом состоянии и передана через физический канал. Однако квантовое состояние и само по себе представляет особого рода информационный ресурс, содержащий сведения о статистике всевозможных измерений над данной квантовой системой. Информация, содержащаяся в неизвестном квантовом состоянии, имеет качественные отличия от классической и поэтому заслуживает специальный термин *квантовая информация*. Наиболее ярким отличием квантовой информации является невозможность копирования произвольного состояния (*no cloning*). Устройства, воспроизводящие в принципе произвольное классическое сообщение, хорошо известны. Однако существование прибора, который выполнял бы аналогичную задачу для квантовой информации, противоречит основному динамическому принципу квантовой механики. В самом деле, преобразование

$$|\psi\rangle \rightarrow |\psi\rangle \otimes \underbrace{\dots \otimes |\psi\rangle}_n$$

является нелинейным и не может быть осуществлено унитарным оператором. Конечно, это можно сделать каждый раз специальным прибором для данного конкретного состояния (и даже для фиксированного набора ортогональных состояний), но не существует универсального прибора, который размножал бы произвольное квантовое состояние.

Кратко остановимся на вопросе, каким вообще образом может быть передано квантовое состояние. Очевидно, что это может быть пересылка самого физического агента, т.е. системы, приготовленной в том или ином состоянии. Одно из ярких достижений квантовой теории информации состоит в открытии принципиальной возможности способа, при котором сама система физически не пересылается, а передается лишь классическая информация. При этом существенным дополнительным ресурсом, который вновь играет роль «катализатора» передачи, является сцепленность между передатчиком и приемником. Заметим, что свести передачу произвольного квантового состояния только к передаче классической

информации, не используя дополнительного квантового ресурса, невозможно: поскольку классическая информация копируема, это означало бы возможность копирования и квантовой информации. Дадим описание этого способа, получившего название *телепортация* квантового состояния.

Пусть имеются два участника A и B , играющие роль передатчика и приемника соответственно. В простейшей версии системы A и B являются двухуровневыми (q-битами).

1. Перед началом передачи система AB готовится в состоянии $|00\rangle + |11\rangle$. (Напомним, что мы всюду опускаем нормировочный множитель $1/\sqrt{2}$.)

2. Третий участник C пересылает A произвольное чистое состояние

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

которое должно быть передано участнику B . На этом шаге совокупность трех систем CAB описывается состоянием

$$(a|0\rangle + b|1\rangle) \otimes (|00\rangle + |11\rangle).$$

3. Затем участник A производит некоторое обратимое преобразование состояния системы CA .

4. Участник A производит определенное измерение (с четырьмя исходами, что составляет 2 бита классической информации) и посылает результат измерения B по классическому каналу связи. Преобразование и измерение будут описаны ниже.

5. В зависимости от полученного результата измерения B производит некоторое преобразование и получает это произвольное состояние $|\psi\rangle$.

Производимые преобразования являются характерными примерами логических операций, используемых в квантовых вычислениях. На третьем шаге над системой CA производится операция CNOT (контролируемое «нет»):

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow |11\rangle, \quad |11\rangle \rightarrow |10\rangle,$$

при которой состояние первого q-бита сохраняется, а состояние второго q-бита не изменяется либо изменяется на противоположное в зависимости от состояния первого q-бита. При этом базис переходит в базис, следовательно, в четырехмерном пространстве CA этому преобразованию соответствует унитарный оператор. Затем к q-биту C применяется операция Адамара H с унитарной матрицей

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Тогда

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

т. е. базис поворачивается на угол $\pi/4$.

Начальное состояние всей системы CAB есть

$$a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle.$$

После действия CNOT на CA получаем

$$a|000\rangle + b|110\rangle + a|011\rangle + b|101\rangle.$$

Потом H действует на C :

$$a(|000\rangle + |100\rangle) + b(|010\rangle - |110\rangle) + a(|011\rangle + |111\rangle) + b(|001\rangle - |101\rangle).$$

Выделяя состояние системы CA , получаем

$$|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle).$$

Теперь производится измерение наблюдаемой в системе CA , соответствующей базису $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Согласно формуле (3.17) апостериорное состояние системы B в зависимости от полученного исхода измерения описывается одним из векторов

$$a|0\rangle + b|1\rangle, \quad a|1\rangle + b|0\rangle, \quad a|0\rangle - b|1\rangle, \quad a|1\rangle - b|0\rangle.$$

Исход измерения посылается от A к B по классическому (идеальному) каналу связи. В зависимости от полученного сообщения B применяет к своему состоянию один из унитарных операторов Паули $\sigma_0 = I, \sigma_x, \sigma_z, \sigma_y$, в каждом случае переводящих вектор состояния B в $a|0\rangle + b|1\rangle$. Таким образом, B переходит в состояние, в котором первоначально находилась система C , и при этом состояние системы C необратимо изменяется (иначе оказалось бы возможным копирование квантовой информации).

§ 3.3. Комментарии

1. Подробнее о тензорном произведении гильбертовых пространств говорится в гл. II.4 книги [24], где можно найти решение задач §3.1. Общую формулировку теоремы Наймарка см. в статье [23], где она доказана для произвольного разложения единицы (вероятностной операторнозначной меры, см. определение 10.7.2) в бесконечномерном гильбертовом пространстве.

Аналог разложения (3.8) в сепарабельном гильбертовом пространстве восходит к работе Шмидта 1907 г., посвященной интегральным уравнениям. Прием очищения смешанного состояния путем введения вспомогательной системы, широко применяемый в квантовой теории информации, использовался еще в работе Линдблада [125].

Термин «сцепленность» (Verschränktheit (нем.), entanglement (англ.)) был введен Шрёдингером, который первым обратил внимание на необычные свойства сцепленных состояний. В российской физической литературе используется термин «запутанность» или «перепутанность». Тщательный логический анализ эксперимента ЭПР проведен Беллом (см. [55]), который, в частности, установил первое из неравенств типа (3.15) и применил его к анализу парадокса ЭПР.

2. Протокол сверхплотного кодирования предложен Беннетом и Виснером; см. [62].

Протокол квантовой телепортации предложен в знаменитой публикации Беннета, Brassara, Крепо, Джоза, Переса и Вуттерса [56]. Возможность телепортации состояния поляризации фотона была продемонстрирована экспериментально Цайлингером в 1997 г.

ЧАСТЬ II

ГЛАВА 4

Классическая энтропия и информация

§ 4.1. Энтропия случайной величины и сжатие данных

Пусть X — дискретная случайная величина, принимающая значения в конечном множестве $\mathcal{X}$, и пусть $P = \{p_x; x \in \mathcal{X}\}$ — ее распределение вероятностей. *Энтропия* $H(X) = H(P)$ определяется соотношением

$$H(X) = \sum_{x \in \mathcal{X}} \eta(p_x), \quad (4.1)$$

где

$$\eta(t) = \begin{cases} -t \log t, & t > 0, \\ 0, & t = 0. \end{cases} \quad (4.2)$$

Энтропия $H(X)$, как мы увидим далее, является мерой неопределенности, изменчивости или информационного содержания случайной величины X . В дальнейшем, не ограничивая общности, можно предполагать, что $p_x > 0$ для всех x .

Пусть d — количество элементов в множестве $\mathcal{X}$. Имеют место неравенства

$$0 \leq H(P) \leq \log d, \quad (4.3)$$

причем минимальное значение принимается на вырожденных распределениях $\{1, 0, \dots, 0\}, \dots, \{0, \dots, 0, 1\}$, а максимальное — на равномерном распределении $\left\{\frac{1}{d}, \dots, \frac{1}{d}\right\}$. Первое неравенство вытекает из неотрицательности функции $\eta(t)$ на отрезке $[0, 1]$, а второе — из вогнутости функции $t \rightarrow \log t$:

$$H(P) = \sum_{x=1}^d p_x \log \frac{1}{p_x} \leq \log \sum_{x=1}^d p_x \frac{1}{p_x} = \log d.$$

Дадим операциональную интерпретацию энтропии $H(X)$ как меры информационного содержания случайной величины X . Рассмотрим «случайный источник», который порождает последовательность независимых одинаково распределенных случайных величин с распределением P . Последовательность $\omega = (x_1, \dots, x_n)$ букв алфавита $\mathcal{X}$ называется *словом* длины n . Общее количество таких слов равно $|\mathcal{X}|^n = 2^{n \log |\mathcal{X}|}$, поэтому

можно закодировать все эти слова, используя двоичные последовательности длины $n \log |\mathcal{X}|$, т. е. $n \log |\mathcal{X}|$ бит. Однако, используя то обстоятельство, что распределение P случайной величины X в общем случае не является равномерным, можно предложить намного лучший способ кодирования. Возможность сжатия данных тесно связана со следующим свойством *асимптотической равномерности*.

Теорема 4.1.1. Если $X_1, \dots, X_n, \dots$ — независимые одинаково распределенные случайные величины с распределением $P = \{p_x\}$, то

$$-\frac{1}{n} \sum_{i=1}^n \log p_{X_i} \rightarrow H(X) \quad \text{по вероятности.} \quad (4.4)$$

Последнее означает, что для любых $\delta, \varepsilon > 0$ найдется такое n_0 , что для всех $n \geq n_0$ имеет место неравенство

$$\mathbf{P} \left\{ \left| -\frac{1}{n} \sum_{i=1}^n \log p_{X_i} - H(X) \right| < \delta \right\} > 1 - \varepsilon. \quad (4.5)$$

Это прямо вытекает из закона больших чисел, примененного к последовательности независимых одинаково распределенных случайных величин $-\log p_{X_i}$, $i = 1, \dots, n$, математическое ожидание которых равно

$$\mathbf{E}(-\log p_{X_i}) = \sum_x p_x (-\log p_x) = H(X).$$

Замечая, что вероятность появления слова $\omega = (x_1, \dots, x_n)$ равна

$$p_\omega = p_{x_1} \cdot \dots \cdot p_{x_n} = 2^{-n \left(-\frac{1}{n} \sum_{i=1}^n \log p_{x_i} \right)}, \quad (4.6)$$

мы теперь можем использовать соотношение (4.5), чтобы ввести понятие *типичного слова*.

Определение 4.1.1. Слово ω , имеющее вероятность p_ω , называется δ -типичным, если

$$2^{-n(H(X)+\delta)} < p_\omega < 2^{-n(H(X)-\delta)}, \quad (4.7)$$

другими словами, для него выполняется событие в формуле (4.5).

Множество всех δ -типичных слов длины n будет обозначаться $T^{n,\delta}$. Из соотношений (4.5), (4.7) вытекают следующие свойства множества δ -типичных слов (где δ, ε — фиксированные положительные числа).

Задача 4.1.1. Докажите следующие утверждения.

1. Существует не более $2^{n(H(X)+\delta)}$ типичных слов.
2. Для достаточно больших n множество нетипичных слов имеет вероятность $\mathbf{P}(\overline{T^{n,\delta}}) \leq \varepsilon$.

3. Для достаточно больших n найдется по крайней мере $(1 - \varepsilon)2^{n(H(X) - \delta)}$ типичных слов.

Теперь можно осуществить эффективное *сжатие данных*, используя все двоичные последовательности длины $n(H(X) + \delta)$, чтобы закодировать все δ -типичные слова, и отбрасывая нетипичные слова (или кодируя их одним и тем же добавочным символом). Вероятность ошибки при таком кодировании будет не больше ε .

Обратно, любой код, использующий двоичные последовательности длины $n(H(X) - \delta)$, имеет асимптотически исчезающую вероятность ошибки, стремящуюся к единице при $n \rightarrow \infty$. В самом деле, пусть C — совокупность слов, которые были использованы для кодирования в $n(H(X) - \delta)$ двоичных последовательностей, тогда как все остальные слова кодируются какой-то другой последовательностью. Тогда вероятность ошибки равна $1 - P(C)$, где

$$P(C) = P(C \cap T^{n, \delta/2}) + P(C \cap \overline{T^{n, \delta/2}}) \leq \quad (4.8)$$

$$\leq |C|2^{-n(H(X) - \delta/2)} + P(\overline{T^{n, \delta/2}}) \leq \quad (4.9)$$

$$\leq 2^{-n\delta/2} + \varepsilon, \quad (4.10)$$

что может быть сделано сколь угодно малым для достаточно больших n .

Поскольку эффективное кодирование требует асимптотически $N \sim 2^{nH(X)}$ слов, энтропия $H(X)$ может быть интерпретирована как мера количества информации (в битах на передаваемый символ) в случайном источнике. Ясно, что для равномерного распределения $p_x = 1/|\mathcal{X}|$ энтропия $H(X)$ равна $\max_x H(X) = \log |\mathcal{X}|$ и сжатие невозможно.

Задача 4.1.2. Пусть $\mathcal{X}$ — конечное подмножество $\mathbb{R}$. Докажите, что в условиях теоремы 4.1.1 имеет место следующее неравенство для вероятностей больших отклонений:

$$P\left\{\frac{1}{n} \sum_{i=1}^n (X_i - EX) \geq \delta\right\} \leq \exp\left\{-n \sup_{s > 0} [s\delta - \mu(s)]\right\}, \quad (4.11)$$

где

$$\mu(s) = \ln Ee^{s(X - EX)} = o(s) \quad \text{при } s \rightarrow 0.$$

Отсюда, в частности, вытекает закон больших чисел с экспоненциальной скоростью убывания «хвостов» распределения, поскольку $s\delta - \mu(s) > 0$ для малых $s > 0$. *Указание.* Докажите и используйте следующую версию неравенства Маркова:

$$P\{X \geq x\} \leq \exp(-sx) Ee^{sX}$$

для любых $x \in \mathbb{R}$ и $s > 0$.

§ 4.2. Условная энтропия, относительная энтропия и информация Шеннона

Если X, Y — случайные величины на одном вероятностном пространстве, имеющие совместное распределение $\{p_{x,y}\}$, то можно определить их *совместную энтропию* $H(X, Y)$ аналогично соотношению (4.1). *Условная энтропия* $H(Y|X)$ определяется как

$$\begin{aligned} H(Y|X) &= \sum_x p_x H(Y|X = x) = - \sum_x p_x \sum_y p(y|x) \log p(y|x) = \\ &= - \sum_{x,y} p_{x,y} \log p_{x,y} + \sum_x p_x \log p_x = H(X, Y) - H(X). \end{aligned} \quad (4.12)$$

Существует полезное общее правило, гласящее, что всякое линейное соотношение для (условных) энтропий продолжает оставаться верным, если в каждый член подставляется одно и то же дополнительное условие, например, из соотношения (4.12) следует, что

$$H(X, Y|Z) = H(X|Z) + H(Y|X, Z). \quad (4.13)$$

Канал связи с шумом описывается вероятностями переходов $p(y|x)$ из входного алфавита $\mathcal{X}$ в выходной алфавит $\mathcal{Y}$, т.е. условными вероятностями того, что принят символ $y \in \mathcal{Y}$, при условии, что был послан символ $x \in \mathcal{X}$. Входное распределение вероятностей $P = \{p_x\}$ трансформируется каналом в совместное распределение $p_{x,y} = p(y|x)p_x$ и порождает выходное распределение $P' = \{p'_y\}$, где $p'_y = \sum_x p(y|x)p_x$. *Шенноновское количество информации* (о случайной величине X , содержащееся в Y) определяется соотношением

$$I(X; Y) = H(Y) - H(Y|X), \quad (4.14)$$

где энтропия $H(Y)$ может быть интерпретирована как информационное содержание выхода, а условная энтропия $H(Y|X)$ — как его бесполезная составляющая, обусловленная *шумом* в канале связи. Подставляя энтропию (4.12) в это выражение для шенноновской информации, мы видим, что оно симметрично по X и Y и поэтому может быть также названо *взаимной информацией*:

$$I(X; Y) = H(X) + H(Y) - H(X, Y). \quad (4.15)$$

Также $I(X; Y) = H(X) - H(X|Y)$, где теперь $H(X)$ может быть интерпретировано как информационное содержание источника, а $H(X|Y)$ — как *потеря* информации в канале связи с шумом. Явное выражение для

шенноновской информации через входное распределение и переходные вероятности канала имеет вид

$$I(X, Y) = \sum_{xy} p_x p(y|x) \log \left(\frac{p(y|x)}{\sum_{x'} p(y|x') p_{x'}} \right). \quad (4.16)$$

В классической статистике весьма полезной характеристикой является относительная энтропия двух распределений $P = \{p_x\}$, $Q = \{q_x\}$ (информационное количество Кульбака—Лейблера—Санова):

$$H(P; Q) = \begin{cases} \sum_{x: p_x > 0} p_x \log \frac{p_x}{q_x}, & \text{если } \{x: p_x > 0\} \subseteq \{x: q_x > 0\}, \\ +\infty & \text{в противном случае.} \end{cases}$$

Используя неравенство $\ln t \leq t - 1$, получаем

$$H(P; Q) \geq -\log e \cdot \sum_{x: p_x > 0} p_x \left(\frac{q_x}{p_x} - 1 \right) \geq 0, \quad (4.17)$$

причем равенство имеет место тогда и только тогда, когда $P = Q$.

Величина $H(P; Q)$ играет важную роль как «асимметричное расстояние» между распределениями вероятностей. Она обладает следующим свойством монотонности. Рассмотрим канал $r(y|x)$ и два распределения $P = \{p_x\}$, $Q = \{q_x\}$ на входе, которые трансформируются в выходные распределения $P' = \{p'_y\}$, $Q' = \{q'_y\}$,

$$p'_y = \sum_x r(y|x) p_x, \quad q'_y = \sum_x r(y|x) q_x.$$

Тогда

$$H(P'; Q') \leq H(P; Q).$$

В самом деле,

$$\begin{aligned} H(P; Q) &= \sum_{xy} p_x r(y|x) \log \frac{r(y|x) p_x}{r(y|x) q_x} = \sum_{xy} p_{x,y} \left(\log \frac{p'_y}{q'_y} + \log \frac{p(x|y)}{q(x|y)} \right) = \\ &= H(P'; Q') + \sum_y p'_y H(p(x|y); q(x|y)) \geq H(P'; Q'). \end{aligned}$$

Задача 4.2.1. Докажите, что $I(X; Y) = H(p_{x,y}; p_x \cdot p_y)$. Поэтому в силу соотношения (4.17) из этого следует, что $I(X; Y) \geq 0$, причем $I(X; Y) = 0$ тогда и только тогда, когда X и Y — независимые случайные величины: $p_{x,y} = p_x \cdot p_y$.

Отсюда непосредственно вытекает монотонность условной энтропии:

$$0 \leq H(Y|X) \leq H(Y),$$

а также субаддитивность энтропии:

$$H(X, Y) \leq H(X) + H(Y). \quad (4.18)$$

Отметим также выражение для информации в терминах относительной энтропии:

$$I(X, Y) = \sum_x p_x H(P'_x; P'), \quad (4.19)$$

где мы ввели обозначения $P'_x = \{p(y|x)\}$ для каждого фиксированного $x \in \mathcal{X}$, а $P' = \sum_x p_x P'_x$ есть безусловное распределение величины Y .

§ 4.3. Шенноновская пропускная способность канала с шумом

Рассмотрим канал $X \rightarrow Y$, определяемый переходной вероятностью $p(y|x)$. Важнейшей характеристикой канала является *шенноновская пропускная способность*

$$C_{\text{Shan}} = \max_X I(X; Y), \quad (4.20)$$

где максимум берется по всевозможным распределениям $P = \{p_x\}$ на входе X . Далее будет показано, что она совпадает с операционально определенной информационной пропускной способностью канала.

В качестве примера вычисления C_{Shan} рассмотрим *двоичный симметричный канал* (см. рис. 4.1). В этом случае алфавиты $\mathcal{X}$ и $\mathcal{Y}$ состоят

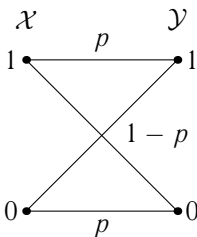


Рис. 4.1. Двоичный симметричный канал

из двух букв 0, 1 которые передаются без ошибки с вероятностью $1 - p$ и изменяются на другую с вероятностью p . Вводя *двоичную энтропию*

$$h_2(p) = -p \log p - (1 - p) \log(1 - p), \quad (4.21)$$

взаимную информацию можно записать как $I(X; Y) = H(Y) - H(Y|X) = H(Y) - h_2(p)$, что ограничено сверху величиной

$$C_{\text{Shan}} = \log 2 - h_2(p) = 1 - h_2(p), \quad (4.22)$$

достигающейся для равномерного распределения: $p_0 = p_1 = \frac{1}{2}$.

В общем случае $I(X; Y)$ является вогнутой функцией входного распределения вероятностей $P = \{p_x\}$. Поэтому для нахождения оптимального входного распределения P , максимизирующего $I(X; Y)$, могут быть применены условия Куна—Таккера из выпуклого анализа.

Задача 4.3.1. Докажите, что энтропия $H(P)$ является вогнутой функцией распределения P . *Указание.* Используя вогнутость функции $t \rightarrow \eta(t)$, убедитесь, что выходная энтропия $H(Y) = H(P')$ также вогнута, тогда как условная энтропия $H(Y|X)$ аффинна. Таким образом, из представления (4.14) следует вогнутость функции $I(X; Y)$.

Задача 4.3.2 (условия Куна—Таккера). Пусть $F(P)$ — вогнутая функция распределения вероятностей P , непрерывно дифференцируемая внутри симплекса распределений на $\mathcal{X}$, так что частные производные имеют пределы, возможно бесконечные, на границе симплекса. Докажите, что для того чтобы распределение P^0 было точкой абсолютного максимума для $F(P)$, необходимо и достаточно, чтобы нашлось такое λ , что

$$\frac{\partial F(P^0)}{\partial p_x} \begin{cases} = \lambda, & \text{если } p_x^0 > 0, \\ \leq \lambda, & \text{если } p_x^0 = 0. \end{cases}$$

В случае шенноновской информации (4.16) имеем

$$\frac{\partial F(P)}{\partial p_x} = H(P_x; P') - \log e,$$

что в сочетании с соотношением (4.19) приводит к следующему условию «максимального расстояния» для оптимального входного распределения:

$$H(P_x^0; (P^0)') \begin{cases} = \mu, & \text{если } p_x^0 > 0, \\ \leq \mu, & \text{если } p_x^0 = 0, \end{cases} \quad (4.23)$$

причем с необходимостью $\mu = C_{\text{Shan}}$.

Предположим, что имеются два канала $\{p_j(y_j|x_j)\}$, $j = 1, 2$, и рассмотрим составной канал, описываемый переходной вероятностью $\{p_1(y_1|x_1)p_2(y_2|x_2)\}$.

Предложение 4.3.1. Шенноновская пропускная способность составного канала равна

$$(C_{\text{Shan}})_{12} = (C_{\text{Shan}})_1 + (C_{\text{Shan}})_2. \quad (4.24)$$

Таким образом, шенноновская пропускная способность аддитивна для независимых каналов.

Доказательство. Пусть P^j — оптимальное входное распределение для j -го канала, тогда оно удовлетворяет условию (4.23) с константами $\mu_j = (C_{\text{Shan}})_j$. Используя тот факт, что

$$H(P^1 \times P^2; Q^1 \times Q^2) = H(P^1; Q^1) + H(P^2; Q^2),$$

получаем, что распределение $P = P^1 \times P^2$ удовлетворяет условию (4.23) для составного канала с константой $\mu = (C_{\text{Shan}})_1 + (C_{\text{Shan}})_2$. $\square$

§ 4.4. Теорема кодирования для канала с шумом

Для данного канала $p(y|x)$ можно рассмотреть составной канал *без памяти*

$$p(y^n|x^n) = p(y_1|x_1) \cdot \dots \cdot p(y_n|x_n), \quad (4.25)$$

который побуквенно передает слова длины n , используя независимо n раз исходный канал:

$$x^n \left\{ \begin{array}{ccc} x_1 & \rightarrow & y_1 \\ x_2 & \rightarrow & y_2 \\ \vdots & & \vdots \\ x_n & \rightarrow & y_n \end{array} \right\} y^n.$$

Обозначим через X^n , Y^n случайные величины на входе и выходе составного канала.

Аналогично определению (4.20) рассмотрим величину

$$C_n = \max_{X^n} I(X^n; Y^n)$$

для составного канала. Используя свойство (4.24), получаем, что последовательность $\{C_n\}$ аддитивна для канала без памяти, откуда следует, что

$$C_n = nC_{\text{Shan}}. \quad (4.26)$$

Чтобы уменьшить влияние шума, используется кодирование сообщений на входе и, соответственно, декодирование на выходе составного канала. Процесс передачи информации тогда изображается следующей диаграммой:

$$i \xrightarrow{\text{кодирование}} x^n \xrightarrow{\text{канал}} y^n \xrightarrow{\text{декодирование}} j, \quad (4.27)$$

где i (соответственно j) обозначает переданное (принятое) сообщение. Можно просто считать $i, j \in \{1, \dots, N\}$ номерами соответствующих сообщений, так как интерес представляет количество N передаваемых сообщений.

Цель состоит в том, чтобы выбрать кодирование и декодирование, которые максимизировали бы *скорость передачи* $R = \frac{\log N}{n}$, равную числу бит на один передаваемый символ, при условии малости вероятности ошибки. Дадим точные определения.

Определение 4.4.1. Код (W, V) размера N для составного канала $p(y^n|x^n)$ состоит из кодирования, задаваемого совокупностью кодовых слов $W = \{\omega^{(1)}, \dots, \omega^{(N)}\}$ длины n , и декодирования, задаваемого совокупностью $V = \{V^{(0)}, V^{(1)}, \dots, V^{(N)}\}$ непересекающихся подмножеств $\mathcal{Y}^n$. Подмножества $V^{(1)}, \dots, V^{(N)}$ интерпретируются как области принятия решения: если сообщение на выходе y^n принадлежит $V^{(j)}$, $j = 1, \dots, N$, то принимается решение, что было послано слово $\omega^{(j)}$; если же $y^n \in V^{(0)} = \bigcup_{j=1}^N V^{(j)}$, то никакого определенного решения не принимается.

Таким образом, *максимальная вероятность ошибки* такого кода есть

$$P_e(W, V) = \max_{1 \leq j \leq N} (1 - p(V^{(j)}|\omega^{(j)})), \quad (4.28)$$

где $p(V^{(j)}|\omega^{(j)}) = P(Y^n \in V^{(j)}|X^n = \omega^{(j)})$ — вероятность правильного решения. *Средняя вероятность ошибки* равна

$$\bar{P}_e(W, V) = \frac{1}{N} \sum_{j=1}^N (1 - p(V^{(j)}|\omega^{(j)})) \leq P_e(W, V), \quad (4.29)$$

и, как показывает следующая лемма, с точки зрения теории информации она асимптотически эквивалентна максимальной вероятности ошибки $P_e(W, V)$.

Лемма 4.4.1. Для любого кода (W, V) размера $2N$ найдется подкод $(\tilde{W}, \tilde{V})$ размера N , который имеет максимальную вероятность ошибки $P_e(\tilde{W}, \tilde{V}) \leq 2\bar{P}_e(W, V)$.

Доказательство. Обозначим $\varepsilon = \bar{P}_e(W, V)$ и предположим, что N -подкода с требуемым свойством не существует. Тогда найдутся по крайней мере $N + 1$ кодовых слов с вероятностью ошибки больше 2ε

и средняя вероятность ошибки $2N$ -кода ограничена снизу величиной

$$\bar{P}_e(W, V) > \frac{1}{2N} 2\varepsilon(N+1) > \varepsilon,$$

что противоречит предположению. $\square$

Обозначим через $p_e(n, N)$ (соответственно $\bar{p}_e(n, N)$) максимальную (соответственно среднюю) вероятность ошибки, минимизированную по всевозможным кодам длины n и размера N . Тогда

$$\frac{1}{2} p_e(n, N) \leq \bar{p}_e(n, 2N) \leq p_e(n, 2N). \quad (4.30)$$

Определение 4.4.2. Число $R \geq 0$ называется *достижимой скоростью передачи*, если

$$\lim_{n \rightarrow \infty} p_e(n, 2^{nR}) = 0.$$

Точная верхняя грань всех достижимых скоростей передачи называется *информационной пропускной способностью* C канала $p(y|x)$.

Теорема 4.4.1 (теорема кодирования для канала с шумом). *Для канала без памяти выполняется соотношение*

$$C = C_{\text{Shan}}.$$

Таким образом, операционально (и асимптотически) определенная информационная пропускная способность оказывается равной удобно вычислимой «однобуквенной» характеристике канала, определенной соотношением (4.20). Неравенство $C \leq C_{\text{Shan}}$ будет следовать из утверждения

$$\lim_{n \rightarrow \infty} p_e(n, 2^{nR}) = 0, \quad \text{если } R < C_{\text{Shan}},$$

называемого *прямой теоремой кодирования*, тогда как *слабое обращение* состоит в том, что

$$\liminf_{n \rightarrow \infty} p_e(n, 2^{nR}) > 0, \quad \text{если } R > C_{\text{Shan}}, \quad (4.31)$$

откуда следует, что $C \geq C_{\text{Shan}}$. На самом деле имеет место более сильное утверждение

$$\lim_{n \rightarrow \infty} p_e(n, 2^{nR}) = 1, \quad \text{если } R > C_{\text{Shan}}.$$

Доказательство. *Слабое обращение.* Благодаря неравенству (4.30) достаточно доказать аналог утверждения (4.31) для вероятности ошибки $\bar{p}_e(n, N)$.

Лемма 4.4.2 (неравенство Фано). Пусть X, Y — случайные величины и $\hat{X} = \hat{X}(Y)$ — оценка случайной величины X по наблюдениям Y с вероятностью ошибки $p_e = P(\hat{X}(Y) \neq X)$, тогда

$$H(X|Y) \leq h_2(p_e) + p_e \log(|\mathcal{X}| - 1) \leq 1 + p_e \log |\mathcal{X}|. \quad (4.32)$$

Доказательство. Пусть E — индикатор ошибки оценивания,

$$E = \begin{cases} 0, & \text{если } \hat{X}(Y) = X, \\ 1 & \text{в противном случае.} \end{cases} \quad (4.33)$$

Поскольку E является функцией от $(X, \hat{X})$ и поэтому имеет определенное значение при фиксированных значениях $X, \hat{X}$, имеем $H(X|Y) = H(E, X|Y)$. Однако из соотношения (4.13) следует, что

$$H(E, X|Y) = H(E|Y) + H(X|E, Y). \quad (4.34)$$

Здесь $H(E|Y) \leq H(E) = h_2(p_e)$ и

$$H(X|E, Y) = (1 - p_e)H(X|E = 0, Y) + p_e H(X|E = 1, Y) \leq p_e \log(|\mathcal{X}| - 1),$$

где был использован тот факт, что $H(X|E = 0, Y)$ также равно нулю, поскольку равенство $E = 0$ означает, что мы знаем X , если известно Y . Условие $E = 1$ равносильно тому, что $X \neq \hat{X}(Y)$, и оставляет возможными не более $|\mathcal{X}| - 1$ значений X , так что энтропия ограничена сверху величиной $\log(|\mathcal{X}| - 1)$. $\square$

Рассмотрим произвольный код (W, V) размера N со словами $w^{(1)}, \dots, w^{(N)}$ и разбиение множества $\mathcal{Y}^n$ на $N + 1$ область принятия решения $V^{(0)}, V^{(1)}, \dots, V^{(N)} \subset \mathcal{Y}^n$. Обозначим через X^n случайную величину, принимающую значения $w^{(1)}, \dots, w^{(N)}$ с равными вероятностями $\frac{1}{N}$, и пусть $\hat{X}^n = \hat{X}(Y^n)$ — такая оценка для X^n , что $\hat{X}^n = w^{(j)}$, если $Y^n \in V^{(j)}$. Тогда

$$\begin{aligned} C_n &\geq I(X^n; Y^n) = H(X^n) - H(X^n|Y^n) \geq \\ &\geq \log N \left(1 - \underbrace{\mathbf{P}\{\hat{X}^n \neq X^n\}}_{=\bar{P}_e(W, V)} \right) - 1 \end{aligned} \quad (4.35)$$

согласно неравенству Фано. Подставляя $N = 2^{nR}$, получаем

$$\bar{P}_e(W, V) \geq 1 - \frac{C_n}{nR} - \frac{1}{nR}. \quad (4.36)$$

Взяв минимум по всевозможным кодам и используя аддитивность (4.26), в пределе при $n \rightarrow \infty$ получаем

$$\liminf_{n \rightarrow \infty} \bar{p}_e(n, 2^{nR}) \geq 1 - \frac{C_{\text{Shan}}}{R} > 0$$

для $R > C_{\text{Shan}}$.

Доказательство прямого утверждения. Основная идея, принадлежащая Шеннону, состоит в использовании *случайного кодирования*.

Рассмотрим N слов $w^{(1)}, \dots, w^{(N)}$, выбираемых случайным образом независимо с распределением вероятностей

$$P\{w^{(i)} = (x_1, \dots, x_n)\} = p_{x_1} \cdot \dots \cdot p_{x_n}, \quad (4.37)$$

где однобуквенное распределение $\{p_x\}$ выбрано так, что оно максимизирует $I(X; Y)$. Заметим, что имеется примерно $2^{nH(Y)}$ типичных слов на выходе и в среднем $2^{nH(Y|X)}$ типичных слов на выходе для каждого входного слова w . Для того чтобы ошибка различения слов на выходе стремилась к нулю, надо, чтобы множества типичных слов на выходе, соответствующие разным словам на входе, асимптотически не пересекались, поэтому размер кода должен удовлетворять оценке

$$N \approx \frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{n(H(Y) - H(Y|X))} = 2^{nI(X; Y)} = 2^{nC_{\text{Shan}}}. \quad (4.38)$$

Чтобы придать этому рассуждению точный смысл, назовем выходное слово y^n *условно типичным* для входного слова $w = x^n$, если

$$2^{-n(H(Y|X) + \delta)} < p(y^n | w) < 2^{-n(H(Y|X) - \delta)}. \quad (4.39)$$

Обозначим через $T_w^{n, \delta} \subset \mathcal{Y}^n$ подмножество всех условно типичных слов для данного входного слова w .

Задача 4.4.1. Предполагая, что w распределено случайно с распределением (4.37), покажите, используя закон больших чисел, что $P\{Y^n \in \overline{T_w^{n, \delta}}\} \leq \varepsilon$ для любого $\varepsilon > 0$ и достаточно больших n .

Для данного кодирования $W = \{w^{(1)}, \dots, w^{(N)}\}$ построим специальное субоптимальное декодирование. Множества $T_{w^{(j)}}^{n, \delta}$ могут пересекаться для разных j , и, чтобы получить непересекающиеся области принятия решений, мы положим

$$V^{(j)} = T_{w^{(j)}}^{n, \delta} \cap \overline{\left(\bigcup_{k: k \neq j} T_{w^{(k)}}^{n, \delta} \right)}. \quad (4.40)$$

Если, например, было передано слово $w^{(1)}$, то ошибка возникает тогда и только тогда, когда

$$y^n \in \overline{V^{(1)}} = \overline{T_{w^{(1)}}^{n, \delta}} \cup \left(\bigcup_{k=2}^N T_{w^{(k)}}^{n, \delta} \right). \quad (4.41)$$

Теперь предположим, что кодовые слова $w^{(1)}, \dots, w^{(N)}$ выбираются случайным образом, как описано выше, т. е. независимо с распределением (4.37), и оценим математическое ожидание средней вероятности ошибки $P_e(W, V)$. Это даст нам требуемую оценку, поскольку очевидно, что

$$\bar{p}_e(n, N) \leq E P_e(W, V).$$

Обозначим через $P_w\{B\}$ вероятность $P\{Y^n \in B | X^n = w\}$, где B — некоторое, возможно случайное, подмножество в $\mathcal{Y}^n$. В силу полной симметрии между кодовыми словами имеем

$$\begin{aligned} E\bar{P}_e(W, V) &= E P_{w^{(1)}}\{\overline{V^{(1)}}\} = \\ &= E P_{w^{(1)}}\{\overline{V^{(1)}} \cap T^{n, \delta}(Y)\} + E P_{w^{(1)}}\{\overline{V^{(1)}} \cap \overline{T^{n, \delta}(Y)}\}, \end{aligned} \quad (4.42)$$

где $T^{n, \delta}(Y)$ есть множество выходных δ -типичных последовательностей y^n , определяемое аналогично определению 4.1.1 с заменой $H(X)$ на $H(Y)$. Тогда, учитывая соотношение (4.41), получаем

$$\begin{aligned} E\bar{P}_e(W, V) &\leq P\{Y^n \in \overline{T^{n, \delta}}\} + \\ &+ \sum_{k=2}^N E P_{w^{(1)}}\{T_{w^{(k)}}^{n, \delta} \cap T^{n, \delta}(Y)\} + P\{\overline{T^{n, \delta}(Y)}\}. \end{aligned} \quad (4.43)$$

Первый и третий члены не превосходят ε для достаточно больших n в силу соответствующих свойств (условно) нетипичных слов. Каждое слагаемое в средней сумме оценивается как

$$\begin{aligned} \sum_{w^{(1)}} \sum_{w^{(k)}} \sum_{y^n \in T_{w^{(k)}}^{n, \delta} \cap T^{n, \delta}(Y)} p(y^n | w^{(1)}) p_{w^{(1)}} p_{w^{(k)}} &\leq \\ &\leq 2^{n(H(Y|X) + \delta)} \sum_{w^{(1)}} \sum_{w^{(k)}} \sum_{y^n \in T^{n, \delta}(Y)} p(y^n | w^{(1)}) p_{w^{(1)}} p(y^n | w^{(k)}) p_{w^{(k)}} = \\ &= 2^{n(H(Y|X) + \delta)} \sum_{y^n \in T^{n, \delta}(Y)} (p_{y^n})^2 \leq 2^{n(H(Y|X) - H(Y) + 2\delta)}. \end{aligned}$$

Здесь первое неравенство получается введением множителя

$$2^{n(H(Y|X) + \delta)} p(y^n | w^{(k)}) > 1$$

на множестве $T_{w^{(k)}}^{n, \delta}$, а последнее — из второго неравенства в определении типичного слова y^n . Окончательно получаем

$$E\bar{P}_e(W, V) \leq 2\varepsilon + (N - 1)2^{n(H(Y|X) - H(Y) + 2\delta)} \leq 2\varepsilon + N2^{-n(C_{\text{Shan}} - 2\delta)},$$

а эта величина может быть сделана меньше 3ε , если $N = 2^{nR}$, где $R < C_{\text{Shan}}$ и δ достаточно мало. $\square$

Следует отметить, что метод случайного кодирования, позволивший доказать существование асимптотически оптимальных кодов, а также раскрывающий природу таких кодов, мало пригоден для практического применения. Его реализация уже при достаточно умеренных значениях n

требует огромного (экспоненциально растущего) объема вычислений. Нахождению практически приемлемых методов кодирования/декодирования посвящен специальный раздел теории информации — теория кодирования, широко использующая методы современной алгебры.

§ 4.5. Канал с перехватом

Другой важнейшей проблемой современной теории информации является изучение систем с многими пользователями, ярким примером которой может служить интернет. Специфическим примером системы с недружественными участниками является канал с перехватом, на котором мы здесь кратко остановимся, поскольку это понадобится в гл. 9, посвященной передаче квантовой информации.

Пусть $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ — три конечных алфавита, причем алфавит $\mathcal{X}$ ассоциируется с передатчиком, $\mathcal{Y}$ — с приемником, а $\mathcal{Z}$ — с перехватчиком данных. *Каналом с перехватом* называется пара каналов $p(y|x)$, $q(z|x)$ от передатчика к приемнику и к перехватчику соответственно. Передатчик посылает слова $w = (x_1, \dots, x_n)$ длины n по составным каналам $p(y^n|x^n)$, $q(y^n|x^n)$, и цель состоит в асимптотически безошибочной передаче максимального количества сообщений приемнику при условии, что перехватчик получит асимптотически исчезающее количество информации.

Определение 4.5.1. Код $(\mathcal{M}, r, V)$ размера N для составного канала с перехватом состоит из множества сообщений $\mathcal{M} = \{1, \dots, N\}$, переходной вероятности $r(x^n|m)$ из $\mathcal{M}$ в $\mathcal{X}^n$, задающей рандомизованное кодирование сообщений $m \in \mathcal{M}$ в слова x^n , и обычного декодирования V для приемника, задаваемого разбиением множества $\mathcal{Y}^n$ на N непересекающихся подмножеств $V^{(0)}, V^{(1)}, \dots, V^{(N)} \subset \mathcal{Y}^n$.

Максимальная вероятность ошибки такого кода равна

$$P_e(\mathcal{M}, r, V) = \max_{1 \leq m \leq N} (1 - p(V^{(m)}|m)), \quad (4.44)$$

где $p(V^{(m)}|m) = \sum_{x^n} P(Y^n \in V^{(m)}|x^n)r(x^n|m)$ — вероятность правильного решения для приемника. Мы будем называть R *достижимой скоростью* для канала с перехватом, если найдется последовательность кодов $(\mathcal{M}^{(n)}, r^{(n)}, V^{(n)})$ размера $N = 2^{nR}$ таких, что

$$\lim_{n \rightarrow \infty} P_e(\mathcal{M}^{(n)}, r^{(n)}, V^{(n)}) = 0$$

и

$$\lim_{n \rightarrow \infty} I(M^n; Z^n) = 0,$$

где M^n — случайная величина, равномерно распределенная на множестве сообщений $\mathcal{M}^{(n)}$. Последнее условие выражает требование, что количество информации перехватчика о посланном сообщении должно стремиться к нулю. Точная верхняя грань множества достижимых скоростей называется *секретной пропускной способностью* C_p канала с перехватом.

Теорема кодирования для канала с перехватом дает следующее выражение:

$$C_p = \max[I(M; Y) - I(M; Z)], \quad (4.45)$$

где максимум берется по всевозможным случайным величинам M, Y, Z таким, что последовательность $M, X, (Y, Z)$ образует цепь Маркова, причем пары X, Y и X, Z связаны каналами $p(y|x)$ и $q(z|x)$ соответственно.

Задача 4.5.1. Докажите слабое обращение теоремы кодирования (неравенство $\leq$ в формуле (4.45)), используя неравенство Фано.

Доказательство прямого утверждения основано на следующей идее. Фиксируем $\delta, \varepsilon > 0$ и некоторое распределение на алфавите $\mathcal{X}$. Рассмотрим новое случайное кодирование $W^{(n)}$ с N независимыми словами, равномерно распределенными на множестве $T^{n, \delta}$ всех δ -типичных слов длины n , а также субоптимальное декодирование $V^{(n)}$, построенное в соответствии с формулой (4.40). Небольшая модификация доказательства теоремы 4.4.1 позволяет доказать, что при $N = 2^{n[I(X; Y) - \delta]}$ с высокой вероятностью выполняется неравенство

$$\bar{P}_e(W^{(n)}, V^{(n)}) \leq \varepsilon. \quad (4.46)$$

Чтобы сделать код секретным, передатчик должен пожертвовать $n[I(X; Z) + \delta/2]$ битами информации, дополнительно рандомизуя входные сообщения. Положим

$$N_Z = 2^{n[I(X; Z) + \delta/2]}, \quad N_Y = 2^{n[I(X; Y) - I(X; Z) - 3\delta/2]},$$

так что $N_Z N_Y = N$; представим набор кодовых слов $W^{(n)}$ в виде прямоугольной таблицы с N_Y строками и N_Z столбцами. Тогда

$$W^{(n)} = \{w^{mj}; m = 1, \dots, N_Y; j = 1, \dots, N_Z\}.$$

Пусть теперь для каждого значения m передатчик выбирает значение j случайным образом с равными вероятностями. Такая рандомизация приводит к тому, что почти вся переданная информация оказывается скрытой для перехватчика: для каждого значения m набор кодовых слов

$$\{w^{mj}; j = 1, \dots, N_Z\}$$

с высокой вероятностью содержит почти максимально возможную информацию $I(X; Z)$ при условии, что перехватчик применяет оптимальное

декодирование. Поэтому взаимная информация между наборами кодовых слов с различными значениями m должна быть близка к нулю, так что рандомизация внутри каждого набора уничтожает почти всю информацию, передаваемую перехватчику. Эти рассуждения вкупе с неравенством (4.46) показывают, что скорость $I(X; Y) - I(X; Z) - \delta$ является достижимой. Они остаются справедливыми и для любой последовательности M, X, YZ , удовлетворяющей условиям теоремы кодирования, поэтому $I(M; Y) - I(M; Z) - \delta$ также является достижимой скоростью.

§ 4.6. Гауссовский канал

Рассмотрим непрерывный аналог канала без памяти (4.25), у которого в качестве входного и выходного алфавитов выступает вещественная прямая $\mathbb{R}$. Канал задается переходной плотностью вероятности

$$p(y_i|x_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(y_i - x_i)^2}{2\sigma^2}\right], \quad i = 1, \dots, n.$$

Эквивалентно, можно считать, что выходные случайные величины Y_i получаются сложением входного сигнала x_i с независимыми одинаково распределенными переменными шума Z_i , $\mathbb{E}Z_i = 0$ и $\mathbb{E}Z_i^2 = \sigma^2$:

$$Y_i = x_i + Z_i, \quad i = 1, \dots, n.$$

Легко видеть, что естественно определенная информационная пропускная способность такого канала бесконечна, если не ввести каких-либо ограничений на сигнал. Обычно рассматривается квадратичное ограничение

$$\sum_{i=1}^n x_i^2 \leq ns^2, \quad (4.47)$$

мотивированное конечностью мощности входного сигнала. При этом ограничении пропускная способность оказывается равной

$$C = \frac{1}{2} \log\left(1 + \frac{s^2}{\sigma^2}\right). \quad (4.48)$$

Эта формула также принадлежит Шеннону и также имеет простое эвристическое истолкование. Неравенства

$$\frac{1}{n} \sum_{i=1}^n Z_i^2 \leq \sigma^2 + \varepsilon, \quad \frac{1}{n} \sum_{i=1}^n Y_i^2 \leq s^2 + \sigma^2 + \varepsilon$$

имеют место с высокой вероятностью для произвольного $\varepsilon > 0$ и достаточно больших n .

Задача 4.6.1. Докажите это утверждение, используя неравенство Чебышёва и неравенство (4.47).

Первое из этих неравенств означает, что для любого входного слова $\omega = (x_1, \dots, x_n)$ выходной вектор $Y^n = (Y_1, \dots, Y_n)$ лежит в n -мерном шаре радиуса $\sqrt{n(\sigma^2 + \varepsilon)}$ с центром ω , тогда как второе — что выходные векторы для всевозможных входов, удовлетворяющих ограничению (4.47), лежат в n -мерном шаре радиуса $\sqrt{n(s^2 + \sigma^2 + \varepsilon)}$. Отношение объемов этих шаров дает приблизительную оценку числа непересекающихся шаров первого типа в большом шаре:

$$N = \left[\frac{\sqrt{n(s^2 + \sigma^2 + \varepsilon)}}{\sqrt{n(\sigma^2 + \varepsilon)}} \right]^n = 2^{nR},$$

где $R = \frac{1}{2} \log \left(1 + \frac{s^2}{\sigma^2 + \varepsilon} \right)$ может быть сделано сколь угодно близким к величине (4.48).

§ 4.7. Комментарии

1. Имеется много прекрасных книг по теории информации. Здесь мы во многом следуем книге Ковера и Томаса [70], которая дает ясное и неформальное введение в предмет.

Метод типов (типичных последовательностей) был систематически разработан Чисаром и Кёрнером; см. [44].

2. Идея использования показательной функции в неравенстве Маркова с последующей оценкой больших отклонений восходит к Бернштейну и была развита Крамером; ее важность для теории информации подчеркивалась Черновым, см., например, [70, лемма 12.9.1], а также [5].

3. Доказательство утверждения задачи 4.3.2 и его приложения в теории информации обсуждаются в книге Галлагера [5, теоремы 4.4.1, 4.5.1].

4. Первоначальные идеи теоремы кодирования были изложены в пионерской работе Шеннона [139]. Наше доказательство отличается от данного в книге [70] тем, что использует условную, а не совместную типичность. Именно такой подход допускает некоммутативное обобщение, см. § 5.6.

5. Теория многотерминальных систем излагается в книгах Чисара и Кёрнера [44], Ковера и Томаса [70]. Доказательство теоремы кодирования для канала с перехватом см. в книге [44].

6. Строгое доказательство формулы (4.48) см., например, в книге [70]. Квантовый аналог канала с аддитивным гауссовским шумом рассматривается в п. 11.5.1.

ГЛАВА 5

Квантовая теорема кодирования

§ 5.1. Пропускная способность классически-квантового канала связи

Как было выяснено в п.3.2.1, простейшая модель квантового канала предполагает, что есть классический параметр x , пробегающий (конечный) входной алфавит $\mathcal{X}$, и отображение $x \rightarrow S_x$ в квантовые состояния на выходе канала. Мы будем называть такую модель классически-квантовым (с-к) каналом. Если на выходе такого канала измеряется наблюдаемая $M = \{M_y\}$, то условная вероятность получить исход y при условии, что был послан сигнал x , дается формулой

$$P(y|x) = \text{Tr } S_x M_y. \quad (5.1)$$

Таким образом, для фиксированного измерения мы получаем обычный классический канал связи. Это приводит к вопросу о максимальном количестве классической информации, которое может быть почти без помех передано по данному квантовому каналу, и о соответствующей предельной характеристике — классической пропускной способности. Этот вопрос будет детально рассмотрен в настоящей главе.

Рассмотрим соответствующий составной с-к-канал, который отображает слово $w = (x_1, \dots, x_n)$ в состояние-произведение $S_w = S_{x_1} \otimes \dots \otimes S_{x_n}$ в пространстве $\mathcal{H}^{\otimes n}$. Процесс передачи классической информации описывается диаграммой

$$i \xrightarrow{\text{кодирование}} w \xrightarrow{\text{канал}} S_w \xrightarrow{\text{декодирование}} j. \quad (5.2)$$

Предположение о том, что слово w отображается в тензорное произведение состояний S_{x_j} , соответствует определению канала без памяти в классическом случае. На выходе канала находится приемник, который производит измерение некоторой наблюдаемой $M = \{M_j^{(n)}\}$ в пространстве $\mathcal{H}^{\otimes n}$ (получив исход измерения j , считаем, что было послано сообщение j). В итоге приемник выдает ответ о принятом решении; таким образом, разложение единицы в пространстве $\mathcal{H}^{\otimes n}$ описывает статистику всей решающей процедуры, которая включает в себя физическое измерение и последующую классическую обработку его результатов. Выбор наблюдаемой M формально аналогичен выбору решающей процедуры

в классическом случае, но как мы увидим, играет здесь гораздо более важную роль.

Определение 5.1.1. Код (W, M) размера N для составного с- q -канала $x^n \rightarrow S_{x^n}$ состоит из (классического) кодирования W , задаваемого набором N кодовых слов $w^{(i)}$, $i = 1, \dots, N$, длины n , и (квантового) декодирования, задаваемого наблюдаемой $M = \{M_j, j = 0, 1, \dots, N\}$ в $\mathcal{H}^{\otimes n}$.

Исход 0 означает уклонение от принятия решения. Вероятность декодировать входное сообщение i как сообщение j равна

$$p_{WM}(j|i) = \text{Tr } S_{w^{(i)}} M_j, \quad j = 0, 1, \dots, N. \quad (5.3)$$

Вероятность правильного решения тогда равна $p_{WM}(i|i) = \text{Tr } S_{w^{(i)}} M_i$, а максимальная (по всем входным сообщениям) вероятность ошибки кода (W, M) есть

$$P_e(W, M) = \max_{1 \leq j \leq N} (1 - p_{WM}(j|j)). \quad (5.4)$$

Средняя ошибка кода равна

$$\bar{P}_e(W, M) = \frac{1}{N} \sum_{j=1}^N [1 - p_{WM}(j|j)]. \quad (5.5)$$

Далее будем обозначать через

$$p_e(n, N) = \min_{W, M} P_e(W, M), \quad \bar{p}_e(n, N) = \min_{W, M} \bar{P}_e(W, M) \quad (5.6)$$

соответственно максимальную и среднюю ошибку, минимизированные по всем кодам (W, M) размера N , использующим слова длины n .

Определение 5.1.2. Классической пропускной способностью S с- q -канала $x \rightarrow S_x$ называется точная верхняя грань скоростей передачи R , которые достижимы в том смысле, что $\lim_{n \rightarrow \infty} p_e(n, 2^{nR}) = 0$, или, что равносильно (в силу неравенств (4.30)), $\lim_{n \rightarrow \infty} \bar{p}_e(n, 2^{nR}) = 0$.

§ 5.2. Формулировка теоремы кодирования

Понятие энтропии квантового состояния является естественным обобщением энтропии распределения вероятностей. Пусть S — оператор плотности в d -мерном гильбертовом пространстве $\mathcal{H}$,

$$S = \sum_{j=1}^d s_j |e_j\rangle \langle e_j|$$

— его спектральное представление. Собственные числа s_j образуют распределение вероятностей. *Энтропия фон Неймана* оператора плотности S определяется соотношением

$$H(S) = \sum_{j=1}^d \eta(s_j) = \text{Tr } \eta(S). \quad (5.7)$$

Далее мы будем использовать более наглядное выражение $H(S) = -\text{Tr } S \log S$, хотя логарифм не определен для вырожденных операторов плотности. Как и в случае распределений, это не приведет к недоразумениям. Из оценки (4.3) следует, что

$$0 \leq H(S) \leq \log d,$$

причем минимум достигается на чистых состояниях, а максимум — на хаотическом состоянии $\bar{S} = \frac{1}{d}I$. Как и в классическом случае, энтропия является мерой неопределенности, а также информационного содержания состояния (последнее утверждение будет подробно обосновано в §5.5).

Легко проверяются следующие свойства квантовой энтропии.

Задача 5.2.1. Докажите следующие утверждения.

1. Унитарная инвариантность: $H(VSV^*) = H(S)$, где V — унитарный оператор. Более того, это равенство справедливо для любого оператора V , изометричного на носителе S .

2. Аддитивность: $H(S_1 \otimes S_2) = H(S_1) + H(S_2)$.

В ранних работах по квантовым оптическим каналам связи для оценки пропускной способности канала $x \rightarrow S_x$ использовалась величина

$$\chi(\{\pi_x\}; \{S_x\}) = H\left(\sum_x \pi_x S_x\right) - \sum_x \pi_x H(S_x), \quad (5.8)$$

которая может рассматриваться как формальный некоммутативный аналог шенноновской информации, причем первое слагаемое играет роль выходной энтропии, а второе — условной энтропии квантового выхода относительно классического входного сигнала. Замечательно, что величина (5.8) действительно оказывается непосредственно связанной с классической пропускной способностью s - q -канала, определенной выше.

В ситуации, когда состояния $\{S_x\}$ фиксированы, мы будем обозначать величину (5.8) просто как $\chi(\pi)$. Основной целью следующих пунктов будет доказательство следующей теоремы.

Теорема 5.2.1 (квантовая теорема кодирования). *Определенная выше классическая пропускная способность C s - q -канала $x \rightarrow S_x$ равна величине*

$$C_\chi = \max_{\pi} \chi(\pi).$$

Заметим, что квантовая энтропия непрерывна на компактном множестве квантовых состояний, поэтому величина χ непрерывна как функция распределения π и максимум в этой формуле действительно достигается. Введем обозначение

$$\bar{S}_\pi = \sum_x \pi_x S_x \quad (5.9)$$

для среднего выходного квантового состояния. В общем случае

$$\chi(\pi) \leq H(\bar{S}_\pi),$$

причем равенство имеет место для канала с чистыми состояниями $S_x = |\psi_x\rangle\langle\psi_x|$. Поскольку максимально возможное значение энтропии равно $\log \dim \mathcal{H}$, из этой теоремы получаем абсолютную верхнюю границу в терминах размерности выходной квантовой системы:

$$C \leq \log \dim \mathcal{H}. \quad (5.10)$$

Таким образом, несмотря на то что в гильбертовом пространстве имеется бесконечно много разных чистых состояний, это обстоятельство не может быть использовано для передачи неограниченного количества информации. Грубо говоря, чем гуще расположены векторы, тем труднее становится их различить. Верхняя граница и максимум информации достигаются, если выходные состояния являются ортогональными и равновероятными. Заметим, что такие состояния, как правило, не могут быть получены на выходе реального канала связи. Замечательно, однако, что, как показывает следующий пример, ортогональность выходных состояний не является необходимой для достижения пропускной способности идеального канала.

Пример 5.2.1. Канал с тремя чистыми состояниями ψ_0, ψ_1, ψ_2 в двумерном пространстве (см. рис. 2.3). Для равномерного распределения ($\pi_x = \frac{1}{3}$), среднее выходное состояние является хаотическим:

$$\bar{S}_\pi = \sum_{x=0}^2 \pi_x |\psi_x\rangle\langle\psi_x| = \frac{1}{2}I, \quad (5.11)$$

откуда следует, что $C_\chi = \log 2 = 1$ бит — пропускная способность идеального канала.

Пример 5.2.2. Двоичный канал с двумя чистыми состояниями ψ_0, ψ_1 (см. рис. 2.2). В этом случае

$$C_\chi = h_2\left(\frac{1+\varepsilon}{2}\right), \quad (5.12)$$

где $\varepsilon = |\langle \psi_0 | \psi_1 \rangle|$. В самом деле, энтропия $H(\bar{S}_\pi)$ максимизируется равномерным распределением $\pi_0 = \pi_1 = \frac{1}{2}$, поскольку в силу вогнутости энтропии (см. далее следствие 7.2.2) справедливо неравенство

$$H\left(\frac{1}{2}|\psi_0\rangle\langle\psi_0| + \frac{1}{2}|\psi_1\rangle\langle\psi_1|\right) = H\left(\frac{S+S'}{2}\right) \geq \frac{1}{2}(H(S) + H(S')),$$

где

$$S = \pi_0|\psi_0\rangle\langle\psi_0| + \pi_1|\psi_1\rangle\langle\psi_1|, \quad S' = \pi_1|\psi_0\rangle\langle\psi_0| + \pi_0|\psi_1\rangle\langle\psi_1|$$

и $H(S') = H(S)$ в силу симметрии относительно биссектрисы угла между векторами. Аналогично решению задачи 2.3.1 получаем, что собственные значения оператора плотности $\frac{1}{2}|\psi_0\rangle\langle\psi_0| + \frac{1}{2}|\psi_1\rangle\langle\psi_1|$ равны $\frac{1 \pm \varepsilon}{2}$, откуда следует соотношение (5.12).

§ 5.3. Верхняя граница

Рассмотрим произвольный с-q-канал $x \rightarrow S_x$ и наблюдаемую $M = \{M_y\}$ на выходе канала. Отметим, что алфавиты $\mathcal{X}$ и $\mathcal{Y}$ могут не совпадать. Переменные x и y связаны классическим каналом $p_M(y|x) = \text{Tr } S_x M_y$. Обозначим через

$$\mathcal{I}_1(\pi, M) = \sum_{xy} \pi_x p_M(y|x) \log \left(\frac{p_M(y|x)}{\sum_{x'} p_M(y|x') \pi_{x'}} \right) \quad (5.13)$$

шенноновскую информацию между переменными x и y , соответствующую некоторому входному распределению $\pi = \{\pi_x\}$.

Задача 5.3.1. Докажите, что для данных π и $\mathcal{Y}$ количество информации $\mathcal{I}_1(\pi, M)$ является непрерывной и выпуклой функцией от $p_M(y|x)$ и, следовательно, от M . *Указание.* Используйте соответствующее свойство шенноновской информации $I(X; Y)$.

Для данного распределения π на входном алфавите рассмотрим достижимую информацию

$$\sup_M \mathcal{I}_1(\pi, M).$$

Здесь точная верхняя грань берется по всевозможным наблюдаемым на выходе канала $x \rightarrow S_x$.

Предложение 5.3.1. Точная верхняя грань количества информации $\mathcal{I}_1(\pi, M)$ достигается на наблюдаемой M^0 вида

$$M_y^0 = |\varphi_y\rangle\langle\varphi_y|, \quad y = 1, \dots, t, \quad (5.14)$$

где $t \leq d^2$ в случае комплексного $\mathcal{H}$ ($t \leq \frac{d(d+1)}{2}$ в случае вещественного $\mathcal{H}$).

Доказательство. Для любого $k = 2, 3, \dots$ множество $\mathfrak{M}_k$ наблюдаемых с k исходами компактно, и непрерывный выпуклый функционал $\mathcal{I}_1(\pi, M)$ достигает максимума на множестве $\mathfrak{M}_k$. Предположим, что $\hat{M}^0$ максимизирует $\mathcal{I}_1(\pi, M)$ на $\mathfrak{M}_k$. Отбрасывая, если необходимо, нулевые компоненты, получаем наблюдаемую $\tilde{M}^0 \in \mathfrak{M}_l$, $l \leq k$, для которой $\mathcal{I}_1(\pi, \tilde{M}^0) = \mathcal{I}_1(\pi, \hat{M}^0)$. Производя спектральное разложение компонент наблюдаемой $\tilde{M}^0$ в виде сумм операторов ранга один, мы можем построить новую наблюдаемую M^0 вида (5.14) с $m \geq l$, для которой $\tilde{M}^0$ является укрупнением:

$$\underbrace{M_1, M_2, \dots}_{=\tilde{M}_1}, \underbrace{\dots}_{=\tilde{M}_2}, \dots, \underbrace{\dots}_{=\tilde{M}_l}, \dots, \underbrace{\dots}_{=\tilde{M}_m}.$$

Тогда $\mathcal{I}_1(\pi, M^0) \geq \mathcal{I}_1(\pi, \tilde{M}^0)$. Это есть на самом деле утверждение о классической шенноновской информации: $I(X; f(Y)) \leq I(X; Y)$, или, что эквивалентно, $H(X|f(Y)) \geq H(X|Y)$, что следует из монотонности классической условной энтропии, поскольку $H(X|Y) = H(X|f(Y), Y)$.

Функция $M \rightarrow \mathcal{I}(\pi, M)$ выпукла, поэтому мы можем предположить, что максимизирующая наблюдаемая $M^0 = \{M_{ij}^0\}$ является крайней точкой множества $\mathfrak{M}_m$. Тогда согласно теореме 2.2.4 операторы M_{ij}^0 линейно независимы, и из задачи 1.4.2 следует оценка $m \leq d^2$. Поскольку k было произвольным, отсюда следует, что $\sup_M \mathcal{I}_1(\pi, M)$ достигается на наблюдаемой из компактного выпуклого множества $\mathfrak{M}_{d^2}$. $\square$

Теорема 5.3.1. Для произвольного распределения π справедливо неравенство

$$\max_M \mathcal{I}_1(\pi, M) \leq \chi(\pi), \quad (5.15)$$

причем равенство достигается тогда и только тогда, когда операторы $\pi_x S_x$, $x \in \mathcal{X}$, коммутируют.

В главе 7 мы получим неравенство (5.15) как следствие весьма общего свойства монотонности относительной энтропии. Здесь же мы дадим набросок оригинального доказательства, которое основано на сравнении свойств выпуклости классической и квантовой энтропий, использует достаточно элементарные факты и позволяет получить необходимое и достаточное условие достижения равенства. Это условие будет использовано в следующем параграфе для установления неклассического свойства супераддитивности шенноновской информации для с-q-канала.

Доказательство. Прежде всего докажем теорему в случае двух состояний S_0, S_1 . Введем обозначение

$$\chi(t) = H((1-t)S_0 + tS_1) - (1-t)H(S_0) - tH(S_1), \quad t \in [0, 1]. \quad (5.16)$$

Положим также $S_t = (1 - t)S_0 + tS_1$, $D = S_1 - S_0$, и пусть $S_t = \sum_k s_k E_k$ — спектральное разложение оператора S_t .

Задача 5.3.2. Используя интегральную формулу Коши, получите представление

$$S_t \log S_t = \frac{1}{2\pi i} \oint (Iz - S_t)^{-1} z \log z \, dz,$$

где $z \log z$ — ветвь функции $z \log z$, аналитическая в правой полуплоскости, а интеграл берется по замкнутому контуру в правой полуплоскости, охватывающему отрезок $[\varepsilon, 1]$, $\varepsilon > 0$.

Дифференцируя дважды по параметру t , получаем

$$[S_t \log S_t]'' = \left[\frac{1}{2\pi i} \oint [(Iz - S_t)^{-1}]'' z \log z \, dz \right],$$

причем

$$\begin{aligned} [(Iz - S_t)^{-1}]'' &= 2(Iz - S_t)^{-1} D (Iz - S_t)^{-1} D (Iz - S_t)^{-1} = \\ &= 2 \sum_{k,j,l} \frac{E_k D E_j D E_l}{(z - s_k)(z - s_j)(z - s_l)}. \end{aligned}$$

Отсюда следует, что

$$\chi''(t) = - \sum_{k,j} (\text{Tr } E_k D E_j D) f(s_k, s_j), \quad t > 0, \quad (5.17)$$

где

$$\begin{aligned} f(a, b) &= \frac{1}{2\pi i} \oint \left[\frac{1}{(z - a)^2(z - b)} + \frac{1}{(z - b)^2(z - a)} \right] z \log z \, dz = \\ &= \frac{\log a - \log b}{a - b}, \quad a \neq b; \end{aligned} \quad (5.18)$$

$f(a, a) = a^{-1}$. Используя элементарное неравенство

$$f(a, b) \geq \frac{2}{a + b}, \quad 0 < a \leq 1, \quad 0 < b \leq 1,$$

в котором равенство достигается тогда и только тогда, когда $a = b$, получаем

$$\chi''(t) \leq - \sum_{k,j} \text{Tr } E_k D E_j D \frac{2}{s_k + s_j}, \quad (5.19)$$

причем равенство достигается тогда и только тогда, когда $[D, S_t] = 0$, т. е. $[S_0, S_1] = 0$.

Задача 5.3.3. Покажите, что оператор

$$L_t = \sum_{k,j} E_k D E_j \frac{2}{s_k + s_j}$$

является решением уравнения

$$S_t \circ L_t \equiv \frac{1}{2}[S_t L_t + L_t S_t] = D,$$

причем

$$\sum_{k,j} \text{Tr} E_k D E_j D \frac{2}{s_k + s_j} = \text{Tr} D L_t = \text{Tr} S_t L_t^2. \quad (5.20)$$

Оператор L_t является некоммутативным аналогом логарифмической производной семейства S_t , а (5.20) — аналогом информационного количества Фишера в математической статистике.

Из соотношений (5.19), (5.20) вытекает, что

$$\chi''(t) \leq -\text{Tr} D L_t = -\text{Tr} S_t L_t^2, \quad (5.21)$$

в частности $\chi''(t) \leq 0$, так что $\chi(t)$ — вогнутая функция на отрезке $[0, 1]$, причем $\chi(0) = \chi(1) = 0$.

Пусть теперь $M = \{M_y\}$ — произвольная наблюдаемая,

$$P_t(y) = \text{Tr} S_t M_y = (1-t)P_0(y) + tP_1(y)$$

— ее распределение в состоянии S_t и $J_M(t) = \mathcal{I}_1(\pi, M)$, где $\pi = \{1-t, t\}$. Положим также $D(y) = P_1(y) - P_0(y)$. Применяя результаты задач 5.3.2, 5.3.3 к диагональной матрице $\text{diag}[P_t(y)]$ в роли состояния S_t , получаем

$$J_M''(t) = -\sum_y \frac{D(y)^2}{P_t(y)} = -\text{Tr} D \Lambda_t, \quad (5.22)$$

где

$$\Lambda_t = \sum_y M_y \frac{D(y)}{P_t(y)}.$$

Отсюда также вытекает, что $J_M''(t) < 0$, так что $J_M(t)$ — вогнутая функция на отрезке $[0, 1]$, причем $J_M(0) = J_M(1) = 0$.

Заметим, что

$$\text{Tr} D \Lambda_t = \sum_y \frac{D(y)^2}{P_t(y)} \geq \text{Tr} S_t \Lambda_t^2, \quad (5.23)$$

поскольку

$$\Lambda_t^2 \leq \sum_y M_y \left[\frac{D(y)}{P_t(y)} \right]^2$$

в силу следующей разновидности неравенства Коши—Буняковского.

Задача 5.3.4. Докажите, что для любых вещественных c_y справедливо неравенство

$$\left(\sum_y c_y M_y \right)^2 \leq \sum_y c_y^2 M_y.$$

Наконец покажем, что $\text{Tr } D\Lambda_t \leq \text{Tr } DL_t$, откуда согласно соотношениям (5.21), (5.22) вытекает, что $J_M''(t) \geq \chi''(t)$, а значит, $J_M(t) \leq \chi(t)$, $0 < t < 1$, причем равенство имеет место тогда и только тогда, когда $[S_0, S_1] = 0$.

В самом деле, используя неравенство (5.23), получаем

$$\begin{aligned} \text{Tr } DL_t &= \text{Tr } S_t L_t^2 = \text{Tr } S_t [\Lambda_t + (L_t - \Lambda_t)]^2 \geq \\ &\geq \text{Tr } S_t \Lambda_t^2 + 2 \text{Tr } S_t (L_t - \Lambda_t) \circ \Lambda_t = \\ &= -\text{Tr } S_t \Lambda_t^2 + 2 \text{Tr } (S_t \circ L_t) \Lambda_t = 2 \text{Tr } D\Lambda_t - \text{Tr } S_t \Lambda_t^2 = \\ &= \text{Tr } D\Lambda_t + [\text{Tr } D\Lambda_t - \text{Tr } S_t \Lambda_t^2] \geq \text{Tr } D\Lambda_t. \end{aligned}$$

Случай нескольких состояний S_x , $x = 0, 1, \dots, k$, с распределением $\pi = \{\pi_x; x = 0, 1, \dots, k\}$ сводится к случаю двух состояний при помощи следующего преобразования (и аналогичного преобразования для $\mathcal{I}_1(\pi, M)$)

Задача 5.3.5. Докажите, что

$$\chi(\pi) = \sum_{m=1}^k (\pi_0 + \dots + \pi_m) \chi_m(t_m),$$

где

$$\begin{aligned} \chi_m(t) &= H((1-t)S_0^m + tS_m) - (1-t)H(S_0^m) - tH(S_m), \\ t_m &= \frac{\pi_m}{\pi_0 + \dots + \pi_m}, \quad S_0^m = \sum_{j=0}^{m-1} \frac{\pi_j S_j}{\pi_0 + \dots + \pi_{m-1}}. \end{aligned}$$

□

§ 5.4. Доказательство слабого обращения

Неравенство (5.15) является основным инструментом в доказательстве слабого обращения квантовой теоремы кодирования, из которого следует, что $C \leq C_\chi$.

Теорема 5.4.1 (слабое обращение). *Справедливо неравенство*

$$\liminf_{n \rightarrow \infty} \bar{p}_e(n, 2^{nR}) > 0 \quad \text{при } R > C_\chi. \quad (5.24)$$

Доказательство. Рассмотрим составной с- q -канал $\omega \rightarrow S_\omega$, где $\omega = x^n$ обозначает слово длины n . Пусть $\mathcal{I}_n(\pi^{(n)}, M^{(n)})$ — шенноновская информация, определенная для этого составного канала аналогично $\mathcal{I}_1(\pi, M)$, где $\pi^{(n)} = \{\pi_\omega\}$ — распределение на словах длины n , а $M^{(n)}$ — наблюдаемая в $\mathcal{H}^{\otimes n}$. Тогда из неравенства (5.15) следует, что

$$\mathcal{I}_n(\pi^{(n)}, M^{(n)}) \leq C_\chi^{(n)}, \quad (5.25)$$

где

$$C_\chi^{(n)} = \max_{\pi^{(n)}} \chi(\{\pi_\omega\}; \{S_\omega\}) = \max_{\pi^{(n)}} \left[H\left(\sum_\omega \pi_\omega S_\omega\right) - \sum_\omega \pi_\omega H(S_\omega) \right]. \quad (5.26)$$

Лемма 5.4.1. Последовательность $C_\chi^{(n)}$ аддитивна, т. е. $C_\chi^{(n)} = nC_\chi$.

Доказательство. Неравенство $C_\chi^{(n)} \geq nC_\chi$ основано на аддитивности энтропии в случае, когда входные распределения $\pi^{(n)}$ являются произведениями. Доказательство обратного неравенства $C_\chi^{(n)} \leq nC_\chi$ следует из субаддитивности энтропии фон Неймана по отношению к тензорным произведениям (см. следствие 7.1.1), из которого вытекает, что

$$\chi_n(\pi^{(n)}) \leq \sum_{k=1}^n \chi(\pi^{(n,k)}), \quad (5.27)$$

где $\pi^{(n,k)}$ есть k -е маргинальное распределение π на $\mathcal{X}$. □

Полагая

$$C_n = \max_{\pi^{(n)}, M^{(n)}} \mathcal{I}_n(\pi^{(n)}, M^{(n)}), \quad (5.28)$$

мы, таким образом, получаем $C_n \leq nC_\chi$, и, применяя классическое неравенство Фано, аналогично неравенству (4.36) получаем

$$\bar{P}_e(W, M) \geq 1 - \frac{C_n}{nR} - \frac{1}{nR} \geq 1 - \frac{C_\chi}{R} - \frac{1}{nR}, \quad (5.29)$$

откуда следует неравенство (5.24). □

Величина C_n равна максимальной шенноновской информации, достижимой при использовании n копий с- q -канала, когда на выходе $\mathcal{H}^{\otimes n}$ допускаются измерения произвольных квантовых наблюдаемых. Следующий результат проясняет ее отношение к классической пропускной способности.

Предложение 5.4.1. Классическая пропускная способность C канала $x \rightarrow S_x$ равна

$$\sup_n \frac{1}{n} C_n = \lim_n \frac{1}{n} C_n. \quad (5.30)$$

Доказательство. Равенство в формуле (5.30) вытекает из супераддитивности последовательности $\{C_n\}$.

Задача 5.4.1. Покажите, что последовательность C_n супераддитивна, $C_{n+m} \geq C_n + C_m$, рассматривая распределения вида $\pi^{(n+m)} = \pi^{(n)} \times \pi^{(m)}$.

Неравенство $C \leq \sup_n \frac{1}{n} C_n$ получается, если перейти к пределу при $n \rightarrow \infty$ в первом соотношении (5.29). Противоположное неравенство $C \geq \sup_n \frac{1}{n} C_n$ вытекает из прямого утверждения классической теоремы кодирования Шеннона, примененной к составным каналам с измерением на выходе. В самом деле, покажем, что всякое значение $R < \sup_n \frac{1}{n} C_n$ является достижимой скоростью. Поскольку $n_0 R < C_{n_0}$ для некоторого n_0 , мы можем выбрать наблюдаемую $M^{(n_0)}$ в $\mathcal{H}^{\otimes n_0}$ такую, что

$$n_0 R < \max_{\pi^{(n_0)}} \mathcal{I}_n(\pi^{(n_0)}, M^{(n_0)}) \equiv C(M^{(n_0)}).$$

Величина $C(M^{(n_0)})$ является шенноновской пропускной способностью классического канала

$$p_M^{(n_0)}(j|x^{n_0}) = \text{Tr } S_{x^{n_0}} M_j^{(n_0)}. \quad (5.31)$$

Поэтому минимальная вероятность ошибки для этого канала удовлетворяет соотношению $\tilde{p}_e(n, 2^{n(n_0 R)}) \rightarrow 0$ при $n \rightarrow \infty$. Очевидно,

$$\bar{p}_e(nn_0, 2^{n(n_0 R)}) \leq \tilde{p}_e(n, 2^{n(n_0 R)}),$$

поскольку канал (5.31) отвечает некоторому специальному блочному декодированию для исходного с-q-канала. Таким образом,

$$\bar{p}_e(nn_0, 2^{n(n_0 R)}) \rightarrow 0 \quad \text{при } n \rightarrow \infty.$$

Для произвольного n' можно найти такое n , что $nn_0 \leq n' \leq (n+1)n_0$. Тогда

$$\bar{p}_e(n', 2^{n'R}) \leq \bar{p}_e(nn_0, 2^{(n+1)n_0 R}) \leq \bar{p}_e(nn_0, 2^{n(n_0 R')}) \rightarrow 0, \quad (5.32)$$

если R' выбрано так, что

$$R \left(1 + \frac{1}{n}\right) \leq R' < \sup_n \frac{1}{n} C_n$$

для достаточно больших n . □

Величина

$$C_1 = \max_{\pi, M} \mathcal{I}_1(\pi, M),$$

которую мы назовем *шенноновской пропускной способностью* с- q -канала $x \rightarrow S_x$, представляет особый интерес: аналогично предложению 5.4.1 можно показать, что она равна пропускной способности с- q -канала $x \rightarrow S_x$ с дополнительным ограничением, что на выходе составного канала допускаются только несцепленные декодирования. Здесь мы называем декодирование $M^{(n)} = \{M_j^{(n)}\}$ в $\mathcal{H}^{\otimes n}$ *несцепленным*, если

$$M_j^{(n)} = \sum_{y^n} p(j|y^n) M_{y_1}^1 \otimes \dots \otimes M_{y_n}^n, \quad (5.33)$$

где $\{M_{y_k}^k\}$ — квантовая наблюдаемая для k -го экземпляра пространства $\mathcal{H}$, а $p(j|y^n)$ — условная вероятность, описывающая классическое преобразование результатов измерения несцепленной наблюдаемой $\{M_{y_1}^1 \otimes \dots \otimes M_{y_n}^n\}$ на выходе.

Задача 5.4.2. Обозначая через C_u точную верхнюю грань достижимых скоростей для кодов (W, M) с дополнительным ограничением (5.33) на декодирования M , покажите, что $C_u = C_1$. *Указание.* Используйте аналог первого неравенства в (5.29), чтобы доказать, что $C_u \leq C_1$. Для доказательства обратного неравенства используйте прямое утверждение классической теоремы кодирования для канала $p_M(y|x) = \text{Tr } S_x M_y$ и с его помощью докажите, что любое значение скорости $R < \max_{\pi} \mathcal{I}_1(\pi, M)$ достижимо. Поскольку декодирование M в $\mathcal{H}$ произвольно, отсюда следует, что любая скорость $R < C_1$ достижима, поэтому $C_1 \leq C_u$.

Пока что было доказано, что

$$C_1 \leq C \leq C_{\mathcal{H}}.$$

Из прямого утверждения теоремы кодирования, которое мы собираемся доказать ниже, будет следовать, что $C = C_{\mathcal{H}}$. Следующий результат означает, что $C_1 < C$ для каналов с существенно квантовым выходом. Таким образом, для с- q -каналов без памяти возможно увеличение пропускной способности благодаря использованию сцепленных декодирований. Отсюда следует, что, тогда как для классического канала без памяти $C_n = nC_1$ (см. предложение 4.3.1), в квантовом случае возможна строгая супераддитивность классической информации: $C_n > nC_1$. Причина этого кроется в том, что на выходе составного квантового канала существуют сцепленные наблюдаемые. Можно сказать, что это есть двойственное проявление корреляций ЭПР. Последние возникают, когда рассматривается сцепленное состояние составной квантовой системы, а измерения локальны, т. е. не сцеплены. Строгая супераддитивность информации имеет место для состояний-произведений и обусловлена существованием сцепленных наблюдаемых.

Предложение 5.4.2. Равенство $C_1 = C$ имеет место тогда и только тогда, когда операторы $\pi_x^0 S_x$ коммутируют для распределения π^0 , максимизирующего $\chi(\pi)$.

Доказательство. Очевидно, что условие является достаточным. Обратно, пусть $C_1 = C$, тогда, используя предложение 5.3.1, компактность множества распределений $\{\pi\}$ и непрерывность шенноновской информации $\mathcal{I}_1(\pi^1, M^1)$, получаем $C_1 = \mathcal{I}_1(\pi^1, M^1)$ для некоторого распределения π^1 и наблюдаемой M^1 , поэтому $\mathcal{I}_1(\pi^1, M^1) = \chi(\pi^0)$. Отсюда следует, что $\chi(\pi^1) = \chi(\pi^0)$, потому что в противном случае, используя неравенство (5.15), мы бы получили

$$\mathcal{I}_1(\pi^1, M^1) \leq \chi(\pi^1) < \chi(\pi^0).$$

Таким образом, мы можем заменить π^0 на π^1 , $\mathcal{I}_1(\pi^1, M^1) = \chi(\pi^1)$, и необходимость следует из второго утверждения теоремы 5.3.1. $\square$

Следующие примеры (подробности см. в § 5.8) иллюстрируют неравенство $C_1 < C$.

Пример 5.4.1. Для канала с тремя «равноугольными» чистыми состояниями значение

$$C_1 = 1 - h_2\left(\frac{1 + \sqrt{3}/2}{2}\right) \approx 0,645 \text{ бит} \quad (5.34)$$

достигается для неравномерного распределения $\pi = [1/2, 1/2, 0]$ и наблюдаемой, оптимальной для двух равновероятных состояний S_0, S_1 . Таким образом, $C_1 < C = 1$, и последовательность $\{C_n\}$ является строго супераддитивной. Заметим, что равномерное распределение $\pi = [1/3, 1/3, 1/3]$ и соответствующая информационно-оптимальная наблюдаемая дают меньшую величину $\log(3/2) \approx 0,585$ бит.

Пример 5.4.2. Шенноновская пропускная способность с-q-канала с двумя чистыми состояниями равна

$$C_1 = \max_{\pi, M} \mathcal{I}(\pi, M) = 1 - h_2\left(\frac{1 + \sqrt{1 - \varepsilon^2}}{2}\right), \quad (5.35)$$

где максимум достигается для равномерного распределения ($\pi_0 = \pi_1 = \frac{1}{2}$) и четкой наблюдаемой M , задаваемой ортонормированным базисом, расположенным симметрично по отношению к векторам $|\psi_0\rangle, |\psi_1\rangle$ (см. рис. 2.2). Здесь $\varepsilon = |\langle\psi_0|\psi_1\rangle| = \cos \alpha$, где α — угол между направлениями векторов. Заметим, что в этом случае информационно-оптимальная наблюдаемая совпадает с полученной согласно критерию максимального правдоподобия (пример 2.3.1), а C_1 — с пропускной способностью

(4.22) соответствующего классического двоичного симметричного канала с вероятностью ошибки

$$p = \sin^2\left(\frac{\pi}{4} - \frac{\alpha}{2}\right) = \frac{1 - \sin \alpha}{2}.$$

График зависимости C_1 , C от ε приведен на рис. 5.1.

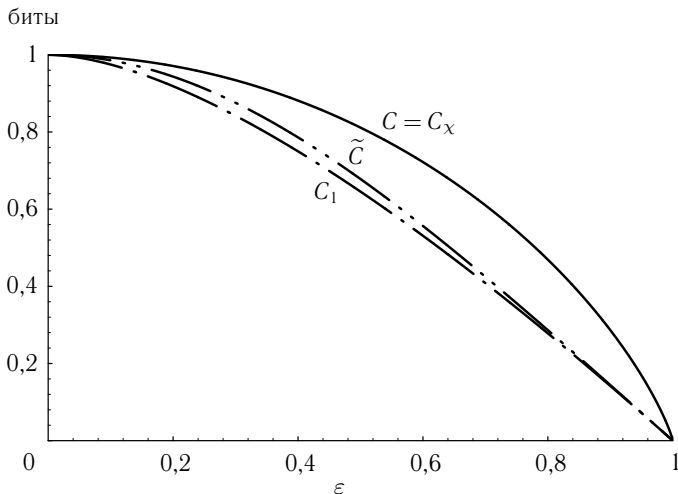


Рис. 5.1. Пропускная способность канала с двумя чистыми состояниями

§ 5.5. Типичные проекторы

Перед тем как приступить к доказательству прямого утверждения теоремы кодирования для величины C_x , рассмотрим важное понятие типичного подпространства.

Рассмотрим тензорное произведение состояний

$$S^{\otimes n} = S \otimes \dots \otimes S$$

в пространстве $\mathcal{H}^{\otimes n}$. Пусть

$$S = \sum_j \lambda_j |e_j\rangle\langle e_j|$$

— спектральное разложение оператора S , где $\{e_j\}$ — ортонормированный базис из собственных векторов, а λ_j — соответствующие собственные

значения. Заметим, что λ_j образуют распределение вероятностей с энтропией

$$\sum_j \eta(\lambda_j) = H(S).$$

Тогда спектральное разложение состояния-произведения $S^{\otimes n}$ может быть записано в виде

$$S^{\otimes n} = \sum_J \lambda_J |e_J\rangle \langle e_J|,$$

где $J = (j_1, \dots, j_n)$, с собственными векторами $|e_J\rangle = |e_{j_1}\rangle \otimes \dots \otimes |e_{j_n}\rangle$ и собственными значениями $\lambda_J = \lambda_{j_1} \cdot \dots \cdot \lambda_{j_n}$, образующими распределение вероятностей независимых одинаково распределенных случайных величин. В соответствии с определением 4.1.1 собственный вектор $|e_J\rangle$ будет называться δ -типичным, если

$$2^{-n(H(S)+\delta)} < \lambda_J < 2^{-n(H(S)-\delta)}.$$

Основываясь на спектральном разложении оператора $S^{\otimes n}$, мы можем определить δ -типичный проектор $P^{n,\delta}$ на подпространство $\mathcal{H}^{n,\delta} = P^{n,\delta} \mathcal{H}^{\otimes n}$ соотношением

$$P^{n,\delta} = \sum_{J \in T^{n,\delta}} |e_J\rangle \langle e_J|.$$

Свойства подпространства $\mathcal{H}^{n,\delta}$ типичных векторов аналогичны соответствующим свойствам подмножества $T^{n,\delta}$ типичных слов (см. § 4.1) и легко из них получаются.

1. Размерность $\dim \mathcal{H}^{n,\delta} = \text{Tr } P^{n,\delta} = |T^{n,\delta}|$ удовлетворяет неравенству

$$\dim \mathcal{H}^{n,\delta} \leq 2^{n(H(S)+\delta)}.$$

2. Вклад не δ -типичных собственных векторов в оператор $S^{\otimes n}$ может быть сделан сколь угодно малым, т. е. для данных $\delta, \varepsilon > 0$ и достаточно больших n выполняется неравенство

$$\text{Tr } S^{\otimes n} (I - P^{n,\delta}) < \varepsilon. \quad (5.36)$$

Чтобы это показать, оценим след в базисе из собственных векторов оператора $S^{\otimes n}$ и получим, что он равен

$$\begin{aligned} \sum_{J \in T^{n,\delta}} \lambda_J &= \text{P} \left\{ \left| -\frac{1}{n} \log \lambda_J - H(S) \right| \geq \delta \right\} = \\ &= \text{P} \left\{ \left| -\frac{1}{n} \sum_{k=1}^n \log \lambda_{j_k} - H(S) \right| \geq \delta \right\}, \quad (5.37) \end{aligned}$$

где P отвечает распределению вероятностей $\{\lambda_j\}$, а последняя вероятность может быть сделана сколь угодно малой для больших n согласно закону больших чисел.

3. Для достаточно больших n выполняется неравенство

$$(1 - \varepsilon)2^{n(H(S) - \delta)} \leq \dim \mathcal{H}^{n, \delta}.$$

Теперь можно так сформулировать некоммутативную версию свойства асимптотической равномерности: при больших n состояние $S^{\otimes n}$ становится похожим на хаотическое состояние в подпространстве $\mathcal{H}^{n, \delta}$ размерности $\approx 2^{nH(S)}$.

Непосредственным приложением этого свойства является квантовый аналог сжатия данных. Как мы уже видели, размерность гильбертова пространства отражает информационный ресурс квантовой системы. С другой стороны, в квантовых вычислениях размерность отражает величину памяти, т. е. число q -битов в регистре, которое желательно минимизировать. Рассмотрим задачу кодирования *чистых* квантовых состояний другими состояниями в гильбертовом пространстве по возможности минимальной размерности, однако без существенной потери «квантовой информации», переносимой состояниями. Для этого рассмотрим квантовый источник, который производит независимые одинаково распределенные *чистые* состояния $S_x = |\psi_x\rangle\langle\psi_x|$ с распределением p_x . Блочные состояния $S_w = |\psi_w\rangle\langle\psi_w|$, где $|\psi_w\rangle = |\psi_{x_1}\rangle \otimes \dots \otimes |\psi_{x_n}\rangle \in \mathcal{H}^{\otimes n}$, кодируются в некоторые состояния S'_w в подпространстве $\mathcal{H}_d \subset \mathcal{H}^{\otimes n}$, размерность которого $d = \dim \mathcal{H}_d$ должна быть по возможности минимальной. При этом требуется, чтобы *средняя точность воспроизведения*

$$F_n = \sum_w \pi_w \langle \psi_w | S'_w | \psi_w \rangle$$

стремила к 1 при $n \rightarrow \infty$.

Пусть

$$\bar{S}_\pi = \sum_{x=1}^d \pi_x |\psi_x\rangle\langle\psi_x|$$

— среднее состояние источника.

Теорема 5.5.1 (сжатие квантовой информации). 1. Для достаточно малых $\varepsilon, \delta > 0$ существуют подпространство $\mathcal{H}_d \subset \mathcal{H}^{\otimes n}$ размерности $d = 2^{n(H(\bar{S}_\pi) + \delta)}$ и операторы плотности S'_w в $\mathcal{H}_d$ такие, что $F_n > 1 - \varepsilon$ для достаточно больших n ;

2. При любом выборе подпространства $\mathcal{H}_d \subset \mathcal{H}^{\otimes n}$ размерности $d = 2^{n(H(\bar{S}_\pi) - \delta)}$ и операторов плотности S'_w в $\mathcal{H}_d$ для достаточно больших n имеет место неравенство $F_n < \varepsilon$.

Доказательство. 1. Для состояния источника $|\psi_w\rangle = |\psi_{x_1}\rangle \otimes \dots \otimes |\psi_{x_n}\rangle$ определим «сжатое» состояние как

$$S'_w = \frac{P^{n,\delta} |\psi_w\rangle \langle \psi_w| P^{n,\delta}}{\langle \psi_w | P^{n,\delta} | \psi_w \rangle}, \quad (5.38)$$

где $P^{n,\delta}$ — типичный проектор состояния $\bar{S}_\pi^{\otimes n}$. Оператор S'_w действует в подпространстве $\mathcal{H}^{n,\delta}$, которое имеет размерность не более $d = 2^{n(H(\bar{S}_\pi) + \delta)}$. Для точности воспроизведения получаем

$$F_n = \sum_w \pi_w \langle \psi_w | S'_w | \psi_w \rangle = \sum_w \pi_w \langle \psi_w | P^{n,\delta} | \psi_w \rangle = \text{Tr} \bar{S}_\pi^{\otimes n} P^{n,\delta},$$

так как $\bar{S}_\pi^{\otimes n} = \sum \pi_w |\psi_w\rangle \langle \psi_w|$. Благодаря второму свойству проектора $P^{n,\delta}$ мы можем ограничить это выражение снизу величиной $1 - \varepsilon$.

2. Учитывая, что $S'_w \leq P_d$ для всех S'_w в $\mathcal{H}_d = P_d \mathcal{H}^{n,\delta}$, получаем

$$\begin{aligned} F_n &= \sum \pi_w \langle \psi_w | S'_w | \psi_w \rangle \leq \text{Tr} \bar{S}_\pi^{\otimes n} P_d = \\ &= \text{Tr} \bar{S}_\pi^{\otimes n} P_{\delta/2, n} P_d + \text{Tr} \bar{S}_\pi^{\otimes n} (I - P_{\frac{\delta}{2}, n}) P_d \leq \\ &\leq \|\bar{S}_\pi^{\otimes n} P_{\delta/2, n}\| \cdot \text{Tr} P_d + \text{Tr} \bar{S}_\pi^{\otimes n} (I - P_{\frac{\delta}{2}, n}) \end{aligned}$$

Здесь было использовано следующее свойство следа: если $T, X \geq 0$, то $\text{Tr} TX \leq \text{Tr} T \|X\|$, что следует из неравенства (1.18). Согласно определению типичных собственных векторов соответствующие собственные значения ограничены сверху величиной

$$\|S^{\otimes n} P^{n,\delta}\| < 2^{-n(H(S) - \delta)}. \quad (5.39)$$

Используя это неравенство и свойство 2 типичного проектора, получаем, что для достаточно больших n величина (5.39) не превосходит

$$2^{-n(H(\bar{S}_\pi) - \delta/2)} d + \varepsilon.$$

Таким образом, если $d = 2^{n(H(\bar{S}_\pi) - \delta)}$, то $F_n \leq 2^{-n\delta/2} + \varepsilon \leq 2\varepsilon$ для достаточно больших n . $\square$

Для доказательства прямого утверждения теоремы кодирования в следующем параграфе нам также понадобится соответствующее понятие условно типичного проектора. Рассмотрим блочные состояния $S_w = S_{x_1} \otimes \dots \otimes S_{x_n}$, где S_x теперь произвольное (не обязательно чистое) состояние, а $w = (x_1, \dots, x_n)$ — слово входного алфавита. Обозначим

$$\bar{H}_\pi(S_{(\cdot)}) = \sum_x \pi_x H(S_x)$$

— квантовый аналог условной энтропии выхода относительно входа. Пусть $P_w = P_w^{n, \delta}$ — спектральный проектор оператора S_w , отвечающий собственным значениям в интервале $(2^{-n[\bar{H}_\pi(S_{(\cdot)})+\delta]}, 2^{-n[\bar{H}_\pi(S_{(\cdot)})-\delta]})$. Более подробно, рассмотрим спектральное разложение

$$S_x = \sum_j \lambda_j^x |e_j^x\rangle \langle e_j^x|.$$

Тогда спектральное разложение оператора S_w имеет вид

$$S_w = \sum_J \lambda_J^w |e_J^w\rangle \langle e_J^w|,$$

где $\lambda_J^w = \lambda_{j_1}^{x_1} \cdot \dots \cdot \lambda_{j_n}^{x_n}$ — собственные значения, а $|e_J^w\rangle = |e_{j_1}^{x_1}\rangle \otimes \dots \otimes |e_{j_n}^{x_n}\rangle$ — собственные векторы. Условно типичный проектор определяется как

$$P_w = \sum_{J \in T_w^{n, \delta}} |e_J^w\rangle \langle e_J^w|,$$

где

$$T_w^{n, \delta} = \{J : 2^{-n[\bar{H}_\pi(S_{(\cdot)})+\delta]} < \lambda_J^w < 2^{-n[\bar{H}_\pi(S_{(\cdot)})-\delta]}\}.$$

Опишем существенные свойства проектора P_w .

1. Согласно определению

$$P_w \leq S_w 2^{n[\bar{H}_\pi(S_{(\cdot)})+\delta]}. \quad (5.40)$$

2. Для $\varepsilon > 0$ и достаточно больших n выполняется неравенство

$$\mathbb{E} \operatorname{Tr} S_w (I - P_w) \leq \varepsilon, \quad (5.41)$$

где $\mathbb{E}$ — математическое ожидание, отвечающее распределению вероятностей

$$\mathbb{P}\{w = (x_1, \dots, x_n)\} = \pi_{x_1} \cdot \dots \cdot \pi_{x_n}. \quad (5.42)$$

Чтобы доказать второе свойство, рассмотрим последовательность независимых испытаний с исходами (x_l, j_l) , $l = 1, \dots, n$, где вероятность исхода (x, j) в каждом испытании равна $\pi_x \lambda_j^x$. Тогда

$$\mathbb{E} \operatorname{Tr} S_w (I - P_w) = \mathbb{P}\{J \in \overline{T_w^{n, \delta}}\}, \quad (5.43)$$

а это выражение стремится к 0 при $n \rightarrow \infty$ согласно закону больших чисел, см. задачу 4.4.1.

§ 5.6. Доказательство прямого утверждения теоремы кодирования

Согласно следствию 5.1.2 достаточно показать, что минимальная средняя вероятность ошибки $\bar{p}_e(n, 2^{nR})$ стремится к нулю при $n \rightarrow \infty$, если $R < C_\chi$.

Рассмотрим среднее состояние

$$\bar{S}_\pi = \sum_x \pi_x S_x$$

и типичный проектор $P = P^{n, \delta}$ состояния $\bar{S}_\pi^{\otimes n}$, определенный в предыдущем параграфе. Для заданного набора кодовых слов $W = \{\omega^{(1)}, \dots, \omega^{(N)}\}$ мы можем также построить условно типичные проекторы $P_{\omega^{(j)}}$, $j = 1, \dots, N$. Теперь мы введем специальную субоптимальную наблюдаемую M . Классическая теорема кодирования Шеннона (теорема 4.4.1) отвечает случаю диагональных операторов плотности S_x с условными вероятностями $p(y|x)$ на диагонали. Проектор P является квантовым аналогом индикатора подмножества всех δ -типичных слов на выходе, а $P_{\omega^{(j)}}$ играет такую же роль для подмножества условно типичных слов на выходе при данном слове $\omega^{(j)}$ на входе. Однако эти проекторы не обязаны коммутировать, что делает невозможным непосредственное обобщение областей принятия решений (4.41) и соответствующее рассуждение в духе теории множеств. Поэтому мы вводим следующую наблюдаемую M в $\mathcal{H}^{\otimes n}$:

$$M_j = \left(\sum_{l=1}^N PP_{\omega^{(l)}}P \right)^{-1/2} PP_{\omega^{(j)}}P \left(\sum_{l=1}^N PP_{\omega^{(l)}}P \right)^{-1/2}, \quad j = 1, \dots, N. \quad (5.44)$$

Нормировка посредством квадратного корня необходима, поскольку сумма операторов $PP_{\omega^{(j)}}P$ может быть не равна единичному оператору, а введение $PP_{\omega^{(j)}}P$ вместо $P_{\omega^{(j)}}$ играет роль пересечения с подмножеством всех

типичных слов в формуле (4.42). Оператор $\left(\sum_{l=1}^N PP_{\omega^{(l)}}P \right)^{-1/2}$ следует

понимать как *обобщенный обратный* к оператору $\left(\sum_{l=1}^N PP_{\omega^{(l)}}P \right)^{1/2}$, который равен 0 на нулевом подпространстве этого оператора, содержащем в себе область значений проектора $I - P$. Обозначая через $\hat{P}$ проектор на область значений оператора $\sum_{l=1}^N PP_{\omega^{(l)}}P$, получаем

$$PP_{\omega^{(l)}}P \leq \hat{P} \leq P, \quad l = 1, \dots, N. \quad (5.45)$$

Для упрощения обозначений мы в дальнейшем будем нумеровать слова индексом ω , опуская j, l . Вводя обозначение

$$A_\omega = P_\omega P \left(\sum_{\omega'=1}^N P P_{\omega'} P \right)^{-1/2}$$

и используя некоммутативный аналог неравенства Коши—Буняковского (2.25) при $X = A_\omega$, $Y = I$, получаем

$$\begin{aligned} \bar{P}_e(W, M) &= \frac{1}{N} \sum_{\omega=1}^N [1 - \text{Tr } S_\omega A_\omega^* A_\omega] \leqslant \\ &\leqslant \frac{1}{N} \sum_{\omega=1}^N [1 - |\text{Tr } S_\omega A_\omega|^2] \leqslant \frac{2}{N} \sum_{\omega=1}^N [1 - \text{Tr } S_\omega A_\omega], \end{aligned}$$

где $\text{Tr } S_\omega A_\omega = \text{Tr } S_\omega P_\omega P \left(\sum_{\omega'=1}^N P P_{\omega'} P \right)^{-1/2}$ является вещественным числом, заключенным между 0 и 1. Применяя неравенство

$$-2x^{-1/2} \leqslant -3 + x, \quad x > 0,$$

и учитывая неравенство (5.45), получаем

$$-2 \left(\sum_{\omega'=1}^N P P_{\omega'} P \right)^{-1/2} \leqslant -3\hat{P} + \sum_{\omega'=1}^N P P_{\omega'} P \leqslant -3P P_\omega P + \sum_{\omega'=1}^N P P_{\omega'} P.$$

Поэтому

$$\begin{aligned} \bar{P}_e(W, M) &\leqslant \frac{1}{N} \sum_{\omega=1}^N \left[2 \text{Tr } S_\omega - 3 \text{Tr } S_\omega P_\omega P P_\omega P + \sum_{\omega'=1}^N \text{Tr } S_\omega P_\omega P P_{\omega'} P \right] = \\ &= \frac{1}{N} \sum_{\omega=1}^N \left[2 \text{Tr } S_\omega (I - P_\omega P P_\omega P) + \sum_{\omega': \omega' \neq \omega} \text{Tr } S_\omega P_\omega P P_{\omega'} P \right]. \end{aligned}$$

Принимая во внимание оценку

$$\begin{aligned} \text{Tr } S_\omega (I - P_\omega P P_\omega P) &= \text{Tr } S_\omega (I - P_\omega) P P_\omega P + \text{Tr } S_\omega (I - P) P_\omega - \\ &- \text{Tr } S_\omega (I - P) P_\omega (I - P) + \text{Tr } S_\omega (I - P_\omega) P + \text{Tr } S_\omega (I - P) \leqslant \\ &\leqslant 2[\text{Tr } S_\omega (I - P_\omega) + \text{Tr } S_\omega (I - P)], \end{aligned}$$

где было использовано неравенство (1.13), получаем

$$\begin{aligned} \bar{P}_e(W, M) &\leq \\ &\leq \frac{1}{N} \sum_{w=1}^N \left\{ 4 \operatorname{Tr} S_w (I - P) + 4 \operatorname{Tr} S_w (I - P_w) + \sum_{w': w' \neq w} \operatorname{Tr} P S_w P P_{w'} \right\}. \end{aligned} \quad (5.46)$$

Это основная оценка, аналогичная неравенству (4.43) в классическом случае.

Теперь применим процедуру случайного кодирования, вновь предполагая, что слова $w^{(1)}, \dots, w^{(N)}$ выбираются случайным образом, независимо друг от друга, с распределением вероятностей (5.42) для каждого слова, где π — оптимальное распределение, для которого

$$H(\bar{S}_\pi) - \bar{H}_\pi(S_{(\cdot)}) = C_\chi.$$

Тогда

$$\mathbb{E} S_w = \sum_{x_1 \dots x_n} \pi_{x_1} \dots \pi_{x_n} S_{x_1} \otimes \dots \otimes S_{x_n} = \bar{S}_\pi^{\otimes n}.$$

Усредняя неравенство (5.46) и учитывая независимость операторов $S_w, P_{w'}$, получаем

$$\begin{aligned} \mathbb{E} \bar{P}_e(W, M) &\leq \\ &\leq 4 \operatorname{Tr} \bar{S}_\pi^{\otimes n} (I - P) + 4 \mathbb{E} \operatorname{Tr} S_w (I - P_w) + (N - 1) \operatorname{Tr} \bar{S}_\pi^{\otimes n} P \mathbb{E} P_{w'}. \end{aligned} \quad (5.47)$$

Используя неравенства (5.36), (5.41), выражающие типичность проекторов P, P_w , и неравенство (1.18), получаем

$$\mathbb{E} \bar{P}_e(W, M) \leq 8\varepsilon + (N - 1) \|\bar{S}_\pi^{\otimes n} P\| \operatorname{Tr} \mathbb{E} P_{w'}$$

для $n \geq n(\pi, \varepsilon, \delta)$. Согласно свойству (5.39) проектора P справедлива оценка

$$\|\bar{S}_\pi^{\otimes n} P\| \leq 2^{-n[H(\bar{S}_\pi) - \delta]},$$

а по свойству 1 проектора P_w имеем

$$\operatorname{Tr} \mathbb{E} P_{w'} = \mathbb{E} \operatorname{Tr} P_{w'} \leq \mathbb{E} \operatorname{Tr} S_{w'} \cdot 2^{n[\bar{H}_\pi(S_{(\cdot)}) + \delta]} = 2^{n[\bar{H}_\pi(S_{(\cdot)}) + \delta]}.$$

Вспоминая, что $H(\bar{S}_\pi) - \bar{H}_\pi(S_{(\cdot)}) = C_\chi$, получаем

$$\bar{p}_e(n, N) \leq \mathbb{E} \bar{P}_e(W, M) \leq 8\varepsilon + N 2^{-n[C_\chi - 2\delta]}.$$

Таким образом, если $R \leq C_\chi - 3\delta$, то

$$\bar{p}_e(n, 2^{nR}) \leq 8\varepsilon + 2^{-n\delta},$$

откуда и следует прямое утверждение теоремы кодирования. $\square$

Небольшая модификация этого рассуждения позволяет доказать экспоненциальное убывание средней вероятности ошибки. А именно, найдется такое $\beta > 0$, что

$$E\bar{P}_e(W, M) \leq 2^{-n\beta}. \quad (5.48)$$

В самом деле, мы уже получили подобную оценку для последнего слагаемого в формуле (5.47) при условии, что $N \leq 2^{n[C_X - 3\delta]}$, так что остается доказать ее для первых двух слагаемых. Но это получается применением неравенства (4.11) к вероятностям больших отклонений (5.37), (5.43).

§ 5.7. Функция надежности для канала с чистыми состояниями

В классическом случае чистые сигнальные состояния соответствуют вырожденным распределениям вероятностей и теорема кодирования очевидным образом дает максимальное значение пропускной способности $\log |\mathcal{X}|$. Однако для чистых квантовых неортогональных состояний утверждение теоремы кодирования остается нетривиальным, хотя ситуация все же упрощается, что позволяет получить более сильный результат. Здесь мы дадим другое доказательство прямого утверждения теоремы кодирования в случае чистых состояний $S_x = |\psi_x\rangle\langle\psi_x|$, которое не использует понятия типичного проектора, однако благодаря более тонкому анализу дает оценку, позволяющую количественно оценить показатель экспоненциальной скорости сходимости вероятности ошибки.

Теорема 5.7.1. *При $R < C_X$ имеет место оценка*

$$\bar{p}_e(n, 2^{nR}) \leq 2 \cdot 2^{-nE(R)},$$

где

$$E(R) = \max_{0 \leq r \leq 1} [-Rr + \max_{\pi} (-\log \text{Tr } \bar{S}_{\pi}^{1+r})] > 0. \quad (5.49)$$

Функция $E(R)$ дает нижнюю границу для так называемой *функции надежности* канала, характеризующей экспоненциальную скорость сходимости к нулю вероятности ошибки $\bar{p}_e(n, 2^{nR})$ при $n \rightarrow \infty$.

Доказательство. Рассмотрим подпространство пространства $\mathcal{H}^{\otimes n}$, порожденное кодовыми векторами $\psi_{w^{(1)}}, \dots, \psi_{w^{(N)}}$. Как было показано в п. 2.2.4, мы можем использовать оператор Грама $G = \sum_j |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}|$, чтобы построить переполненную систему

$$|\hat{\psi}_j\rangle = G^{-\frac{1}{2}} |\psi_{w^{(j)}}\rangle, \quad j = 1, \dots, N,$$

а значит, и наблюдаемую M с компонентами

$$M_j = |\hat{\psi}_j\rangle\langle\hat{\psi}_j|, \quad j = 1, \dots, N, \quad (5.50)$$

которая может быть продолжена на все пространство $\mathcal{H}^{\otimes n}$ путем присоединения проектора M_0 на ортогональное дополнение к $\psi_{w^{(1)}}, \dots, \psi_{w^{(N)}}$. Это будет нашим субоптимальным декодированием для составного канала. Заметим, что оно отличается от наблюдаемой (5.44) отсутствием типичного проектора P (тогда как условно типичные проекторы в случае чистых состояний суть $P_w = |\psi_w\rangle\langle\psi_w|$). Так мы получаем оценку сверху для средней вероятности ошибки через оператор Грама кодовых векторов:

$$\begin{aligned} \bar{P}_e(W, M) &= \frac{1}{N} \sum_{j=1}^N (1 - \langle \hat{\psi}_j | G^{\frac{1}{2}} | \hat{\psi}_j \rangle)^2 \leq \\ &\leq \frac{2}{N} \sum_{j=1}^N (1 - \langle \hat{\psi}_j | G^{\frac{1}{2}} | \hat{\psi}_j \rangle) = \frac{2}{N} (N - \text{Tr } G^{\frac{1}{2}}) \end{aligned} \quad (5.51)$$

Предполагая, что кодовые слова $\{w^{(j)}\}$ выбираются случайно, независимо и с распределением (5.42), получаем

$$\mathbb{E} \bar{P}_e(W, M) \leq \frac{2}{N} (N - \mathbb{E} \text{Tr } G^{\frac{1}{2}}). \quad (5.52)$$

Используя неравенство

$$-2x^{\frac{1}{2}} \leq x^2 - 3x, \quad x \geq 0, \quad (5.53)$$

в сочетании с очевидным неравенством $-2x^{\frac{1}{2}} \leq 0$, получаем оценку

$$-2G^{\frac{1}{2}} \leq \begin{cases} G^2 - 3G, \\ 0. \end{cases} \quad (5.54)$$

Математическое ожидание оператора Грама равно

$$\begin{aligned} \mathbb{E} G &= \mathbb{E} \sum_{j=1}^N |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}| = N \mathbb{E} |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}| = \\ &= N \sum_{x_1 \dots x_n} \pi_{x_1} \dots \pi_{x_n} (|\psi_{x_1}\rangle \otimes \dots \otimes |\psi_{x_n}\rangle) (\langle\psi_{x_1}| \otimes \dots \otimes \langle\psi_{x_n}|) = \\ &= N \left[\sum_x \pi_x |\psi_x\rangle\langle\psi_x| \right]^{\otimes n} = N \bar{S}_{\pi}^{\otimes n}. \end{aligned} \quad (5.55)$$

Аналогично

$$\begin{aligned} \mathbb{E} (G^2 - G) &= \mathbb{E} \left(\sum_{j,k=1}^N |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}| |\psi_{w^{(k)}}\rangle\langle\psi_{w^{(k)}}| - \sum_{j=1}^N |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}| \right) = \\ &= \mathbb{E} \left(\sum_{j \neq k} |\psi_{w^{(j)}}\rangle\langle\psi_{w^{(j)}}| |\psi_{w^{(k)}}\rangle\langle\psi_{w^{(k)}}| \right) = N(N-1) (\bar{S}_{\pi}^{\otimes n})^2, \end{aligned} \quad (5.56)$$

так что в сочетании с неравенством (5.54) получаем

$$-2\mathbb{E}G^{\frac{1}{2}} \leq \begin{cases} N(N-1)(\bar{S}_{\pi}^{\otimes n})^2 - 2N\bar{S}_{\pi}^{\otimes n}, \\ 0. \end{cases} \quad (5.57)$$

Пусть $\{|e_J\rangle\}$ — ортонормированный базис из собственных векторов и $\{\lambda_J\}$ — соответствующие собственные значения оператора $\bar{S}_{\pi}^{\otimes n}$. Тогда

$$-2\langle e_J | \mathbb{E}G^{-\frac{1}{2}} | e_J \rangle \leq \begin{cases} N(N-1)\lambda_J^2 - 2N\lambda_J, \\ 0, \end{cases} \quad (5.58)$$

и, используя неравенства $\min(a, b) \leq a^r b^{1-r}$ и $2^{1-r} \leq 2$ при $0 \leq r \leq 1$, получаем

$$N\lambda_J \min[(N-1)\lambda_J, 2] - 2N\lambda_J \leq 2N(N-1)^r \lambda_J^{1+r} - 2N\lambda_J, \quad (5.59)$$

откуда следует, что

$$-2\mathbb{E} \operatorname{Tr} G^{\frac{1}{2}} \leq -2N + 2N(N-1)^r \operatorname{Tr} (\bar{S}_{\pi}^{\otimes n})^{1+r}.$$

Возвращаясь к неравенству (5.52), мы можем оценить среднюю вероятность ошибки, минимизированную по всем кодам:

$$\bar{p}_e(n, N) \leq 2N^r (\operatorname{Tr} \bar{S}_{\pi}^{1+r})^n$$

для любого $0 \leq r \leq 1$. Полагая $N = 2^{nR}$, получаем

$$\bar{p}_e(n, 2^{nR}) \leq 2 \cdot 2^{n(Rr + \log \operatorname{Tr} \bar{S}_{\pi}^{1+r})}. \quad (5.60)$$

Теперь можно использовать свободу в выборе параметров r и π . Заметим, что $-\log \operatorname{Tr} \bar{S}_{\pi}^{1+r}$ является вогнутой функцией от r , что доказывается вычислением второй производной (**задача**). Также справедливо равенство

$$\left. \frac{d}{dr} \right|_{r=0} (-\log \operatorname{Tr} \bar{S}_{\pi}^{1+r}) = -\operatorname{Tr} \bar{S}_{\pi} \log \bar{S}_{\pi} = H(\bar{S}_{\pi}). \quad (5.61)$$

Возьмем в качестве π распределение, для которого $H(\bar{S}_{\pi}) = C_{\chi}$. Тогда при $R < C_{\chi}$ имеем $\bar{p}_e(n, 2^{nR}) \leq 2 \cdot 2^{-nE(R)}$, где $E(R)$ дается выражением (5.49). $\square$

§ 5.8. Комментарии

1. Проблема определения пропускной способности квантового канала связи сформировалась в 1960-е годы и восходит к более ранним классическим трудам Габора и Бриллюэна, в которых был поставлен

вопрос о квантовомеханических пределах точности и скорости передачи информации (см. книги А. А. Курикси [14], В. В. Митюгова [19] и обзор Кейвса и Драммонда [68]). Эти работы заложили физические основы и подняли проблему адекватного математического рассмотрения круга вопросов, связанного с классической пропускной способностью квантовых каналов.

2. Доказательство теоремы 5.3.1, включающее критерий достижимости верхней границы и опирающееся на сравнение свойств выпуклости величин в неравенстве (5.15), было дано А. С. Холево; см. [34].

3. Детальное сравнение величин C_1 , C_X для различных каналов проведено в работе Хирота и др. [110].

Сильное обращение

$$\lim_{n \rightarrow \infty} \bar{p}_e(n, 2^{nR}) = 1 \quad \text{при } R \geq C_X$$

получено в работе Огава и Нагаока, см. [90].

Формула (5.35) вытекает из работы Л. Б. Левитина [120], в которой автор нашел максимум величины $\mathcal{I}_1(\pi, M)$ по четким наблюдаемым с двумя значениями, и из работы Шора [144]. В последней работе было показано, что в данном случае достаточно ограничиться такими наблюдаемыми и что $\max_M \mathcal{I}(\pi, M)$ является вогнутой симметричной функцией от π , откуда вытекает, что оптимальное распределение является равномерным.

Канал с тремя чистыми состояниями был введен в работе А. С. Холево [33], где было показано, что для равномерного распределения π максимум $\max_M \mathcal{I}(\pi, M) = \log(3/2) \approx 0,585$ бит по всем наблюдаемым строго

больше максимума по четким наблюдаемым, равного $\log(\sqrt{3}/\sqrt[3]{2}) \approx 0,459$ бит. Полное исследование проблемы максимизации величины $\mathcal{I}_1(\pi, M)$ для произвольного симметричного семейства чистых состояний в двумерном пространстве дано в работе Сасаки, Барнета, Джоза, Осаки и Хирота [134], где также была предложена экспериментальная реализация оптимальной процедуры измерения. Детальный анализ канала с тремя линейно независимыми чистыми состояниями в вещественном трехмерном пространстве проведен в работе Шора [144], где, в частности, показано, что информационно-оптимальная наблюдаемая в этой задаче имеет в общем случае 6 значений (т. е. максимальное количество, допускаемое предложением 5.3.1 в случае $d = 3$).

4. Идея сжатия данных в квантовой теории информации принадлежит Шумахеру; доказательство теоремы 5.5.1 дано в совместной работе Шумахера и Джоза [108]. Обзор результатов различных авторов, относящихся к значительно более сложной проблеме сжатия для квантового источника со смешанными состояниями, имеется в книге Хайаши [90].

5. Доказательство прямой теоремы кодирования для произвольного s - q -канала дано А. С. Холево (см. [98]), а также Шумахером и Вестморлендом (см. [135]). Другое доказательство в духе подхода Чисара и Кёрнера (см. [44]) к классическим теоремам кодирования предложено впоследствии Винтером в работе [156]. Этому предшествовало рассмотрение канала с чистыми состояниями в работе Джоза, Шумахера, Вестморленда, Вуттерса и Хаусладена (см. [89]). Следует отметить, что еще до этого шенноновский метод случайного кодирования для квантового канала с чистыми почти ортогональными состояниями был применен Р. Л. Стратоновичем и А. Г. Ванцяном (см. [28]), которые на основании первого приближения для минимальной вероятности ошибки пришли к выводу, что этот метод позволяет получить лишь значение

$$\tilde{C} = -\log \min_{\pi} \text{Tr } \bar{S}_{\pi}^2 < C. \quad (5.62)$$

На самом деле надлежащим образом примененный метод случайного кодирования в случае канала с произвольными чистыми состояниями позволил получить даже оценку функции надежности в духе классических результатов Галлагера, изложенных в книге [5]; см. работу М. В. Бурнашева и А. С. Холево [1], причем величина (5.62) оказалась равной так называемой урезанной пропускной способности (cut-off rate). В работе [1] также высказана до сих пор не доказанная гипотеза о функции надежности для общего канала со смешанными состояниями. В этом случае, как и в ряде других, рассмотрение смешанных состояний переводит проблему на качественно более высокий уровень сложности.

ЧАСТЬ III

ГЛАВА 6

Квантовые эволюции и каналы

§ 6.1. Эволюции квантовой системы

В этом параграфе понятие квантового канала будет рассмотрено с общей точки зрения. Как мы видели в гл. 4, классический канал полностью определяется переходной матрицей вероятностей:

$$\mathcal{X} \xrightarrow{p(y|x)} \mathcal{Y}.$$

Такой канал описывает аффинное преобразование $p_x \rightarrow p'_y = \sum_x p(y|x) p_x$ классических состояний (распределений вероятностей) $p = \{p_x\}$ на некотором входном алфавите $\mathcal{X}$ в классические состояния $p' = \{p'_y\}$ на выходном алфавите $\mathcal{Y}$. По аналогии в квантовом случае мы сначала рассмотрим аффинные отображения, которые переводят операторы плотности в операторы плотности $\Phi: \mathfrak{S}(\mathcal{H}) \rightarrow \mathfrak{S}(\mathcal{H})$,

$$\Phi \left[\sum_j p_j S_j \right] = \sum_j p_j \Phi[S_j], \quad p_j \geq 0, \quad \sum_j p_j = 1, \quad S_j \in \mathfrak{S}(\mathcal{H}).$$

Задача 6.1.1. Докажите, что аффинное отображение Φ множества состояний $\mathfrak{S}(\mathcal{H})$ в себя единственным образом продолжается до отображения линейного пространства $\mathfrak{T}(\mathcal{H})$ со следующими свойствами:

- 1) Φ линейно: $\Phi[\sum_j c_j T_j] = \sum_j c_j \Phi[T_j]$, $c_j \in \mathbb{C}$;
- 2) Φ положительно: $T \in \mathfrak{T}(\mathcal{H})$, $T \geq 0 \Rightarrow \Phi[T] \geq 0$;
- 3) Φ сохраняет след: $\text{Tr } \Phi[T] = \text{Tr } T$, $T \in \mathfrak{T}(\mathcal{H})$.

Указание. Следуя доказательству теоремы 2.2.1, постройте линейное продолжение отображения Φ на $\mathfrak{T}(\mathcal{H})$; свойства 2, 3 доказываются непосредственной проверкой.

Определение 6.1.1. Для любого отображения $\Phi: \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{H})$, удовлетворяющего свойствам 1—3, *сопряженное отображение* $\Phi^*: \mathfrak{B}(\mathcal{H}) \rightarrow \mathfrak{B}(\mathcal{H})$ определяется формулой

$$\text{Tr } \Phi[T]X = \text{Tr } T\Phi^*[X], \quad T \in \mathfrak{T}(\mathcal{H}), \quad X \in \mathfrak{B}(\mathcal{H}). \quad (6.1)$$

Задача 6.1.2. Докажите, что свойства отображения Φ из задачи 6.1.1 равносильны следующим:

- 1) Φ^* линейно;
- 2) Φ^* положительно: $X \geq 0 \Rightarrow \Phi^*[X] \geq 0$;
- 3) Φ^* унитарно: $\Phi^*[I] = I$.

Отображение Φ описывает эволюцию квантовой системы в терминах состояний (картина Шрёдингера), в то время как отображение Φ^* — в терминах наблюдаемых (картина Гейзенберга).

Пример 6.1.1. Пусть U — унитарный оператор, тогда $\Phi[S] = USU^*$ является аффинным и взаимно однозначным отображением множества квантовых состояний $\mathfrak{S}(\mathcal{H})$ на себя, т. е. задает *обратимую* эволюцию. В картине Гейзенберга $\Phi^*[X] = U^*XU$.

Следующий результат характеризует все обратимые эволюции.

Теорема 6.1.1. Пусть Φ — аффинное взаимно однозначное отображение выпуклого множества квантовых состояний $\mathfrak{S}(\mathcal{H})$ на себя, тогда

$$\Phi[S] = USU^*, \quad S \in \mathfrak{S}(\mathcal{H}), \quad (6.2)$$

где U — унитарный или антиунитарный оператор.

В случае унитарного оператора продолжение Φ до линейного положительного отображения имеет тот же вид (6.2) для всех $S \in \mathfrak{T}(\mathcal{H})$. Антиунитарный оператор U характеризуется следующими свойствами:

- 1) $\|U\psi\| = \|\psi\|$, $\psi \in \mathcal{H}$;
- 2) $U(\sum c_j \psi_j) = \sum \bar{c}_j U\psi_j$.

Такой оператор всегда можно представить в виде $U = \tilde{U}\Lambda$, где $\tilde{U}$ — унитарный оператор, а $\Lambda = \Lambda^*$ — антиунитарный оператор комплексного сопряжения в некотором фиксированном базисе¹. Соответствующая ему эволюция состояний задается транспонированием матрицы плотности в этом базисе:

$$S^\top = \Lambda S \Lambda^*.$$

Учитывая, что в общем случае $T^* = \Lambda T^\top \Lambda^*$, получаем, что в случае антиунитарного оператора U линейное продолжение Φ дается формулой

$$\Phi[T] = UT^*U^*, \quad T \in \mathfrak{T}(\mathcal{H}). \quad (6.3)$$

Доказательство. Доказательство в случае q -бита ($\dim \mathcal{H} = 2$) дано в § 6.8; из него вытекает, что в общем случае сужение Φ на подмножество состояний, сосредоточенных на любом двумерном подпространстве $\mathcal{H}_2 \subset \mathcal{H}$, дается формулой (6.2), где U , однако, может зависеть от выбранного подпространства. Доказательство в общем случае состоит в том, чтобы, производя подходящие деформации этого подпространства,

¹ В физике операция комплексного сопряжения связана с обращением времени.

показать, что эта зависимость сводится к несущественному фазовому множителю.

Пусть $\psi_1, \psi_2 \in \mathcal{H}$. Поскольку аффинное взаимно однозначное отображение множества квантовых состояний на себя взаимно однозначно переводит крайние точки в крайние точки, мы получаем

$$\Phi[|\psi_j\rangle\langle\psi_j|] = |\varphi_j\rangle\langle\varphi_j|, \quad j = 1, 2.$$

Рассматривая двумерное подпространство $\mathcal{H}_2 \subset \mathcal{H}$, содержащее ψ_1, ψ_2 , и применяя упомянутый выше результат для q -бита, из формул (6.2), (6.3) получаем

$$\Phi[|\psi_1\rangle\langle\psi_2|] = z|\varphi_1\rangle\langle\varphi_2| \quad \text{либо} \quad z|\varphi_2\rangle\langle\varphi_1|, \quad (6.4)$$

где $|z| = 1$. Отсюда следует, что

$$|\langle\varphi_1|\varphi_2\rangle| = |\langle\psi_1|\psi_2\rangle|.$$

Пусть теперь $\{e_j, j = 1, \dots, d\}$ — ортонормированный базис в $\mathcal{H}$, тогда

$$\Phi[|e_j\rangle\langle e_j|] = |h_j\rangle\langle h_j|,$$

где $\{h_j\}$ — ортонормированный базис в $\mathcal{H}$. Из соотношения (6.4) следует, что

$$\Phi[|e_j\rangle\langle e_k|] = z_{jk}|h_j\rangle\langle h_k| \quad \text{либо} \quad z_{kj}|h_k\rangle\langle h_j|. \quad (6.5)$$

Если $\Phi[|e_1\rangle\langle e_2|] = z_{12}|h_1\rangle\langle h_2|$, но $\Phi[|e_1\rangle\langle e_3|] = z_{31}|h_3\rangle\langle h_1|$, то

$$\Phi[|e_1\rangle\langle e_2 + e_3|] = z_{12}|h_1\rangle\langle h_2| + z_{31}|h_3\rangle\langle h_1|$$

является оператором ранга 2, что противоречит равенству (6.4). Повторяя это рассуждение, получаем, что в формуле (6.5) для всех j, k имеет место одна и та же из двух альтернатив.

Рассмотрим вторую из них, когда

$$\Phi[|e_j\rangle\langle e_k|] = z_{kj}|h_k\rangle\langle h_j|,$$

тогда, полагая $\psi = e_1 + \dots + e_d$, получаем, что оператор

$$\Phi[|\psi\rangle\langle\psi|] = \sum_{j,k=1}^d z_{kj}|h_k\rangle\langle h_j|$$

является проектором ранга 1, поэтому $z_{kj} = a_k \bar{a}_j$, где $|a_j| = 1$ для всех j . Обозначая через U антиунитарный оператор, для которого $U|e_j\rangle = a_j h_j$, получаем формулу (6.3). Аналогично в случае первой альтернативы получаем $\Phi[T] = UTU^*$, где U — унитарный оператор. $\square$

§ 6.2. Вполне положительные отображения

Обобщая предыдущие рассуждения, рассмотрим линейное отображение Φ , действующее из $\mathfrak{T}(\mathcal{H}_1)$ в $\mathfrak{T}(\mathcal{H}_2)$, тогда сопряженное отображение Φ^* действует из $\mathfrak{B}(\mathcal{H}_2)$ в $\mathfrak{B}(\mathcal{H}_1)$.

Определение 6.2.1. Отображение Φ^* (Φ) называется *вполне положительным*, если выполнено одно из следующих эквивалентных условий:

- 1) отображение $\Phi^* \otimes \text{Id}_n$ положительно для всех $n = 1, 2, \dots$, где Id_n обозначает тождественное отображение в алгебре всех $(n \times n)$ -матриц $\mathfrak{B}_n$;
- 2) для любых конечных наборов векторов $\{\varphi_j\} \subset \mathcal{H}_2$, $\{\psi_j\} \subset \mathcal{H}_1$ выполнено неравенство

$$\sum_{j,k} \langle \varphi_j | \Phi[|\psi_j\rangle\langle\psi_k|] \varphi_k \rangle \geq 0.$$

Чтобы доказать эквивалентность этих условий, рассмотрим пространства $\mathcal{H}_i^{(n)}$, которые являются прямыми ортогональными суммами n копий $\mathcal{H}_i$, $i = 1, 2$, где n — количество векторов в наборах $\{\varphi_j\}$, $\{\psi_j\}$. Как мы уже видели в п. 3.1.1, $\mathcal{H}_i^{(n)}$ может быть отождествлено с пространством $\mathcal{H}_i \otimes \ell_n^2$. Таким образом, вводя обозначение

$$\varphi^{(n)} = \sum_{j=1}^n \bigoplus \varphi_j, \quad \psi^{(n)} = \sum_{j=1}^n \bigoplus \psi_j,$$

получаем

$$\sum_{j,k} \langle \varphi_j | \Phi[|\psi_j\rangle\langle\psi_k|] \varphi_k \rangle = \langle \psi^{(n)} | (\Phi^* \otimes \text{Id}_n) [|\varphi^{(n)}\rangle\langle\varphi^{(n)}|] |\psi^{(n)}\rangle,$$

откуда вытекает импликация $1) \Rightarrow 2)$. Обратно, любой положительный оператор $A^{(n)}$ в $\mathcal{H}_2^{(n)} \simeq \mathcal{H}_2 \otimes \ell_n^2$ может быть представлен в виде суммы положительных операторов $|\varphi^{(n)}\rangle\langle\varphi^{(n)}|$ ранга 1. Следовательно, из свойства 2, означающего положительность отображения $\Phi^* \otimes \text{Id}_n$ на таких операторах, вытекает свойство 1.

Задача 6.2.1. Докажите, что если отображение Φ удовлетворяет условию 1 при $n = 2$, то для него выполняется неравенство Кэдисона

$$\Phi^*[A]^* \Phi^*[A] \leq \|\Phi^*\| \Phi^*[A^*A], \quad (6.6)$$

где A — произвольный оператор.

Задача 6.2.2. Покажите, что для операции транспонирования в некотором базисе условие 1 нарушается уже при $n = 2$. *Указание.* Рассмотрите условие 2, где $\{\psi_j\}$ — базис, в котором происходит транспонирование.

Понятие вполне положительного отображения было введено Стайнс-прингом, который доказал важный результат, обобщающий теорему Наймарка. Мы получим уточнение этого результата в конечномерном случае.

Теорема 6.2.1. Для любого вполне положительного отображения $\Phi^*: \mathfrak{B}(\mathcal{H}_2) \rightarrow \mathfrak{B}(\mathcal{H}_1)$ найдутся гильбертово пространство $\mathcal{H}_0$ и оператор $V: \mathcal{H}_1 \rightarrow \mathcal{H}_2 \otimes \mathcal{H}_0$ такие, что

$$\Phi^*[X] = V^*(X \otimes I_0)V, \quad X \in \mathfrak{B}(\mathcal{H}_2). \quad (6.7)$$

Двойственным образом,

$$\Phi[S] = \text{Tr}_{\mathcal{H}_0} VSV^*, \quad S \in \mathfrak{T}(\mathcal{H}_1). \quad (6.8)$$

Отображение Φ^* унитарно, т. е. $\Phi^*[I_2] = I_1$ (отображение Φ сохраняет след), тогда и только тогда, когда оператор V изометричен.

Доказательство. Рассмотрим алгебраическое тензорное произведение $\mathcal{L} = \mathcal{H}_1 \otimes \mathfrak{B}(\mathcal{H}_2)$, порожденное элементами $\Psi = \psi \otimes X$, $\psi \in \mathcal{H}_1$, $X \in \mathfrak{B}(\mathcal{H}_2)$. Введем в $\mathcal{L}$ псевдоскалярное произведение с квадратом нормы

$$\left\| \sum_j \psi_j \otimes X_j \right\|^2 = \sum_{j,k} \langle \psi_j | \Phi^*[X_j^* X_k] | \psi_k \rangle.$$

Эта величина неотрицательна, так как блочный оператор

$$A^{(n)} = [X_j^* X_k]_{j,k=\overline{1,n}}$$

в $\mathcal{H}_2^{(n)}$ положителен. После факторизации по подпространству $\mathcal{L}_0$ элементов с нулевой нормой мы получим гильбертово пространство $\mathcal{K} = \mathcal{L}/\mathcal{L}_0$. Определим V и π соотношениями $V\psi = \psi \otimes I$ и $\pi[Y]\Psi = \pi[Y](\psi \otimes X) = \psi \otimes YX$. Нетрудно проверить, что эти определения выдерживают факторизацию. Тогда π — *-гомоморфизм алгебры $\mathfrak{B}(\mathcal{H}_2)$ в $\mathfrak{B}(\mathcal{K})$, т. е. линейное отображение, сохраняющее алгебраические операции и инволюцию:

$$\pi[XY] = \pi[X]\pi[Y], \quad \pi[X^*] = \pi[X]^*.$$

Отображение π унитарно, более того,

$$\langle \varphi | \Phi^*[X] | \psi \rangle = \langle \varphi \otimes I | \psi \otimes X \rangle = \langle \varphi | V^* \pi[X] V | \psi \rangle, \quad X \in \mathfrak{B}(\mathcal{H}_2),$$

т. е.

$$\Phi^*[X] = V^* \pi[X] V. \quad (6.9)$$

Однако согласно лемме 6.2.1 (см. ниже) любой унитарный $*$ -гомоморфизм алгебры $\mathfrak{B}(\mathcal{H})$ унитарно эквивалентен отображению $\pi[X] = X \otimes I_0$, где I_0 — единичный оператор в некотором гильбертовом пространстве $\mathcal{H}_0$, поэтому мы можем положить $\mathcal{K} = \mathcal{H}_2 \otimes \mathcal{H}_0$ и представление Стайнспринга (6.9) принимает вид (6.7).

Двойственное представление (6.8) вытекает из соотношения (6.7) и определения сопряженного отображения (6.1). $\square$

Лемма 6.2.1. Пусть π — унитарный $*$ -гомоморфизм алгебры $\mathfrak{B}(\mathcal{H})$ в алгебру $\mathfrak{B}(\mathcal{K})$, тогда найдутся гильбертово пространство $\mathcal{H}_0$ и изометричное отображение U пространства $\mathcal{K}$ на $\mathcal{H} \otimes \mathcal{H}_0$ такие, что

$$\pi[X] = U^*(X \otimes I_0)U, \quad X \in \mathfrak{B}(\mathcal{H}). \quad (6.10)$$

Доказательство. Выберем ортономированный базис $\{e_j, j = 1, \dots, d\}$ в $\mathcal{H}$ и рассмотрим матричные единицы $|e_j\rangle\langle e_k|$ и их образы

$$V_{jk} = \pi[|e_j\rangle\langle e_k|] \in \mathfrak{B}(\mathcal{K}).$$

Поскольку π — $*$ -гомоморфизм, операторы V_{jk} удовлетворяют тем же алгебраическим соотношениям, что и матричные единицы:

$$V_{jk}V_{lm} = \delta_{kl}V_{jm}, \quad V_{jk}^* = V_{kj}. \quad (6.11)$$

Рассмотрим подпространство $\mathcal{H}_0 = V_{11}\mathcal{K} \subseteq \mathcal{K}$ и определим отображение $U: \mathcal{K} \rightarrow \mathcal{H} \otimes \mathcal{H}_0$ соотношением

$$U\psi = \sum_j |e_j\rangle \otimes V_{1j}\psi.$$

(Заметим, что $V_{1j}\psi = V_{11}V_{1j}\psi \in \mathcal{H}_0$.) Тогда

$$\langle U\psi_1 | (X \otimes I_0) U\psi_2 \rangle = \sum_{j,k} \langle e_j | X e_k \rangle \langle V_{1j}\psi_1 | V_{1k}\psi_2 \rangle. \quad (6.12)$$

Поскольку в силу соотношений (6.11) выполняется равенство

$$\langle V_{1j}\psi_1 | V_{1k}\psi_2 \rangle = \langle \psi_1 | V_{jk}\psi_2 \rangle = \langle \psi_1 | \pi[|e_j\rangle\langle e_k|] \psi_2 \rangle,$$

правая часть соотношения (6.12) равна $\sum_{j,k} \langle e_j | X e_k \rangle \langle \psi_1 | \pi[|e_j\rangle\langle e_k|] \psi_2 \rangle = \langle \psi_1 | \pi[X] \psi_2 \rangle$. Отсюда следует равенство (6.10). Полагая $X = I$ и используя унитарность гомоморфизма π , получаем, что U — изометричное отображение $\mathcal{K}$ в $\mathcal{H} \otimes \mathcal{H}_0$.

Задача 6.2.3. Покажите, что образ пространства $\mathcal{K}$ при отображении U совпадает с $\mathcal{H} \otimes \mathcal{H}_0$. $\square$

Представление Стайнспринга не единственно. Представление, для которого размерность $\dim \mathcal{H}_0$ минимальна, называется *минимальным*.

Теорема 6.2.2. *Пусть*

$$\Phi^*[X] = \tilde{V}^*(X \otimes \tilde{I}_0)\tilde{V}, \quad X \in \mathfrak{B}(\mathcal{H}_2), \quad (6.13)$$

— *другое представление* ($\tilde{I}_0$ — *единичный оператор в пространстве* $\tilde{\mathcal{H}}_0$). *Тогда существует частичная изометрия* W_0 *из* $\mathcal{H}_0$ *в* $\tilde{\mathcal{H}}_0$ *такая, что*

$$(I_2 \otimes W_0)V = \tilde{V}; \quad (6.14)$$

если оба представления минимальны, то W_0 *изометрично отображает* $\mathcal{H}_0$ *на* $\tilde{\mathcal{H}}_0$.

Доказательство. Для представления (6.7) рассмотрим подпространство

$$\mathcal{M} = \{(X \otimes I_0)V\psi : \psi \in \mathcal{H}_1, X \in \mathfrak{B}(\mathcal{H}_2)\} \subset \mathcal{K} = \mathcal{H}_2 \otimes \mathcal{H}_0.$$

Пространство $\mathcal{M}$ инвариантно относительно умножения на операторы вида $Y \otimes I_0$, следовательно, оно имеет вид $\mathcal{M} = \mathcal{H}_2 \otimes \mathcal{M}_0$, $\mathcal{M}_0 \subseteq \mathcal{H}_0$. Для минимального представления имеем $\mathcal{M}_0 = \mathcal{H}_0$, поскольку в противном случае найдется собственное подпространство.

Рассмотрим аналогичное подпространство $\tilde{\mathcal{M}} = \mathcal{H}_2 \otimes \tilde{\mathcal{M}}_0$ пространства $\tilde{\mathcal{K}} = \mathcal{H}_2 \otimes \tilde{\mathcal{H}}_0$ для другого представления (6.13). Определим оператор W , действующий из $\mathcal{M}$ в $\tilde{\mathcal{M}}$, равенством

$$W(X \otimes I_0)V\psi = (X \otimes \tilde{I}_0)\tilde{V}\psi. \quad (6.15)$$

Согласно соотношениям (6.7), (6.13) нормы векторов и их образов при отображении W равны $\langle \psi | \Phi[X^*X] | \psi \rangle$, поэтому оператор W изометричен.

Из соотношения (6.15) получаем, что для всех $Y \in \mathfrak{B}(\mathcal{H}_2)$ справедливо равенство

$$W(YX \otimes I_0)V\psi = (Y \otimes \tilde{I}_0)W(X \otimes \tilde{I}_0)\tilde{V}\psi$$

и, следовательно,

$$W(Y \otimes I_0) = (Y \otimes \tilde{I}_0)W \quad (6.16)$$

на $\mathcal{M}$. Продолжая оператор W на $\mathcal{K}$, полагая его равным нулю на ортогональном дополнении к $\mathcal{M}$, получаем, что соотношение (6.16) выполнено на $\mathcal{K}$. Отсюда следует, что $W = I_2 \otimes W_0$, где W_0 изометрично отображает $\mathcal{M}_0$ на $\tilde{\mathcal{M}}_0$. Из соотношения (6.15) следует равенство (6.14). $\square$

Следствие 6.2.1 (представление Крауса). *Отображение* Φ^* *вполне положительно тогда и только тогда, когда оно может быть*

представлено в виде

$$\Phi^*[X] = \sum_k V_k^* X V_k, \quad X \in \mathfrak{B}(\mathcal{H}_2), \quad (6.17)$$

где $V_k: \mathcal{H}_1 \rightarrow \mathcal{H}_2$, или, двойственным образом,

$$\Phi[T] = \sum_k V_k T V_k^*, \quad T \in \mathfrak{T}(\mathcal{H}_1). \quad (6.18)$$

Отображение Φ^* унитарно (Φ сохраняет след) тогда и только тогда, когда

$$\sum V_k^* V_k = I. \quad (6.19)$$

Доказательство. Полагая $I_0 = \sum |e_j^0\rangle\langle e_j^0|$, где e_j^0 — ортонормированный базис в $\mathcal{H}_0$, рассмотрим операторы V_j , действующие из $\mathcal{H}_1$ в $\mathcal{H}_2$, которые определяются формулой

$$\langle \varphi | V_j \psi \rangle = \langle \varphi \otimes e_j^0 | V \psi \rangle, \quad \varphi \in \mathcal{H}_2, \psi \in \mathcal{H}_1. \quad (6.20)$$

Для операторов, определяемых формулой (6.20), мы будем иногда использовать обозначение $V_j = \langle e_j^0 | V$. Представление (6.17) следует тогда из формулы (6.7). $\square$

Как и представление Стайнспринга, представление Крауса не единственно. Представление Крауса с минимальным количеством ненулевых компонент называется *минимальным*.

Задача 6.2.4. Опираясь на теорему 6.2.2, покажите, что для любых двух представлений Крауса вполне положительного отображения Φ с операторами $V_j, \tilde{V}_k$ найдется прямоугольная частично изометрическая матрица $[u_{kj}]$ такая, что $\tilde{V}_k = \sum_j u_{kj} V_j$. Если оба представления минимальны, то эта матрица унитарна.

Задача 6.2.5. Пусть $M = \{M_x\}$ — наблюдаемая и

$$M_x = V^* E_x V = \tilde{V}^* \tilde{E}_x \tilde{V} \quad (6.21)$$

— два расширения Наймарка для M в пространствах $\mathcal{K}, \tilde{\mathcal{K}}$. Докажите, что тогда найдется частичная изометрия $W: \mathcal{K} \rightarrow \tilde{\mathcal{K}}$ такая, что

$$WV = \tilde{V}, \quad WE_x = \tilde{E}_x W,$$

причем если расширения минимальны в смысле размерностей пространств $\mathcal{K}$ и $\tilde{\mathcal{K}}$, то W — изометрическое отображение $\mathcal{K}$ на $\tilde{\mathcal{K}}$.

§ 6.3. Определение канала

Дадим физическую интерпретацию свойства полной положительности. Рассмотрим (вообще говоря, необратимую) эволюцию открытой системы, взаимодействующей с окружением (см. рис. 6.1). Пусть $\mathcal{H}$ — гильбертово

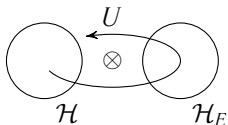


Рис. 6.1. Открытая квантовая система

пространство системы, $\mathcal{H}_E$ — пространство окружения, и пусть S_E — начальное состояние окружения. Предположим, что обратимая эволюция, описывающая взаимодействие системы с окружением, задается унитарным оператором U . Тогда эволюция системы дается формулой

$$\Phi[S] = \text{Tr}_{\mathcal{H}_E} U(S \otimes S_E)U^*. \quad (6.22)$$

Теорема 6.3.1. *Всякое вполне положительное сохраняющее след отображение Φ , для которого $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}$, может быть расширено до эволюции открытой системы, взаимодействующей с окружением, так что выполнено соотношение (6.22).*

Доказательство. Рассмотрим пространство $\mathcal{H}_E$ N -мерных векторов, где N — количество компонент в представлении Крауса для Φ . Пространство $\mathcal{H} \otimes \mathcal{H}_E$ может быть представлено как прямая сумма N копий пространства $\mathcal{H}$, т. е. как пространство вектор-столбцов $[\psi_1, \dots, \psi_N]^T$, $\psi_j \in \mathcal{H}$; операторы в этом пространстве суть блочные матрицы $[X_{jk}]_{j,k=1,\dots,N}$, $X_{jk} \in \mathfrak{B}(\mathcal{H})$. Рассмотрим вектор $|\psi_E\rangle = [1, 0, \dots, 0]^T$, тогда

$$S \otimes |\psi_E\rangle\langle\psi_E| = \begin{bmatrix} S & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{bmatrix}.$$

Введем оператор

$$U = \begin{bmatrix} V_1 & \dots & \dots \\ \dots & \dots & \dots \\ V_N & \dots & \dots \end{bmatrix}, \quad (6.23)$$

где первый столбец состоит из операторов $V_1, \dots, V_N$, а остальные столбцы могут быть выбраны таким образом, что оператор будет унитарным; возможность такого выбора вытекает из соотношения (6.19). Имеем

$$U(S \otimes |\psi_E\rangle\langle\psi_E|)U^* = [V_j S V_k^*]_{j,k=1,\dots,N}.$$

Частичный след в $\mathcal{H} \otimes \mathcal{H}_E$ по пространству $\mathcal{H}_E$ есть сумма диагональных элементов матрицы, что соответствует представлению Крауса для отображения Φ . $\square$

Предыдущие рассуждения мотивируют следующее определение. Будем обозначать систему на входе канала через A , а систему на выходе через B .

Определение 6.3.1. *Каналом* в картине Шрёдингера называется линейное вполне положительное сохраняющее след отображение $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$. Двойственным образом, каналом в картине Гейзенберга называется линейное вполне положительное унитарное отображение $\Phi^*: \mathfrak{B}(\mathcal{H}_B) \rightarrow \mathfrak{B}(\mathcal{H}_A)$.

Канал Φ называется *бистохастическим*, если он отображает хаотическое состояние в $\mathcal{H}_A$ в хаотическое состояние в $\mathcal{H}_B$, $\Phi[I_A/d_A] = I_B/d_B$. Если размерности входной и выходной систем совпадают, т. е. $d_A = d_B$, то бистохастический канал Φ является унитарным. В этом случае Φ^* обладает также свойством сохранения следа, и как Φ , так и Φ^* являются каналами в картинах Шрёдингера и Гейзенберга.

Пусть $S = S_A$ — входное состояние канала Φ , и пусть $\mathcal{L} = \text{supp } S$ — носитель оператора плотности S . Рассмотрим очищение $S_{AR} = |\psi_{AR}\rangle\langle\psi_{AR}|$ состояния S_A , где R обозначает очищающую систему и

$$|\psi_{AR}\rangle = \sum_j \sqrt{\lambda_j} |e_j\rangle \otimes |h_j\rangle, \quad \lambda_j > 0, \quad e_j \in \mathcal{L},$$

см. (3.9). Обозначим через Id_R тождественное отображение в $\mathfrak{T}(\mathcal{H}_R)$, тогда тензорное произведение $\Phi \otimes \text{Id}_R$ описывает канал, действующий из AR в BR , причем R не изменяется. В связи с этим R называется также *эталонной* системой. Выходным состоянием канала является

$$(\Phi \otimes \text{Id}_R)[S_{AR}] = S_{BR}. \quad (6.24)$$

Ввиду того что состояние S_{AR} в общем случае является сцепленным, такую операцию иногда называют «передачей сцепленности».

Предложение 6.3.1. *Состояние S_{BR} единственным образом определяет ограничение $\Phi_{\mathcal{L}}$ канала Φ на состояния $\tilde{S}$, $\text{supp } \tilde{S} \subset \mathcal{L}$. В частности, если состояние S_A невырожденное, то S_{BR} единственным образом определяет канал Φ .*

Доказательство. Имеем

$$(\Phi \otimes \text{Id}_R)[S_{AR}] = \sum_{j,k} \sqrt{\lambda_j} \sqrt{\lambda_k} \Phi[|e_j\rangle\langle e_k|] \otimes |h_j\rangle\langle h_k|. \quad (6.25)$$

Набор операторов $\Phi[|e_j\rangle\langle e_k|]$ единственным образом определяет $\Phi_{\mathcal{L}}$, откуда и следует утверждение. $\square$

В частности, взяв максимально сцепленное состояние S_{AR} , для которого $\lambda_j = 1/d$, $j = 1, \dots, d$, из соотношения (6.25) получаем

$$\Phi[S] = d \operatorname{Tr}_R S_{BR} (I_B \otimes S_R^\top), \quad (6.26)$$

где $S_R^\top = \sum_{j,k} \langle e_k | S | e_j \rangle | h_j \rangle \langle h_k |$. Это взаимно однозначное соответствие между каналами и состояниями S_{BR} иногда называют *соответствием Чоя—Ямилковского*.

§ 6.4. Каналы, разрушающие сцепленность

В этом параграфе вводится важный класс каналов, содержащих классический этап переработки информации. Мы начнем рассмотрение с частных случаев.

1. Классически-квантовый (с-q) канал:

$$\Phi[S] = \sum_x \langle e_x | S | e_x \rangle S_x,$$

где $\{e_x\}$ — ортонормированный базис в $\mathcal{H}_A$, а S_x — операторы плотности в $\mathcal{H}_B$, соответствующие значениям символа x . Каналы этого типа, которые определяются отображением $x \rightarrow S_x$, описывающим кодирование классического входного сигнала x в квантовое состояние S_x , фактически уже рассматривались в гл. 5.

2. Квантово-классический (q-с) канал:

$$\Phi[S] = \sum_y |e_y\rangle \langle e_y| \operatorname{Tr} S M_y,$$

где $\{e_y\}$ — ортонормированный базис в $\mathcal{H}_B$, а $M = \{M_y\}$ — наблюдаемая в $\mathcal{H}_A$. Такой канал соответствует измерению наблюдаемой M (см. далее § 6.5); при этом возникает распределение вероятностей на множестве исходов измерения. Сопряженный канал действует по формуле

$$\Phi^*[X] = \sum_y \langle e_y | X | e_y \rangle M_y.$$

Представление Стайнспринга (6.7) для q-с-канала Φ связано с расширением Наймарка для наблюдаемой M : полагая $X = |e_y\rangle \langle e_y|$, получаем

$$M_y = V^* (|e_y\rangle \langle e_y| \otimes I_0) V,$$

где $E = \{|e_y\rangle \langle e_y| \otimes I_0\}$ — четкая наблюдаемая в $\mathcal{K}$.

3. Композиция q-с- и с-q-каналов с одним и тем же ортонормированным базисом $\{e_j\}$ дает q-с-q-канал

$$\Phi[S] = \sum_j S_j \operatorname{Tr} S M_j, \quad (6.27)$$

для которого каналы из п. 1 и 2 являются частными случаями. Такой канал содержит промежуточное классическое звено преобразования информации (в котором она представляется символом j).

Определение 6.4.1. Канал Φ из A в B обладает свойством *разрушения сцепленности*, если для произвольного входного состояния S_{AR} канала $\Phi \otimes \text{Id}_R$ его выходное состояние S_{BR} *разделимое* (несцепленное), т. е. является смесью состояний-произведений:

$$S_{BR} = \sum_j p_j S_B^j \otimes S_R^j, \quad (6.28)$$

где $\{p_j\}$ — распределение вероятностей.

Понятие сцепленности состояний будет подробнее рассмотрено в §7.4.

Предложение 6.4.1. Для того чтобы канал обладал свойством разрушения сцепленности, необходимо и достаточно, чтобы он был q -с- q -каналом.

Доказательство. Действительно, для канала (6.27) и любого входного состояния S_{AR} канала $\Phi \otimes \text{Id}_R$ выполняется соотношение (6.28) с $S_B^j = S_j$, $p_j S_R^j = \text{Tr}_A S_{AR} M_j$. Обратно, пусть канал Φ разрушает сцепленность, тогда, взяв в качестве S_{AR} максимально сцепленное состояние и используя соотношения (6.28), (6.26), получаем представление (6.27), в котором $S_j = S_B^j$, $M_j = d p_j (S_R^j)^T$. $\square$

Пример 6.4.1. Важным частным случаем с- q -канала является *полностью деполяризующий канал*, который описывает необратимую эволюцию к финальному состоянию S_f :

$$\Phi[S] = S_f \cdot \text{Tr } S, \quad S \in \mathfrak{T}(\mathcal{H}).$$

Пример 6.4.2. Пусть $p \in [0, 1]$, тогда канал $\Phi: \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{H} \oplus \mathbb{C})$, определяемый соотношением

$$\Phi(S) = \begin{bmatrix} (1-p)S & 0 \\ 0 & p \text{Tr } S \end{bmatrix},$$

сохраняет входное состояние S с вероятностью $1-p$ и «стирает» его с вероятностью p , посылая сигнал о стирании. Этот канал называется *квантовым стирающим каналом*.

Задача 6.4.1. Докажите полную положительность и найдите разложения Крауса для всех рассмотренных выше каналов.

§ 6.5. Процессы квантовых измерений

Важнейший пример необратимой эволюции — изменение состояния квантовой системы в результате производимого над ней измерения. Пол-

ное идеальное квантовое измерение связывается с ортонормированным базисом $|e_x\rangle$, векторы которого индексированы возможными исходами измерения x . Постулируется, что система, находящаяся перед измерением в состоянии S , в результате такого измерения переходит в состояния $|e_x\rangle\langle e_x|$ с вероятностями $\langle e_x|Se_x\rangle$. Таким образом, статистический ансамбль после измерения разбивается на подансамбли, соответствующие различным исходам x , и в целом описывается состоянием

$$S' = \sum_x |e_x\rangle\langle e_x|Se_x\rangle\langle e_x|. \quad (6.29)$$

Отметим, что отображение $S \rightarrow S'$ является частным случаем q -с-канала, отвечающего наблюдаемой $M = \{|e_x\rangle\langle e_x|\}$.

При *неполном* идеальном измерении некоторые исходы группируются, порождая ортогональное разложение единицы $E = \{E_x\}$,

$$E_x E_{x'} = \delta_{xx'} E_x, \quad \sum_x E_x = I,$$

другими словами, четкую наблюдаемую в пространстве $\mathcal{H}$. Согласно *проеекционному постулату фон Неймана—Людера* идеальное измерение четкой наблюдаемой E дает значение x с вероятностью

$$p_x = \text{Tr} SE_x = \text{Tr} E_x SE_x,$$

при этом *апостериорное состояние*, т. е. состояние подансамбля, в котором был получен исход измерения x , равно

$$S_x = \frac{E_x SE_x}{\text{Tr} E_x SE_x}, \quad \text{если } p_x > 0.$$

Для состояния всего ансамбля после измерения имеет место квантовый аналог формулы Байеса:

$$S' = \sum_x p_x S_x = \sum_x E_x SE_x = \Phi[S]. \quad (6.30)$$

Заметим, что, в отличие от классической формулы Байеса, квантовое состояние (6.30) всего ансамбля после идеального измерения может отличаться от начального состояния S . Таким образом, даже идеальное квантовое измерение не сводится к простому наблюдению выходного символа и включает в себя воздействие, которое изменяет состояние системы, даже если исходы «не считываются». В этом принципиальное отличие квантовых наблюдаемых от классических случайных величин, наблюдение которых не изменяет статистический ансамбль, а сводится к простому отбору его представителей в соответствии со значениями случайных величин.

В картине Шрёдингера изменение системы в результате измерения описывается вполне положительным отображением

$$\Phi^*[X] = \sum_x E_x X E_x = \Phi[X], \quad (6.31)$$

которое может быть интерпретировано как условное математическое ожидание относительно алгебры операторов, коммутирующих со всеми проекторами E_x ; при этом выполнены следующие характеристические свойства:

- 1) $\Phi^2 = \Phi$;
- 2) $\Phi[X\Phi[Y]] = \Phi[X]\Phi[Y]$, $X, Y \in \mathfrak{B}(\mathcal{H})$.

Идеальное квантовое измерение удовлетворяет *гипотезе воспроизводимости*: при повторном измерении исход с вероятностью 1 равен исходу первого измерения (в предположении, что никаких изменений между измерениями не произошло). Большинство реальных процедур измерения не удовлетворяют этому ограничению, и мы переходим к описанию таких неидеальных измерений.

Рассмотрим следующий процесс *косвенного* измерения: система $\mathcal{H}$ в начальном состоянии S взаимодействует с некоторой пробной системой $\mathcal{H}_0$, над которой затем производится идеальное измерение четкой наблюдаемой E^0 . Тогда в соответствии с постулатом фон Неймана—Людерса вероятность исхода x равна

$$p_x = \text{Tr } U(S \otimes S_0)U^*(I \otimes E_x^0),$$

а апостериорное состояние описывается оператором плотности S_x , удовлетворяющим соотношению

$$p_x S_x = \text{Tr}_{\mathcal{H}_0} U(S \otimes S_0)U^*(I \otimes E_x^0) \equiv \Phi_x[S]. \quad (6.32)$$

Таким образом, состояние системы после измерения может быть записано как

$$\Phi[S] = \sum_x p_x S_x = \sum_x \Phi_x[S].$$

Отображения Φ_x являются вполне положительными, причем их сумма Φ сохраняет след. Любое такое семейство отображений $\{\Phi_x\}$ называется *инструментом*. Инструмент описывают статистику и апостериорные состояния неидеального измерения, которое в общем случае не обязано удовлетворять гипотезе воспроизводимости.

Заметим, что

$$p_x = \text{Tr } S M_x,$$

где $M_x = \Phi_x^*[I]$ — разложение единицы, описывающее наблюдаемую, связанную с данным косвенным измерением. Обратно, по данной наблюдаемой $M = \{M_x\}$ можно построить связанные с ней (не единственный)

инструмент и косвенное измерение. Рассмотрим произвольное представление $M_x = V_x^* V_x$; построим по нему унитарный оператор (6.23) в пространстве $\mathcal{H} \otimes \mathcal{H}_E$, тогда семейство вполне положительных отображений

$$\Phi_x[S] = \text{Tr}_{\mathcal{H}_E} U(S \otimes |\psi_E\rangle\langle\psi_E|) U^*(I \otimes |e_x\rangle\langle e_x|), \quad (6.33)$$

где $|e_x\rangle$ — базисный вектор-столбец с единицей на x -м месте, так что $|\psi_E\rangle = |e_1\rangle$, образует инструмент. При этом

$$M_x = \text{Tr}_{\mathcal{H}_E} (I \otimes |\psi_E\rangle\langle\psi_E|) U^*(I \otimes |e_x\rangle\langle e_x|) U = \Phi_x^*[I]. \quad (6.34)$$

Таким образом, процесс косвенного измерения наблюдаемой M реализуется пробной системой $\mathcal{H}_E$ в начальном состоянии $|\psi_E\rangle\langle\psi_E|$, унитарным оператором U в пространстве $\mathcal{H} \otimes \mathcal{H}_E$ и четкой наблюдаемой $\{|e_x\rangle\langle e_x|\}$ в $\mathcal{H}_E$.

Задача 6.5.1. Для полного идеального измерения с наблюдаемой $M_x = |e_x\rangle\langle e_x|$ положим $V_x = M_x$ и построим унитарный оператор U по формуле (6.23) (в этом случае $\mathcal{H}_E = \mathcal{H}$). Покажите, что

$$U(|e_x\rangle \otimes |e_1\rangle) = |e_x\rangle \otimes |e_x\rangle.$$

Для произвольного вектора $\psi \in \mathcal{H}$ выполняется равенство

$$U(|\psi\rangle \otimes |e_1\rangle) = \sum_x \langle e_x | \psi \rangle |e_x\rangle \otimes |e_x\rangle,$$

таким образом, взаимодействие U порождает сцепленность между исходной и пробной системами, которая позволяет свести идеальное измерение в исходной системе к измерению четкой наблюдаемой $\{|e_x\rangle\langle e_x|\}$ в пробной системе.

§ 6.6. Комплементарные каналы

Рассмотрим три квантовые системы A, B, C с пространствами $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$ и линейный оператор $V: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_C$; соотношения

$$\Phi_B[S] = \text{Tr}_{\mathcal{H}_C} V S V^*, \quad \Phi_C[S] = \text{Tr}_{\mathcal{H}_B} V S V^*, \quad S \in \mathfrak{T}(\mathcal{H}_A), \quad (6.35)$$

определяют два вполне положительных отображения $\Phi_B: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$, $\Phi_C: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_C)$, которые мы называем взаимно *комплементарными*. Если V — изометрия, то оба отображения сохраняют след, т. е. являются каналами.

Из теоремы Стайнспринга вытекает, что для заданного вполне положительного отображения всегда существует комплементарное отображение. Кроме того, комплементарное отображение единственно в следующем смысле: для данного вполне положительного отображения Φ_B

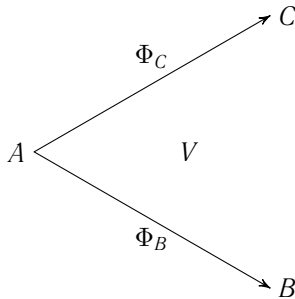


Рис. 6.2. Комплементарные каналы

любые два отображения $\Phi_C, \Phi_{C'}$, комплементарные к Φ_B , эквивалентны в том смысле, что найдется частичная изометрия $W: \mathcal{H}_C \rightarrow \mathcal{H}_{C'}$ такая, что

$$\Phi_{C'}[S] = W \Phi_C[S] W^*, \quad \Phi_C[S] = W^* \Phi_{C'}[S] W \quad (6.36)$$

для всех S . Если размерности пространств $\mathcal{H}_C, \mathcal{H}_{C'}$ минимальны, то W является изометрией $\mathcal{H}_C$ на $\mathcal{H}_{C'}$. Таким образом, комплементарность есть отношение на классах эквивалентности вполне положительных отображений.

Если $A = B$ — открытая квантовая система, взаимодействующая с окружением $C = E$ в произвольном начальном состоянии S_E , а Φ_B — соответствующий канал

$$\Phi_B[S] = \text{Tr}_E U(S \otimes S_E) U^*, \quad (6.37)$$

описывающий изменение состояния A , то конечное состояние окружения является выходным для канала

$$\Phi_E[S] = \text{Tr}_B U(S \otimes S_E) U^*. \quad (6.38)$$

Мы будем называть каналы Φ_B, Φ_E *слабо комплементарными*. Если же состояние окружения чистое, $S_E = |\psi_E\rangle\langle\psi_E|$, то, вводя изометрию $V = U|\psi_E\rangle: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$, мы получаем, что Φ_E является комплементарным каналом к Φ_B . Если состояние S_E не является чистым, то, рассматривая его очищение $S_{E'}$ в пространстве $\mathcal{H}_{E'} = \mathcal{H}_E \otimes \mathcal{H}_R$ и полагая $U' = U \otimes I_R$, получаем представление вида (6.38) с заменой E на E' , где состояние $S_{E'}$ уже чистое; следовательно, канал $\Phi_{E'}$ комплементарен к Φ_B , и $\Phi_E[S] = \text{Tr}_R \Phi_{E'}[S]$. В отличие от комплементарного, слабо комплементарный канал не единствен и зависит от представления (6.37).

Чтобы упростить формулы, будем использовать обозначение $\tilde{\Phi}$ для отображения, комплементарного к Φ .

Предположим, что вполне положительное отображение $\Phi: \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{H}')$ задано представлением Крауса

$$\Phi[S] = \sum_{\alpha=1}^{\tilde{d}} V_{\alpha} S V_{\alpha}^*, \quad (6.39)$$

тогда комплементарное отображение $\tilde{\Phi}: \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{M}_{\tilde{d}}$ задается формулой

$$\tilde{\Phi}[S] = [\text{Tr } V_{\alpha} S V_{\beta}^*]_{\alpha, \beta=1, \overline{\tilde{d}}} = \sum_{\alpha, \beta=1}^{\tilde{d}} (\text{Tr } S V_{\beta}^* V_{\alpha}) |e_{\alpha}\rangle \langle e_{\beta}|, \quad (6.40)$$

где $\{e_{\alpha}\}$ — канонический базис в координатном пространстве $\ell_{\tilde{d}}^2$, которое играет роль $\mathcal{H}_C$, так что $\tilde{d} = d_C$. Это утверждение вытекает из того, что

$V = \sum_{\alpha=1}^{\tilde{d}} \oplus V_{\alpha}$ является отображением $\mathcal{H}_A$ в $\sum_{\alpha=1}^{\tilde{d}} \oplus \mathcal{H}_B \simeq \mathcal{H}_B \otimes \mathcal{H}_C$, для

которого $\Phi, \tilde{\Phi}$ задаются частичными следами (6.35), см. задачу 3.1.4. Записывая след в пространстве $\mathcal{H}_B$ в ортонормированном базисе $\{e_j^B\}$, получаем представление Крауса для комплементарного отображения

$$\tilde{\Phi}[S] = \sum_{j=1}^{d_B} \tilde{V}_j S \tilde{V}_j^*, \quad (6.41)$$

где $\langle e_{\alpha} | \tilde{V}_j = \langle e_j^B | V_{\alpha}$ (см. определение (6.20)).

Задача 6.6.1. Покажите непосредственным вычислением, что применение аналогичной процедуры к $\tilde{\Phi}$ дает отображение $\tilde{\tilde{\Phi}}$, которое унитарно эквивалентно Φ .

Пример 6.6.1. Рассмотрим канал

$$\Phi[S] = S \otimes S_C, \quad (6.42)$$

где S_C — фиксированное состояние в пространстве $\mathcal{H}_C$. Если S_C — чистое состояние, то этот канал унитарно эквивалентен идеальному (тождественному) каналу Id . Записывая спектральное разложение

$$S_C = \sum_{\alpha=1}^{\tilde{d}} \lambda_{\alpha} |e_{\alpha}\rangle \langle e_{\alpha}|,$$

получаем представление Крауса с операторами $V_{\alpha} = \sqrt{\lambda_{\alpha}} (I \otimes |e_{\alpha}\rangle)$, следовательно, из соотношения (6.40) вытекает равенство

$$\tilde{\Phi}[S] = [\lambda_{\alpha} \delta_{\alpha\beta} \text{Tr } S]_{\alpha, \beta=1, \overline{\tilde{d}}} \simeq S_C \text{Tr } S,$$

т. е. $\tilde{\Phi}$ — полностью деполяризующий канал. Для произвольного состояния S_C идеальный канал Id слабо комплементарен к этому каналу.

Этот пример иллюстрирует тот факт, что идеальная передача квантовой информации из A в B равносильна отсутствию утечки информации из A в окружение C и наоборот. Далее мы увидим, что приближенная версия этого свойства — чем канал Φ ближе к идеальному, тем комплементарный канал $\tilde{\Phi}$ ближе к полностью деполяризующему — играет решающую роль в теореме кодирования для квантовой информации.

Полностью деполяризующий канал является частным случаем канала, разрушающего сцепленность (q-c-q) (см. § 6.4); вычисления могут быть обобщены на весь этот класс. Пусть $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$ — канал вида (6.27), тогда он имеет представление Крауса с операторами V_α ранга 1:

$$\Phi[S] = \sum_{\alpha=1}^{\tilde{d}} |\varphi_\alpha\rangle\langle\psi_\alpha| S |\psi_\alpha\rangle\langle\varphi_\alpha|, \quad (6.43)$$

где

$$\sum_{\alpha=1}^{\tilde{d}} |\psi_\alpha\rangle\langle\varphi_\alpha| \varphi_\alpha\rangle\langle\psi_\alpha| = I.$$

Задача 6.6.2. Используя спектральное разложение операторов S_j , M_j в формуле (6.27), покажите, что существование представления Крауса вида (6.43) является необходимым и достаточным для того, чтобы канал Φ разрушал сцепленность.

Комплементарный канал $\tilde{\Phi}: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{M}_{\tilde{d}}$ имеет вид

$$\tilde{\Phi}[S] = [c_{\alpha\beta}\langle\psi_\alpha|S|\psi_\beta\rangle]_{\alpha,\beta=1,\tilde{d}} = \sum_{\alpha,\beta=1}^{\tilde{d}} c_{\alpha\beta} |e_\alpha\rangle\langle\psi_\alpha| S |\psi_\beta\rangle\langle e_\beta|, \quad (6.44)$$

где $c_{\alpha\beta} = \langle\varphi_\beta|\varphi_\alpha\rangle$. Заметим, что произвольная положительно определенная матрица $[c_{\alpha\beta}]$ может быть представлена как матрица Грама некоторой системы векторов в гильбертовом пространстве (разложение Колмогорова). В частном случае, когда система $\{\psi_\alpha\}_{\alpha=1,\tilde{d}}$ является ортонормированным базисом в $\mathcal{H}$, соотношение (6.44) задает вполне положительное отображение, называемое *диагональным*. Из соотношения (6.43) мы видим, что диагональные каналы являются комплементарными к c-q-каналам. Для q-c-каналов $\{\varphi_\alpha\}_{\alpha=1,\tilde{d}}$ является ортонормированным базисом в $\mathcal{H}$, так что $c_{\alpha\beta} = \delta_{\alpha\beta}$ и комплементарный канал также является q-c-каналом.

Используя разложение Колмогорова $c_{\alpha\beta} = \sum_j \bar{v}_{\beta j} v_{\alpha j}$ и вводя обозначения

$$\tilde{V}_j = \sum_{\alpha=1}^{\tilde{d}} v_{\alpha j} |e_\alpha\rangle\langle\psi_\alpha|, \quad (6.45)$$

получаем представление Крауса (6.41) для комплементарного канала. Для диагональных отображений $|\psi_\alpha\rangle = |e_\alpha\rangle$, следовательно, из соотношения (6.44) можно видеть, что диагональные каналы характеризуются представлением Крауса с одновременно диагонализруемыми операторами $\tilde{V}_j$.

Определение 6.6.1. Пусть $\{p_j\}$ — конечное распределение вероятностей и $\Phi_j: \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}(\mathcal{H}'_j)$ — некоторое семейство каналов. Канал $\Phi: \mathfrak{T}(\mathcal{H}) \rightarrow \mathfrak{T}\left(\sum_j \oplus \mathcal{H}'_j\right)$ называется *ортогональной выпуклой комбинацией* каналов Φ_j ,

$$\Phi = \sum_j \oplus p_j \Phi_j,$$

если $\Phi[S] = \sum_j \oplus p_j \Phi_j[S]$ для всех $S \in \mathfrak{S}(\mathcal{H})$.

Задача 6.6.3. Покажите, что канал, комплементарный к ортогональной выпуклой комбинации каналов, является ортогональной выпуклой комбинацией комплементарных каналов:

$$\widetilde{\sum_j \oplus p_j \Phi_j} = \sum_j \oplus p_j \widetilde{\Phi_j}.$$

В частности, используя пример (6.42) (с $\tilde{d} = \dim \mathcal{H}_C = 1$), получаем, что канал, комплементарный к стирающему каналу Φ_p , унитарно эквивалентен стирающему Φ_{1-p} .

§ 6.7. Ковариантные каналы

Прежде чем перейти к дальнейшим примерам, рассмотрим важную конструкцию — дискретную версию операторов Вейля и канонических коммутационных соотношений (ККС) в конечномерном гильбертовом пространстве. Фиксируем ортонормированный базис $\{e_k; k = 1, \dots, d\}$ в $\mathcal{H}$. *Дискретными операторами Вейля* называются унитарные операторы в $\mathcal{H}$, определяемые соотношением

$$W_{\alpha\beta} = U^\alpha V^\beta, \quad \alpha, \beta = 0, \dots, d-1, \quad (6.46)$$

где

$$V|e_k\rangle = \exp\left(\frac{2\pi i k}{d}\right)|e_k\rangle, \quad U|e_k\rangle = |e_{k+1 \pmod{d}}\rangle, \quad k = 0, \dots, d-1. \quad (6.47)$$

Заметим, что $W_{00} = I$. Операторы Вейля удовлетворяют дискретному аналогу канонических коммутационных соотношений Вейля—Сигала для бозонных систем, которые будут подробно рассмотрены в гл. 11:

$$W_{\alpha\beta} W_{\alpha'\beta'} = \exp \frac{2\pi i \beta \alpha'}{d} W_{\alpha+\alpha', \beta+\beta'} = \exp \frac{2\pi i (\beta' \alpha - \beta \alpha')}{d} W_{\alpha'\beta'} W_{\alpha\beta}. \quad (6.48)$$

Первое равенство выражает тот факт, что отображение $(\alpha, \beta) \rightarrow W_{\alpha\beta}$ является проективным представлением аддитивной циклической группы $\mathbb{Z}_d \times \mathbb{Z}_d$.

Заметим, что оператор A , коммутирующий со всеми операторами Вейля $W_{\alpha,\beta}$, кратен единичному оператору. В самом деле, из равенства $[A, V] = 0$ согласно формулам (6.47) вытекает, что $A|e_k\rangle = a_k|e_k\rangle$, а из равенства $[A, U] = 0$ следует, что $a_k \equiv a$. Отсюда вытекает важное тождество

$$\sum_{\alpha, \beta=0}^{d-1} W_{\alpha\beta} S W_{\alpha\beta}^* = d(\text{Tr } S)I, \quad (6.49)$$

так как из равенства (6.48) следует, что левая часть коммутирует со всеми операторами Вейля. Константа в правой части находится из равенства следов. В действительности равенство (6.49) является следствием соотношений ортогональности для неприводимого унитарного представления произвольной компактной группы.

Заметим, что в случае $d = 2$ дискретные операторы Вейля сводятся к матрицам Паули; а именно, полагая $|e_0\rangle = |\uparrow\rangle$, $|e_1\rangle = |\downarrow\rangle$, получаем

$$W_{01} = V = \sigma_z, \quad W_{10} = U = \sigma_x, \quad W_{11} = UV = -i\sigma_y, \quad (6.50)$$

при этом дискретные ККС переходят в правила умножения (2.17).

Определение 6.7.1. *Деполаризующий канал в $\mathcal{H}$, $\dim \mathcal{H} = d$, определяется соотношением*

$$\Phi[S] = (1 - p)S + p \frac{I}{d} \text{Tr } S, \quad 0 \leq p \leq \frac{d^2}{d^2 - 1}. \quad (6.51)$$

Если $p \leq 1$, то это соотношение описывает смесь идеального канала Id и полностью деполаризующего канала, который переводит любое состояние в хаотическое состояние $\bar{S} = \frac{I}{d}$. Для любого значения параметра p , $0 \leq p \leq \frac{d^2}{d^2 - 1}$, полная положительность следует из представления Крауса

$$\Phi[S] = \left(1 - p \frac{d^2 - 1}{d^2}\right)S + \frac{p}{d^2} \sum_{\alpha + \beta > 0} W_{\alpha\beta} S W_{\alpha\beta}^*, \quad (6.52)$$

которое получается при подстановке выражения для $\text{Tr } S$ из формулы (6.49) в равенство (6.51). В этом выражении все коэффициенты положительны, что следует из условия $0 \leq p \leq \frac{d^2}{d^2 - 1}$.

Деполаризующий канал удовлетворяет соотношению $\Phi^* = \Phi$ и является унитарным, а значит, и бистохастическим.

Пусть G — группа и $g \rightarrow V_g^j$, $g \in G$, — два (проективных) унитарных представления группы G в $\mathcal{H}_j$, $j = A, B$. Канал $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$ называется *ковариантным*, если

$$\Phi[V_g^A S (V_g^A)^*] = V_g^B \Phi[S] (V_g^B)^* \quad (6.53)$$

для всех $g \in G$ и S . Если представление V_g^B неприводимое, то канал Φ является бистохастическим. В самом деле, из свойства $V_g^B \Phi[I_A] = \Phi[I_A] V_g^B$ (для всех g) и из неприводимости представления V_g^B следует, что оператор $\Phi[I_A]$ пропорционален I_B , а коэффициент пропорциональности получается из равенства следов.

Задача 6.7.1. Покажите, что деполяризующий канал характеризуется свойством унитарной ковариантности: $\Phi[USU^*] = U\Phi[S]U^*$ для произвольного унитарного оператора U в $\mathcal{H}$.

Задача 6.7.2. Покажите, что канал, комплементарный к ковариантному каналу, сам является ковариантным:

$$\Phi[V_g^A S (V_g^A)^*] = V_g^E \Phi[S] (V_g^E)^*,$$

где $g \rightarrow V_g^E$ — (проективное) унитарное представление группы G в $\mathcal{H}_E$.

Указание. Используйте тот факт, что для произвольного ковариантного канала имеется представление Крауса (6.18), в котором операторы V_j удовлетворяют соотношениям

$$V_g^B V_j (V_g^A)^* = \sum_k d_{jk}(g) V_k,$$

где $g \rightarrow D(g) = [d_{jk}(g)]$ — некоторое матричное унитарное представление группы G . Отсюда следует, что комплементарное отображение (6.40) ковариантно, причем роль второго представления V_g^E играет $D(g)$.

§ 6.8. Q-битные каналы

Рассмотрим каналы в пространстве состояний q-бита $\mathcal{H}_2$, которые соответствуют аффинным преобразованиям шара Блоха (единичного шара в $\mathbb{R}^3$), удовлетворяющим дополнительному ограничению, налагаемому полной положительностью.

Предложение 6.8.1. Произвольное положительное сохраняющее след отображение Φ пространства $\mathfrak{T}(\mathcal{H}_2)$ может быть представлено в виде

$$\Phi[S] = U_2 \Lambda[U_1 S U_1^*] U_2^*, \quad (6.54)$$

где U_1, U_2 — унитарные операторы, а Λ имеет следующую каноническую форму в базисе матриц Паули:

$$\Lambda[I] = I + \sum_{\gamma=x,y,z} t_\gamma \sigma_\gamma, \quad \Lambda[\sigma_\gamma] = \lambda_\gamma \sigma_\gamma, \quad \gamma = x, y, z, \quad (6.55)$$

λ_γ, t_γ — действительные числа.

Доказательство. Ограничение отображения Φ на множество состояний q -бита является аффинным преобразованием, поэтому оно переводит состояние $S(\mathbf{a})$, задаваемое соотношением (2.8), в состояние $S(T\mathbf{a} + \mathbf{b})$, где T — вещественная (3×3) -матрица, $\mathbf{b}$ — вектор в $\mathbb{R}^3$. Используя полярное разложение для T и спектральное разложение для $|T|$, получаем

$$T = O|T| = O_2 L O_1,$$

где O, O_1, O_2 — ортогональные матрицы, $\det O_1 = \det O_2 = 1$, а $L = \text{diag}[\lambda_x, \lambda_y, \lambda_z]$ — диагональная матрица с диагональными элементами λ , вещественными, но необязательно неотрицательными. Таким образом,

$$\Phi[S(\mathbf{a})] = S(O_2[L(O_1\mathbf{a}) + \mathbf{t}]), \quad (6.56)$$

где $\mathbf{t} = O_2^{-1}\mathbf{b}$.

Матрицы O_1, O_2 описывают повороты шара Блоха в $\mathbb{R}^3$. Покажем, что они отвечают преобразованиям квантовых состояний, которые порождаются унитарными операторами U в $\mathcal{H}$ согласно формуле (6.2). Достаточно рассмотреть поворот O вокруг оси z на угол α . При этом единичный вектор $\mathbf{a}$ с углами Эйлера θ, φ преобразуется в вектор $O\mathbf{a}$ с углами $\theta, \varphi + \alpha$, поэтому вектор состояния (2.9) в $\mathcal{H}$ переходит в вектор

$$|\psi(O\mathbf{a})\rangle = \begin{bmatrix} \cos \frac{\theta}{2} e^{-i(\varphi+\alpha)/2} \\ \sin \frac{\theta}{2} e^{i(\varphi+\alpha)/2} \end{bmatrix} = U|\psi(\mathbf{a})\rangle, \quad (6.57)$$

где $U = \text{diag}[e^{-i\alpha/2}, e^{i\alpha/2}]$ — унитарная матрица. Тогда

$$S(O\mathbf{a}) = US(\mathbf{a})U^* \quad (6.58)$$

для всех $\mathbf{a}$.

Учитывая равенство (6.56), получаем доказываемое соотношение (6.54). $\square$

Задача 6.8.1. Покажите, что повороту шара Блоха на угол α вокруг оси $\mathbf{a}$ отвечает унитарный оператор

$$U = \exp\left[-\frac{i\alpha}{2}\sigma(\mathbf{a})\right] = \cos \frac{\alpha}{2} I - i \sin \frac{\alpha}{2} \sigma(\mathbf{a}).$$

Рассмотрим подробнее отображения вида (6.55). Разумеется, условие полной положительности накладывает нетривиальные ограничения на параметры λ_γ , t_γ . Наиболее прозрачным является случай $t_\gamma \equiv 0$, когда отображения Φ и, следовательно, Λ унитарны. В этом случае Λ является сжатием шара Блоха вдоль осей x , y , z с коэффициентами $|\lambda_x|$, $|\lambda_y|$, $|\lambda_z|$, которое комбинируется с отражениями, если некоторые из чисел λ_γ отрицательны (например, $\lambda_y < 0$ влечет отражение относительно плоскости xz). Транспонированию матрицы плотности $S(\mathbf{a})$, которое заведомо не является вполне положительным отображением, отвечает отображение Λ с параметрами $\lambda_x = 1$, $\lambda_y = -1$, $\lambda_z = 1$. Отсюда, в частности, получаем, что соотношение типа (6.58) имеет место и для ортогональных матриц O , $\det O = -1$, однако им соответствуют антиунитарные преобразования U . Поскольку всякое взаимно однозначное аффинное преобразование шара Блоха, очевидно, задается ортогональной матрицей O , отсюда вытекает теорема 6.1.1 для q -бита.

Задача 6.8.2. Используя правила умножения (2.17), покажите, что в случае $t_\gamma \equiv 0$ имеет место представление

$$\Lambda[S] = \sum_{\gamma=0,x,y,z} \mu_\gamma \sigma_\gamma S \sigma_\gamma, \quad (6.59)$$

где

$$\begin{aligned} \mu_0 &= \frac{1}{4}(1 + \lambda_x + \lambda_y + \lambda_z), & \mu_x &= \frac{1}{4}(1 + \lambda_x - \lambda_y - \lambda_z), \\ \mu_y &= \frac{1}{4}(1 - \lambda_x + \lambda_y - \lambda_z), & \mu_z &= \frac{1}{4}(1 - \lambda_x - \lambda_y + \lambda_z). \end{aligned}$$

Неотрицательность этих чисел необходима и достаточна для полной положительности отображения Λ , а значит, и Φ .

Задача 6.8.3. Покажите, что q -битные унитарные каналы (6.59) ковариантны по отношению к проективному унитарному представлению группы $\mathbb{Z}_2 \times \mathbb{Z}_2$, определяемому соотношениями (6.50).

§ 6.9. Комментарии

1. Доказательство теоремы 6.1.1, восходящей к утверждению Вигнера (см. [4]), следует книге Дэвиса [73] (см. § 2.3 и комментарии к нему).

2. Понятие вполне положительного отображения введено Стайнс-прингом в работе [149] в более общем контексте C^* -алгебр. Математический обзор свойств вполне положительных отображений, включая доказательство неравенства из задачи 6.2.1, имеется в статье Штермера (с. 85—106 сборника [82]). В конечномерном случае, имеющем свою спе-

цифику, вполне положительные отображения подробно рассматривались в работе Чоя [69].

В основе приведенного доказательства теоремы 6.2.1 лежит конструкция Гельфанда—Наймарка—Сигала: построение гильбертова пространства и представления в этом пространстве, опирающееся на объект с подходящими свойствами положительности. Такое доказательство с небольшими изменениями проходит для вполне положительных отображений C^* -алгебр. В случае алгебры $\mathfrak{B}(\mathcal{H})$ лемма 6.2.1 позволяет получить более подробное представление (6.7). Представление Крауса детально обсуждается в книге [116].

3. На свойство полной положительности динамики открытой квантовой системы было обращено внимание в работах А. С. Холево [31], и Линдблада [124]. Большое число работ посвящено изучению марковской динамики открытой квантовой системы, которая описывается полугруппой вполне положительных отображений. Обзор теории квантовых динамических полугрупп и квантовых случайных процессов см. в книге [36].

Соответствие Чоя—Ямилковского вытекает из результатов работы [69]. В квантовой теории информации оно используется весьма плодотворно; например, представление Крауса (6.17) в конечномерном случае легко получается из формулы (6.26), см. [22, теорема 8.1].

4. Каналы типа q -с- q были введены в работе А. С. Холево [35]. Подробное рассмотрение каналов, разрушающих сцепленность, включающее доказательство предложения 6.4.1, дано в работе Городецкого, Шора и Рускаи [107].

5. Детальное обсуждение математических моделей квантового измерения см., например, в книгах Людвига [127], Дэвиса [73], Крауса [116], А. С. Холево [36], работах Линдблада [122], Озавы [130].

6. Понятие комплементарного канала введено в работе Деветака и Шора [77]. Результаты настоящего параграфа принадлежат А. С. Холево (см. [40]), а также Кингу, Мацумото, Натансону и Рускаи (см. [114]).

7. Дискретные операторы Вейля использовались в знаменитой статье Беннета, Brassara, Крепо, Джоза, Переса и Вуттерса [56] о телепортации. Относительно ковариантности комплементарного канала (задача 6.7.2) см. работу А. С. Холево [40].

8. Реальные примеры q -битных каналов подробно рассматриваются в книге Нильсена и Чанга [22]. Общая структура q -битных каналов детально описана в работе Рускаи, Шарека и Вернер [133].

ГЛАВА 7

Квантовая энтропия и информация

§ 7.1. Квантовая относительная энтропия

Определение 7.1.1. Пусть S, T — операторы плотности. Если оператор T невырожден, то *квантовая относительная энтропия* определяется формулой

$$H(S; T) = -H(S) - \text{Tr } S \log T = \text{Tr } S(\log S - \log T). \quad (7.1)$$

Случай, когда $\text{supp } S \subseteq \text{supp } T$ ($\text{supp } S$ обозначает носитель оператора S , см. § 1.3), сводится к предыдущему путем рассмотрения сужения операторов S, T на $\text{supp } T$, где оператор T невырожден. Если же $\text{supp } S \not\subseteq \text{supp } T$, то полагаем $H(S; T) = +\infty$.

Задача 7.1.1. Пусть λ_j, μ_k — собственные значения, а $|e_j\rangle, |h_k\rangle$ — собственные векторы операторов плотности S, T соответственно. Докажите, что тогда

$$H(S; T) = \sum_{j,k} |\langle e_j | h_k \rangle|^2 (\lambda_j \log \lambda_j - \lambda_j \log \mu_k). \quad (7.2)$$

Предложение 7.1.1. *Справедливо неравенство*

$$H(S; T) \geq \frac{\log e}{2} \text{Tr}(S - T)^2 \geq 0, \quad (7.3)$$

причем равенство имеет место тогда и только тогда, когда $S = T$.

Доказательство. Используя для функции (4.2) формулу

$$\eta(\lambda) - \eta(\mu) = (\lambda - \mu)\eta'(\mu) + \frac{1}{2}(\lambda - \mu)^2\eta''(\xi),$$

где $0 \leq \lambda < \xi < \mu$, получаем неравенство

$$\lambda \log \lambda - \lambda \log \mu \geq (\lambda - \mu) \log e + \frac{\log e}{2}(\mu - \lambda)^2;$$

подстановка этого неравенства в формулу (7.2) приводит к требуемому результату. $\square$

Следствие 7.1.1 (субаддитивность квантовой энтропии). Пусть S_{12} — оператор плотности в $\mathcal{H}_1 \otimes \mathcal{H}_2$ с частичными следами $S_1 = \text{Tr}_{\mathcal{H}_2} S_{12}$ и $S_2 = \text{Tr}_{\mathcal{H}_1} S_{12}$. Тогда

$$H(S_1) + H(S_2) \geq H(S_{12}), \quad (7.4)$$

причем равенство имеет место тогда и только тогда, когда $S_{12} = S_1 \otimes S_2$.

Доказательство. Доказательство вытекает из равенства $H(S_1) + H(S_2) - H(S_{12}) = H(S_{12}; S_1 \otimes S_2)$ и неравенства (7.3). $\square$

Подобно энтропии, относительная энтропия обладает следующими свойствами.

Задача 7.1.2. Докажите следующие утверждения.

1. Изометрическая инвариантность: $H(VSV^*; VS'V^*) = H(S; S')$ для произвольного оператора V , изометричного на носителях операторов S, S' .

2. Аддитивность: $H(S_1 \otimes S_2; S'_1 \otimes S'_2) = H(S_1; S'_1) + H(S_2; S'_2)$.

§ 7.2. Монотонность относительной энтропии

Теорема 7.2.1. Для произвольных операторов плотности S, T в $\mathcal{H}_1$ и произвольного канала Φ из $\mathfrak{T}(\mathcal{H}_1)$ в $\mathfrak{T}(\mathcal{H}_2)$ справедливо неравенство

$$H(S; T) \geq H(\Phi[S]; \Phi[T]). \quad (7.5)$$

Этот важный результат вытекает из доказываемой ниже теоремы 7.2.2, которая устанавливает аналогичное свойство монотонности для целого класса функций пары квантовых состояний.

Рассмотрим гильбертово пространство $L^2(\mathcal{H})$ операторов в $\mathcal{H}$ со скалярным произведением

$$(X, Y) = \text{Tr} X^* Y.$$

Пусть S, T — невырожденные операторы плотности. В $L^2(\mathcal{H})$ введем оператор L_T левого умножения на T и оператор R_S правого умножения на S , а именно $L_T X = TX$, $R_S X = XS$. Эти операторы являются коммутирующими эрмитовыми положительными операторами в $L^2(\mathcal{H})$.

Относительная g -энтропия операторов S, T определяется соотношением

$$H_g(S; T) = (S^{1/2}, g(L_T R_S^{-1}) S^{1/2}) \quad (7.6)$$

для любой функции $g \in \mathcal{G}$, где $\mathcal{G}$ — класс функций вида

$$g(w) = a(w-1) + b(w-1)^2 + \int_0^\infty \frac{(w-1)^2}{w+s} d\nu(s), \quad (7.7)$$

a — действительное число, $b \geq 0$ и ν — положительная мера на $[0, \infty)$, удовлетворяющая условию $\int_0^\infty \frac{1}{s+1} d\nu(s) < \infty$ (о внутренней характеристике этого класса говорится в § 7.7). Для доказательства следующей

теоремы важно лишь то обстоятельство, что функция $g(w)$, входящая в определение относительной g -энтропии, имеет такое представление.

Теорема 7.2.2. *Для произвольной функции $g \in \mathcal{G}$ относительная g -энтропия $H_g(S; T)$ обладает свойством монотонности:*

$$H_g(S; T) \geq H_g(\Phi[S]; \Phi[T]) \quad (7.8)$$

для любого канала Φ .

Теорема 7.2.1 тогда вытекает из двух наблюдений.

1. Функция $g(w) = -\log w$ принадлежит классу $\mathcal{G}$. В самом деле, легко проверяется, что

$$-\ln w = \int_0^\infty \left[\frac{1}{w+s} - \frac{1}{1+s} \right] ds = -(w-1) + \int_0^\infty \frac{(w-1)^2}{(w+s)(s+1)^2} ds.$$

2. Справедливо равенство

$$H_{-\log}(S; T) = H(S; T).$$

Действительно,

$$-\log(L_T R_S^{-1})X = \log R_S X - \log L_T X = X(\log S) - (\log T)X$$

в силу коммутирования операторов L_T , R_S , откуда следует, что

$$-\log(L_T R_S^{-1})S^{1/2} = (\log S - \log T)S^{1/2},$$

и результат вытекает из формулы (7.6).

Доказательство теоремы 7.2.2.

Лемма 7.2.1. *Для произвольной функции $g \in \mathcal{G}$ выполняется равенство*

$$H_g(S; T) = b \operatorname{Tr}(T - S)S^{-1}(T - S) + \int_0^\infty \operatorname{Tr}(T - S)(L_T + sR_S)^{-1}(T - S)d\nu(s) \quad (7.9)$$

Доказательство. Вводя обозначение $\Delta_{T,S} = L_T R_S^{-1}$, заметим, что

$$(\Delta_{T,S} - I)S^{1/2} = (T - S)S^{-1/2} = R_{S^{-1/2}}(T - S), \quad (7.10)$$

так что

$$H_{w^{-1}}(S; T) = \operatorname{Tr} S^{1/2}(T - S)S^{-1/2} = 0, \quad (7.11)$$

и, следовательно, линейный член в формуле (7.7) не дает вклада в соотношения (7.9). Для $g(w) = \frac{(w-1)^2}{(w+s)}$, используя равенство (7.10), получаем

$$\begin{aligned} H_g(S; T) &= ((\Delta_{T,S} - I)S^{1/2}, (\Delta_{T,S} + sI)^{-1}(\Delta_{T,S} - I)S^{1/2}) = \\ &= \operatorname{Tr}[(T - S)(\Delta_{T,S} + sI)^{-1}R_{S^{-1}}(T - S)] = \\ &= \operatorname{Tr}(T - S)(L_T + sR_S)^{-1}(T - S). \end{aligned} \quad (7.12)$$

При $s = 0$ имеем

$$H_{(\omega-1)^2/\omega}(S; T) = \text{Tr}(T - S)T^{-1}(T - S) = H_{(\omega-1)^2}(T; S). \quad (7.13)$$

Подставляя эти соотношения в формулу (7.7), получаем соотношение (7.9). $\square$

Если не учитывать первый член в формуле (7.7) (который не дает вклада в $H_g(S; T)$), то функции (7.7) являются «континуальными выпуклыми комбинациями» функций $(\omega - 1)^2$ и $\frac{(\omega - 1)^2}{\omega + s}$, $s \geq 0$; таким образом, достаточно доказать монотонность относительной g -энтропии для таких функций g , т. е. для (7.12).

Доказательство теоремы 7.2.2 теперь вытекает из интегрального представления (7.9) и следующей леммы.

Лемма 7.2.2. *Для произвольного канала Φ , $s \geq 0$ и оператора A выполняется равенство*

$$\text{Tr} A^*(L_T + sR_S)^{-1}A \geq \text{Tr} \Phi[A^*](L_{\Phi[T]} + sR_{\Phi[S]})^{-1}\Phi[A]. \quad (7.14)$$

Доказательство. Так как операторы L_T, R_S являются положительными в $L^2(\mathcal{H})$, оператор $L_T + sR_S$ также положителен. Положим $X = (L_T + sR_S)^{-1/2}A - (L_T + sR_S)^{1/2}\Phi^*[B]$, где $B = (L_{\Phi[T]} + sR_{\Phi[S]})^{-1}\Phi[A]$. Тогда $\text{Tr} X^*X \geq 0$, так что

$$\begin{aligned} \text{Tr} A^*(L_T + sR_S)^{-1}A - \text{Tr} A^*\Phi^*[B] - \text{Tr} \Phi^*[B^*]A + \\ + \text{Tr} \Phi^*[B^*](L_T + sR_S)\Phi^*[B] \geq 0. \end{aligned} \quad (7.15)$$

Имеем

$$\text{Tr} A^*\Phi^*[B] + \text{Tr} \Phi^*[B^*]A = 2 \text{Tr} \Phi[A^*](L_{\Phi[T]} + sR_{\Phi[S]})^{-1}\Phi[A],$$

таким образом, для доказательства леммы достаточно показать, что последний член в формуле (7.14) меньше или равен, чем правая часть формулы (7.14). Имеем

$$\begin{aligned} \text{Tr} \Phi^*[B^*](L_T + sR_S)\Phi^*[B] &= \text{Tr}[\Phi^*[B^*]\Phi^*[B]sS + \Phi^*[B^*]T\Phi^*[B]] = \\ &= \text{Tr}[\Phi^*[B^*]\Phi^*[B]sS + \Phi^*[B]\Phi^*[B^*]T] \leq \\ &\leq \text{Tr}[\Phi^*[B^*B]sS + \Phi^*[BB^*]T], \end{aligned}$$

где неравенство вытекает из положительности операторов S, T и неравенства Кэдисона (6.6), которое в случае канала Φ принимает вид

$$\Phi^*[B^*]\Phi^*[B] \leq \Phi^*[B^*B].$$

Далее, используя соотношение $\text{Tr } \Phi^*[B^*B]S = \text{Tr } B^*B\Phi[S]$, получаем

$$\begin{aligned} \text{Tr } \Phi^*[B^*](L_T + sR_S)\Phi^*[B] &\leq \text{Tr}(B^*Bs\Phi[S] + BB^*\Phi[T]) = \\ &= \text{Tr } B^*(Bs\Phi[S] + \Phi[T]B) = \\ &= \text{Tr } B^*(L_{\Phi[T]} + sR_{\Phi[S]})(B) = \text{Tr } B^*\Phi[A] = \\ &= \text{Tr } \Phi[A^*](L_{\Phi[T]} + sR_{\Phi[S]})^{-1}\Phi[A]. \end{aligned}$$

Это доказывает теорему 7.2.2 в случае невырожденных операторов S, T . В общем случае либо $H(S; T) = +\infty$ и неравенство (7.5) тривиально, либо $\text{supp } S \subseteq \text{supp } T$, и тогда можно считать, что $\text{supp } T = \mathcal{H}$, т. е. оператор T невырожден, а для $H(S; T)$ имеет место соотношение (7.1). Аппроксимируя произвольный оператор S невырожденными операторами и используя непрерывность энтропии (см. § 7.3), убеждаемся в справедливости теоремы в общем случае. $\square$

Следствие 7.2.1 (обобщенная H -теорема). Пусть Φ — бистохастический (унитальный) канал в $\mathcal{H} = \mathcal{H}_1 = \mathcal{H}_2$. Тогда

$$H(\Phi[S]) \geq H(S). \quad (7.16)$$

Доказательство. Из соотношения (7.1) следует, что

$$H(S) = \log d - H(S; \bar{S}), \quad (7.17)$$

где $\bar{S} = \frac{1}{d}I$ — хаотическое состояние, а значит, и

$$H(\Phi[S]) = \log d - H(\Phi[S]; \bar{S}),$$

в силу того что $\Phi[\bar{S}] = \bar{S}$. Теперь утверждение непосредственно вытекает из теоремы 7.2.1 о монотонности. $\square$

Покажем, как из теоремы 7.2.1 можно получить верхнюю границу для шенноновской информации (5.15). Вводя среднее состояние $\bar{S}_\pi = \sum \pi_x S_x$, получаем важное соотношение

$$\chi(\pi) \equiv H(\bar{S}_\pi) - \sum \pi_x H(S_x) = \sum_x \pi_x H(S_x; \bar{S}_\pi). \quad (7.18)$$

Выберем произвольный базис $\{e_y\}$ в $\mathcal{H}$ и рассмотрим q -с-канал $\Psi[S] = \sum_y \text{Tr } S M_y |e_y\rangle\langle e_y|$, отвечающий измерению наблюдаемой $M = \{M_y\}$, тогда

$$\Psi[S_x] = \sum_y p_M(y|x) |e_y\rangle\langle e_y|, \quad \Psi[\bar{S}_\pi] = \sum_y \left(\sum_x \pi_x p_M(y|x) \right) |e_y\rangle\langle e_y|,$$

где $p_M(y|x) = \text{Tr } S_x M_y$ — операторы плотности, диагональные в базисе $\{e_y\}$. Поэтому квантовая относительная энтропия на выходе канала Ψ

превращается в классическую, и из соотношения (7.18) следует, что

$$\sum_x \pi_x H(\Psi[S_x]; \Psi[\bar{S}_\pi]) = \mathcal{I}_1(\pi, M).$$

Применяя теорему 7.2.1 о монотонности относительной энтропии к каналу Ψ и еще раз используя соотношение (7.18), получаем искомое неравенство.

Теорема 7.2.3. *Следующие свойства эквивалентны.*

1. *Монотонность относительной энтропии.*

2. *Сильная субаддитивность квантовой энтропии: пусть S_{123} — оператор плотности в $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$, тогда, в очевидных обозначениях для частичных следов,*

$$H(S_{123}) + H(S_2) \leq H(S_{12}) + H(S_{23}). \quad (7.19)$$

3. *Совместная выпуклость относительной квантовой энтропии $H(S; T)$ по аргументам S, T .*

Доказательство. $1 \Rightarrow 2$. Обозначая через $\bar{S}_\alpha = (\dim \mathcal{H}_\alpha)^{-1} I_\alpha$ хаотическое состояние в $\mathcal{H}_\alpha$, получаем

$$\begin{aligned} H(S_{123}; \bar{S}_{123}) &= H(S_{123}; S_{12} \otimes \bar{S}_3) + H(S_{12}; \bar{S}_{12}), \\ H(S_{23}; \bar{S}_{23}) &= H(S_{23}; S_2 \otimes \bar{S}_3) + H(S_2; \bar{S}_2). \end{aligned}$$

Вычитая одно равенство из другого и используя соотношение (7.17), получаем

$$H(S_{12}) + H(S_{23}) - H(S_{123}) - H(S_2) = H(S_{123}; S_{12} \otimes \bar{S}_3) - H(S_{23}; S_2 \otimes \bar{S}_3).$$

Рассмотрим канал $\Phi[S_{123}] = S_{23}$. Применяя к нему теорему 7.2.1, убеждаемся, что правая часть неотрицательна, т. е. выполнено свойство сильной субаддитивности.

$2 \Rightarrow 3$. Рассмотрим оператор плотности в $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ вида

$$S_{123} = \sum_{kl} |e_k\rangle\langle e_k| \otimes A_{kl} \otimes |h_l\rangle\langle h_l|,$$

где $\{e_k\}$ — ортонормированный базис в $\mathcal{H}_1$, $\{h_l\}$ — ортонормированный базис в $\mathcal{H}_3$, A_{kl} — положительные операторы в $\mathcal{H}_2$. Тогда

$$S_{12} = \sum_k |e_k\rangle\langle e_k| \otimes \sum_l A_{kl}, \quad S_{23} = \sum_k A_{kl} \otimes |h_l\rangle\langle h_l|, \quad S_2 = \sum_{kl} A_{kl},$$

и из свойства сильной субаддитивности вытекает следующее неравенство:

$$-\sum_{kl} H(A_{kl}) + \sum_k H\left(\sum_l A_{kl}\right) + \sum_l H\left(\sum_k A_{kl}\right) - H\left(\sum_{kl} A_{kl}\right) \geq 0,$$

где введено обозначение $H(A) = -\operatorname{Tr} A \log A$ для любого положительного оператора A . Тогда, в частности, для любых положительных операторов A_1, A_2, B_1, B_2 получаем

$$\begin{aligned} H(A_1 + A_2 + B_1 + B_2) - H(A_1 + A_2) - H(B_1 + B_2) &\leq \\ &\leq H(A_1 + B_1) - H(A_1) - H(B_1) + H(A_2 + B_2) - H(A_2) - H(B_2), \end{aligned}$$

что равносильно совместной выпуклости функции

$$\Delta(A, B) = H(A + B) - H(A) - H(B)$$

по аргументам A, B . Из следующей леммы вытекает, что относительная энтропия $H(A; B)$ также является выпуклой как точная верхняя грань семейства выпуклых функций. $\square$

Лемма 7.2.3. *Для любых двух операторов плотности A, B выполняется равенство*

$$H(A; B) = \sup_{\lambda > 0} \lambda^{-1} \chi_\lambda(A; B), \quad (7.20)$$

где

$$\begin{aligned} \chi_\lambda(A; B) &= H(\lambda A + (1 - \lambda)B) - \lambda H(A) - (1 - \lambda)H(B) = \\ &= \Delta(\lambda A, (1 - \lambda)B) + h(\lambda). \end{aligned}$$

Доказательство. Из доказанного выше следует, что функция $\chi_\lambda(A; B)$ выпукла по A, B . Как функция аргумента $\lambda \in [0, 1]$ она вогнута и равна нулю при $\lambda = 0; 1$ (это было доказано в § 5.3). Значит, при фиксированных A, B выполняется равенство

$$\sup_{\lambda > 0} \lambda^{-1} \chi_\lambda(A; B) = \lim_{\lambda \rightarrow 0} \lambda^{-1} \chi_\lambda(A; B) = \left. \frac{d}{d\lambda} \right|_{\lambda=0} \chi_\lambda(A; B).$$

Задача 7.2.1. Пусть F — непрерывно дифференцируемая функция в интервале $(0, +\infty)$. Покажите, что для любых положительных операторов A, B выполняется равенство

$$\frac{d}{d\lambda} \operatorname{Tr} F(\lambda A + (1 - \lambda)B) = \operatorname{Tr} F'(\lambda A + (1 - \lambda)B)(A - B). \quad (7.21)$$

Указание. Докажите равенство (7.21) в случае, когда F — многочлен, а затем используйте аппроксимацию.

Пусть теперь $\operatorname{supp} A \subset \operatorname{supp} B$, так что $H(A; B) < +\infty$. Без ограничения общности будем считать, что оператор B невырожден. Вычисляя производную от

$$H(\lambda A + (1 - \lambda)B) = \operatorname{Tr} \eta(\lambda A + (1 - \lambda)B)$$

по формуле (7.21), получаем, что

$$\frac{d}{d\lambda} \Big|_{\lambda=0} \chi_\lambda(A; B) = \text{Tr } A(\log A - \log B) + \log e \text{Tr}(B - A) = H(A; B),$$

откуда вытекает равенство (7.20).

Задача 7.2.2. Проведите доказательство в случае $H(A; B) = +\infty$. $\square$

$3 \Rightarrow 1$. Рассмотрим оператор плотности S_{12} в $\mathcal{H}_1 \otimes \mathcal{H}_2$ и положим $S_1 = \text{Tr}_2 S_{12}$. Используя свойство (6.49) дискретных операторов Вейля, получаем

$$S_1 \otimes \bar{S}_2 = \frac{1}{d^2} \sum_{\alpha, \beta=0}^{d-1} (I_1 \times W_{\alpha\beta}) S_{12} (I_1 \times W_{\alpha\beta})^*.$$

Используя выпуклость относительной энтропии и свойства из упражнения 7.1.2, получаем неравенство

$$H(S_1; S'_1) \leq H(S_{12}; S'_{12}),$$

которое является свойством монотонности для частичных следов. Но по теореме 6.2.1 всякий канал может быть представлен в виде суперпозиции изометрического вложения (сохраняющего относительную энтропию) и частичного следа. Таким образом, свойство 1 доказано. $\square$

Используя равенство (7.17) и выпуклость относительной энтропии, мы попутно получаем следующий результат.

Следствие 7.2.2. *Квантовая энтропия вогнута: для произвольных состояний S_j и распределения вероятностей $\{p_j\}$ выполняется неравенство*

$$H\left(\sum_j p_j S_j\right) \geq \sum_j p_j H(S_j).$$

Задача 7.2.3. Докажите вогнутость непосредственно, используя спектральное разложение оператора $\sum_j p_j S_j$ и вогнутость функции $\eta(t)$.

§ 7.3. Свойства непрерывности

В рассматриваемом здесь конечномерном случае квантовая энтропия является непрерывной функцией от состояния. В самом деле, функция $\eta(x) = -x \log x$ (равномерно) непрерывна на отрезке $[0, 1]$, значит, если $S_n \rightarrow S$, то $\|\eta(S_n) - \eta(S)\| \rightarrow 0$, где $\|\cdot\|$ — операторная норма. Следовательно,

$$|H(S_n) - H(S)| = |\text{Tr}(\eta(S_n) - \eta(S))| \leq d \|\eta(S_n) - \eta(S)\| \rightarrow 0.$$

Следующая лемма дает более точную оценку, которая понадобится в дальнейшем.

Лемма 7.3.1. Пусть S_1, S_2 — два оператора плотности в d -мерном гильбертовом пространстве, причем $\|S_1 - S_2\|_1 \leq \frac{1}{e}$. Тогда

$$|H(S_1) - H(S_2)| \leq \log d \cdot \|S_1 - S_2\|_1 + \eta(\|S_1 - S_2\|_1). \quad (7.22)$$

Так как функция $\eta(x)$ монотонно возрастает при $x \in \left[0, \frac{1}{e}\right]$, из леммы следует оценка

$$|H(S_1) - H(S_2)| \leq \log d \cdot \|S_1 - S_2\|_1 + \frac{\log e}{e}. \quad (7.23)$$

Доказательство. Пусть $\lambda_1 \geq \lambda_2 \geq \dots$ ($\mu_1 \geq \mu_2 \geq \dots$) — собственные значения оператора S_1 (соответственно оператора S_2).

Задача 7.3.1. Пусть $\Delta_i = |\lambda_i - \mu_i|$. Покажите, что

$$\Delta = \sum_{i=1}^d \Delta_i \leq \|S_1 - S_2\|_1. \quad (7.24)$$

Задача 7.3.2. Докажите неравенство

$$|\eta(y) - \eta(x)| \leq \eta(y - x), \quad 0 \leq x \leq y \leq 1.$$

Комбинируя результаты этих задач, получаем

$$\begin{aligned} |H(S_1) - H(S_2)| &\leq \sum_{i=1}^d |\eta(\lambda_i) - \eta(\mu_i)| \leq \sum_{i=1}^d |\eta(\Delta_i)| = \\ &= \Delta \sum_{i=1}^d |\eta(\Delta_i/\Delta)| + \eta(\Delta) \leq \Delta \log d + \eta(\Delta). \end{aligned}$$

Принимая во внимание монотонность функции $\eta(x)$ и используя неравенство (7.24), получаем неравенство (7.22). $\square$

Задача 7.3.3. Покажите, что относительная энтропия полунепрерывна снизу в следующем смысле: если $S_n \rightarrow S$ и $S'_n \rightarrow S'$, то

$$\liminf_{n \rightarrow \infty} H(S_n; S'_n) \geq H(S; S').$$

Указание. Используйте непрерывность энтропии, представление (7.20) и тот факт, что точная верхняя грань семейства непрерывных функций полунепрерывна снизу.

Как мы увидим позже в гл. 10, в бесконечномерном гильбертовом пространстве свойство полунепрерывности снизу выполнено как для энтропии, так и для относительной энтропии, тогда как непрерывность энтропии уже не имеет места.

§ 7.4. Информационная корреляция, сцепленность формирования и условная энтропия

В классическом случае мерой количества информации, содержащейся в одной из случайных величин X , Y относительно другой, является взаимная информация $I(X; Y) = H(X) + H(Y) - H(XY)$. В квантовой статистике нет прямого аналога совместной энтропии $H(XY)$, так как совместное распределение наблюдаемых существует лишь в специальных случаях. Рассмотрим один из таких случаев. Пусть S_{12} — состояние составной квантовой системы в гильбертовом пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$. В этой ситуации очевидным аналогом шенноновской взаимной информации является величина

$$I(1; 2) = H(S_1) + H(S_2) - H(S_{12}) = H(S_{12}; S_1 \otimes S_2). \quad (7.25)$$

Будем называть эту величину *информационной корреляцией*. Из предложения 7.1.1 вытекает, что $I(1; 2) \geq 0$ и $I(1; 2) = 0$ тогда и только тогда, когда $S_{12} = S_1 \otimes S_2$.

Рассмотрим составную систему и наблюдаемые M_1 , M_2 в соответствующих подсистемах. Их совместное распределение существует и выражается формулой $p(x, y) = \text{Tr } S_{12} M_{1x} M_{2y}$. Обозначим через $I(M_1; M_2)$ шенноновскую взаимную информацию между исходами измерений наблюдаемых M_1 , M_2 .

Задача 7.4.1. Покажите, что для чистого состояния $S_{12} = |\psi\rangle\langle\psi|$ выполняется равенство

$$I(1; 2) = 2 \max_{M_1, M_2} I(M_1, M_2). \quad (7.26)$$

В случае чистого состояния S_{12} имеем $H(S_{12}) = 0$ и, используя теорему 3.1.2, получаем

$$H(S_1) = H(S_2); \quad I(1; 2) = 2H(S_1). \quad (7.27)$$

Энтропия $H(S_1)$ является естественной мерой сцепленности чистого состояния S_{12} . Она равна нулю для несцепленных состояний и принимает максимальное значение $\log d$ для состояния (3.7), что объясняет название «максимально сцепленное» для этого состояния.

Вопрос определения меры сцепленности для смешанных состояний является значительно более сложным. Наибольший интерес для нас представляет *сцепленность формирования*, которая определяется для произвольного состояния S_{12} в $\mathcal{H}_1 \otimes \mathcal{H}_2$ как

$$E_F(S_{12}) = \inf_j \sum \pi_j H(S_1^j), \quad (7.28)$$

где точная нижняя грань берется по всем возможным разложениям

$$S_{12} = \sum_j \pi_j S_{12}^j$$

состояния S_{12} в выпуклую комбинацию состояний S_{12}^j ; в терминах выпуклого анализа $E_F(S_{12})$ является *выпуклой оболочкой* непрерывной функции $S_{12} \rightarrow H(S_1)$.

Предложение 7.4.1. *Функция $S_{12} \rightarrow E_F(S_{12})$ является непрерывной и выпуклой, а точная нижняя грань в формуле (7.28) достигается на выпуклой комбинации не более чем $(d_1 d_2)^2$ чистых состояний S_{12}^j . Имеет место соотношение двойственности:*

$$E_F(S_{12}) = \max_{A_{12}} \text{Tr } S_{12} A_{12}, \quad (7.29)$$

где максимум берется по всем эрмитовым операторам A_{12} из $\mathcal{H}_1 \otimes \mathcal{H}_2$, удовлетворяющим условию

$$\text{Tr } T_{12} A_{12} \leq H(T_1) \quad (7.30)$$

для всех (чистых) состояний T_{12} в $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Доказательство. Обозначим $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, $S = S_{12}$ и $f(S) = H(\text{Tr}_{\mathcal{H}_2} S)$; функция f является непрерывной вогнутой функцией на компактном выпуклом множестве квантовых состояний $\mathfrak{S} = \mathfrak{S}(\mathcal{H})$. В доказательстве, приведенном ниже, практически не используются другие специальные свойства функции f и множества $\mathfrak{S}$, и оно может быть получено из общих фактов выпуклого анализа, но мы дадим здесь самостоятельный вывод.

Конечный набор состояний с соответствующими вероятностями обычно называют *ансамблем*. Для доказательства теоремы нам понадобится «континуальное» обобщение этого понятия, описываемое вероятностной мерой $\pi(dS)$ на множестве состояний $\mathfrak{S}(\mathcal{H})$ (концепция таких обобщенных ансамблей подробно обсуждается в гл. 10). При таком подходе обычные ансамбли описываются мерами с конечным носителем. Используя общие факты теории меры (см. комментарии), можно показать, что множество $\mathcal{P}(\mathfrak{S}(\mathcal{H}))$ всех вероятностных мер на $\mathfrak{S}(\mathcal{H})$ является компактным в топологии слабой сходимости, которая определяется как сходимость интегралов от всевозможных ограниченных непрерывных функций на $\mathfrak{S}(\mathcal{H})$.

Рассмотрим функционал

$$F(\pi) = \int_{\mathfrak{S}} f(T) \pi(dT) \quad (7.31)$$

на $\mathcal{P}(\mathfrak{S}(\mathcal{H}))$, который для мер π с конечным носителем совпадает с минимизируемым выражением в формуле (7.28). Согласно определению

этот функционал является непрерывным аффинным функционалом на $\mathcal{P}(\mathfrak{S}(\mathcal{H}))$. Нас будет интересовать его минимум на замкнутом выпуклом подмножестве $\mathcal{P}_S$ вероятностных мер π с фиксированным барицентром

$$S = \int_{\mathfrak{S}(\mathcal{H})} T \pi(dT).$$

Непрерывный функционал $F(\pi)$ достигает минимума на выпуклом множестве $\mathcal{P}_S$. Из вогнутости функции f следует, что можно выбрать минимизирующую меру π с носителем на чистых состояниях, так как всегда можно произвести спектральные разложения для всех операторов плотности $T = T_{12}$ на чистые состояния без изменения барицентра и увеличения значения $F(\pi)$.

Покажем, что всякая крайняя точка $\pi \in \mathcal{P}_S$ имеет носитель, состоящий не более чем из $(d_1 d_2)^2$ состояний. Заметим, что состояния из носителя меры π линейно независимы в том смысле, что если

$$\int_{\mathfrak{S}(\mathcal{H})} c(T) T \pi(dT) = 0 \quad (7.32)$$

для некоторой вещественной ограниченной измеримой функции $c(T)$, то $c(T) = 0$ почти всюду по мере π . Действительно, из соотношения (7.32) следует, что $\pi = \frac{1}{2}\pi_+ + \frac{1}{2}\pi_-$, где

$$\pi_{\pm}(dT) = (1 \pm \varepsilon c(T))\pi(dT)$$

для достаточно малого ε ; из того, что π — крайняя точка, следует, что $\pi_{\pm}(dT) = \pi(dT)$, а значит, $c(T) = 0 \pmod{\pi}$. Рассматривая матричные элементы (7.32), получаем, что вещественное гильбертово пространство $L^2_{\mathbb{R}}(\pi)$ натянуто на $(d_1 d_2)^2$ функций

$$\begin{aligned} T &\rightarrow \operatorname{Re}\langle e_j | T | e_k \rangle, & 1 \leq j \leq k \leq d_1 d_2, \\ T &\rightarrow \operatorname{Im}\langle e_j | T | e_k \rangle, & 1 \leq j < k \leq d_1 d_2. \end{aligned}$$

Действительно, любая функция $c(T)$, ортогональная к этим функциям в $L^2_{\mathbb{R}}(\pi)$, должна равняться нулю $\pmod{\pi}$. Оставшаяся часть доказательства предоставляется в качестве задачи.

Задача 7.4.2. Покажите, что если $\dim L^2(\pi) = n$, то носитель меры π состоит из n точек.

Неравенство $\geq$ в соотношении двойственности (7.29) получается путем интегрирования неравенства $f(T) \geq \operatorname{Tr} TA$ по любой вероятностной мере $\pi \in \mathcal{P}_S$. Для доказательства обратного неравенства рассмотрим только меры с фиксированным (но произвольным) конечным носителем, содержащим носитель оптимальной (минимизирующей) меры π^0 . Тогда

минимизация становится задачей в конечномерном пространстве с конечным числом линейных ограничений (7.30). Заметим, что эти ограничения включают в себя нормировку вероятностной меры. Применяя метод Лагранжа, получаем, что найдется эрмитов оператор Λ такой, что π^0 минимизирует функционал

$$F(\pi) - \text{Tr} \left(\int_{\mathfrak{S}} T \pi(dT) \right) \Lambda = \int_{\mathfrak{S}} [f(T) - \text{Tr} T \Lambda] \pi(dT) \quad (7.33)$$

по всем (ненормированным) положительным мерам π с заданным конечным носителем. Здесь эрмитов оператор Λ описывает набор вещественных множителей Лагранжа для ограничений (7.30). Отсюда следует, что

$$f(T) - \text{Tr} T \Lambda \geq 0, \quad f(T) - \text{Tr} T \Lambda = 0 \pmod{\pi^0}. \quad (7.34)$$

Интегрируя второе равенство по π^0 и учитывая неравенство (7.30), получаем равенство

$$\text{Tr} S \Lambda = \int_{\mathfrak{S}} f(T) \pi^0(dS) = F(\pi^0),$$

которое вместе с неравенством в формулах (7.34) означает, что Λ является решением двойственной задачи и что соотношение (7.29) имеет место с общим значением $\text{Tr} S \Lambda$.

Из соотношения двойственности вытекает, что функция $E_F(S)$ полунепрерывна снизу, как максимум непрерывных (аффинных) функций $S \rightarrow \text{Tr} S \Lambda$. Остается показать, что эта функция является и полунепрерывной сверху, т. е.

$$\limsup_{n \rightarrow \infty} E_F(S^{(n)}) \leq E_F(S^{(n)})$$

для любой последовательности состояний $S^{(n)} \rightarrow S$. Пусть

$$E_F(S) = \sum_{j=1}^N \pi_j^0 H(\text{Tr}_{\mathcal{H}_2} S_j), \quad (7.35)$$

где $S = \sum_{j=1}^N \pi_j^0 S_j$. Тогда, если оператор S невырожден, положим

$$S^{(n)} = \sum_{j=1}^N \pi_j^{(n)} S_j^{(n)},$$

где

$$\pi_j^{(n)} = t^{(n)} \pi_j^0,$$

$$S_j^{(n)} = (t^{(n)})^{-1} (S^{(n)})^{1/2} S^{-1/2} S_j S^{-1/2} (S^{(n)})^{1/2}$$

и

$$t^{(n)} = \text{Tr}(S^{(n)})^{1/2} S^{-1/2} S_j S^{-1/2} (S^{(n)})^{1/2}.$$

Эти выражения имеют смысл и для вырожденного оператора S , если под $S^{-1/2}$ понимается обобщенный обратный оператор к $S^{1/2}$, т. е. оператор, который равен обратному на носителе и нулю на ортогональном дополнении. Тогда

$$E_F(S^{(n)}) \leq \sum_{j=1}^N \pi_j^{(n)} H(\text{Tr}_{\mathcal{H}_2} S_j^{(n)}),$$

и выражение в левой части сходится к функции (7.35). Поэтому

$$\limsup_{n \rightarrow \infty} E_F(S^{(n)}) \leq E_F(S^{(n)}),$$

т. е. функция E_F является полунепрерывной сверху и, следовательно, непрерывной. $\square$

Вернемся к случаю чистых состояний S_{12} . Заметим, что в классической статистике частичные следы чистого состояния (маргинальные распределения вырожденного распределения) вновь являются чистыми и операция очищения не имеет аналога. В этой связи отметим следующее необычное свойство квантового аналога условной энтропии. В классическом случае условная энтропия всегда неотрицательна:

$$H(X|Y) = H(XY) - H(Y) = \sum_y p_y H(X|Y = y) \geq 0. \quad (7.36)$$

Определяя квантовую условную энтропию как

$$H(1|2) = H(S_{12}) - H(S_2),$$

получаем, что эта величина отрицательна, если S_{12} — чистое сцепленное состояние. Другими словами, в отличие от классической энтропии, квантовая энтропия не является монотонной по отношению к расширению системы: $H(S_1) \not\leq H(S_{12})$. Тем не менее, как и в классическом случае, имеют место следующие свойства:

- 1) монотонность условной энтропии: $H(1|23) \leq H(1|2)$;
- 2) $H(1|2) + H(1|3) \geq 0$.

Задача 7.4.3. Покажите, что эти свойства являются переформулировкой свойства строгой субаддитивности энтропии (7.19).

Приведем еще одно полезное свойство квантовой условной энтропии.

Следствие 7.4.1. Условная энтропия $H(1|2)$ является вогнутой функцией состояния S_{12} .

Доказательство. Имеем

$$\begin{aligned} H(1|2) &= H(S_{12}) - H(S_2) = \\ &= \log d_1 - \text{Tr } S_{12}(\log S_{12} + I_{12} \log d_1 - I_1 \otimes \log S_2) = \\ &= \log d_1 - H(S_{12}; \bar{S}_1 \otimes S_2), \end{aligned}$$

и утверждение вытекает из совместной выпуклости относительной энтропии и аффинности отображения $S_{12} \rightarrow \bar{S}_1 \otimes S_2$. $\square$

Благодаря этим свойствам квантовая условная энтропия является полезным аналитическим инструментом в квантовой теории информации.

§ 7.5. Обменная энтропия

Пусть Φ — канал с входным пространством $\mathcal{H}_A$ и выходным пространством $\mathcal{H}_B$ и $S = S_A$ — оператор плотности в $\mathcal{H}_A$, задающий входное состояние канала. По теореме 6.3.1 канал допускает представление Стайнспринга

$$\Phi[S_A] = \text{Tr}_{\mathcal{H}_E} V S_A V^*, \quad (7.37)$$

где V — изометрический оператор из $\mathcal{H}_A$ в $\mathcal{H}_{BE} = \mathcal{H}_B \otimes \mathcal{H}_E$, а $\mathcal{H}_E$ можно рассматривать как пространство «окружения». Передача состояния S_A порождает состояние в пространстве окружения

$$S_E = \text{Tr}_{\mathcal{H}_B} V S_A V^* = \tilde{\Phi}[S_A], \quad (7.38)$$

где $\tilde{\Phi}$ — комплементарный канал, см. § 6.6. В дальнейшем мы упростим обозначения для энтропий, опуская обозначения состояний, т. е. будем писать $H(A)$ вместо $H(S_A)$ и т. п., как это уже делалось в предыдущей главе.

Определение 7.5.1. *Обменной энтропией* называется величина $H(S_E) = H(\tilde{\Phi}[S_A])$, равная выходной энтропии окружения. Мы будем обозначать ее $H(S, \Phi)$ или просто $H(E)$.

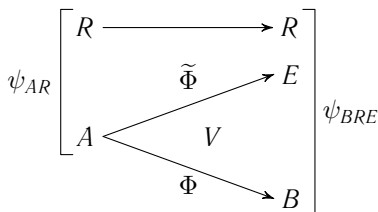


Рис. 7.1. Очищение с эталонной системой

Чтобы показать, что величина $H(S, \Phi)$ не зависит от выбора представления для канала, введем эталонную систему $\mathcal{H}_R$. Состояние S_A может быть очищено до чистого состояния $|\psi_{AR}\rangle\langle\psi_{AR}| \in \mathcal{H}_A \otimes \mathcal{H}_R$. Имеем

$$H((\Phi \otimes \text{Id}_R)|\psi_{AR}\rangle\langle\psi_{AR}|) = H(S_{BR}). \quad (7.39)$$

Составная система BRE , описываемая гильбертовым пространством $\mathcal{H}_{BRE} = \mathcal{H}_B \otimes \mathcal{H}_R \otimes \mathcal{H}_E$, описывается чистым состоянием

$$|\psi_{BR}\rangle \otimes |\psi_E\rangle = (V \otimes I_R)|\psi_{AR}\rangle. \quad (7.40)$$

Рассматривая разделение $BR|E$, получаем совокупность двух систем в чистом состоянии, значит, согласно соотношению (7.27) справедливо равенство

$$H(S_E) = H(S_{BR}), \quad (7.41)$$

где согласно формуле (7.39) правая часть зависит только от канала Φ и не зависит от выбора представления Стайнспринга. С другой стороны, (7.41) представляет собой выражение для выходной энтропии расширенного канала $\Phi \otimes \text{Id}_R$, примененного к чистому состоянию S_{AR} . Так как левая часть не содержит R , это равенство также показывает, что $H(S_{BR})$ не зависит от способа очищения состояния $S = S_A$.

Используя конструкцию комплементарного канала из формулы (6.40), мы видим, что S_E задается матрицей плотности $[\text{Tr } SV_j^* V_k]_{j,k=1,\dots,N}$, следовательно, имеет место такой результат.

Предложение 7.5.1. Пусть $\Phi[S] = \sum_{j=1}^N V_j S V_j^*$, где $\sum_{j=1}^N V_j^* V_j = I$, тогда

$$H(S, \Phi) = H([\text{Tr } SV_j^* V_k]_{j,k=1,\dots,N}). \quad (7.42)$$

Обменная энтропия удовлетворяет следующему полезному неравенству.

Пусть $S = \sum_j p_j S_j$ — смесь чистых состояний S_j , тогда

$$H(S, \Phi) \geq \sum_j p_j H(\Phi[S_j]). \quad (7.43)$$

Действительно, благодаря выпуклости квантовой энтропии $H(S, \Phi) = H(\Phi_E[\sum_j p_j S_j]) \geq \sum_j p_j H(\Phi_E[S_j])$. Но $H(\Phi_E[S_j]) = H(\Phi[S_j])$, так как система BE находится в чистом состоянии, если на вход подается чистое состояние S_j . $\square$

Пример 7.5.1. Рассмотрим деполяризующий канал (6.51) и хаотическое входное состояние $\bar{S} = I_d/d$. Используя представление Крауса (6.52) и свойства операторов Вейля, находим

$$\text{Tr } \bar{S} W_{\alpha\beta}^* W_{\alpha'\beta'} = \delta_{(\alpha\beta), (\alpha'\beta')} \begin{cases} \frac{p}{d^2}, & (\alpha\beta) \neq (00), \\ 1 - p \frac{d^2 - 1}{d^2}, & (\alpha\beta) = (00). \end{cases}$$

Следовательно,

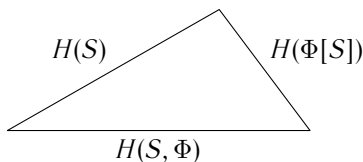
$$H(\bar{S}, \Phi) = -\left(1 - p \frac{d^2 - 1}{d^2}\right) \log \left(1 - p \frac{d^2 - 1}{d^2}\right) - p \frac{d^2 - 1}{d^2} \log \frac{p}{d^2}. \quad (7.44)$$

§ 7.6. Квантовая взаимная информация

Выше были рассмотрены три энтропийные величины: входная энтропия $H(S)$, выходная энтропия $H(\Phi[S])$ и обменная энтропия $H(S, \Phi)$. Между ними имеются соотношения, позволяющие рассматривать их как длины сторон треугольника: сумма любых двух из них больше или равна третьей. Например,

$$\begin{aligned} I(S, \Phi) &= H(S) + H(\Phi[S]) - H(S, \Phi) = \\ &= H(A) + H(B) - H(E) = H(R) + H(B) - H(BR) \geq 0 \end{aligned} \quad (7.45)$$

по свойству субаддитивности квантовой энтропии.



Так как R имеет ту же энтропию, что и A , величину $I(S, \Phi)$ можно назвать *квантовой взаимной информацией* между входом и выходом. Взаимная информация $I(S, \Phi)$ обладает целым рядом хороших свойств, аналогичных свойствам шенноновской информации.

Предложение 7.6.1. Квантовая взаимная информация $I(S, \Phi)$

- 1) *вогнута по S* ;
- 2) *выпукла по Φ* ;
- 3) *субаддитивна: $I(S_{12}, \Phi_1 \otimes \Phi_2) \leq I(S_1, \Phi_1) + I(S_2, \Phi_2)$* ;
- 4) *удовлетворяет неравенствам об обработке информации:*

$$I(S, \Phi_2 \circ \Phi_1) \leq \min \{I(S, \Phi_1), I(\Phi_1(S), \Phi_2)\}.$$

Доказательство. Доказательство основано на рассмотрении различных разделений составной системы BRE , находящейся в чистом состоянии (7.40), и на использовании свойств условной энтропии.

1. Имеем

$$\begin{aligned} I(S, \Phi) &= H(R) + H(B) - H(E) = \\ &= H(BE) + H(B) - H(E) = H(B|E) + H(B), \end{aligned} \quad (7.46)$$

где первое слагаемое является вогнутой функцией от S_{BE} согласно следствию 7.2.2, а второе — вогнутой функцией от S_B . Остается заметить, что отображения $S \rightarrow S_{BE}$ и $S \rightarrow S_B$ аффинны.

2. Имеем

$$\begin{aligned} I(S, \Phi) &= H(R) + H(B) - H(E) = \\ &= H(BE) + H(B) - H(BR) = H(R) - H(R|B), \end{aligned}$$

где первый член не зависит от Φ , а второй является вогнутой функцией от состояния $S_{BR} = (\Phi \times \text{Id}_R)[S_{AR}]$, которое аффинно зависит от Φ .

3. Пусть S_{12} — состояние в A_1A_2 , и пусть R — эталонная система такая, что S_{12} — частичный след в A_1A_2 чистого состояния в системе A_1A_2R . Обозначим через E_1, E_2 окружения каналов Φ_1, Φ_2 соответственно. Докажем неравенство

$$\begin{aligned} I(S_{12}, \Phi_1 \otimes \Phi_2) &= H(S_{12}) + H((\Phi_1 \otimes \Phi_2)(S_{12})) - H(S_{12}, \Phi_1 \otimes \Phi_2) = \\ &= H(R) + H(B_1B_2) - H(E_1E_2) \leq \\ &\leq \underbrace{H(R_1) + H(B_1) - H(E_1)}_{=RA_2} + \underbrace{H(R_2) + H(B_2) - H(E_2)}_{=RA_1}. \end{aligned}$$

Так как полная система $B_1B_2E_1E_2R$ описывается чистым состоянием, это эквивалентно неравенству

$$\begin{aligned} H(B_1B_2E_1E_2) + H(B_1B_2) - H(E_1E_2) &\leq \\ &\leq H(B_1E_1) + H(B_1) - H(E_1) + H(B_2E_2) + H(B_2) - H(E_2), \end{aligned}$$

откуда

$$H(B_1B_2E_1E_2) + H(E_1) + H(E_2) \leq H(E_1E_2) + H(B_1E_1) + H(B_2E_2),$$

что может быть получено повторным использованием свойства строгой субаддитивности.

Заметим, что последнее неравенство выражает *субаддитивность условной энтропии*:

$$H(B_1B_2|E_1E_2) \leq H(B_1|E_1) + H(B_2|E_2).$$

4. Обозначим через A входное пространство канала Φ_1 , через B — выходное пространство для Φ_1 , которое является входным для Φ_2 , и через C — выходное пространство для Φ_2 . Через $E_{1,2}$ обозначим окружения каналов $\Phi_{1,2}$. Имеем

$$I(S, \Phi_2 \circ \Phi_1) = H(R) + H(C) - H(E_1E_2). \quad (7.47)$$

Для доказательства первого неравенства об обработке информации заметим, что

$$I(S, \Phi_1) = H(R) + H(B) - H(E_1), \quad (7.48)$$

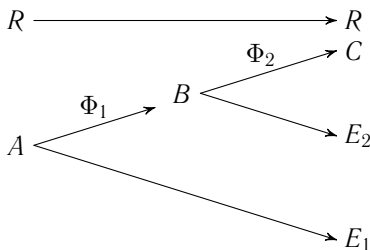


Рис. 7.2. Композиция каналов

так что доказываемое неравенство принимает вид $H(C) - H(E_1 E_2) \leq H(B) - H(E_1)$. Поскольку системы $CRE_1 E_2$ и BRE_1 описываются чистыми состояниями, это эквивалентно неравенству

$$H(R|E_1 E_2) \leq H(R|E_1),$$

которое выполнено в силу монотонности условной энтропии.

Для доказательства второго неравенства заметим, что

$$I(\Phi_1[S], \Phi_2) = H(B) + H(C) - H(E_2), \quad (7.49)$$

так что нужно доказать неравенство $H(R) - H(E_1 E_2) \leq H(B) - H(E_2)$. Поскольку системы BRE_1 и $CRE_1 E_2$ описываются чистыми состояниями, это равносильно неравенству $H(R) - H(CR) \leq H(RE_1) - H(CRE_1)$, или

$$H(C|RE_1) \leq H(C|R).$$

Последнее же неравенство выполнено в силу монотонности условной энтропии. $\square$

§ 7.7. Комментарии

1. Энтропия оператора плотности была введена фон Нейманом в книге [21]. Подробный обзор свойств квантовой энтропии и квантовой относительной энтропии можно найти в статье Верля [152] и книге Ойя и Петца [128].

Можно усилить неравенство (7.3) посредством замены $\text{Tr}(S - T)^2$ на $\|S - T\|_1^2$, см. [138]; доказательство основано на соответствующем классическом неравенстве Пинскера, см. [70, лемма 12.6.1].

2. Вещественная функция g , определенная на интервале $I \subseteq \mathbb{R}$, называется *операторно-монотонной*, если для любого n и эрмитовых $(n \times n)$ -матриц $A \leq B$ со спектром в I выполняется неравенство $g(A) \leq g(B)$. Аналогично определяются операторно-выпуклые функции. Ос-

новные результаты теории операторно-монотонных и операторно-выпуклых функций, а также большое количество полезных матричных неравенств можно найти в книге Бхатиа [63]. Используя классические результаты из теории операторно-монотонных и операторно-выпуклых функций, можно показать, что класс $\mathcal{G}$ состоит из таких операторно-выпуклых функций g на $(0, \infty)$, что $g(1) = 0$.

Известны и другие доказательства теоремы о монотонности 7.2.1, которые также достаточно сложны. Обычный подход состоит в использовании «свойства выпуклости Либана»; см. [22, 128]. В серии работ [122–124] Линдبلاد установил ряд последовательных приближений к свойству монотонности и в итоге доказал его эквивалентность сильной субаддитивности квантовой энтропии, доказанной ранее Либом и Рускаи; см. [121]. Ульман в статье [151] дал другое доказательство, основанное на интерполяционном методе (см. обзоры [132, 152]). Здесь мы опираемся на работу Лесниевски и Рускаи [119], в которой дается наиболее прямое доказательство. Оно основано на обобщении неравенства Коши—Буняковского и позволяет установить монотонность для целого класса инвариантов пар состояний в «квантовой геометростатистике», инициированной Е. А. Морозовой и Н. Н. Ченцовым [20]. Эфрос указал на связь этого круга вопросов с операторным обобщением неравенства Йенсена и понятием матричной перспективы операторно-выпуклой функции; см. [80].

Недавно было предложено новое «естественное» доказательство свойства монотонности (см. работу Белаковича и Зигмунда-Шульце [64] и книгу Хайяши [90]), основанное на операторной интерпретации квантовой относительной энтропии как оптимального показателя экспоненциального убывания ошибки в задаче различения двух квантовых состояний (квантовый аналог леммы Стейна в математической статистике — теорема 12.8.1 из книги [70]).

3. Лемма 7.3.1 была доказана Фаннесом в статье [81]. Решение задачи 7.3.1 см. в книге [128, лемма 1.7]. Ауденаэрт (см. [52]) установил неулучшаемое неравенство

$$|H(S_1) - H(S_2)| \leq \log(d-1) \cdot \|S_1 - S_2\|_1 + h_2(\|S_1 - S_2\|_1).$$

В книге [132] указано на связь этого неравенства с леммой Фано 4.4.2.

4. Информационная корреляция была введена Линдبلادом (см. [122]), который высказал следующую гипотезу:

$$I(1; 2) \leq 2 \max_{M_1, M_2} I(M_1, M_2).$$

Сцепленность формирования введена в основополагающей работе Беннета, Ди Винченцо, Смолина и Вуттерса [58]. Для смешанных состо-

яний имеется целый ряд других важных других мер сцепленности. Количественная теория сцепленности является еще одним разделом квантовой информатики, в котором математические методы получили существенное приложение и развитие, см., например, обзоры Кейля [111], Альбера и др. [50], книгу Хайаши [90].

Определение и свойства выпуклой оболочки, а также общая теорема двойственности выпуклого программирования имеются, например, в книгах Рокафеллара [25], Г. Г. Магарил-Ильяева и В. М. Тихомирова [17]. Доказательство полунепрерывности сверху сцепленности формирования опирается на конструкцию из работы М. Е. Широкова [140].

Квантовая условная энтропия введена Адами и Серфом; см. [48]. Операциональное истолкование отрицательных значений условной энтропии как своего рода кредита информации предложено Городецким, Оппенхаймом и Винтером; см. [106].

5. Обменная энтропия была введена Линдбладом в статье [125] (однако он использовал другую терминологию) и впоследствии, в контексте квантовой теории информации, независимо Барнумом, Нильсеном и Шумахером; см. [54].

6. Квантовая взаимная информация также появилась в работе Линдблада [125], а впоследствии — в работе Адами и Серфа [48], где были подробно рассмотрены ее свойства.

ГЛАВА 8

Классическая пропускная способность квантового канала связи

§ 8.1. Теорема кодирования

В главе 5 была установлена фундаментальная теорема кодирования для классически-квантового канала связи. В настоящей главе, используя этот результат, мы получим теорему кодирования для произвольного квантового канала.

Рассмотрим канал $\Phi: \mathfrak{I}(\mathcal{H}_1) \rightarrow \mathfrak{I}(\mathcal{H}_2)$ и соответствующий составной канал $\Phi^{\otimes n} = \Phi \otimes \dots \otimes \Phi: \mathfrak{I}(\mathcal{H}_1^{\otimes n}) \rightarrow \mathfrak{I}(\mathcal{H}_2^{\otimes n})$. Блочный код для такого составного канала включает с-q-канал, кодирующий классические сообщения i состояниями во входном пространстве $\mathcal{H}_1^{\otimes n}$, и q-с-канал (наблюдаемую) $M^{(n)}$ в пространстве $\mathcal{H}_2^{\otimes n}$, декодирующий выходные состояния в классические сообщения j :

$$i \rightarrow \underbrace{S_i^{(n)}}_{\text{входное состояние}} \rightarrow \underbrace{\Phi^{\otimes n}[S_i^{(n)}]}_{\text{выходное состояние}} \xrightarrow{M^{(n)}} j.$$

Это приводит к следующему определению.

Определение 8.1.1. Код $(\Sigma^{(n)}, M^{(n)})$ размера N для составного канала $\Phi^{\otimes n}$ состоит из кодирования, задаваемого набором $\Sigma^{(n)} = \{S_i^{(n)}; i = 1, \dots, N\}$ состояний в $\mathcal{H}_1^{\otimes n}$, и декодирования, описываемого наблюдаемой $M^{(n)} = \{M_j^{(n)}; j = 0, 1, \dots, N\}$, в $\mathcal{H}_2^{\otimes n}$.

Максимальная вероятность ошибки такого кода равна

$$P_e(\Sigma^{(n)}, M^{(n)}) = \max_{i=1, \dots, N} \{1 - p_{\Sigma M}(i|i)\}, \quad (8.1)$$

где $p_{\Sigma M}(j|i) = \text{Tr} \Phi^{\otimes n}[S_i^{(n)}] M_j^{(n)}$ — вероятность принятия решения j при условии, что было послано сообщение i . Минимум ошибки $P_e(\Sigma^{(n)}, M^{(n)})$ по всевозможным кодам длины n и размера N по-прежнему обозначается $p_e(n, N)$. Классическая пропускная способность $C(\Phi)$ квантового канала Φ определяется как точная верхняя грань достижимых скоростей R , для которых

$$\lim_{n \rightarrow \infty} p_e(n, 2^{nR}) = 0.$$

Напомним, что конечное распределение вероятностей π на множестве квантовых состояний $\mathfrak{S}(\mathcal{H})$, которое приписывает вероятности π_i состояниям S_i , называется *ансамблем*. Если задан ансамбль $\pi^{(n)}$ с вероятностями $\{\pi_i^{(n)}\}$ входных состояний $S_i^{(n)}$, то, используя условную вероятность $p_{\Sigma M}(j|i)$, можно найти совместное распределение входа i и выхода j и вычислить шенноновскую информацию $\mathcal{I}_n(\pi^{(n)}, M^{(n)})$. Аналогично предложению 5.4.1 получаем

$$C(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{\{\pi^{(n)}, M^{(n)}\}} \mathcal{I}_n(\pi^{(n)}, M^{(n)}). \quad (8.2)$$

Отличие от случая с- q -канала состоит в том, что здесь нет фиксированного входного алфавита и приходится оптимизировать не только входное распределение $\{\pi^{(n)}\}$ и выходную наблюдаемую $M^{(n)}$, но и всевозможные состояния $S_i^{(n)}$ на входе канала $\Phi^{\otimes n}$.

Предложение 8.1.1. *Классическая пропускная способность канала Φ равна*

$$C(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}), \quad (8.3)$$

где

$$C_\chi(\Phi) = \sup_{\{\pi_i, S_i\}} \chi(\{\pi_i\}; \{\Phi[S_i]\}), \quad (8.4)$$

величина χ определяется соотношением (5.8) и точная верхняя грань берется по всевозможным входным ансамблям $\pi = \{\pi_i, S_i\}$ в $\mathcal{H}$.

Заметим, что аналогично предложению 5.4.1 в соотношениях (8.2), (8.3) предел при $n \rightarrow \infty$ равен точной верхней грани по n благодаря супераддитивности соответствующих последовательностей.

Доказательство. Неравенство $\leq$ в формуле (8.3) вытекает из соотношения (8.2) и из верхней границы в теореме 5.3.1. Покажем, что

$$C(\Phi) \geq \lim_{n \rightarrow \infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}) \equiv \bar{C}(\Phi). \quad (8.5)$$

Возьмем $R < \bar{C}(\Phi)$, тогда можно выбрать n_0 и ансамбль $\pi^{(n_0)} = \{\pi_i^{(n_0)}, S_i^{(n_0)}\}$ в $\mathcal{H}_1^{\otimes n_0}$ такие, что

$$n_0 R < \chi(\{\pi_i^{(n_0)}\}; \{\Phi^{\otimes n_0}[S_i^{(n_0)}]\}). \quad (8.6)$$

Рассмотрим с- q -канал $\tilde{\Phi}$ в $\mathcal{H}_2^{\otimes n_0}$, определенный соотношением

$$i \rightarrow \Phi^{\otimes n_0}[S_i^{(n_0)}]. \quad (8.7)$$

Согласно теореме кодирования 5.2.1 для s - q -каналов пропускная способность канала $\tilde{\Phi}$ равна

$$C(\tilde{\Phi}) = \max_{\pi} \chi(\{\pi_i\}; \{\Phi^{\otimes n_0}[S_i^{(n_0)}]\}), \quad (8.8)$$

где состояния фиксированы и максимум берется по распределению вероятностей π . В силу неравенства (8.6) это значение больше, чем $n_0 R$. Обозначая через $\tilde{p}_e(n, N)$ минимальную вероятность ошибки для канала $\tilde{\Phi}$, получаем

$$p_e(nn_0, 2^{(nn_0)R}) \leq \tilde{p}_e(n, 2^{(n_0 R)}), \quad (8.9)$$

поскольку любой код размера N для канала $\tilde{\Phi}^{\otimes n}$ определяет код того же размера для $\Phi^{\otimes nn_0}$. Таким образом, при $R < \tilde{C}(\Phi)$ правая, а значит, и левая части соотношения (8.9) стремятся к нулю при $n \rightarrow \infty$. Рассуждая, как в предложении 5.4.1, получаем $p_e(n', 2^{n'R}) \rightarrow 0$ при $n' \rightarrow \infty$, и, следовательно, неравенство (8.5) выполняется. $\square$

§ 8.2. χ -пропускная способность

Мы будем называть величину $C_\chi(\Phi)$, определенную формулой (8.4), χ -пропускной способностью канала Φ . Итак,

$$C_\chi(\Phi) = \sup_{\{\pi_i, S_i\}} \left[H\left(\sum_i \pi_i \Phi[S_i]\right) - \sum_i \pi_i H(\Phi[S_i]) \right], \quad (8.10)$$

а это соотношение можно также переписать в виде

$$C_\chi(\Phi) = \sup_{S \in \mathfrak{S}(\mathcal{H})} [H(\Phi(S)) - \hat{H}_\Phi(S)], \quad (8.11)$$

где введена новая характеристика канала

$$\hat{H}_\Phi(S) = \inf_{\pi: \sum_i \pi_i S_i = S} \sum_i \pi_i H(\Phi(S_i)) \quad (8.12)$$

— *выпуклая оболочка* выходной энтропии $H(\Phi[S])$. Здесь точная нижняя грань берется по всевозможным ансамблям π с фиксированным средним состоянием $\sum_i \pi_i S_i = S$.

Задача 8.2.1. Докажите, что для идеального канала $\hat{H}_{\text{Id}}(S) \equiv 0$.

Величина (8.12) тесно связана со сцепленностью формирования (7.28), а именно,

$$\hat{H}_\Phi(S) = E_F(VSV^*),$$

где V — изометрия в представлении Стайнспринга (6.8) канала Φ , так что VSV^* является состоянием составной системы «выход-окружение». Доказательство следующей леммы аналогично доказательству предложения 7.4.1.

Лемма 8.2.1. *Выпуклая оболочка выходной энтропии $\hat{H}_\Phi(S)$ является непрерывной выпуклой функцией на $\mathfrak{S}(\mathcal{H})$. Точная нижняя грань в выражении (8.12) достигается на ансамбле, состоящем не более чем из d_1^2 чистых состояний, $d_1 = \dim \mathcal{H}_1$.*

Следствие 8.2.1. *Точная верхняя грань в выражении (8.10) для χ -пропускной способности достигается на ансамбле, состоящем не более чем из d_1^2 чистых состояний.*

Задача 8.2.2. Используя задачу 4.3.2, докажите необходимость и достаточность для оптимальности ансамбля $\pi = \{\pi_i, S_i\}$ со средним состоянием $\bar{S}_\pi = \sum_i \pi_i S_i$ следующего условия *максимальной удаленности*: найдется положительное число μ такое, что

$$H(\Phi[S]; \Phi[\bar{S}_\pi]) \leq \mu \quad \text{для всех (чистых) входных состояний } S, \quad (8.13)$$

причем равенство достигается для членов ансамбля $S = S_j$, $\pi_j > 0$; при этом с необходимостью $\mu = C_\chi(\Phi)$. *Указание.* Используйте равенство

$$\frac{\partial}{\partial \pi_j} \chi(\{\pi_i\}; \{\Phi[S_i]\}) = H(\Phi[S_j]; \Phi[\bar{S}_\pi]) - \log e.$$

χ -пропускная способность может быть вычислена для ряда интересных каналов.

Задача 8.2.3. Покажите, что $C_\chi(\text{Id}) = \log d$ для идеального канала в d -мерном гильбертовом пространстве. Для квантового стирающего канала $C_\chi(\Phi_p) = (1 - p) \log d$, где p — вероятность стирания. В обоих случаях оптимальный ансамбль состоит из равновероятных чистых состояний, отвечающих ортонормированному базису в $\mathcal{H}$.

Предложение 8.2.1. Пусть Φ — ковариантный канал (см. § 6.7),

$$\Phi[U_g^{(1)} S (U_g^{(1)})^*] = U_g^{(2)} \Phi[S] (U_g^{(2)})^*.$$

Если представление $U_g^{(1)}$ неприводимо, то

$$C_\chi(\Phi) = H\left(\Phi\left[\frac{I_1}{d_1}\right]\right) - \min_S H(\Phi[S]), \quad (8.14)$$

где минимум берется по множеству чистых состояний.

Доказательство. Предположим сначала, что группа симметрий G конечна. Неприводимость представления означает отсутствие нетривиальных инвариантных подпространств, что эквивалентно следующему

свойству: всякий оператор, коммутирующий со всеми $U_g^{(1)}$, кратен единичному оператору. Отсюда аналогично доказательству соотношения (6.49) получаем

$$|G|^{-1} \sum_{g \in G} U_g^{(1)} S(U_g^{(1)})^* = \frac{I_1}{d_1}. \quad (8.15)$$

Покажем, что

$$\max_{S \in \mathfrak{S}(\mathcal{H})} H(\Phi[S]) = H\left(\Phi\left[\frac{I_1}{d_1}\right]\right). \quad (8.16)$$

Это вытекает из того, что функция $S \rightarrow H(\Phi[S])$ вогнута и инвариантна относительно преобразований $S \rightarrow U_g^{(1)} S U_g^{A*}$, поэтому для произвольного S справедливо неравенство

$$\begin{aligned} H(\Phi[S]) &= |G|^{-1} \sum_{g \in G} H(\Phi[U_g^{(1)} S(U_g^{(1)})^*]) \leq \\ &\leq H\left(\Phi\left[|G|^{-1} \sum_{g \in G} U_g^{(1)} S(U_g^{(1)})^*\right]\right). \end{aligned} \quad (8.17)$$

Неравенство $\leq$ вытекает тогда из соотношения (8.15), так что достаточно показать, что

$$C_\chi(\Phi) \geq H\left(\Phi\left[\frac{I_1}{d_1}\right]\right) - \min_S H(\Phi[S]). \quad (8.18)$$

Выберем состояние S_0 , минимизирующее выходную энтропию. Поскольку выходная энтропия вогнута, она достигает минимума на множестве чистых состояний. Поэтому значение в правой части равенства (8.14) достигается для ансамбля состояний $S_g = U_g^{(1)} S_0 U_g^{A*}$, $g \in G$, взятых с равными вероятностями $\pi_g = |G|^{-1}$.

Если группа $|G|$ непрерывна, то применимо аналогичное рассуждение, но оптимизирующее распределение будет непрерывным, а именно равномерным распределением на G . Затем можно использовать конечную аппроксимацию и свойство непрерывности. $\square$

Пример 8.2.1. Для деполяризующего канала (6.51) имеем

$$C_\chi(\Phi) = \log d + \left(1 - p \frac{d-1}{d}\right) \log \left(1 - p \frac{d-1}{d}\right) + p \frac{d-1}{d} \log \frac{p}{d}, \quad (8.19)$$

что достигается для ансамбля равновероятных чистых состояний, отвечающих ортонормированному базису в $\mathcal{H}$.

В самом деле, канал является неприводимо ковариантным, поэтому применимо предложение 8.2.1. Для произвольного чистого входного состояния выход $\Phi[|\psi\rangle\langle\psi|]$ имеет простое собственное значение $1 - p \frac{d-1}{d}$

и $d - 1$ собственных значений $\frac{p}{d}$. Поэтому выходная энтропия равна

$$-\left(1 - p\frac{d-1}{d}\right) \log \left(1 - p\frac{d-1}{d}\right) - p\frac{d-1}{d} \log \frac{p}{d}$$

для всех чистых входных состояний, откуда следует соотношение (8.19).

Пример 8.2.2. Вычислим χ -пропускную способность произвольного q -битного унитарного канала Φ . Такой канал неприводимо ковариантен по отношению к представлению (6.50) (см. задачу 6.8.3), поэтому мы вновь можем применить предложение 8.2.1.

При вычислении $\min_{S \in \mathcal{S}(\mathcal{H})} H(\Phi(S))$ можно считать, что $\Phi = \Lambda$, если принять во внимание унитарную инвариантность квантовой энтропии. Заметим также, что согласно задаче 2.1.2 энтропия q -битного состояния (2.8) равна

$$H(S(a)) = h_2\left(\frac{1 - |a|}{2}\right). \quad (8.20)$$

Теперь учтем, что шар Блоха сжимается каналом Λ в эллипсоид с полуосями $|\lambda_\gamma|$, $\gamma = x, y, z$, и минимум выходной энтропии достигается на конце самой длинной полуоси, отвечающем состоянию с собственными значениями $\frac{1 \pm \max_\gamma |\lambda_\gamma|}{2}$. Отсюда следует, что значение χ -пропускной способности равно

$$C_\chi(\Phi) = 1 - h_2\left(\frac{1 - \max_\gamma |\lambda_\gamma|}{2}\right). \quad (8.21)$$

§ 8.3. Проблема аддитивности

8.3.1. Эффект сцепленности в кодировании и декодировании

Одной из наиболее интересных и трудных математических проблем в квантовой теории информации является *гипотеза аддитивности*:

$$C_\chi(\Phi_1 \otimes \Phi_2) = C_\chi(\Phi_1) + C_\chi(\Phi_2) \quad (8.22)$$

для произвольных каналов Φ_1, Φ_2 . Если свойство (8.22) выполнено для некоторого канала $\Phi = \Phi_1$ и произвольного канала Φ_2 , то имеет место равенство

$$C_\chi(\Phi^{\otimes n}) = nC_\chi(\Phi) \quad (8.23)$$

и в силу соотношения (8.3) классическая пропускная способность канала Φ равна его χ -пропускной способности:

$$C(\Phi) = C_\chi(\Phi). \quad (8.24)$$

Свойство аддитивности было установлено для некоторых важных классов, таких как каналы, разрушающие сцепленность, q -битные унитарные каналы и деполяризующий канал. Однако недавно было доказано, что по крайней мере в высоких размерностях могут существовать каналы, для которых свойства (8.22), (8.23), (8.24) не выполняются (см. Комментарии).

Аддитивность шенноновской пропускной способности обусловлена в конечном счете отсутствием сцепленности в классических системах. Чтобы увидеть это, попытаемся обобщить на квантовый случай классическое доказательство аддитивности, использующее условия Куна—Таккера (см. предложение 4.3.1). Пусть Φ_1, Φ_2 — два канала, оптимальные ансамбли которых имеют средние состояния $\bar{S}_{\pi^1}, \bar{S}_{\pi^2}$, и мы хотим доказать, что

$$C_\chi(\Phi_1 \otimes \Phi_2) \leq C_\chi(\Phi_1) + C_\chi(\Phi_2). \quad (8.25)$$

Тогда условие (8.13), примененное к произведению каналов $\Phi_1 \otimes \Phi_2$, требует выполнения неравенства

$$H((\Phi_1 \otimes \Phi_2)(S_{12}); (\Phi_1 \otimes \Phi_2)(\bar{S}_{\pi^1} \otimes \bar{S}_{\pi^2})) \leq C_\chi(\Phi_1) + C_\chi(\Phi_2) \quad (8.26)$$

для *всех* чистых входных состояний S_{12} произведения каналов. Равенство должно выполняться для тензорных произведений членов оптимальных ансамблей с положительными вероятностями, что легко получается из соответствующих равенств для каналов Φ_1, Φ_2 , как и неравенство (8.26) для состояний-произведений $S_{12} = S_1 \otimes S_2$. Однако доказательство неравенства (8.26) для *сцепленных* состояний не проще, чем доказательство самой гипотезы аддитивности.

Аддитивность величины $C_\chi(\Phi)$ имела бы удивительное физическое следствие — это означало бы, что использование сцепленных кодовых состояний не увеличивает пропускную способность квантового канала. С другой стороны, в § 5.4 мы видели, что использование сцепленных декодирований приводит к такому эффекту. Рассмотрим это подробнее.

Кодирование $\Sigma^{(n)} = \{S_i^{(n)}\}$ в определении 8.1.1 назовем *несцепленным*, если

$$S_i^{(n)} = \sum_{x^n} p(x^n|i) S_{x_1} \otimes \dots \otimes S_{x_n}, \quad (8.27)$$

где S_{x_k} — состояние в k -й копии пространства $\mathcal{H}$, а $p(x^n|i)$ — условная вероятность, описывающая предварительную обработку классического входного сообщения. Напомним, что декодирование $M^{(n)}$ называется *несцепленным*, если оно имеет вид (5.33).

Для данного квантового канала Φ можно определить четыре классические пропускные способности $C_{1,1}, C_{1,\infty}, C_{\infty,1}, C_{\infty,\infty}$, где первый

(второй) индекс относится к кодированию (декодированию), а ∞ означает использование произвольных сцепленных блочных кодирований (декодирований), тогда как 1 означает ограничение несцепленными кодированиями (декодированиями) в определении 8.1.1 и соответственно в формуле (8.2). Очевидно, что $C_{\infty, \infty} = C(\Phi)$.

Задача 8.3.1. Используя классическую теорему кодирования, покажите, что $C_{1,1} = \max_{\pi, M} \mathcal{I}_1(\pi, M)$.

Величину $C_{1,1}$ будем называть *шенноновской пропускной способностью* квантового канала Φ .

Задача 8.3.2. Используя квантовую теорему кодирования 5.2.1, покажите, что $C_{1,\infty} = C_\chi(\Phi)$.

Соотношения между четырьмя пропускными способностями показаны на следующей диаграмме:

$$\begin{array}{ccc} C_{\infty,1} & \leq & C_{\infty,\infty} (= C) \\ \parallel & & \vee \\ C_{1,1} & \leq & C_{1,\infty} (= C_\chi) \end{array} \quad (8.28)$$

где $\leq$ в данном случае следует понимать как «меньше или равно для всех каналов и строго меньше для некоторых».

Равенство

$$C_{1,1} = C_{\infty,1} \quad (8.29)$$

означает, что использование сцепленных входных состояний при несцепленных выходных наблюдаемых не увеличивает количество информации; оно будет доказано ниже. Верхнее неравенство $C_{\infty,1} \leq C_{\infty,\infty}$ следует из этого равенства и нижнего неравенства, которое выражает возможность строгой супераддитивности по отношению к декодированиям, продемонстрированную в § 5.4.

Доказательство равенства (8.29). Пусть Φ — некоторый канал и π — распределение вероятностей, приписывающее вероятность π_k входному состоянию S_k , и пусть $M = \{M_j\}$ — наблюдаемая, измеряемая на выходе канала. Обозначим через $\mathcal{I}_\Phi(\pi, M)$ классическую шенноновскую информацию, отвечающую входному распределению π и переходной вероятности $p(j|k) = \text{Tr } \Phi[S_k]M_j = \text{Tr } S_k \Phi^*[M_j]$. Чтобы доказать равенства (8.29), достаточно установить неравенство

$$\begin{aligned} \max_{\{\pi, M^1, M^2\}} \mathcal{I}_{\Phi_1 \otimes \Phi_2}(\pi, M^1 \otimes M^2) &\leq \\ &\leq \max_{\{\pi^1, M^1\}} \mathcal{I}_{\Phi_1}(\pi^1, M^1) + \max_{\{\pi^2, M^2\}} \mathcal{I}_{\Phi_2}(\pi^2, M^2), \end{aligned} \quad (8.30)$$

В терминах классической взаимной информации имеем

$$\mathcal{I}_{\Phi}(\pi, M) = I(X; Y),$$

где X — входная случайная величина, принимающая значения k , а Y — выходная величина, принимающая значения j . Чтобы доказать неравенство (8.30), рассмотрим состояния S_k в гильбертовом пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$ канала $\Phi_1 \otimes \Phi_2$ с наблюдаемой $M^1 \otimes M^2$. Тогда условная вероятность равна

$$p(j_1, j_2|k) = \text{Tr} S_k(\Phi_1^*[M_{j_1}] \otimes \Phi_2^*[M_{j_2}]) = p^1(j_1|j_2, k)p^2(j_2|k), \quad (8.31)$$

где

$$p^1(j_1|j_2, k) = \text{Tr}_1 S_{j_2, k}^1 \Phi_1^*[M_{j_1}], \quad p^2(j_2|k) = \text{Tr}_2 S_k^2 \Phi_2^*[M_{j_2}]$$

и

$$S_k^2 = \text{Tr}_1 S_k, \quad S_{j_2, k}^1 = \frac{\text{Tr}_2 S_k(I \otimes \Phi_2^*[M_{j_2}])}{\text{Tr} S_k(I \otimes \Phi_2^*[M_{j_2}])}.$$

Здесь Tr_s обозначает частичный след по s -й подсистеме ($s = 1, 2$) в $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Имеем

$$I(X; Y_1 Y_2) = H(Y_1 Y_2) - H(Y_1 Y_2|X),$$

где $H(\cdot)$, $H(\cdot|\cdot)$ — энтропия и условная энтропия случайных величин соответственно. В силу субаддитивности классической энтропии имеем

$$H(Y_1 Y_2) \leq H(Y_1) + H(Y_2).$$

С другой стороны,

$$H(Y_1 Y_2|X) = H(Y_1|Y_2 X) + H(Y_2|X).$$

Сопоставляя эти соотношения, получаем

$$I(X; Y_1 Y_2) \leq I(X Y_2; Y_1) + I(X; Y_2),$$

а это неравенство в силу соотношения (8.31) сводится к неравенству

$$\mathcal{I}_{\Phi_1 \otimes \Phi_2}(\pi, M^1 \otimes M^2) \leq \mathcal{I}_{\Phi_1}(\pi^1, M^1) + \mathcal{I}_{\Phi_2}(\pi^2, M^2),$$

где π^1 — распределение, приписывающее вероятности $\pi_k p^2(j_2|k)$ состояниям $S_{j_2, k}^1$, а π^2 — распределение, приписывающее вероятности π_k состояниям S_k^2 . Взяв максимум по π и S , получаем неравенство (8.30). $\square$

8.3.2. Иерархия свойств аддитивности

Важной характеристикой квантового канала Φ , которая уже появлялась в § 8.2, является минимальная выходная энтропия

$$\check{H}(\Phi) = \min_{S \in \mathfrak{S}(\mathcal{H})} H(\Phi(S)). \quad (8.32)$$

Соответствующая ей гипотеза аддитивности имеет вид

$$\check{H}(\Phi_1 \otimes \Phi_2) = \check{H}(\Phi_1) + \check{H}(\Phi_2). \quad (8.33)$$

В силу вогнутости энтропии минимум в формуле (8.32) достигается на чистом состоянии $S \in \text{extr } \mathfrak{S}(\mathcal{H})$. Из этого следует, что классический аналог величины $\check{H}(\Phi)$ аддитивен, поскольку всякое чистое состояние составной классической системы является произведением чистых состояний подсистем. В квантовом случае для тензорного произведения $\mathcal{H}_1 \otimes \mathcal{H}_2$, описывающего составную систему, выполняется соотношение

$$\text{extr } \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2) \supsetneq \text{extr } \mathfrak{S}(\mathcal{H}_1) \times \text{extr } \mathfrak{S}(\mathcal{H}_2), \quad (8.34)$$

которое следует из наличия сцепленных состояний, так что для аддитивности (8.33) нет очевидной причины.

Ясно, что в формуле (8.33) всегда имеет место неравенство $\leq$. Отсюда следует, что эта формула, очевидно, выполняется для каналов с нулевой минимальной выходной энтропией, т. е. таких, для которых существует чистое выходное состояние, например для идеального и стирающего каналов.

Задача 8.3.3. Свойства (8.22) и (8.33) равносильны для двух ковариантных каналов, удовлетворяющих условиям предложения 8.2.1. *Указание.* Используйте тот факт, что тензорное произведение неприводимых представлений двух групп симметрий G_1, G_2 является неприводимым представлением группы $G_1 \times G_2$.

Рассмотрим теперь выпуклую оболочку выходной энтропии $\hat{H}_\Phi(S)$, определенную соотношением (8.12). Гипотетическое свойство супераддитивности для этой величины формулируется следующим образом: для произвольного состояния $S_{12} \in \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ и каналов Φ_1, Φ_2 справедливо неравенство

$$\hat{H}_{\Phi_1 \otimes \Phi_2}(S_{12}) \geq \hat{H}_{\Phi_1}(S_1) + \hat{H}_{\Phi_2}(S_2), \quad (8.35)$$

где S_1, S_2 — частичные следы состояния S_{12} в $\mathcal{H}_1, \mathcal{H}_2$.

Свойство супераддитивности (8.35) связано со следующим свойством сцепленности формирования: пусть $\mathcal{H}_1 = \mathcal{H}_1^A \otimes \mathcal{H}_1^B$ и $\mathcal{H}_2 = \mathcal{H}_2^A \otimes \mathcal{H}_2^B$, и пусть S_{12}^{AB} — произвольное состояние в $\mathcal{H}_1 \otimes \mathcal{H}_2$, тогда

$$E_F(S_{12}^{AB}) \geq E_F(S_1^{AB}) + E_F(S_2^{AB}), \quad (8.36)$$

где сцепленность формирования определяются по отношению к разбиению $A|B$. А именно, если бы гипотеза (8.36) выполнялась для всех состояний S_{12}^{AB} , то гипотеза (8.35) выполнялась бы для всех каналов Φ_1, Φ_2 и всех состояний S_{12} , тогда как если бы гипотеза (8.35) выполнялась для всех состояний S_{12} и каналов частичного следа, то гипотеза (8.36) выполнялась бы для всех состояний S_{12}^{AB} .

Предложение 8.3.1. *Для данных каналов Φ_1, Φ_2 из свойства супераддитивности (8.35) следует аддитивность как минимальной выходной энтропии (8.33), так и χ -пропускной способности (8.22).*

Доказательство. В самом деле, пусть S_{12}^0 доставляет минимум функции $H(\Phi_1 \otimes \Phi_2)(S_{12})$, тогда

$$\begin{aligned} \check{H}(\Phi_1 \otimes \Phi_2) &= H((\Phi_1 \otimes \Phi_2)(S_{12}^0)) \geq \hat{H}_{\Phi_1 \otimes \Phi_2}(S_{12}^0) \geq \\ &\geq \hat{H}_{\Phi_1}(S_1^0) + \hat{H}_{\Phi_2}(S_2^0) \geq \check{H}(\Phi_1) + \check{H}(\Phi_2), \end{aligned}$$

откуда следует соотношение (8.33). С другой стороны, из гипотезы (8.35) и субаддитивности квантовой энтропии следует, что

$$\begin{aligned} H((\Phi_1 \otimes \Phi_2)(S_{12})) - \hat{H}_{\Phi_1 \otimes \Phi_2}(S_{12}) &\leq \\ &\leq H((\Phi_1 \otimes \Phi_2)(S_{12})) - \hat{H}_{\Phi_1}(S_1) - \hat{H}_{\Phi_2}(S_2) \leq \\ &\leq [H(\Phi_1(S_1)) - \hat{H}_{\Phi_1}(S_1)] + [H(\Phi_2(S_2)) - \hat{H}_{\Phi_2}(S_2)]. \quad (8.37) \end{aligned}$$

Используя соотношение (8.11), получаем

$$C_\chi(\Phi_1 \otimes \Phi_2) \leq C_\chi(\Phi_1) + C_\chi(\Phi_2),$$

откуда и следует равенство (8.22). $\square$

Далее, свойство (8.35) тесно связано с аддитивностью χ -пропускной способности с ограничениями на входе. Пусть F — положительный оператор во входном гильбертовом пространстве $\mathcal{H}$ канала, E — положительная постоянная. Рассмотрим χ -пропускную способность при линейном ограничении $\text{Tr } SF \leq E$ на входное состояние S :

$$C_\chi(\Phi, F, E) = \max_{S: \text{Tr } SF \leq E} [H(\Phi(S)) - \hat{H}_\Phi(S)]. \quad (8.38)$$

Задача 8.3.4. Пусть имеется два канала Φ_1, Φ_2 с соответствующими ограничениями F_1, F_2 . Докажите, что тогда из неравенства (8.35) и соотношения (8.11) следует, что

$$\begin{aligned} C_\chi(\Phi_1 \otimes \Phi_2, F_1 \otimes I_2 + I_1 \otimes F_2, E) &= \\ &= \max_{E_1 + E_2 = E} [C_\chi(\Phi_1, F_1, E_1) + C_\chi(\Phi_2, F_2, E_2)]. \quad (8.39) \end{aligned}$$

Замечательно, однако, что все сформулированные гипотезы аддитивности оказываются равносильными в следующем смысле.

Теорема 8.3.1. *Гипотезы (8.33), (8.22), (8.23) и (8.35) глобально эквивалентны в том смысле, что если одна из них выполняется для всех каналов, то и другие выполняются для всех каналов. Более того, они глобально эквивалентны супераддитивности сцепленности формирования (8.36) и аддитивности χ -пропускной способности с произвольными входными ограничениями.*

Из этой теоремы также вытекает, что контрпример к одной из гипотез влечет существование контрпримеров ко всем остальным.

Мы не будем приводить доказательство этой теоремы и ограничимся рассмотрением некоторых случаев, в которых удастся доказать наиболее сильное свойство (8.35).

Предложение 8.3.2. *Пусть Φ_2 — произвольный канал. Свойство (8.35) выполняется, если Φ_1 — ортогональная выпуклая сумма (см. определение 6.6.1) идеального канала и такого канала $\Phi_{(0)}$, что это свойство выполняется для пары $\Phi_{(0)}, \Phi_2$.*

Отсюда следует, что для такого канала Φ_1 выполняется также аддитивность минимальной выходной энтропии (8.33) и χ -пропускной способности (8.22). Например, это верно для стирающего канала, поскольку он является ортогональной прямой суммой идеального канала и канала, разрушающего сцепленность, для которого свойство (8.35) будет установлено в п. 8.3.3.

Доказательство. Пусть $\Phi^{(q)} = q \text{Id} \oplus (1 - q)\Phi^{(0)}$. Тогда

$$H(\Phi^{(q)}(S)) = qH(S) + (1 - q)H(\Phi^{(0)}(S)) + h_2(q),$$

где $h_2(q) = -q \log q - (1 - q) \log(1 - q)$ — двоичная энтропия,

$$\hat{H}_{\Phi^{(q)}}(S) = (1 - q)\hat{H}_{\Phi^{(0)}}(S) + h_2(q), \quad (8.40)$$

поскольку минимум в выражении для $\hat{H}_{\Phi^{(0)}}(S)$ достигается для ансамбля чистых состояний S_j , для которого $H(S_j) = 0$. Для произвольного канала Φ_2 имеем

$$\Phi^{(q)} \otimes \Phi_2 = q(\text{Id} \otimes \Phi_2) \oplus (1 - q)(\Phi^{(0)} \otimes \Phi_2).$$

Тогда

$$\begin{aligned} \hat{H}_{\Phi^{(q)} \otimes \Phi_2}(S_{12}) &\geq q\hat{H}_{\text{Id} \otimes \Phi_2}(S_{12}) + (1 - q)\hat{H}_{\Phi^{(0)} \otimes \Phi_2}(S_{12}) + h_2(q) \geq \\ &\geq q\hat{H}_{\Phi_2}(S_2) + (1 - q)[\hat{H}_{\Phi^{(0)}}(S_1) + \hat{H}_{\Phi_2}(S_2)] + h_2(q), \end{aligned}$$

где использована супераддитивность величины $\hat{H}_{\text{Id} \otimes \Phi_2}(S_{12})$, $\hat{H}_{\Phi^{(0)} \otimes \Phi_2}(S_{12})$ и тот факт, что $\hat{H}_{\text{Id}}(S_1) \equiv 0$. Используя соотношение (8.40), получаем, что правая часть равна $\hat{H}_{\Phi^{(q)}}(S_1) + \hat{H}_{\Phi_2}(S_2)$. $\square$

Задача 8.3.5. Используя разложение Шмидта (теорема 3.1.2), покажите, что $H(\Phi[S]) = H(\tilde{\Phi}[S])$ для любого чистого состояния S , где $\tilde{\Phi}$ — канал, комплементарный к Φ . Поэтому если какое-либо из свойств (8.35), (8.33) выполняется для каналов Φ_1, Φ_2 , то аналогичное свойство выполняется для комплементарных каналов $\tilde{\Phi}_1, \tilde{\Phi}_2$.

Отсюда, в частности, следует, что предложение 8.3.2 имеет место с заменой идеального канала на комплементарный ему полностью деполаризующий канал.

8.3.3. Некоторые энтропийные неравенства

Получим неравенства, которые позволяют в некоторых случаях доказать супераддитивность выпуклой оболочки (8.35) и, следовательно, аддитивность минимальной выходной энтропии (8.33) и χ -пропускной способности (8.22).

Рассмотрим состояние S и измерение, описываемое семейством операторов A_k , удовлетворяющих условию нормировки $\sum_k A_k^* A_k = I$, так что исход k появляется с вероятностью $\pi_k = \text{Tr} S A_k^* A_k$ и приводит к апостериорному состоянию системы $S_k = A_k S A_k^* / \pi_k$. Энтропии начального и апостериорных состояний связаны *неравенством Линдблада—Озавы*

$$H(S) \geq \sum_k \pi_k H(S_k). \quad (8.41)$$

Для доказательства положим $\mathcal{H} = \mathcal{H}_1$ и рассмотрим очищение $|\psi\rangle$ состояния S в $\mathcal{H}_1 \otimes \mathcal{H}_2$. Тогда

$$\pi_k S_k = \text{Tr}_{\mathcal{H}_2} (A_k \otimes I) |\psi\rangle \langle \psi| (A_k \otimes I)^*$$

и $S_2 = \text{Tr}_{\mathcal{H}_1} S = \sum_k \pi_k S_2^k$, где

$$\pi_k S_2^k = \text{Tr}_{\mathcal{H}_1} (A_k \otimes I) |\psi\rangle \langle \psi| (A_k \otimes I)^*.$$

Применяя теорему 3.1.2 дважды и используя вогнутость квантовой энтропии, получаем

$$H(S) = H(S_2) = H\left(\sum_k \pi_k S_2^k\right) \geq \sum_k \pi_k H(S_2^k) = \sum_k \pi_k H(S_k). \quad \square$$

Частным случаем является следующее неравенство для составной системы. Пусть S_{12} — состояние составной системы в $\mathcal{H}_1 \otimes \mathcal{H}_2$, и пусть

$\{|e_k^2\rangle\}$ — ортонормированный базис в $\mathcal{H}_2$. Полагая $A_k = I_1 \otimes |e_k^2\rangle\langle e_k^2|$, получаем

$$H(S_{12}) \geq \sum_k \pi_k H(S_1^k), \quad (8.42)$$

где $\pi_k S_1^k = \langle e_k^2 | S_{12} | e_k^2 \rangle$. Это может быть использовано для доказательства гипотезы аддитивности в следующем частном случае.

Предложение 8.3.3. *Свойство (8.35) выполняется в случае, когда $\Phi_1 = \Phi$ — произвольный канал в $\mathcal{H}_1$, а $\Phi_2 = \text{Id}_2$ — идеальный канал в $\mathcal{H}_2$.*

Доказательство. Поскольку $\hat{H}_{\text{Id}}(S) \equiv 0$ согласно задаче 8.2.1, мы должны доказать, что

$$\hat{H}_{(\Phi \otimes \text{Id}_2)}(S_{12}) \geq \hat{H}_{\Phi}(S_1). \quad (8.43)$$

Пусть $S_{12} = \sum_i \pi_i S_{12}^i$ — оптимальное разложение, т. е.

$$\hat{H}_{(\Phi \otimes \text{Id}_2)}(S_{12}) = \sum_i \pi_i H((\Phi \otimes \text{Id}_2)[S_{12}^i]).$$

Используя неравенство (8.42), получаем

$$\sum_i \pi_i H((\Phi \otimes \text{Id}_2)[S_{12}^i]) \geq \sum_{ik} \pi_i \pi_{ik} H(\Phi[S_1^{ik}]), \quad (8.44)$$

где $\pi_{ik} S_1^{ik} = \langle e_k^2 | S_{12}^i | e_k^2 \rangle$. Теперь мы имеем разложение S_1 в состояния S_1^{ik} с вероятностями $\pi_i \pi_{ik}$ для канала Φ , поэтому правая часть соотношения (8.44) больше или равна $\hat{H}_{\Phi}(S_{12})$. $\square$

Предложение 8.3.4. *Свойство (8.35) выполняется в случае, когда $\Phi_1 = \Phi$ — канал, разрушающий сцепленность (см. § 6.4), а $\Phi_2 = \Psi$ — произвольный канал.*

Лемма 8.3.1. *Пусть $\pi_j \geq 0$, $\sum \pi_j = 1$ и S_1^j, S_2^j — произвольные состояния систем 1, 2. Тогда*

$$H\left(\sum_j \pi_j S_1^j \otimes S_2^j\right) \geq H\left(\sum_j \pi_j S_1^j\right) + \sum_j \pi_j H(S_2^j).$$

Доказательство. Введем обозначения

$$(\bar{S}_{12})_{\pi} = \sum_j \pi_j S_1^j \otimes S_2^j, \quad (\bar{S}_1)_{\pi} = \sum_j \pi_j S_1^j.$$

Тогда, используя свойство аддитивности энтропии, доказываемое неравенство можно переписать как

$$H((\bar{S}_{12})_{\pi}) - \sum_j \pi_j H(S_1^j \otimes S_2^j) \geq H((\bar{S}_1)_{\pi}) - \sum_j \pi_j H(S_1^j),$$

что в силу тождества (7.18) равносильно неравенству

$$\sum_j \pi_j H(S_1^j \otimes S_2^j; (\bar{S}_{12})_\pi) \geq \sum_j \pi_j H(S_1^j; (\bar{S}_1)_\pi).$$

Последнее же неравенство вытекает из свойства монотонности относительной энтропии (по отношению к взятию частичного следа по второй системе). $\square$

Доказательство. Возвращаясь к доказательству предложения, предположим, что Φ — канал, разрушающий сцепленность, так что $\Phi[S] = \sum_j S_1^j \text{Tr} S M_1^j$, где $\{M_1^j\}$ является наблюдаемой в системе 1, тогда

$$(\Phi \otimes \text{Id}_2)[S_{12}] = \sum_j p_j S_1^j \otimes S_2^j, \quad (8.45)$$

где $p_j S_2^j = \text{Tr}_{\mathcal{H}_1} S_{12} (M_1^j \otimes I_2)$ для произвольного состояния S_{12} составной системы. Взяв частичные следы, получаем, в частности,

$$\Phi[S_1] = \sum_j p_j S_1^j, \quad S_2 = \sum_j p_j S_2^j. \quad (8.46)$$

Если Ψ — произвольный канал в системе 2, то

$$(\Phi \otimes \Psi)[S_{12}] = \sum_j p_j S_1^j \otimes \Psi[S_2^j]. \quad (8.47)$$

Имеем

$$\hat{H}_{\Phi \otimes \Psi}(S_{12}) = \inf \sum_i \pi_i H((\Phi \otimes \Psi)[S_{12}^i]), \quad (8.48)$$

где $S_{12} = \sum_i \pi_i S_{12}^i$ — произвольное разложение. Записывая соотношение (8.45) для состояний S_{12}^i , получаем

$$(\Phi \otimes \text{Id}_2)[S_{12}^i] = \sum_j p_{ij} S_1^{ij} \otimes S_2^{ij},$$

причем имеют место разложения

$$S_1 = \sum_i \pi_i S_1^i, \quad S_2 = \sum_{ij} \pi_i p_{ij} S_2^{ij}. \quad (8.49)$$

Используя равенства (8.47), доказанную лемму и равенства (8.46), получаем

$$\begin{aligned} H((\Phi \otimes \Psi)[S_{12}^i]) &= H\left(\sum_j p_{ij} S_1^{ij} \otimes \Psi[S_2^{ij}]\right) \geq \\ &\geq H\left(\sum_j p_{ij} S_1^{ij}\right) + \sum_j p_{ij} H(\Psi[S_2^{ij}]) \geq H(\Phi[S_1^i]) + \sum_j p_{ij} H(\Psi[S_2^{ij}]), \end{aligned}$$

что в сочетании с соотношениями (8.48), (8.49) приводит к неравенству

$$\hat{H}_{\Phi \otimes \Psi}(S_{12}) \geq \hat{H}_{\Phi}[S_1] + \hat{H}_{\Psi}[S_2]. \quad \square$$

§ 8.4. Передача классической информации с помощью сцепленного состояния

8.4.1. Выигрыш благодаря сцепленности

Конструкция протокола сверхплотного кодирования (п. 3.2.3) допускает обобщение на случай пространства произвольной конечной размерности, а также неидеального квантового канала Φ между A и B . Рассмотрим следующий протокол передачи информации через канал Φ . Системы A (приемник) и B (передатчик) имеют общее сцепленное состояние S_{AB} , которое распределяется им перед началом связи с помощью некоторой процедуры типа описанной в п. 3.1.4. Будем предполагать, что $\dim \mathcal{H}_A \leq \dim \mathcal{H}_B$. Система A кодирует классические сообщения i , поступающие с вероятностями π_i , в операции (каналы) $\mathcal{E}_A^i$, действующие в $\mathcal{H}_A$. Эти операции применяются системой A к ее части состояния S_{AB} , при этом состояние системы AB преобразуется в $(\mathcal{E}_A^i \otimes \text{Id}_B)[S_{AB}]$. После этого A посылает свою часть состояния по данному каналу Φ , в результате чего на конце B становится доступной измерению система AB в состоянии $(\Phi \circ \mathcal{E}_A^i \otimes \text{Id}_B)[S_{AB}]$. Классическая информация извлекается путем измерения некоторой наблюдаемой в пространстве $\mathcal{H}_{AB}$. Разрешается блочное кодирование, так что на самом деле все это описание относится к n -й тензорной степени пространства $\mathcal{H}_{AB}$. Нас интересует пропускная способность такого протокола, которая называется *пропускной способностью протокола передачи классической информации с помощью сцепленного состояния* (*entanglement-assisted classical capacity*).

Максимум по измерениям системы B может быть оценен с помощью теоремы кодирования 5.2.1 для классической пропускной способности. Сначала введем величину

$$C_{ea}^{(1)}(\Phi) = \sup_{\pi_i, \mathcal{E}_A^i, S_{AB}^i} \chi(\{\pi_i\}; (\Phi \otimes \text{Id}_B)[S_{AB}^i]), \quad (8.50)$$

в которой уже учтены измерения в системе B . Используя канал n раз и произвольные (сцепленные) измерения в системе B , получаем величину

$$C_{ea}^{(n)}(\Phi) = C_{ea}^{(1)}(\Phi^{\otimes n}). \quad (8.51)$$

Тогда полная классическая пропускная способность с использованием сцепленного состояния есть

$$C_{ea}(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} C_{ea}^{(1)}(\Phi^{\otimes n}). \quad (8.52)$$

Следующая теорема дает простое «однобуквенное» выражение для $C_{ea}(\Phi)$ в терминах квантовой взаимной информации.

Теорема 8.4.1. *Классическая пропускная способность с использованием сцепленного состояния равна*

$$C_{ea}(\Phi) = \max_{S_A} I(S_A, \Phi) = \max_{S_A} [H(S_A) + H(\Phi(S_A)) - H(S_A; \Phi)]. \quad (8.53)$$

Доказательство этой теоремы будет приведено в последующих пунктах. Здесь мы проведем сравнение классических пропускных способностей с использованием и без использования сцепленного состояния.

Пример 8.4.1. Рассмотрим квантовый стирающий канал Φ_p . Имеем $H(\Phi_p[S_A]) = (1 - p)H(S_A) + h_2(p)$. Используя тот факт, что комплементарный канал имеет вид $\tilde{\Phi}_p = \Phi_{1-p}$ (см. задачу 6.6.3), и определение 7.5.1 обменной энтропии, получаем $H(S_A; \Phi) = H(\tilde{\Phi}[S_A]) = pH(S_A) + h_2(p)$. Поэтому

$$I(S_A, \Phi_p) = H(S_A) + (1 - p)H(S_A) - pH(S_A) = 2(1 - p)H(S_A),$$

следовательно, $C_{ea}(\Phi_p) = 2(1 - p) \log d$, что в два раза превышает классическую пропускную способность $C(\Phi_p)$ стирающего канала.

Предложение 8.4.1. *Если канал Φ ковариантен, то максимум в соотношении (8.53) достигается на инвариантном состоянии S_A . В частности, если канал Φ неприводимо ковариантен, то максимум достигается на хаотическом состоянии.*

Доказательство. Пусть канал Φ удовлетворяет условию ковариантности (6.53), тогда

$$I(V_g^{(1)} S_A V_g^{(1)*}, \Phi) = I(S_A, \Phi). \quad (8.54)$$

Это следует из выражения (7.45) для взаимной информации, унитарной инвариантности входной и выходной энтропий и соответствующего свойства обменной энтропии:

$$H(V_g^{(1)} S_A V_g^{(1)*}, \Phi) = H(S_A, \Phi). \quad (8.55)$$

Чтобы доказать это свойство, рассмотрим формулу (7.39) для обменной энтропии и заметим, что очищение состояния $V_g^{(1)} S_A V_g^{(1)*}$ дается вектором $(V_g^{(1)} \otimes I_R) |\psi_{AR}\rangle$. Подставляя его в формулу (7.39) и вновь используя ковариантность канала Φ и унитарную инвариантность энтропии, получаем соотношение (8.55).

Пусть теперь S_A — оптимальное состояние для канала Φ . Рассмотрим $V_g^{(1)}$ -инвариантное состояние

$$\bar{S} = \frac{1}{|G|} \sum_{g \in G} V_g^{(1)} S_A V_g^{(1)*}.$$

В силу предложения 7.6.1 функция $S \rightarrow I(S, \Phi)$ вогнута, поэтому

$$I(\bar{S}, \Phi) \geq \frac{1}{|G|} \sum_{g \in G} I(V_g^{(1)} S_A V_g^{(1)*}, \Phi) = I(S_A, \Phi),$$

где последнее равенство следует из соотношения (8.54). $\square$

Пример 8.4.2. Рассмотрим деполяризующий канал (6.51). Используя унитарную ковариантность, получаем, что $I(S, \Phi)$ достигает максимума на хаотическом состоянии $\bar{S} = \frac{I}{d}$, для которого $H(\bar{S}) = H(\Phi[\bar{S}]) = \log d$. Обменная энтропия $H(\bar{S}, \Phi)$ дается соотношением (7.44), откуда получаем

$$C_{ea}(\Phi) = \log d^2 + \left(1 - p \frac{d^2 - 1}{d^2}\right) \log \left(1 - p \frac{d^2 - 1}{d^2}\right) + p \frac{d^2 - 1}{d^2} \log \frac{p}{d^2}. \quad (8.56)$$

Сравним это значение с величиной $C_\chi(\Phi)$, которая дается формулой (8.19).

Мы видим, в частности, что $\frac{C_{ea}(\Phi)}{C_\chi(\Phi)} \rightarrow d + 1$ в пределе сильного шума $p \rightarrow 1$ (когда обе пропускные способности стремятся к нулю!). Для максимального значения $p = \frac{d^2}{d^2 - 1}$ имеем

$$C_{ea}(\Phi) = \log \frac{d^2}{d^2 - 1},$$

$$C_\chi(\Phi) = \frac{1}{d + 1} \log \frac{d}{d + 1} + \frac{d}{d + 1} \log \frac{d^2}{d^2 - 1}.$$

Отношение $\frac{C_{ea}(\Phi)}{C_\chi(\Phi)}$ монотонно возрастает от значения 5,08 при $d = 2$, приближаясь к асимптоте $2(d + 1)$ с ростом d .

Таким образом, сцепленные состояния вновь выступают как «катализатор» при передаче классической информации — они могут в принципе неограниченно увеличить классическую пропускную способность существующего канала, хотя сами по себе передавать информацию не могут.

Задача 8.4.1. Покажите, что для q -битного унитарного канала вида (6.54), где Λ дается соотношением (6.59), выполняется равенство

$$C_{ea}(\Phi) = I(\bar{S}, \Phi) = 2 \log 2 + \sum_{\gamma=0, x, y, z} \mu_\gamma \log \mu_\gamma.$$

Обменная энтропия $H(\bar{S}, \Phi)$ может быть вычислена с помощью предложения 7.5.1 и представления Крауса (6.59):

$$H(\bar{S}, \Phi) = - \sum_{\gamma=0, x, y, z} \mu_\gamma \log \mu_\gamma.$$

Сравните это с пропускной способностью $C_\chi(\Phi)$, даваемой формулой (8.21).

В общем случае имеются простые неравенства, связывающие две классические пропускные способности:

$$C_\chi(\Phi) \leq C_{ea}(\Phi) \leq \log d + C_\chi(\Phi). \quad (8.57)$$

В самом деле, пусть S_A — смесь произвольных чистых состояний S_j с вероятностями p_j . Тогда из неравенства (7.43) следует, что

$$I(S_A, \Phi) \leq H\left(\sum_j p_j S_j\right) + H\left(\sum_j p_j \Phi(S_j)\right) - \sum_j p_j H(\Phi(S_j)).$$

Взяв максимум и используя соотношение (8.53), получаем второе из неравенств (8.57).

Хотя использование сцепленного состояния и представляет собой дополнительный ресурс, первое неравенство не вполне очевидно в силу специального характера процедуры кодирования, используемой стороной A . Чтобы избежать этой трудности, покажем, что определение величины $C_{ea}^{(1)}(\Phi)$, а значит, и $C_{ea}(\Phi)$, может быть сформулировано без явного использования кодирующих операций $\mathcal{E}_A^i$, а именно

$$C_{ea}^{(1)}(\Phi) = \sup_{\pi_i, \{S_{AB}^i\} \in \Sigma_B} \left[H\left(\sum_i \pi_i(\Phi \otimes \text{Id}_B)[S_{AB}^i]\right) - \sum_i \pi_i H((\Phi \otimes \text{Id}_B)[S_{AB}^i]) \right], \quad (8.58)$$

где Σ_B обозначает множество семейств состояний $\{S_{AB}^i\}$, удовлетворяющих тому условию, что частичные следы S_B^i не зависят от i , $S_B^i = S_B$.

Первое из неравенств (8.57) тогда получается, если положить $S_{AB}^i = S_A^i \otimes S_B$. Чтобы доказать соотношение (8.58), достаточно установить следующий факт.

Лемма 8.4.1. Пусть $\{S_{AB}^i\}$ — семейство состояний, удовлетворяющих условию $S_B^i = S_B$. Тогда найдутся чистое состояние S_{AB} и кодирования $\mathcal{E}_A^i$ такие, что

$$S_{AB}^i = (\mathcal{E}_A^i \otimes \text{Id}_B)[S_{AB}]. \quad (8.59)$$

Доказательство. Для простоты предположим сначала, что оператор S_B невырожден. Тогда

$$S_B = \sum_{k=1}^d \lambda_k |e_k^B\rangle \langle e_k^B|,$$

где $\lambda_k > 0$, а $\{|e_k^B\rangle\}$ — ортонормированный базис в $\mathcal{H}_B$. Пусть $\{|e_k^A\rangle\}$ — ортонормированный базис в $\mathcal{H}_A$. Для вектора $|\psi^A\rangle = \sum_{k=1}^d c_k |e_k^A\rangle$ положим $|\bar{\psi}^B\rangle = \sum_{k=1}^d \bar{c}_k |e_k^B\rangle$. Отображение $|\psi^A\rangle \rightarrow |\bar{\psi}^B\rangle$ является антиизоморфизмом пространств $\mathcal{H}_A$ и $\mathcal{H}_B$. Положим

$$|\psi_{AB}\rangle = \sum_{k=1}^d \sqrt{\lambda_k} |e_k^A\rangle \otimes |e_k^B\rangle,$$

так что $S_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, и определим кодирования соотношением

$$\mathcal{E}_A^i[|\psi^A\rangle\langle\varphi^A|] = \langle\bar{\psi}^B|S_B^{-1/2}S_{AB}^iS_B^{-1/2}|\bar{\varphi}^B\rangle, \quad |\psi^A\rangle, |\varphi^A\rangle \in \mathcal{H}_A.$$

(Здесь обозначения Дирака используются для определения «частичного» скалярного произведения в пространстве $\mathcal{H}_B$.) Нетрудно проверить, что отображения $\mathcal{E}_A^i$ действительно являются каналами, удовлетворяющими соотношению (8.59).

Если оператор S_B вырожден, то приведенную выше конструкцию следует модифицировать, заменив в предыдущей формуле $S_B^{-1/2}S_{AB}^iS_B^{-1/2}$ на $\sqrt{S_B^-}S_{AB}^i\sqrt{S_B^-} + P_B^0$, где S_B^- — обобщенный обратный оператора S_B , а P_B^0 — проектор на нулевое подпространство оператора S_B . $\square$

8.4.2. Доказательство обращения теоремы кодирования

Чтобы доказать неравенство

$$C_{ea}(\Phi) \leq \max_{S_A} I(S_A, \Phi), \quad (8.60)$$

покажем сначала, что

$$C_{ea}^{(1)}(\Phi) \leq \max_{S_A} I(S_A, \Phi). \quad (8.61)$$

Обозначим через $\mathcal{E}_A^i$ кодирования, используемые стороной A . Пусть S_{AB} — исходное чистое состояние системы AB , тогда состояние системы AB (соответственно A) после кодирования есть

$$S_{AB}^i = (\mathcal{E}_A^i \otimes \text{Id}_B)[S_{AB}] \quad (\text{соответственно } S_A^i = \mathcal{E}_A^i[S_A]). \quad (8.62)$$

Заметим, что частичное состояние B не изменяется после кодирования, $S_B^i = S_B$. Докажем, что

$$\begin{aligned} H\left(\sum_i \pi_i(\Phi_A \otimes \text{Id}_B)[S_{AB}^i]\right) - \sum_i \pi_i H\left((\Phi_A \otimes \text{Id}_B)[S_{AB}^i]\right) &\leq \\ &\leq I\left(\sum_i \pi_i S_A^i, \Phi_A\right). \end{aligned} \quad (8.63)$$

Максимум левой части по всевозможным π_i , $\mathcal{E}_A^i$ равен $C_{ea}^{(1)}(\Phi)$, откуда и следует неравенство (8.61).

Используя субаддитивность квантовой энтропии, мы можем оценить первое слагаемое в левой части неравенства (8.63) как

$$H\left(\sum_i \pi_i \Phi_A[S_A^i]\right) + H(S_B) = H\left(\Phi_A\left[\sum_i \pi_i S_A^i\right]\right) + \sum_i \pi_i H(S_B).$$

Первый член уже дает выходную энтропию из $I\left(\sum_i \pi_i S_A^i; \Phi_A\right)$. Оценим остальные члены

$$\sum_i \pi_i [H(S_B) - H((\Phi_A \otimes \text{Id}_B)[S_{AB}^i])].$$

Покажем сначала, что слагаемое в квадратных скобках не превосходит $H(S_A^i) - H((\Phi_A \otimes \text{Id}_{R^i})[S_{AR^i}^i])$, где R^i — эталонная система для очищения S_A^i , а $S_{AR^i}^i$ — соответствующее чистое состояние. С этой целью рассмотрим унитарное расширение кодирования $\mathcal{E}_A^i$ с окружением E_i , которое находится в начальном чистом состоянии в соответствии с теоремой 6.3.1. Из соотношений (8.62) видно, что можно положить $R^i = BE_i$ (после взаимодействия, которое затрагивает только AE_i). Тогда, обозначая штрихом состояния после применения канала Φ_A , получаем

$$H(S_B) - H((\Phi_A \otimes \text{Id}_B)[S_{AB}^i]) = H(S_B) - H(S_{A'B}^i) = -H_i(A'|B), \quad (8.64)$$

где нижний индекс i условной энтропии указывает на состояние $S_{A'B}^i$. Аналогично

$$\begin{aligned} H(S_A^i) - H((\Phi_A \otimes \text{Id}_{R^i})[S_{AR^i}^i]) &= H(S_{R^i}^i) - H(S_{A'R^i}^i) = \\ &= -H_i(A'|R^i) = -H_i(A'|BE_i), \end{aligned}$$

а это выражение не меньше величины (8.64) согласно монотонности условной энтропии.

Используя вогнутость функции $S_A \rightarrow H(S_A) - H((\Phi_A \otimes \text{Id}_R)[S_{AR}])$, которая будет установлена ниже, получаем

$$\begin{aligned} \sum_i \pi_i [H(S_A^i) - H((\Phi_A \otimes \text{Id}_{R^i})[S_{AR^i}^i])] &\leq \\ &\leq H\left(\sum_i \pi_i S_A^i\right) - H((\Phi_A \otimes \text{Id}_R)[\hat{S}_{AR}]), \end{aligned}$$

где $\hat{S}_{AR}$ — состояние, очищающее $\sum_i \pi_i S_A^i$, с эталонной системой R . Для доказательства вогнутости обозначим через E окружение для канала Φ_A ,

тогда получим

$$\begin{aligned} H(S_A) - H((\Phi_A \otimes \text{Id}_R)[S_{AR}]) &= H(S_R) - H(S_{A'R}) = \\ &= H(S_{A'E'}) - H(S_{E'}) = H(A'|E') \end{aligned}$$

Условная энтропия $H(A'|E')$ — вогнутая функция состояния $S_{A'E'}$ согласно следствию 7.4.1. Отображение $S_A \rightarrow S_{A'E'}$ аффинно, поэтому $H(A'|E')$ — вогнутая функция состояния S_A .

Применяя это рассуждение к каналу $\Phi^{\otimes n}$, получаем

$$C_{ea}^{(n)}(\Phi) \leq \max_{S_A} I(S_A, \Phi^{\otimes n}). \quad (8.65)$$

Согласно субаддитивности квантовой взаимной информации (свойство 3 в лемме 7.6.1) имеем

$$\max_{S_{12}} I(S_{12}, \Phi_1 \otimes \Phi_2) = \max_{S_1} I(S_1, \Phi_1) + \max_{S_2} I(S_2, \Phi_2),$$

откуда вытекает замечательное свойство аддитивности

$$\max_{S_A} I(S_A, \Phi^{\otimes n}) = n \max_{S_A} I(S_A, \Phi).$$

Окончательно получаем неравенство (8.60). □

8.4.3. Доказательство прямого утверждения теоремы кодирования

Здесь будет доказано неравенство

$$C_{ea}(\Phi) \geq \max_{S_A} I(S_A, \Phi). \quad (8.66)$$

Сначала покажем, используя обобщение протокола сверхплотного кодирования, что

$$C_{ea}^{(1)}(\Phi^{\otimes n}) \geq I\left(\frac{P}{\dim P}, \Phi^{\otimes n}\right) \quad (8.67)$$

для произвольного проектора P в $\mathcal{H}_A^{\otimes n}$.

В самом деле, пусть $P = \sum_{k=1}^m |e_k\rangle\langle e_k|$, где $\{e_k; k=1, \dots, m=\dim P\}$ — ортонормированная система. Рассмотрим дискретную систему Вейля $\{W(x, y); x, y=1, \dots, m\}$, определенную соотношениями (6.46) на подпространстве $\mathcal{H}_P = P\mathcal{H}_A^{\otimes n}$.

Поскольку $\dim \mathcal{H}_A \leq \dim \mathcal{H}_B$, мы можем предположить, что $\mathcal{H}_A \subseteq \mathcal{H}_B$. Пусть

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{m}} \sum_{k=1}^m |e_k\rangle \otimes |e_k\rangle.$$

Задача 8.4.2. Докажите, что система $\{(W(x, y) \otimes I_B)|\psi_{AB}\rangle; x, y = 1, \dots, m\}$ является ортонормированным базисом в $\mathcal{H}_P \otimes \mathcal{H}_P$. В частности,

$$\sum_{x, y=1}^m (W(x, y) \otimes I_B)|\psi_{AB}\rangle\langle\psi_{AB}|(W(x, y) \otimes I_B)^* = P \otimes P. \quad (8.68)$$

Операторы $W(x, y)$ будут играть роль, аналогичную матрицам Паули в протоколе сверхплотного кодирования для q -бита. Пусть теперь классический сигнал принимает значения $i = (x, y)$ с равными вероятностями $1/m^2$. В качестве сцепленного состояния возьмем $|\psi_{AB}\rangle\langle\psi_{AB}|$, а в качестве кодирующих отображений — $\mathcal{E}_A^i[S] = W(x, y)SW(x, y)^*$. Тогда получим

$$C_{ea}^{(1)}(\Phi^{\otimes n}) \geq H\left(\frac{1}{m^2} \sum_{x, y} (\Phi \otimes \text{Id}_B)^{\otimes n} [S_{AB}^{xy}]\right) - \frac{1}{m^2} \sum_{x, y} H((\Phi \otimes \text{Id}_B)^{\otimes n} [S_{AB}^{xy}]),$$

где $S_{AB}^{xy} = (W(x, y) \otimes I_B^{\otimes n})|\psi_{AB}\rangle\langle\psi_{AB}|(W(x, y) \otimes I_B^{\otimes n})^*$. Согласно соотношению (8.68) первое слагаемое в правой части равно

$$H\left((\Phi \otimes \text{Id}_B)\left[\frac{P}{m} \otimes \frac{P}{m}\right]\right) = H\left(\frac{P}{m}\right) + H\left(\Phi\left[\frac{P}{m}\right]\right).$$

Поскольку состояние S_{AB}^{xy} очищает смешанное состояние $\frac{P}{m}$, все энтропии во втором слагаемом одинаковы и равны $H\left(\frac{P}{m}, \Phi\right)$. Учитывая выражение для квантовой взаимной информации

$$I(S_A, \Phi) = H(S_A) + H(\Phi[S_A]) - H(S_A; \Phi),$$

получаем неравенство (8.67). В дальнейшем нам понадобится то обстоятельство, что последнее слагаемое — обменная энтропия — равно энтропии окружения $H(S'_E) = H(\Phi_E[S_A])$, где Φ_E — канал из пространства системы $\mathcal{H}_A$ в пространство окружения $\mathcal{H}_E$, задаваемый формулой (7.38).

Пусть теперь $S_A = S$ — произвольное состояние в $\mathcal{H}_A$, и пусть $\hat{P}^{n, \delta}$ — *сильно типичный проектор* состояния $S^{\otimes n}$ в пространстве $\mathcal{H}_A^{\otimes n}$, определяемый ниже. Докажем, что для *произвольного* канала Ψ из $\mathcal{H}_A$ в какое-либо гильбертово пространство $\tilde{\mathcal{H}}$ имеет место соотношение

$$\lim_{\delta \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H\left(\Psi^{\otimes n}\left[\frac{\hat{P}^{n, \delta}}{\dim \hat{P}^{n, \delta}}\right]\right) = H(\Psi[S]).$$

Отсюда согласно выражениям для взаимной информации и обменной энтропии будет следовать равенство

$$\lim_{\delta \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} I\left(\frac{\hat{P}^{n, \delta}}{\dim \hat{P}^{n, \delta}}, \Phi^{\otimes n}\right) = I(S, \Phi), \quad (8.69)$$

а значит, согласно оценке (8.67), и доказываемое неравенство (8.66).

Определение 8.4.1. Фиксируем положительное δ и обозначим через λ_j собственные числа, а через $|e_j\rangle$ — собственные векторы оператора плотности S . Тогда собственные числа и собственные векторы оператора плотности $S^{\otimes n}$ суть $\lambda_J = \lambda_{j_1} \cdot \dots \cdot \lambda_{j_n}$, $|e_J\rangle = |e_{j_1}\rangle \otimes \dots \otimes |e_{j_n}\rangle$, где $J = (j_1, \dots, j_n)$. Последовательность J называется *сильно типичной*, если числа $N(j|J)$ появлений символов j в последовательности J удовлетворяют условию

$$\left| \frac{N(j|J)}{n} - \lambda_j \right| < \delta, \quad j = 1, \dots, d,$$

причем $N(j|J) = 0$, если $\lambda_j = 0$. Обозначим через $\hat{T}^{n,\delta}$ совокупность всех сильно типичных последовательностей. *Сильно типичный проектор* определяется как следующий спектральный проектор оператора плотности $S^{\otimes n}$:

$$\hat{P}^{n,\delta} = \sum_{J \in \hat{T}^{n,\delta}} |e_J\rangle \langle e_J|.$$

Пусть P^n — распределение вероятностей, задаваемое собственными числами λ_j . Согласно закону больших чисел $P^n(\hat{T}^{n,\delta}) \rightarrow 1$ при $n \rightarrow \infty$. Для произвольной функции $f(j)$, $j = 1, \dots, d$, и последовательности $J = (j_1, \dots, j_n) \in \hat{T}^{n,\delta}$ справедливо неравенство

$$\left| \frac{f(j_1) + \dots + f(j_n)}{n} - \sum_{j=1}^d \lambda_j f(j) \right| < \delta d \max f. \quad (8.70)$$

В частности, любая сильно типичная последовательность является типичной в обычном (энтропийном) смысле: полагая $f(j) = -\log \lambda_j$, получим

$$n[H(S) - \delta_1] < -\log \lambda_J < n[H(S) + \delta_1], \quad (8.71)$$

где $\delta_1 = \delta d \max_{\lambda_j > 0} (-\log \lambda_j)$ (обратное неверно — не всякая типичная последовательность сильно типична).

В дальнейшем нам понадобится следующая комбинаторная лемма.

Задача 8.4.3. Покажите, что размер множества $\hat{T}^{n,\delta}$ оценивается как

$$2^{n[H(S) - \Delta_n(\delta)]} < |\hat{T}^{n,\delta}| < 2^{n[H(S) + \Delta_n(\delta)]}, \quad (8.72)$$

где $H(S) = -\sum_{j=1}^d \lambda_j \log \lambda_j$ и $\lim_{\delta \rightarrow 0} \lim_{n \rightarrow \infty} \Delta_n(\delta) = 0$.

Доказательство соотношения (8.69). Положим $d_{n,\delta} = \dim \hat{P}^{n,\delta} = |\hat{T}^{n,\delta}|$ и $\bar{S}^{n,\delta} = \frac{\hat{P}^{n,\delta}}{d_{n,\delta}}$ и докажем, что

$$\lim_{\delta \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H(\Psi^{\otimes n}(\bar{S}^{n,\delta})) = H(\Psi[S]) \quad (8.73)$$

для произвольного канала Ψ . Имеем

$$\begin{aligned} nH(\Psi[S]) - H(\Psi^{\otimes n}[\bar{S}^{n,\delta}]) &= H(\Psi[S]^{\otimes n}) - H(\Psi^{\otimes n}[\bar{S}^{n,\delta}]) = \\ &= H(\Psi^{\otimes n}[\bar{S}^{n,\delta}]; \Psi^{\otimes n}[S^{\otimes n}]) + \text{Tr} \log \Psi[S]^{\otimes n} (\Psi^{\otimes n}[\bar{S}^{n,\delta}] - \Psi[S]^{\otimes n}). \end{aligned} \quad (8.74)$$

Строго говоря, это преобразование имеет смысл, если оператор плотности $\Psi(S)^{\otimes n}$ невырожден, что мы сначала и предположим.

Для первого слагаемого, используя свойство монотонности относительной энтропии, получаем

$$H(\Psi^{\otimes n}[\bar{S}^{n,\delta}]; \Psi^{\otimes n}[S^{\otimes n}]) \leq H(\bar{S}^{n,\delta}; S^{\otimes n}),$$

где правая часть имеет вид

$$H(\bar{S}^{n,\delta}; S^{\otimes n}) = \sum_{J \in \hat{T}^{n,\delta}} \frac{1}{d_{n,\delta}} \log \frac{1}{d_{n,\delta} \lambda_J} = -\log d_{n,\delta} - \sum_{J \in \hat{T}^{n,\delta}} \frac{1}{d_{n,\delta}} \log \lambda_J,$$

а согласно оценкам (8.71), (8.72) это выражение меньше или равно величины $n(\delta_1 + \Delta_n(\delta))$, стремящейся к нулю при $n \rightarrow \infty$, $\delta \rightarrow 0$.

Используя соотношение

$$\log \Psi[S]^{\otimes n} = \log \Psi[S] \otimes I \otimes \dots \otimes I + \dots + I \otimes \dots \otimes I \otimes \log \Psi[S]$$

и вводя оператор $F = \Psi^*[\log \Psi[S]]$, где Ψ^* — сопряженный канал, мы можем переписать второе слагаемое в виде

$$\begin{aligned} n \text{Tr} \frac{(F \otimes I \otimes \dots \otimes I + \dots + I \otimes \dots \otimes I \otimes F)}{n} (\bar{S}^{n,\delta} - S^{\otimes n}) &= \\ &= \frac{n}{d_{n,\delta}} \sum_{J \in \hat{T}^{n,\delta}} \left[\frac{f(j_1) + \dots + f(j_n)}{n} - \sum_{j=1}^d \lambda_j f(j) \right], \end{aligned} \quad (8.75)$$

где $f(j) = \langle e_j | F | e_j \rangle$, что оценивается величиной $n\delta \max f$ в силу неравенства (8.70). Это доказывает соотношение (8.73) в случае невырожденного оператора $\Psi[S]$.

В общем случае обозначим через P_Ψ проектор на носитель оператора $\Psi[S]$. Тогда соответствующий проектор оператора $\Psi[S]^{\otimes n}$ есть $P_\Psi^{\otimes n}$, и носитель оператора $\Psi^{\otimes n}(\bar{S}^{n,\delta})$ содержится в носителе оператора $\Psi[S]^{\otimes n} = \Psi^{\otimes n}[S^{\otimes n}]$, поскольку носитель оператора $\bar{S}^{n,\delta}$ содержится в носителе оператора $S^{\otimes n}$. Поэтому второе слагаемое в формуле (8.74) следует понимать как

$$\text{Tr} P_\Psi^{\otimes n} \log [P_\Psi^{\otimes n} \Psi[S]^{\otimes n} P_\Psi^{\otimes n}] P_\Psi^{\otimes n} (\Psi^{\otimes n}[\bar{S}^{n,\delta}] - \Psi[S]^{\otimes n}),$$

где логарифм берется от невырожденного оператора в подпространстве $P_\Psi^{\otimes n} \mathcal{H}_A^{\otimes n}$. Теперь можно повторить рассуждения, определив F как $\Psi^*[P_\Psi(\log P_\Psi \Psi[S] P_\Psi) P_\Psi]$. Это завершает доказательство соотношения (8.69), откуда вытекает неравенство (8.66). $\square$

§ 8.5. Комментарии

1. Предложение 8.1.1, доказанное в работе А. С. Холево [35], было обобщено на квантовые каналы с памятью Кречманом и Вернером; см. [118]. Обобщение на произвольные последовательности каналов в духе информационного спектра Хана и Верду дано Хайаши и Нагаока; см. [90, 91].

2. Плодотворная связь между χ -пропускной способностью и относительной энтропией, в частности свойство максимальной равноудаленности, отмечена в работе Шумахера и Вестморленда [137].

3. Проблема аддитивности упоминается в работе Беннета, Фукса и Смолина [59]. Формулировка в терминах четырех пропускных способностей была дана Беннетом и Шором; см. [60]. Шор в работе [144] определил классическую пропускную способность с использованием адаптивных измерений на выходе и показал, что она находится строго между $C_{1,1}$ и $C_{1,\infty}$.

Полная формулировка теоремы 8.3.1 состоит из нескольких утверждений, часть из которых носит индивидуальный характер, тогда как другие выполняются только глобально, например, «если минимальная выходная энтропия аддитивна для всех каналов, то это же верно и для χ -пропускной способности». Ряд авторов (Мацумото, Шимоно и Винтер, Ауденаэрт и Браунштейн, Померанский, А. С. Холево и М. Е. Широков) внесли вклад в доказательство отдельных индивидуальных импликаций, тогда как наиболее неожиданные глобальные утверждения были получены Шором, который предложил оригинальную конструкцию расширения канала, позволяющую усилить его индивидуальные свойства. Подробности и ссылки см. в работе Шора [145]. Тот факт, что из глобального выполнения свойства (8.23) следует аддитивность (8.22) для всех пар каналов Φ_1, Φ_2 (а также аналогичное утверждение для минимальной выходной энтропии), доказан Фукудой и Вольфом; см. [84]. Предложение 8.3.2 доказано в работе А. С. Холево и М. Е. Широкова [102], где была систематически исследована гипотеза (8.35) и установлена ее эквивалентность аддитивности χ -пропускной способности с ограничениями. Решение задачи 8.3.5 см. в работе [40].

Неравенство Линдблада—Озавы установлено в работе [129]. Выполнение гипотезы аддитивности для каналов, разрушающих сцепленность, доказано Шором; см. [143]. Другие важные достижения включают доказательство Кингом свойств (8.22) и (8.33) для q -битных унитарных (см. [112]) и деполяризующих (см. [113]) каналов с использованием весьма специальных структурных свойств этих каналов и неравенства Либса—Тирринга, см. [63], раздел X.2. Подробный обзор прогресса в реше-

нии проблемы аддитивности до 2006 г. имеется в докладе А. С. Холево [104]. Из последних достижений следует отметить результаты Винтера (см. [158]) и Хайдена (см. [92]), которые показали, что гипотеза аддитивности не выполняется для минимальной выходной энтропии Реньи со значениями параметра $p > 2$ и $1 < p \leq 2$ соответственно при достаточно высоких размерностях. (Напомним, что энтропия фон Неймана соответствует значению $p = 1$.) В работе [158] рассматривались каналы вида

$$\Phi(\rho) = \frac{1}{n} \sum_{j=1}^n U_j \rho U_j^*, \quad (8.76)$$

где U_j , $j = 1, \dots, n$, — последовательность независимых случайных унитарных операторов, распределенных равномерно (т. е. в соответствии с нормированной мерой Хаара на группе унитарных операторов), и $n = O(d \log d)$, $d \rightarrow \infty$. Нарушение аддитивности с вероятностью, близкой к 1, следует из оценки больших отклонений для сумм случайных операторов.

Наконец, совсем недавно, основываясь на методах из этих работ, Хастингс (см. [88]) рассмотрел смеси случайных унитарных операторов со случайными весами и анонсировал построение примера, в котором нарушена аддитивность минимальной выходной энтропии при достаточно больших n , n/d . Подробное доказательство было проведено Фукудой, Кингом и Мозером; см. [85]. Отсюда в силу теоремы 8.3.1 должно следовать существование контрпримеров ко всем формам аддитивности, а также к равенству (8.24). Следует, однако, заметить, что эти методы, идейно родственные методу случайного кодирования Шеннона, не позволяют получить конструктивные контрпримеры.

4. Теорема 8.4.1 доказана Беннетом, Шором, Смолиным и Таплиалом [61]. Здесь приводится упрощенное доказательство, следующее работе А. С. Холево [99]. По поводу сильно типичных проекторов и доказательства результата задачи 8.4.3 см. [44].

ГЛАВА 9

Передача квантовой информации

Как уже неоднократно подчеркивалось, квантовое состояние само по себе представляет особого рода информационный ресурс постольку, поскольку имеет статистическую неопределенность. Статистическая механика изучает необратимые изменения состояния системы в результате естественной эволюции (следствием которых является и потеря информации). Теория информации ставит перед собой в некотором смысле обратную задачу: как свести к пренебрежимой величине эти необратимые изменения, используя некоторые специальные преобразования состояний — кодирование и декодирование — до и после эволюции, задаваемой каналом с шумом. Этому кругу вопросов и посвящена настоящая глава.

При этом мы начнем с рассмотрения методов кодирования квантовой информации, устойчивого по отношению к данному ограниченному набору ошибок (например, к произвольной ошибке в одном произвольном q -бите), когда требуется передача с абсолютной точностью. Затем мы перейдем к приближенной постановке, когда вводится некоторая мера точности воспроизведения квантового состояния. Тогда цель состоит в том, чтобы, используя блочное кодирование и передачу через составные каналы $\Phi^{\otimes n}$, добиться асимптотически точной передачи квантовых состояний с максимально высокой скоростью при $n \rightarrow \infty$. Таким образом возникает аналог шенноновской теоремы кодирования для квантовой информации. Это приводит к понятию квантовой пропускной способности, которое тесно связано с так называемой когерентной информацией.

§ 9.1. Квантовые коды, исправляющие ошибки

9.1.1. Постановка вопроса

При передаче сообщений по каналу с шумом желательно иметь код, который был бы устойчив относительно возможных ошибок. В случае классической информации принципиальная осуществимость такого кодирования при скоростях передачи, меньших пропускной способности, вытекает из теоремы Шеннона. Однако эта теорема не дает конструктивного способа построения помехоустойчивого (пусть даже не оптимального) кода, и практическому решению этой проблемы посвящен специальный раздел теории информации.

Самый незамысловатый способ застраховаться от ошибок состоит в простом повторении сообщений (что, конечно, снижает скорость передачи). Рассмотрим двоичный сигнал (бит), принимающий значения 0, 1, который может кодироваться последовательностью битов. Предположим, что вероятность ошибки — изменения значения одного бита в процессе передачи — равна малой величине p , так что вероятность изменения двух битов p^2 пренебрежимо мала. Рассмотрим код $0 \rightarrow 00$, $1 \rightarrow 11$. Тогда, получив 00 или 11, можно с высокой достоверностью утверждать, что был послан 0 или, соответственно, 1. Однако, получив 01 либо 10, можно лишь констатировать наличие ошибки, но исправить ее (т.е. восстановить с высокой степенью достоверности посланный сигнал) нельзя. От этого недостатка можно избавиться, если добавить еще один кодирующий разряд: $0 \rightarrow 000$, $1 \rightarrow 111$. Такой код будет уже помехоустойчивым по отношению к ошибке в любом одном бите, т.е. позволяющим восстановить посланный сигнал.

Прямолинейное обобщение такого рецепта на случай квантовой информации наталкивается на трудность — квантовую информацию невозможно размножить. Кроме того, при передаче через квантовый канал с шумом безошибочно должны передаваться не только базисные состояния, но и всевозможные их суперпозиции. На первый взгляд задача может показаться неразрешимой, однако это не так. Рассмотрим пример кода Шора, который решает такую задачу в важном модельном случае.

Предположим, что ставится задача безошибочной передачи любого чистого состояния q -бита $\psi = a|0\rangle + b|1\rangle$, причем разрешается кодировать эти состояния состояниями нескольких q -битов. Кодирование в квантовом случае задается изометричным отображением. Следуя классической аналогии, рассмотрим сначала код, отображающий базисные векторы согласно правилу

$$|0\rangle \rightarrow |000\rangle, \quad |1\rangle \rightarrow |111\rangle. \quad (9.1)$$

Такой код исправляет «переворот q -бита», т.е. переход $|0\rangle \leftrightarrow |1\rangle$ в любом одном q -бите кода. Нас же интересует произвольное состояние $\psi = a|0\rangle + b|1\rangle$, которое при выбранном способе кодируется в $a|000\rangle + b|111\rangle$. Пусть, например, произошла ошибка в первом q -бите кода:

$$a|0\rangle + b|1\rangle \rightarrow a|100\rangle + b|011\rangle.$$

Состояния $a|000\rangle + b|111\rangle$, $a|100\rangle + b|011\rangle$ ортогональны, следовательно, их можно безошибочно различить.

Однако такой код не исправляет ошибки типа «переворота фазы» $|0\rangle \leftrightarrow |0\rangle$, $|1\rangle \leftrightarrow -|1\rangle$. В самом деле, в результате такой фазовой ошибки в одном q -бите получим $a|000\rangle - b|111\rangle$ вместо $a|000\rangle + b|111\rangle$, и эти со-

стояния, вообще говоря, не ортогональны, т. е. не являются безошибочно различимыми в квантовой статистике.

Теперь заметим, что преобразование Адамара

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

отображает переворот фазы в переворот бита и наоборот. Преобразуя соответствующим образом код (9.1), получим код

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{2^{3/2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle), \\ |1\rangle &\rightarrow \frac{1}{2^{3/2}}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle), \end{aligned} \quad (9.2)$$

который исправляет переворот фазы в любом одном q -бите, однако уже не исправляет переворот бита.

Код Шора, который исправляет как переворот бита, так и переворот фазы в любом одном q -бите, получается комбинированием кодов (9.1), (9.2) и требует девять q -битов:

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{2^{3/2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \\ |1\rangle &\rightarrow \frac{1}{2^{3/2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \end{aligned} \quad (9.3)$$

Более того, оказывается, что этот код исправляет не только битовую и фазовую, но любую ошибку, возникающую в одном (любом) из q -битов, поскольку любая ошибка может быть сведена к этим двум видам ошибок. Это вытекает из выполнения общих условий, рассматриваемых в следующем пункте.

9.1.2. Общая формулировка

Пусть $\mathcal{M}$ — гильбертово пространство, которое играет роль пространства квантовых сигналов, S — произвольное состояние в $\mathcal{M}$. *Кодом* называется изометричное отображение $V: \mathcal{M} \rightarrow \mathcal{N}$, переводящее состояния S в кодированные состояния VSV^* в гильбертовом пространстве кодированного сигнала $\mathcal{N}$. Система $\mathcal{N}$ может быть подвержена ошибкам, которые описываются вполне положительными отображениями Φ в $\mathfrak{T}(\mathcal{N})$, образующими в каждой конкретной задаче некоторый класс $\mathcal{E}$. Физический смысл необратимых эволюций имеют отображения, удовлетворяющие условию $\Phi(I) \leq I$ (см. §6.5), однако в рассматриваемой ниже постановке это ограничение несущественно, так как эффект ошибки определяется с точностью до постоянного множителя.

Итак, преобразования квантовой информации описываются диаграммой

$$S \longrightarrow VSV^* \longrightarrow \Phi(VSV^*), \quad \Phi \in \mathcal{E}.$$

Определение 9.1.1. Код V называется *кодом, исправляющим ошибки* из класса $\mathcal{E}$, если существует *восстанавливающий канал* $\mathcal{D}$ такой, что

$$\mathcal{D}[\Phi(VSV^*)] = c(\Phi)S \quad (9.4)$$

для любого состояния S и любого $\Phi \in \mathcal{E}$, где $c(\Phi)$ — некоторая постоянная, зависящая только от Φ .

На самом деле код можно задавать самым подпространством $\mathcal{L} = V\mathcal{M} \subset \mathcal{N}$, не вводя явно $\mathcal{M}$, V .

Пример 9.1.1 (хранение квантовой информации в памяти квантового компьютера). Пусть $\mathcal{N} = \mathcal{H}_2^{\otimes n}$ — квантовый регистр, в котором предполагается хранить информацию из $\mathcal{M}$. Рассмотрим ошибки, при которых изменению может подвергнуться не более m q -битов регистра. Соответствующее множество $\mathcal{E}(n, m)$ состоит из отображений $\Phi = \Phi_1 \otimes \dots \otimes \Phi_n$, где количество отображений $\Phi_k \neq \text{Id}$ не превышает m , причем ошибка в k -м q -бите Φ_k может быть произвольным вполне положительным отображением. Операторами элементарных ошибок в каждом q -бите могут служить матрицы Паули, причем σ_x описывает переворот бита, σ_z — переворот фазы, а $\sigma_y = i\sigma_x\sigma_z$ — их комбинацию. Вместе с единичным оператором I , который соответствует отсутствию ошибки, они образуют базис в алгебре наблюдаемых q -бита.

Код Шора демонстрирует возможность исправления ошибок из $\mathcal{E}(n, 1)$, если n достаточно велико (можно доказать, что наименьшее значение n для кода, исправляющего одну ошибку, равно 5). Возможность исправления только одной ошибки является, конечно, серьезным ограничением. Однако известно, что существуют коды, исправляющие ошибки из $\mathcal{E}(n, m)$, где m может быть сколь угодно большим для достаточно больших размеров регистра n .

9.1.3. Необходимые и достаточные условия исправления ошибок

Класс ошибок $\mathcal{E}$ обычно имеет следующую структуру: он состоит из всевозможных отображений вида $\Phi(S) = \sum_j V_j S V_j^*$, где $V_j \in \text{Lin}(B_1, \dots, B_p)$, а B_j — фиксированные операторы *элементарных ошибок*.

Теорема 9.1.1. Следующие утверждения эквивалентны:

- 1) код $\mathcal{L}$ исправляет ошибки класса $\mathcal{E}$;
- 2) код $\mathcal{L}$ исправляет ошибку $\Phi[S] = \sum_{j=1}^p B_j S B_j^*$;

3) для $\varphi, \psi \in \mathcal{L}$ таких, что $\langle \varphi | \psi \rangle = 0$, имеет место равенство $\langle \varphi | B_i^* B_j | \psi \rangle = 0$ для всех $i, j = 1, \dots, p$;

4) для любого ортонормированного базиса $\{|k\rangle\}$ в $\mathcal{L}$ выполняются условия

$$\begin{aligned} \langle k | B_i^* B_j | k \rangle &= \langle l | B_i^* B_j | l \rangle \quad \text{для всех } k, l, \\ \langle k | B_i^* B_j | l \rangle &= 0 \quad \text{для } k \neq l; \end{aligned}$$

5) $P_{\mathcal{L}} B_i^* B_j P_{\mathcal{L}} = b_{ij} P_{\mathcal{L}}$, где $P_{\mathcal{L}}$ — проектор на $\mathcal{L}$.

Доказательство. 1) $\Rightarrow$ 2). Очевидно.

2) $\Rightarrow$ 3). Пусть существует восстанавливающий канал $\mathcal{D}[S] = \sum_r R_r S R_r^*$ для ошибки Φ . Рассмотрим чистое входное состояние $S = |\psi\rangle\langle\psi|$, $|\psi\rangle \in \mathcal{L}$. Тогда

$$\sum_r \sum_j R_r B_j |\psi\rangle\langle\psi| B_j^* R_r^* = c |\psi\rangle\langle\psi|.$$

Но это возможно, лишь если $R_r B_j |\psi\rangle = c_{jr} |\psi\rangle$, при этом $c = \sum_r \sum_j |c_{jr}|^2$.

Пусть $|\varphi\rangle, |\psi\rangle \in \mathcal{L}$ — два ортогональных вектора. Поскольку восстанавливающий канал сохраняет след, мы получаем $I = \sum_r R_r^* R_r$, и, значит,

$$\langle \varphi | B_i^* B_j | \psi \rangle = \sum_r \langle \varphi | B_i^* R_r^* R_r B_j | \psi \rangle = \left(\sum_r \bar{c}_{ir} c_{jr} \right) \langle \varphi | \psi \rangle = 0.$$

3) $\Rightarrow$ 4). Второе равенство очевидно, а первое получается из рассмотрения ортогональных векторов $|\varphi\rangle = |k+l\rangle$, $|\psi\rangle = |k-l\rangle$.

4) $\Rightarrow$ 5). Вводя обозначение $b_{ij} = \langle k | B_i^* B_j | k \rangle$, мы можем записать условие 4 в виде

$$\langle k | B_i^* B_j | l \rangle = \delta_{kl} b_{ij},$$

что эквивалентно условию 5.

5) $\Rightarrow$ 1). Матрица $[b_{ij}]$ эрмитова неотрицательно определенная, поэтому найдется унитарная матрица $[u_{ij}]$ такая, что

$$\sum_{ij} \bar{u}_{ir} b_{ij} u_{js} = \delta_{rs} \lambda_r,$$

где $\lambda_r \geq 0$. Полагая $\tilde{B}_s = \sum_j u_{js} B_j$, получаем $\Phi[S] = \sum_{s=1}^p \tilde{B}_s S \tilde{B}_s^*$ и

$$P_{\mathcal{L}} \tilde{B}_r^* \tilde{B}_s P_{\mathcal{L}} = \delta_{rs} \lambda_r P_{\mathcal{L}}.$$

Таким образом, при $\lambda_r > 0$ имеем

$$\lambda_s^{-1/2} \tilde{B}_s P_{\mathcal{L}} = U_s P_{\mathcal{L}},$$

где U_s — частично изометричные операторы, отображающие $\mathcal{L}$ на взаимно ортогональные подпространства $\mathcal{L}_s \subset \mathcal{H}$. Отсюда следует, что

$$\Phi[S] = \sum_{s=1}^p \lambda_s U_s S U_s^* \quad (9.5)$$

для любого состояния S , $\text{supp } S \subset \mathcal{L}$.

Пусть P_s — проектор на подпространство $\mathcal{L}_s$, и пусть $P_0 = I - \sum_s P_s$. Определим канал

$$\mathcal{D}[S] = \sum_s U_s^* P_s S P_s U_s + P_0 S P_0$$

и покажем, что он является восстанавливающим для всех ошибок из $\mathcal{E}$. Поскольку линейная комбинация элементарных ошибок B_j является также линейной комбинацией операторов $\tilde{B}_r$, принимая во внимание, что $U_s^* P_s \tilde{B}_r P_s = \lambda_r^{1/2} \delta_{sr} P_s$, мы получаем соотношение (9.4) для произвольного $\Phi \in \mathcal{E}$. $\square$

Задача 9.1.1. Проверьте выполнение условий 4 для кода Шора (9.3) и операторов элементарных ошибок, задаваемых матрицами Паули в первом q -бите кода.

9.1.4. Когерентная информация и точное исправление ошибок

Рассмотрим произвольный канал Φ , действующий из A в B , и пусть $S = S_A$ — входное состояние канала. Введем эталонное пространство R , так что $S_{AR} = |\psi_{AR}\rangle\langle\psi_{AR}|$ является очищением состояния S_A . Пусть $V: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$ — изометрия представления Стайнспринга (6.8) для канала Φ , где E — пространство окружения.

Важной компонентой квантовой взаимной информации $I(S, \Phi)$ является *когерентная информация*

$$I_c(S, \Phi) = H(\Phi[S]) - H(S; \Phi) = H(B) - H(E) = H(B) - H(RB) = -H(R|B).$$

Как мы увидим позже, это понятие тесно связано с квантовой пропускной способностью канала Φ .

Особенностью когерентной информации является *отсутствие* некоторых «естественных» свойств, таких как выпуклость по S , субаддитивность, второе неравенство об обработке информации. Кроме того, эта величина может принимать отрицательные значения. Ее классический аналог вообще не бывает положительным: $H(Y) - H(XY) = -H(X|Y) \leq 0$. Однако функция $I_c(S, \Phi)$ является выпуклой по Φ и удовлетворяет первому неравенству об обработке информации:

$$I_c(S, \Phi_2 \circ \Phi_1) \leq I_c(S, \Phi_1), \quad (9.6)$$

что легко выводится из соотношения $I_c(S, \Phi) = I(S, \Phi) - H(S)$ и соответствующих свойств квантовой взаимной информации $I(S, \Phi)$. Покажем, почему второе неравенство об обработке информации $I_c(S, \Phi_2 \circ \Phi_1) \leq I_c(\Phi_1[S], \Phi_2)$, вообще говоря, не выполняется. Если предположить, что оно верно, то

$$H(\Phi_2 \circ \Phi_1[S]) - H(S, \Phi_2 \circ \Phi_1) \leq H(\Phi_2 \circ \Phi_1[S]) - H(\Phi_1[S], \Phi_2),$$

т. е. $H(S, \Phi_2 \circ \Phi_1) \geq H(\Phi_1[S], \Phi_2)$. Это равносильно тому, что $H(E_1 E_2) \geq H(E_2)$, где E_j — окружение для j -го канала. Но свойство монотонности для квантовой энтропии в общем случае не выполняется.

Задача 9.1.2. Используя идею доказательства субаддитивности квантовой взаимной информации (утверждение 7.6.1), покажите, что субаддитивность функции $I_c(S, \Phi)$ эквивалентна следующему неравенству:

$$H(B_1 B_2) - H(B_1) - H(B_2) \leq H(E_1 E_2) - H(E_1) - H(E_2),$$

которое может быть не выполнено в общем случае.

Существует тесная связь между точной передачей квантовой информации, исправлением ошибок и свойствами когерентной информации.

Определение 9.1.2. Канал Φ называется *точно обратимым* на состоянии $S = S_A$, если найдется восстанавливающий канал $\mathcal{D}$ из B в A такой, что

$$(\mathcal{D} \circ \Phi \otimes \text{Id}_R)[S_{AR}] = S_{AR}.$$

Предложение 9.1.1. Следующие условия эквивалентны:

- 1) канал Φ точно обратим на состоянии S ;
- 2) $I(R; E) = 0$, т. е. $S_{RE} = S_R \otimes S_E$;
- 3) $I_c(S, \Phi) = H(S)$;
- 4) канал Φ допускает представление (9.5) на носителе состояния S .

Условие 2 означает, что информация не уходит в окружение, т. е. канал является «секретным». Таким образом, точная обратимость канала равносильна его секретности. Условие 3 означает, что при обратимой передаче каналом Φ состояния S когерентная информация $I_c(S, \Phi)$ должна достигать своего максимально возможного значения $H(S)$. В частности, взяв хаотическое состояние $S = \bar{S}_A = I_A/d_A$, мы получаем условие $\log d_A = I_c(\bar{S}_A, \Phi)$. Это показывает, что когерентная информация должна быть связана с квантовой пропускной способностью канала Φ , характеризующей максимальную размерность обратимо передаваемых квантовых состояний. В следующем параграфе мы увидим, что для асимптотически точной передачи через канал без памяти $\Phi^{\otimes n}$ такая связь действительно имеет место при $n \rightarrow \infty$.

Доказательство. 1) $\Rightarrow$ 2). Вектор $|\psi_{BRE}\rangle = (V \otimes I_R)|\psi_{AR}\rangle$ является вектором чистого состояния S_{BRE} составной системы BRE . Из точной обратимости вытекает, что

$$(\mathcal{D} \otimes \text{Id}_{RE})[S_{BRE}] = S_{ARE}.$$

Так как состояние S_{AR} чистое, согласно следствию 3.1.2 мы имеем $S_{ARE} = S_{AR} \otimes S_E$. Взяв частичный след по пространству A , получаем

$$S_{RE} = S_R \otimes S_E, \quad (9.7)$$

т. е. условие 2 выполнено.

2) $\Leftrightarrow$ 3). Имеем

$$H(S) - I_c(S, \Phi) = H(A) + H(E) - H(B) = \quad (9.8)$$

$$= H(R) + H(E) - H(RE) = I(R; E) \geq 0, \quad (9.9)$$

причем равенство имеет место тогда и только тогда, когда $I(R; E) = 0$, т. е. $S_{RE} = S_R \otimes S_E$.

3) $\Rightarrow$ 1). Вектор $|\psi_{BRE}\rangle = (V \otimes I_R)|\psi_{AR}\rangle$ является вектором чистого состояния S_{BRE} составной системы BRE , очищающего состояние S_{RE} . Равенство (9.7) дает другое очищение $|\psi_{AR}\rangle \otimes |\psi_{EE'}\rangle$, где E' — очищающая система для S_E . Выбирая E' , мы всегда можем считать, что пространство второго очищения имеет не меньшую размерность, чем первое; следовательно, согласно замечанию после теоремы 3.1.2 найдется изометрия $W: \mathcal{H}_B \rightarrow \mathcal{H}_A \otimes \mathcal{H}_{E'}$ такая, что

$$(I_{RE} \otimes W)|\psi_{BRE}\rangle = |\psi_{AR}\rangle \otimes |\psi_{EE'}\rangle. \quad (9.10)$$

Взяв частичные следы по пространствам E, E' от соответствующих операторов плотности, получаем точную обратимость

$$(\text{Id}_R \otimes \mathcal{D} \circ \Phi)[S_{AR}] = S_{AR}, \quad (9.11)$$

где восстанавливающий канал определяется как

$$\mathcal{D}[S_B] = \text{Tr}_{E'} W S_B W^*. \quad (9.12)$$

3) $\Rightarrow$ 4) $\Rightarrow$ 1). Далее будет доказано следствие 9.2.1, из утверждения 1) $\Leftrightarrow$ 3) которого с заменой Φ на $\mathcal{D} \circ \Phi$ вытекает, что канал Φ точно обратим на состоянии S тогда и только тогда, когда

$$\mathcal{D} \circ \Phi[\tilde{S}] = \tilde{S}$$

для всех $\tilde{S}$, $\text{supp } \tilde{S} \subset \mathcal{L} \equiv \text{supp } S$, где $\text{supp } S$ — носитель оператора плотности S (см. § 1.3). Мы можем выразить это же свойство, сказав, что канал Φ является *точно обратимым на подпространстве $\mathcal{L}$* . Другими

словами, подпространство $\mathcal{L}$ является квантовым кодом, исправляющим ошибку Φ (а значит, и все ошибки ассоциированного с ней класса $\mathcal{E}$). Утверждение 4, а также импликация $4) \Rightarrow 1)$ следуют тогда из доказательства теоремы 9.1.1. $\square$

Следующее предложение дает характеристику в терминах комплементарного канала, которая лежит в основе теоремы о секретной классической пропускной способности в п. 9.4.1.

Предложение 9.1.2. *Для заданного расширения Стайнспринга канала Φ следующие условия эквивалентны:*

- 1) канал Φ точно обратим на подпространстве $\mathcal{L}$;
- 2) комплементарный канал (7.38) является полностью деполяризующим на $\mathcal{L}$, т. е.

$$\Phi_E[\tilde{S}] = S_E \quad (9.13)$$

для любого состояния $\tilde{S}$, $\text{supp } \tilde{S} \subset \mathcal{L}$, где S_E — фиксированное состояние.

Доказательство. $1) \Rightarrow 2)$. Пусть канал Φ точно обратим, тогда соотношение (9.10) выполнено для некоторой изометрии W и для всех векторов $|\psi_{AR}\rangle$, имеющих тензорное разложение с A -компонентами в $\mathcal{L}$. Здесь $|\psi\rangle_{EE'}$ не зависит от входного вектора $|\psi_{AR}\rangle$, так как иначе правая часть не была бы линейной по $|\psi_{AR}\rangle$. Взяв частичный след по RAE' от соответствующего оператора плотности, получаем соотношение (9.13).

$2) \Rightarrow 1)$. Имеет место представление Стайнспринга $\Phi_E[\tilde{S}] = \text{Tr}_B V \tilde{S} V^*$, где B играет роль окружения для системы E . Пусть соотношение (9.13) выполнено, и пусть $|\psi_{EE'}\rangle$ — очищение состояния S_E ; тогда имеет место представление Стайнспринга для ограничения канала Φ_E на состояния с носителем в $\mathcal{L}$:

$$\Phi_E[\tilde{S}] = \text{Tr}_{AE'} V' \tilde{S} V'^*, \quad (9.14)$$

где $V' = I_A \otimes |\psi_{EE'}\rangle$ — изометричный оператор, действующий из $\mathcal{H}_A$ в $\mathcal{H}_{AEE'} = \mathcal{H}_E \otimes \mathcal{H}_{AE'}$ по формуле $V'|\psi_A\rangle = |\psi_A\rangle \otimes |\psi_{EE'}\rangle$. В этом представлении роль окружения играет система AE' . По теореме 6.2.2 найдется такая частичная изометрия $W: \mathcal{H}_B \rightarrow \mathcal{H}_{AE'}$, что

$$(W \otimes I_{RE})V = V' = I_A \otimes |\psi_{EE'}\rangle.$$

Следовательно, соотношение (9.10) выполнено для всех векторов $|\psi\rangle_{RA}$ с тензорным разложением, у которого A -компоненты принадлежат $\mathcal{L}$. Расширяя, если необходимо, пространство $\mathcal{H}_{E'}$, мы можем заменить W на изометрию, для которой продолжает выполняться соотношение (9.10). Рассуждая, как в доказательстве предыдущего утверждения, возьмем

частичный след по REE' от соответствующего оператора плотности и получим точную обратимость на $\mathcal{L}$:

$$\mathcal{D} \circ \Phi[\tilde{S}] = \tilde{S}, \quad (9.15)$$

где восстанавливающий канал определяется, как в формуле (9.12). $\square$

§ 9.2. Точность воспроизведения квантовой информации

В качестве меры точности передачи состояния S каналом Φ можно использовать следовую норму $\|S - \Phi[S]\|_1$. Однако более удобными оказываются другие меры точности, которые играют ту же роль, что вероятность правильного решения в классическом случае. Дадим их описание и рассмотрим взаимосвязи между ними.

9.2.1. Точность воспроизведения чистых состояний

Лемма 9.2.1. Пусть ψ — единичный вектор и S — произвольное состояние. Имеют место неравенства

$$2[1 - \langle \psi | S | \psi \rangle] \leq \| |\psi\rangle\langle\psi| - S \|_1 \leq 2\sqrt{1 - \langle \psi | S | \psi \rangle}. \quad (9.16)$$

Если $S = |\varphi\rangle\langle\varphi|$ — чистое состояние, то второе неравенство превращается в равенство, т. е.

$$\| |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi| \|_1 = 2\sqrt{1 - |\langle \psi | \varphi \rangle|^2}. \quad (9.17)$$

Доказательство. Согласно соотношению (1.19) имеем

$$\| |\psi\rangle\langle\psi| - S \|_1 = \max_U |\mathrm{Tr}(|\psi\rangle\langle\psi| - S)U|,$$

где максимум берется по всем унитарным операторам U . Полагая $U = 2|\psi\rangle\langle\psi| - I$, получаем первое неравенство.

Равенство (9.17) получается аналогично соотношению (2.46). Для вычисления следовой нормы достаточно найти собственные значения оператора $|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|$, который имеет ранг 2 (см. задачу 2.3.1).

Пусть теперь S — произвольный оператор плотности; рассмотрим его спектральное разложение $S = \sum \lambda_i S_i$. Используя выпуклость нормы, вогнутость функции $\sqrt{\cdot}$ и соотношение (9.17), получаем

$$\begin{aligned} \| |\psi\rangle\langle\psi| - S \|_1 &\leq \sum_i \lambda_i \| |\psi\rangle\langle\psi| - S_i \|_1 = \\ &= 2 \sum_i \lambda_i \sqrt{1 - \langle \psi | S_i | \psi \rangle} \leq 2\sqrt{1 - \langle \psi | S | \psi \rangle}. \quad \square \end{aligned}$$

Для чистого состояния $|\psi\rangle\langle\psi|$ и произвольного состояния S величина

$$F(|\psi\rangle\langle\psi|, S) = \langle\psi|S|\psi\rangle \quad (9.18)$$

называется *точностью воспроизведения* (состояния $|\psi\rangle\langle\psi|$ состоянием S). Очевидно, что $F \leq 1$, причем равенство имеет место тогда и только тогда, когда $S = |\psi\rangle\langle\psi|$. Заметим, что, рассматривая проблему сжатия квантовых данных (§ 5.5), мы уже фактически использовали точность воспроизведения (9.18). Там состояние $|\psi_i\rangle\langle\psi_i|$ появлялось с вероятностью p_i и среднее значение точности воспроизведения определялось как $\bar{F} = \sum_i p_i \langle\psi_i|S_i|\psi_i\rangle$.

В связи с понятием кода, исправляющего ошибки, естественно определить точность воспроизведения следующим образом. Пусть заданы подпространство (квантовый код) $\mathcal{L} \subset \mathcal{H}$ и канал Φ в $\mathcal{H}$, для которого входное и выходное пространства совпадают: $\mathcal{H}_B = \mathcal{H}_A = \mathcal{H}$. Точность воспроизведения подпространства $\mathcal{L}$ определяется как

$$F_s(\mathcal{L}, \Phi) = \min_{\psi \in \mathcal{L}, \|\psi\|=1} F(|\psi\rangle\langle\psi|, \Phi[|\psi\rangle\langle\psi|]) = \min_{\psi \in \mathcal{L}, \|\psi\|=1} \langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle.$$

Согласно лемме 9.2.1 имеем

$$2[1 - F_s(\mathcal{L}, \Phi)] \leq \max_{\psi \in \mathcal{L}} \|\psi\rangle\langle\psi| - \Phi[|\psi\rangle\langle\psi|]\|_1 \leq 2\sqrt{1 - F_s(\mathcal{L}, \Phi)}. \quad (9.19)$$

Другой важной величиной является точность воспроизведения сцепленности. Рассмотрим очищение $|\psi_{AR}\rangle\langle\psi_{AR}|$ состояния $S = S_A$ в гильбертовом пространстве $\mathcal{H}_A \otimes \mathcal{H}_R$. Точность воспроизведения этого чистого состояния под действием тривиального расширения канала Φ равна

$$F_e(S, \Phi) = \langle\psi_{AR}|(\Phi \otimes \text{Id}_R)[|\psi_{AR}\rangle\langle\psi_{AR}|]|\psi_{AR}\rangle$$

и называется *точностью воспроизведения сцепленности*. Дадим удобное выражение для $F_e(S, \Phi)$, которое также показывает независимость этой величины от выбора очищения исходного состояния.

Пусть канал имеет представление Крауса

$$\Phi[S] = \sum_i V_i S V_i^*, \quad (9.20)$$

тогда

$$F_e(S, \Phi) = \sum_i |\text{Tr } V_i S|^2. \quad (9.21)$$

В самом деле,

$$\begin{aligned} \langle\psi_{AR}| \sum_i (V_i \otimes I_R) |\psi_{AR}\rangle\langle\psi_{AR}| (V_i \otimes I_R)^* |\psi_{AR}\rangle &= \\ &= \sum_i |\langle\psi_{AR}| (V_i \otimes I_R) |\psi_{AR}\rangle|^2 = \sum_i |\text{Tr } V_i S|^2. \end{aligned}$$

Заметим, что для чистого состояния $S = |\psi\rangle\langle\psi|$ выполняется равенство

$$F_e(S, \Phi) = \langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle = F(|\psi\rangle\langle\psi|, \Phi[|\psi\rangle\langle\psi|]).$$

Задача 9.2.1. Докажите, что $F_e(S, \Phi)$ — выпуклая функция состояния S . *Указание.* Согласно соотношению (9.21) функция $F_e(S, \Phi)$ является суммой квадратов аффинных функций.

9.2.2. Соотношения между мерами точности воспроизведения

Лемма 9.2.2. Для произвольного состояния S справедлива оценка

$$1 - F_e(S, \Phi) \leq 4\sqrt{1 - F_s(\text{supp } S, \Phi)}.$$

Доказательство. Имеем

$$\begin{aligned} 1 - F_e(S, \Phi) &= 1 - \langle\psi_{AR}|(\Phi \otimes \text{Id}_R)(|\psi_{AR}\rangle\langle\psi_{AR}|)|\psi_{AR}\rangle = \\ &= \langle\psi_{AR}|(\text{Id}_A - \Phi) \otimes \text{Id}_R[|\psi_{AR}\rangle\langle\psi_{AR}|]|\psi_{AR}\rangle. \end{aligned}$$

Представляя $|\psi_{AR}\rangle = \sum_j |\psi_j\rangle \otimes |e_j\rangle$, где $\{|e_j\rangle\}$ — ортонормированный базис в $\mathcal{H}_R$, $\sum_j \|\psi_j\|^2 = 1$, $\psi_j \in \text{supp } S$, получаем равносильное соотношение

$$\sum_{jk} \langle\psi_j|(\text{Id} - \Phi)[|\psi_j\rangle\langle\psi_k|]|\psi_k\rangle = \sum_{jk} \text{Tr} |\psi_k\rangle\langle\psi_j| (|\psi_j\rangle\langle\psi_k| - \Phi[|\psi_j\rangle\langle\psi_k|]).$$

Используя неравенство (1.18) и тот факт, что и следовая, и операторная нормы оператора $|\psi_j\rangle\langle\psi_k|$ равны $\|\psi_j\| \|\psi_k\|$, получаем, что это выражение не превосходит

$$\max_T \frac{\|T - \Phi[T]\|_1}{\|T\|_1},$$

где максимум берется по всем операторам $T \neq 0$, действующим в $\mathcal{L} = \text{supp } S$. Рассматривая разложение $T = T_1 + iT_2$, где $T_1^* = T_1$, $T_2^* = T_2$ — эрмитовы операторы, также действующие в $\mathcal{L}$, принимая во внимание, что $\|T_{1,2}\|_1 \leq \|T\|_1$, и используя неравенство треугольника, получаем, что это выражение не превосходит величину

$$2 \max_{T^*=T} \frac{\|T - \Phi[T]\|_1}{\|T\|_1} = 2 \max_{S: \text{supp } S \in \mathcal{L}} \|S - \Phi[S]\|_1. \quad (9.22)$$

Здесь неравенство $\geq$ получается при переходе к положительным T . С другой стороны,

$$\begin{aligned} \max_{T^*=T} \frac{\|T - \Phi[T]\|_1}{\|T\|_1} &\leq \\ &\leq \|S_+ - \Phi[S_+]\|_1 \frac{p_+}{p_+ + p_-} + \|S_- - \Phi[S_-]\|_1 \frac{p_-}{p_+ + p_-}, \quad (9.23) \end{aligned}$$

где использованы обозначения $p_{\pm} = \text{Tr } T_{\pm}$, $S_{\pm} = p_{\pm}^{-1} T_{\pm}$. Правая часть этого неравенства меньше или равна правой части в соотношении (9.22), которое таким образом установлено. Далее,

$$\max_{S: \text{supp } S \in \mathcal{L}} \|S - \Phi[S]\|_1 = \max_{\psi: \psi \in \mathcal{L}, \|\psi\|=1} \| |\psi\rangle\langle\psi| - \Phi[|\psi\rangle\langle\psi|] \|_1,$$

поскольку максимум непрерывной выпуклой функции на выпуклом множестве достигается в его крайней точке. Используя второе из неравенств (9.19), получаем, что оцениваемое выражение не превосходит $4\sqrt{1 - F_s(\mathcal{L}, \Phi)}$. $\square$

Задача 9.2.2. Используя свойство выпуклости из задачи 9.2.1, докажите неравенство

$$1 - F_s(\mathcal{L}, \Phi) \leq 1 - \min_{S: \text{supp } S \in \mathcal{L}} F_e(S, \Phi). \quad (9.24)$$

Пусть теперь $\mathcal{L} = \mathcal{H}$, тогда

$$\max_T \frac{\|T - \Phi[T]\|_1}{\|T\|_1} = \|\text{Id} - \Phi\|.$$

Из доказательства леммы 9.2.2 следует справедливость цепочки неравенств

$$\begin{aligned} 1 - \min_S F_e(S, \Phi) &\leq \|\text{Id} - \Phi\| \leq \\ &\leq 2 \max_{\|\psi\|=1} \| |\psi\rangle\langle\psi| - \Phi[|\psi\rangle\langle\psi|] \|_1 \leq 2\|\text{Id} - \Phi\|. \end{aligned} \quad (9.25)$$

Вместе с соотношениями (9.24) это означает, что отклонение канала Φ от идеального канала Id эквивалентным образом описывается одной из величин

$$\|\text{Id} - \Phi\|, \quad \max_S \|S - \Phi[S]\|_1, \quad 1 - F_s(\mathcal{H}, \Phi), \quad 1 - \min_S F_e(S, \Phi).$$

При рассмотрении квантовой пропускной способности канала нам понадобится очевидное следствие леммы 9.2.2:

$$1 - F_e(\tilde{S}, \Phi) \leq 4\sqrt{1 - F_s(\mathcal{H}, \Phi)}, \quad (9.26)$$

где $\tilde{S}$ — хаотическое состояние в $\mathcal{H}$.

Поучительно рассмотреть случай «идеальной» точности воспроизведения.

Следствие 9.2.1. Следующие условия эквивалентны:

- 1) $F_e(S, \Phi) = 1$;
- 2) $F_s(\text{supp } S, \Phi) = 1$;
- 3) $\Phi[\tilde{S}] = \tilde{S}$ для произвольного состояния $\tilde{S}$, $\text{supp } \tilde{S} \subset \text{supp } S$;
- 4) $F_e(\tilde{S}, \Phi) = 1$ для произвольного состояния $\tilde{S}$, $\text{supp } \tilde{S} \subset \text{supp } S$.

Доказательство. Докажем, что из условия 1 следует условие 2. Пусть $|\psi\rangle \in \text{supp } S$, тогда

$$S = p|\psi\rangle\langle\psi| + (1-p)S',$$

где $p > 0$, а S' — оператор плотности. Согласно задаче 9.2.1 функция $S \rightarrow F_e(S, \Phi)$ выпукла, поэтому

$$pF_e(|\psi\rangle\langle\psi|, \Phi) + (1-p)F_e(S', \Phi) \geq F_e(S, \Phi) = 1,$$

и, значит, $F_e(|\psi\rangle\langle\psi|, \Phi) = 1$. Но отсюда следует, что

$$\langle\psi|\Phi[|\psi\rangle\langle\psi|]|\psi\rangle = 1$$

для всех $|\psi\rangle \in \text{supp } S$ и $F_s(\text{supp } S, \Phi) = 1$.

Из леммы 9.2.2 вытекает утверждение $2) \Rightarrow 1)$. Кроме того, так как из условия 2 очевидным образом следует аналогичное условие с $\text{supp } \tilde{S}$ вместо $\text{supp } S$, мы также установили и справедливость свойства 4, которое формально является усилением свойства 1.

По определению величины F_s свойство 2 равносильно свойству 3 для чистых, а следовательно, и для смешанных состояний $\tilde{S}$. $\square$

9.2.3. Точность воспроизведения и расстояние Бюреса

В этом пункте мы обсудим понятие точности воспроизведения для двух произвольных состояний. Этот материал понадобится нам лишь в п. 9.4.4.

Для чистых состояний $S = |\varphi\rangle\langle\varphi|$, $T = |\psi\rangle\langle\psi|$ точность воспроизведения равна $F(T, S) = |\langle\varphi|\psi\rangle|^2$, при этом связь между точностью воспроизведения и следовой нормой разности состояний S и T выражается формулой (9.17). Пусть теперь S, T — произвольные операторы плотности.

Определение 9.2.1. Точность воспроизведения определяется соотношением

$$F(T, S) = \max |\langle\psi_T|\psi_S\rangle|^2, \quad (9.27)$$

где максимум берется по всем возможным очищениям ψ_S, ψ_T состояний S, T в одном и том же пространстве $\mathcal{H} \otimes \mathcal{H}'$.

Используя теорему 3.1.3, видим, что

$$F(T, S) = \max_W |\langle\psi_T|(I \otimes W)\psi_S\rangle|^2, \quad (9.28)$$

где ψ_S, ψ_T — фиксированные очищения состояний S, T в некотором гильбертовом пространстве $\mathcal{H} \otimes \mathcal{H}'$, а максимум берется по всем унитарным операторам W из $\mathcal{H}'$. В частности, рассматривая очищения $\sqrt{S}, \sqrt{T}$ в $L^2(\mathcal{H}) \simeq \mathcal{H} \otimes \mathcal{H}^*$, получаем

$$F(T, S) = \max_W |\text{Tr } \sqrt{S}\sqrt{T}W|^2,$$

где максимум берется по всем унитарным операторам W в $\mathcal{H}$. Используя полярное разложение оператора $\sqrt{S}\sqrt{T} = U|\sqrt{S}\sqrt{T}|$, можно видеть, что максимум достигается при $W = U^*$ и равен

$$F(T, S) = (\text{Tr}|\sqrt{S}\sqrt{T}|)^2 = \|\sqrt{S}\sqrt{T}\|_1^2.$$

Эта формула переходит в (9.18), если $T = |\psi\rangle\langle\psi|$. Из этого рассуждения вытекает также, что в определении (9.27) можно ограничиться максимизацией по очищениям только одного состояния, при том что очищение другого состояния фиксировано.

Задача 9.2.3. Покажите, что $F(T, S) \leq 1$, причем равенство имеет место тогда и только тогда, когда $T = S$.

С понятием точности воспроизведения (9.27) связана метрика на множестве всех состояний, называемая *расстоянием Бюреса*, которая определяется как

$$\beta(T, S) = \min \|\psi_T - \psi_S\|, \quad (9.29)$$

где минимум берется по всем возможным очищениям ψ_S, ψ_T состояний S, T . Рассматривая квадрат нормы и используя определение (9.27), получаем

$$\beta(T, S) = \sqrt{2(1 - \|\sqrt{S}\sqrt{T}\|_1)} = \sqrt{2(1 - \sqrt{F(T, S)})}. \quad (9.30)$$

В частности, для чистых состояний $T = |\psi\rangle\langle\psi|$, $S = |\varphi\rangle\langle\varphi|$ имеем

$$\beta(T, S) = \sqrt{2(1 - |\langle\psi|\varphi\rangle|)}.$$

Отсюда также видно, что, как и при определении точности воспроизведения, в формуле (9.29) можно брать максимум по всевозможным очищениям лишь одного состояния.

Неравенство треугольника для $\beta(T, S)$ следует из определения (9.29) и соответствующего неравенства для нормы. Для чистых состояний оно принимает вид

$$\sqrt{1 - |\langle\varphi|\psi\rangle|} \leq \sqrt{1 - |\langle\varphi|\chi\rangle|} + \sqrt{1 - |\langle\chi|\psi\rangle|}, \quad (9.31)$$

где φ, χ, ψ — произвольные единичные векторы.

Лемма 9.2.3. Для любых двух операторов плотности S_1, S_2 в $\mathcal{H}$ справедливо неравенство

$$\beta(S_1, S_2)^2 \leq \|S_1 - S_2\|_1 \leq 2\beta(S_1, S_2). \quad (9.32)$$

Рассматривая первое неравенство вместе с соотношениями (9.30) и (9.28), получаем следствие.

Следствие 9.2.2. Для любых двух операторов плотности S_1, S_2 в $\mathcal{H}$ и их очищений ψ_{S_1}, ψ_{S_2} в $\mathcal{H} \otimes \mathcal{H}'$ имеет место неравенство

$$\|S_1 - S_2\|_1 \geq 2 \left(1 - \max_W |\langle \psi_{S_1} | (I \otimes W) \psi_{S_2} \rangle| \right), \quad (9.33)$$

где максимум берется по всем унитарным операторам W в $\mathcal{H}'$.

Доказательство леммы 9.2.3. Так как $\text{Tr} \sqrt{S_1} \sqrt{S_2} \leq \text{Tr} |\sqrt{S_1} \sqrt{S_2}|$, для доказательства первого из неравенств (9.32) достаточно доказать, что

$$2(1 - \text{Tr} \sqrt{S_1} \sqrt{S_2}) \leq \|S_1 - S_2\|_1.$$

Это вытекает из более общего неравенства

$$\text{Tr}(\sqrt{S_1} - \sqrt{S_2})^2 \leq \|S_1 - S_2\|_1,$$

справедливого для произвольных положительных операторов S_1, S_2 . Докажем последнее неравенство. Для эрмитова оператора K мы обозначаем через $1_+(K)$ (соответственно $1_-(K)$) спектральный проектор, соответствующий положительным (соответственно неотрицательным) собственным значениям. Тогда $\sigma(K) = 1_+(K) - 1_-(K)$ является унитарным эрмитовым оператором, причем $\sigma(K)K = K\sigma(K) = |K|$. Вводя операторы $K = \sqrt{S_1} - \sqrt{S_2}$, $L = \sqrt{S_1} + \sqrt{S_2}$, получаем $S_1 - S_2 = \frac{1}{2}(KL + LK) \equiv K \circ L$; следовательно,

$$\begin{aligned} \|S_1 - S_2\|_1 &\geq |\text{Tr} \sigma(K)K \circ L| = \text{Tr} |K|L = \\ &= \text{Tr} |K| (1_+(K)L1_+(K) + 1_-(K)L1_-(K)). \end{aligned}$$

Так как $L \geq K \geq -L$, мы получаем $1_+(K)L1_+(K) \geq 1_+(K)K$ и $1_-(K)L1_-(K) \geq -1_-(K)K$. Таким образом, $(1_+(K)L1_+(K) + 1_-(K)L1_-(K)) \geq |K|$, и в итоге получаем

$$\|S_1 - S_2\|_1 \geq \text{Tr} |K|^2 = \text{Tr}(\sqrt{S_1} - \sqrt{S_2})^2.$$

Для доказательства второго из неравенств (9.32) рассмотрим представление $S_1 = T_1^* T_1$, $S_2 = T_2^* T_2$, где T_1, T_2 — некоторые (не обязательно эрмитовы) операторы. Вводя обозначения $K = T_1 - T_2$, $L = T_1 + T_2$, получаем

$$\begin{aligned} \|S_1 - S_2\|_1 &= \text{Tr} \sigma(S_1 - S_2)(S_1 - S_2) = \\ &= \frac{1}{2} [\text{Tr} \sigma(S_1 - S_2)K^* L + \text{Tr} \sigma(S_1 - S_2)L^* K]. \end{aligned}$$

Используя неравенство Коши—Буняковского для следа, имеем

$$|\text{Tr} \sigma(K \circ L)K^* L| \leq [\text{Tr} \sigma(S_1 - S_2)^2 K^* K \cdot \text{Tr} L^* L]^{1/2} = [\text{Tr} K^* K \cdot \text{Tr} L^* L]^{1/2};$$

аналогичная оценка имеет место и для второго слагаемого. Тогда

$$\|S_1 - S_2\|_1 \leq [\mathrm{Tr} K^* K \cdot \mathrm{Tr} L^* L]^{1/2}.$$

Используя нормировку операторов S_1, S_2 , получаем

$$\mathrm{Tr} K^* K = 2(1 - \mathrm{Re} \mathrm{Tr} T_1^* T_2), \quad \mathrm{Tr} L^* L = 2(1 + \mathrm{Re} \mathrm{Tr} T_1^* T_2).$$

Полагая $T_1 = \sqrt{S_1}$, $T_2 = U \sqrt{S_2}$, где U — унитарный оператор из полярного разложения оператора $\sqrt{S_1} \sqrt{S_2}$, получаем $\mathrm{Re} \mathrm{Tr} T_1^* T_2 = \mathrm{Re} \mathrm{Tr} T_2^* T_1 = \mathrm{Tr} |\sqrt{S_1} \sqrt{S_2}|$. Таким образом,

$$\mathrm{Tr} K^* K = 2(1 - \|\sqrt{S_1} \sqrt{S_2}\|_1) = \beta(S_1, S_2)^2,$$

$$\mathrm{Tr} L^* L = 2(1 + \|\sqrt{S_1} \sqrt{S_2}\|_1) \leq 4,$$

откуда следует второе из неравенств (9.32). □

§ 9.3. Квантовая пропускная способность

9.3.1. Достижимые скорости

Пусть $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$ — некоторый квантовый канал. Рассмотрим составной канал $\Phi^{\otimes n}: \mathfrak{T}(\mathcal{H}_A^{\otimes n}) \rightarrow \mathfrak{T}(\mathcal{H}_B^{\otimes n})$.

Определение 9.3.1. Величина $R \geq 0$ называется *достижимой скоростью* (для передачи квантовой информации), если существуют последовательность пространств $\mathcal{H}^{(n)}$ такая, что

$$\overline{\lim}_{n \rightarrow \infty} \frac{1}{n} \log \dim \mathcal{H}^{(n)} = R,$$

и последовательности каналов $\mathcal{E}^{(n)}: \mathfrak{T}(\mathcal{H}^{(n)}) \rightarrow \mathfrak{T}(\mathcal{H}_A^{\otimes n})$ (кодирований) и $\mathcal{D}^{(n)}: \mathfrak{T}(\mathcal{H}_B^{\otimes n}) \rightarrow \mathfrak{T}(\mathcal{H}^{(n)})$ (декодирований) такие, что

$$\lim_{n \rightarrow \infty} F_s(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) = 1. \quad (9.34)$$

Точная верхняя грань множества достижимых скоростей обозначается $Q(\Phi)$ и называется *квантовой пропускной способностью* канала Φ .

При доказательстве классической теоремы кодирования было удобно использовать среднюю вероятность ошибки вместо максимальной; равносильность соответствующих критериев была доказана в лемме 4.4.1. В квантовом случае роль средней вероятности ошибки играет величина $1 - F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)})$, где $\bar{S}^{(n)} = \frac{1}{d_n} I_{\mathcal{H}^{(n)}}$ — хаотическое состояние в $\mathcal{H}^{(n)}$, тогда как аналогом максимальной ошибки является $1 - F_s(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)})$. В самом деле, из того, что

$F_s(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) \rightarrow 1$, следует, что

$$F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) \rightarrow 1$$

(согласно лемме 9.2.2). В обратном направлении справедлив следующий аналог леммы 4.4.1.

Лемма 9.3.1. Пусть $\mathcal{H}$ — гильбертово пространство размерности $2d$, Φ — канал в $\mathcal{H}$. Тогда найдется подпространство $\mathcal{H}'$ размерности d такое, что

$$1 - F_s(\mathcal{H}', \mathcal{D}' \circ \Phi) \leq 2(1 - F_e(\bar{S}, \Phi)),$$

где $\bar{S} = \frac{1}{2d}I_{\mathcal{H}}$, а $\mathcal{D}'[S] = P'SP' + \frac{P'}{d} \text{Tr}(I - P')S$ для всех $S \in \mathfrak{S}(\mathcal{H})$; P' — проектор на $\mathcal{H}'$.

Доказательство. На единичном шаре в $\mathcal{H}$ рассмотрим непрерывную функцию $|\psi\rangle \rightarrow f(\psi) = \langle \psi | \Phi[|\psi\rangle\langle\psi|] | \psi \rangle = F_e(|\psi\rangle\langle\psi|, \Phi)$. Пусть $|\psi_1\rangle$ — вектор, минимизирующий $f(\psi)$. Определим ортонормированный базис $\{|\psi_j\rangle; j = 1, \dots, 2d\}$ в $\mathcal{H} \equiv \mathcal{H}_0$ с помощью следующей рекуррентной процедуры: $|\psi_{j+1}\rangle$ есть вектор в подпространстве $\mathcal{H}_j = \{|\psi_1\rangle, \dots, |\psi_j\rangle\}^\perp$, минимизирующий $f(\psi)$. Тогда $\mathcal{H}_j \supset \mathcal{H}_{j+1}$ и $\dim \mathcal{H}_j = 2d - j$. Используя выпуклость функции $F_e(S, \Phi)$ (см. задачу 9.2.1), получаем

$$\begin{aligned} 1 - F_e(\bar{S}, \Phi) &\geq \frac{1}{2d} \sum_{j=1}^{2d} (1 - F_e(|\psi_j\rangle\langle\psi_j|, \Phi)) \geq \frac{1}{2d} \sum_{j=d+1}^{2d} (1 - f(\psi_j)) \geq \\ &\geq \frac{1}{2} \left(1 - \min_{|\psi\rangle \in \mathcal{H}_d} f(\psi) \right) \geq \frac{1}{2} (1 - F_s(\mathcal{H}', \mathcal{D}' \circ \Phi)), \end{aligned}$$

где $\mathcal{H}' = \mathcal{H}_d$. □

Из доказанной леммы вместе с неравенством (9.26) следует, что в определении достижимых скоростей мы можем заменить требование (9.34) на требование

$$\lim_{n \rightarrow \infty} F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) = 1. \quad (9.35)$$

Теперь покажем, что в определении квантовой пропускной способности достаточно ограничиться *изометричными* кодированиями, т. е. кодированиями вида

$$\mathcal{E}[S] = \text{Ad } V[S] = VSV^*, \quad (9.36)$$

где V — изометричное отображение пространства $\mathcal{H}^{(n)}$ во входное пространство канала $\mathcal{H}^{\otimes n}$. Мы докажем, что если существует кодирование общего вида, при котором достигается высокая точность воспроизведения данного состояния, то найдется и изометричное кодирование

с аналогичным свойством. Чтобы пояснить это на интуитивном уровне, рассмотрим случай точного воспроизведения. Если композиция кодирование-канал-декодирование точно воспроизводит некоторое состояние S , то кодирующий канал $\mathcal{E}$ является точно обратимым на S , причем восстанавливающим каналом является композиция канал-декодирование. Тогда согласно предложению 9.1.1 канал $\mathcal{E}$ на $\text{supp } S$ представляется в виде (9.5) как выпуклая комбинация изометричных кодирований $\mathcal{U}_j = \text{Ad } U_j$. Следовательно, каждый из каналов $\mathcal{U}_j$ является точно обратимым на S с тем же самым восстанавливающим каналом.

Лемма 9.3.2. Пусть S — состояние в гильбертовом пространстве $\mathcal{L}$, $\mathcal{L} = \text{supp } S$, $\mathcal{E}$ — вполне положительное отображение из $\mathfrak{T}(\mathcal{L})$ в $\mathfrak{T}(\mathcal{H})$, для которого $\text{Tr } \mathcal{E}[S] = 1$, и $\mathcal{A}$ — канал из $\mathfrak{T}(\mathcal{H})$ в $\mathfrak{T}(\mathcal{L})$. Предположим, что $\dim \mathcal{L} \leq \dim \mathcal{H}$, тогда найдется изометрия V из $\mathcal{L}$ в $\mathcal{H}$ такая, что

$$F_e(S, \mathcal{A} \circ \text{Ad } V) \geq F_e(S, \mathcal{A} \circ \mathcal{E})^2. \quad (9.37)$$

Эта лемма будет использована в ситуации, когда $\mathcal{E}$ — кодирующее отображение, а $\mathcal{A}$ — композиция канал-декодирование. Для доказательства потребуется следующее обобщение полярного разложения: если X — оператор из $\mathcal{L}$ в $\mathcal{H}$, $\dim \mathcal{L} \leq \dim \mathcal{H}$, то $X = V|X|$, где $|X| = \sqrt{X^*X}$ — положительный оператор в $\mathcal{L}$, а V — изометрия из $\mathcal{L}$ в $\mathcal{H}$. Отсюда вытекает следующее представление для произвольной квадратной матрицы X : $X = VDU$, где D — диагональная матрица с неотрицательными элементами, а V, U — унитарные матрицы.

Доказательство. Пусть $A_i: \mathcal{H} \rightarrow \mathcal{L}$ и $E_j: \mathcal{L} \rightarrow \mathcal{H}$ — компоненты разложения Крауса для отображений $\mathcal{A}$ и $\mathcal{E}$ соответственно. Обозначим через X матрицу с элементами $X_{ij} = \text{Tr } A_i E_j S$. Тогда

$$F_e(S, \mathcal{A} \circ \mathcal{E}) = \sum_{ij} |X_{ij}|^2.$$

Добавляя, если необходимо, нулевые компоненты в разложения Крауса, можно считать, что X — квадратная матрица. Из представления $X = VDU$ следует, что, преобразуя разложения Крауса для $\mathcal{A}$ и $\mathcal{E}$, можно добиться, чтобы матрица X стала диагональной. Тогда $F_e(S, \mathcal{A} \circ \mathcal{E}) = \sum_k \text{Tr}(A_k E_k S)^2$.

Введем обозначение $\lambda_k = \text{Tr } S E_k^* E_k$ и ограничимся рассмотрением случая, когда $\lambda_k > 0$. Тогда $\sum_k \lambda_k (\text{Tr}(A_k E_k S)^2 / \lambda_k) = F_e(S, \mathcal{A} \circ \mathcal{E})$ и $\sum_k \lambda_k = 1$, так что найдется такое k , что $\text{Tr}(A_k E_k S)^2 / \lambda_k \geq F_e(S, \mathcal{A} \circ \mathcal{E})$. Вводя обозначения $E = E_k / \sqrt{\lambda_k}: \mathcal{L} \rightarrow \mathcal{H}$, $A = A_k: \mathcal{H} \rightarrow \mathcal{L}$, получаем $A^* A \leq I_{\mathcal{H}}$, $\text{Tr } S E^* E = 1$ и

$$F_e(S, \mathcal{A} \circ \mathcal{E}) \leq F_e(S, \text{Ad } A \circ \text{Ad } E) = |\text{Tr } AES|^2.$$

Пусть $A^* = V|A^*|$ — полярное разложение оператора $A^*: \mathcal{L} \rightarrow \mathcal{H}$, где $V: \mathcal{L} \rightarrow \mathcal{H}$ — изометрия. Согласно некоммутативному неравенству Коши—Буняковского (2.25) имеем

$$|\mathrm{Tr} AES|^2 = |\mathrm{Tr} SAE|^2 \leq \mathrm{Tr} SAA^* \mathrm{Tr} SE^*E = \mathrm{Tr} S|A^*|^2. \quad (9.38)$$

Поскольку $A^*A \leq I_{\mathcal{H}}$, также справедливо неравенство $AA^* \leq I_{\mathcal{L}}$, следовательно, $|A^*|^2 \leq |A^*|$, и поэтому

$$\mathrm{Tr} S|A^*|^2 \leq \mathrm{Tr} S|A^*| = \mathrm{Tr} AVS.$$

Тогда

$$|\mathrm{Tr} AVS|^2 \leq \sum_k |\mathrm{Tr} A_k VS|^2 = F_e(S, \mathcal{A} \circ \mathrm{Ad} V).$$

Из полученной цепочки неравенств следует неравенство (9.37). $\square$

Пусть теперь даны последовательности пространств $\mathcal{H}^{(n)}$, кодирований $\mathcal{E}^{(n)}$ и декодирований $\mathcal{D}^{(n)}$, для которых выполнено условие (9.35), тогда согласно лемме 9.3.2 найдется последовательность изометричных кодирований $\mathcal{V}^{(n)} = \mathrm{Ad} V^{(n)}$ такая, что

$$\lim_{n \rightarrow \infty} F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{V}^{(n)}) = 1. \quad (9.39)$$

Отсюда следует, что в определении квантовой пропускной способности можно ограничиться изометричными кодированиями.

9.3.2. Квантовая пропускная способность и когерентная информация

Следующий фундаментальный результат является теоремой кодирования для квантовой пропускной способности и устанавливает связь квантовой пропускной способности с когерентной информацией.

Теорема 9.3.1. *Имеет место соотношение*

$$Q(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_S I_c(S, \Phi^{\otimes n}). \quad (9.40)$$

Существование предела может быть доказано так же, как и в случае классической пропускной способности, — с помощью свойства субаддитивности последовательности $\bar{Q}_n = \max_S I_c(S, \Phi^{\otimes n})$. Простым следствием соотношения (9.40) является неравенство, связывающее квантовую и классическую пропускные способности:

$$Q(\Phi) \leq C(\Phi), \quad (9.41)$$

которое доказывается так же, как и неравенство (8.57). Действительно, выбирая S в виде смеси произвольных чистых состояний S_j с вероятностями p_j и применяя неравенство (7.43), получаем

$$I_c(S, \Phi) \leq H\left(\sum_j p_j \Phi[S_j]\right) - \sum_j p_j H(\Phi[S_j]) = \chi(\{p_j\}, \{\Phi[S_j]\}).$$

Взяв максимум, получаем $\max_S I_c(S, \Phi) \leq C_\chi(\Phi)$. Применяя это неравенство к $\Phi^{\otimes n}$, получаем неравенство (9.41).

Доказательство неравенства $\leq$. Обозначим через $\bar{Q}(\Phi)$ правую часть соотношения (9.40). Более простой частью доказательства является доказательство неравенства $Q(\Phi) \leq \bar{Q}(\Phi)$. Пусть $\mathcal{H}^{(n)}$ — входное пространство размерности $d_n = \dim \mathcal{H}^{(n)} = 2^{n(R+o(1))}$, и пусть $\mathcal{E}^{(n)}$, $\mathcal{D}^{(n)}$ — кодирующие и декодирующие каналы такие, что

$$1 - F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) \leq \varepsilon,$$

где $\bar{S}^{(n)} = \frac{1}{d_n} I_{\mathcal{H}^{(n)}}$ — хаотическое состояние в $\mathcal{H}^{(n)}$ с энтропией $H(\bar{S}^{(n)}) = \log d_n = nR$. Здесь мы используем требование (9.35) в определении достижимых скоростей. Согласно лемме 9.3.2 можно считать, что $\mathcal{E}^{(n)}$ — *изометричные* кодирования. Так как

$$F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) = \langle \Omega^{(n)} | (\text{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) [|\Omega^{(n)}\rangle\langle\Omega^{(n)}|] | \Omega^{(n)} \rangle,$$

где

$$|\Omega^{(n)}\rangle = \frac{1}{\sqrt{d_n}} \sum_{m=1}^{d_n} |m\rangle \otimes |m\rangle \quad (9.42)$$

— максимально сцепленный вектор в пространстве $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$, из леммы 9.2.1 следует, что для максимально сцепленного состояния $|\Omega^{(n)}\rangle\langle\Omega^{(n)}|$ в $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$ выполняется неравенство

$$\left\| |\Omega^{(n)}\rangle\langle\Omega^{(n)}| - (\text{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) [|\Omega^{(n)}\rangle\langle\Omega^{(n)}|] \right\|_1 \leq 2\sqrt{\varepsilon}. \quad (9.43)$$

Это означает, что скорость R достижима для асимптотически безошибочной передачи хаотического состояния в $\mathcal{H}^{(n)}$.

Вводя обозначение $S^{(n)} = \mathcal{E}^{(n)}[\bar{S}^{(n)}]$ и используя цепное правило (9.6) для когерентной информации, получаем

$$I_c(S^{(n)}, \Phi^{\otimes n}) \geq I_c(S^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n}) = H(S_{B'}) - H(S_{B'R'}), \quad (9.44)$$

где $S_{B'R'} = (\text{Id}_{\mathcal{H}^{(n)}} \otimes (\mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)})) [|\Omega^{(n)}\rangle\langle\Omega^{(n)}|]$, так что

$$S_{B'} = (\mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)})[\bar{S}^{(n)}].$$

Тот факт, что $H(S_{B'R'}) = H(S^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n})$, следует из того, что в силу изометричности кодирования $\mathcal{E}^{(n)}$ состояние $(\text{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{E}^{(n)})[|\Omega^{(n)}\rangle\langle\Omega^{(n)}|]$ является чистым и его можно рассматривать как очищение состояния $S^{(n)}$. Согласно неравенству (9.43) имеем

$$\|\bar{S}^{(n)} - S_{B'}\|_1 \leq \| |\Omega^{(n)}\rangle\langle\Omega^{(n)}| - S_{B'R'} \|_1 \leq 2\sqrt{\varepsilon}.$$

Здесь первое неравенство вытекает из следующего простого наблюдения.

Задача 9.3.1. Докажите, что следовая норма монотонна по отношению к взятию частичного следа:

$$\|\mathrm{Tr}_{\mathcal{H}_0} T\|_1 \leq \|T\|_1$$

для любого положительного оператора $T \in \mathcal{H} \otimes \mathcal{H}_0$. *Указание.* Используйте выражение (1.19) для следовой нормы.

Дважды используя оценку (7.23) для модуля непрерывности энтропии, получаем

$$\begin{aligned} H(S_{B'}) - H(S_{B'R'}) &= H(\bar{S}^{(n)}) + [H(S_{B'}) - H(\bar{S}^{(n)})] + [H(|\Omega^{(n)}\rangle\langle\Omega^{(n)}|) - \\ &- H(S_{B'R'})] \geq H(\bar{S}^{(n)}) - 6 \log \dim \mathcal{H}^{(n)} \sqrt{\varepsilon} - \frac{2 \log e}{e} = nR(1 - 6\sqrt{\varepsilon}) - \frac{2 \log e}{e}. \end{aligned}$$

Поэтому, принимая во внимание неравенство (9.44), получаем

$$\bar{Q}_n = \max_{S^{(n)}} I_c(S^{(n)}, \Phi^{\otimes n}) \geq nR(1 - 6\sqrt{\varepsilon}) - \frac{2 \log e}{e},$$

откуда следует, что $R \leq \lim_{n \rightarrow \infty} \frac{1}{n} \bar{Q}_n = \bar{Q}(\Phi)$.

Это завершает доказательство неравенства $Q(\Phi) \leq \bar{Q}(\Phi)$, т. е. слабого обращения теоремы кодирования. Доказательство прямого утверждения будет дано в п. 9.4.4. $\square$

Следующее неравенство об обработке информации полезно для оценки квантовой пропускной способности.

Предложение 9.3.1. Для любых двух каналов Φ_1, Φ_2 выполнено неравенство

$$Q(\Phi_2 \circ \Phi_1) \leq \min\{Q(\Phi_1), Q(\Phi_2)\}. \quad (9.45)$$

В частности, если один из этих каналов имеет нулевую пропускную способность, то это же верно для их композиции.

Доказательство. Чтобы доказать неравенство $Q(\Phi_2 \circ \Phi_1) \leq Q(\Phi_2)$, достаточно заметить, что пропускная способность $Q(\Phi_2 \circ \Phi_1)$ равна точной верхней грани достижимых скоростей для канала Φ_2 при специальном выборе кодирующих каналов, включающих заключительную обработку каналом Φ_1 ; следовательно, эта величина не превосходит $Q(\Phi_2)$. Неравенство $Q(\Phi_2 \circ \Phi_1) \leq Q(\Phi_1)$ доказывается аналогично, путем рассмотрения декодирующих каналов для Φ_1 , включающих в себя предварительную обработку каналом Φ_2 . $\square$

9.3.3. Деградируемые каналы

Прежде всего получим важные соотношения, связывающие когерентную информацию и величину

$$\chi(\{\pi_x\}, \{S_x\}) = H\left(\sum_x \pi_x S_x\right) - \sum_x \pi_x H(S_x),$$

дающую оценку (5.15) для количества классической информации и, как следствие, соотношение между квантовой и классической пропускными способностями канала и его комплементарного.

Рассмотрим канал $\Phi: \mathfrak{I}(\mathcal{H}_A) \rightarrow \mathfrak{I}(\mathcal{H}_B)$, его расширение Стайнспринга с изометрией $V: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$ и комплементарный канал

$$\tilde{\Phi}[S] = \text{Tr}_{\mathcal{H}_B} V S V^*, \quad S \in \mathfrak{I}(\mathcal{H}_A) \quad (9.46)$$

(см. § 6.6).

Пусть $S = \sum_x \pi_x S_x$ — произвольное разложение по чистым состояниям (например, спектральное разложение). Тогда имеет место цепочка равенств

$$\begin{aligned} I_c(S, \Phi) &= H(\Phi[S]) - H(\tilde{\Phi}[S]) = \\ &= \left[H(\Phi[S]) - \sum_x \pi_x H(\Phi[S_x]) \right] - \left[H(\tilde{\Phi}[S]) - \sum_x \pi_x H(\tilde{\Phi}[S_x]) \right] = \end{aligned} \quad (9.47)$$

$$= \chi(\{\pi_x\}, \{\Phi[S_x]\}) - \chi(\{\pi_x\}, \{\tilde{\Phi}[S_x]\}) = \quad (9.48)$$

$$= \sum_x \pi_x [H(\Phi[S_x]; \Phi[S]) - H(\tilde{\Phi}[S_x]; \tilde{\Phi}[S])]. \quad (9.49)$$

Здесь равенство (9.47) следует из того, что состояние $S_{BEx} = V S_x V^*$ является чистым и, значит,

$$H(\Phi[S_x]) = H(S_{Bx}) = H(S_{Ex}) = H(\tilde{\Phi}[S_x])$$

для всех x , а равенство (9.49) следует из тождества (7.18). Взяв в соотношении (9.48) верхнюю и нижнюю грани по всевозможным ансамблям чистых состояний, получаем

$$Q_1(\Phi) \geq C_\chi(\Phi) - C_\chi(\tilde{\Phi}) \geq -Q_1(\tilde{\Phi}), \quad (9.50)$$

где введено обозначение

$$Q_1(\Phi) = \max_S I_c(S, \Phi). \quad (9.51)$$

Применяя неравенство (9.50) к каналу $\Phi^{\otimes n}$, переходя к пределу при $n \rightarrow \infty$ и используя теоремы кодирования, получаем

$$Q(\Phi) \geq C(\Phi) - C(\tilde{\Phi}) \geq -Q(\tilde{\Phi}).$$

Введем важный класс каналов, для которых квантовая пропускная способность дается «однобуквенным» выражением (9.51).

Определение 9.3.2. Канал Φ называется *деградируемым*, если найдется канал T такой, что $\tilde{\Phi} = T \circ \Phi$, и *антидеградируемым*, если найдется канал T' такой, что $\Phi = T' \circ \tilde{\Phi}$.

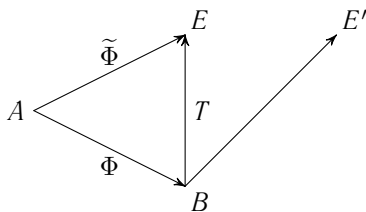


Рис. 9.1. Деградируемый канал

Очевидно, что канал Φ является деградируемым тогда и только тогда, когда канал $\tilde{\Phi}$ антидеградируемый. Из соотношения (9.49), используя свойство монотонности относительной энтропии, получаем, что если Φ — антидеградируемый канал, то

$$I_c(S, \Phi) \leq 0 \quad (9.52)$$

для любого состояния S (соответственно $I_c(S, \Phi) \geq 0$ для деградируемого канала).

Предложение 9.3.2. Если Φ — антидеградируемый канал, то $Q(\Phi) = 0$. Если Φ — деградируемый канал, то

$$Q(\Phi) = Q_1(\Phi) = \max_S I_c(S, \Phi). \quad (9.53)$$

Доказательство. Первое утверждение следует из неравенства (9.52) и теоремы кодирования (9.40).

Пусть Φ — деградируемый канал и $W: \mathcal{H}_B \rightarrow \mathcal{H}_E \otimes \mathcal{H}_{E'}$ — изометрия Стайнспринга для канала $T: \mathfrak{T}(\mathcal{H}_B) \rightarrow \mathfrak{T}(\mathcal{H}_E)$. Тогда $I_c(S, \Phi) = H(B) - H(E) = H(E E') - H(E)$, так что

$$I_c(S, \Phi) = H(E'|E).$$

Для двух деградируемых каналов Φ_1, Φ_2 и произвольного состояния S_{12} в $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ имеем

$$I_c(S_{12}, \Phi_1 \otimes \Phi_2) = H(E'_1 E'_2 | E_1 E_2),$$

следовательно, по свойству субаддитивности условной энтропии

$$I_c(S_{12}, \Phi_1 \otimes \Phi_2) \leq I_c(S_1, \Phi_1) + I_c(S_2, \Phi_2),$$

откуда получаем

$$I_c(S^{(n)}, \Phi^{\otimes n}) = n \max_S I_c(S, \Phi), \quad (9.54)$$

и, таким образом, соотношение (9.53) выполнено. $\square$

Пример 9.3.1. Рассмотрим канал, разрушающий сцепленность:

$$\Phi[S] = \sum_{\alpha=1}^{\tilde{d}} |\varphi_{\alpha}\rangle \langle \psi_{\alpha}| S |\psi_{\alpha}\rangle \langle \varphi_{\alpha}|,$$

где $\{\psi_{\alpha}\}$ — переполненная система в $\mathcal{H}$, а $\{\varphi_{\alpha}\}$ — система единичных векторов в выходном пространстве $\mathcal{H}'$. Комплементарным является диагональный канал

$$\tilde{\Phi}[S] = \sum_{\alpha, \beta=1}^{\tilde{d}} c_{\alpha\beta} |e_{\alpha}\rangle \langle \psi_{\alpha}| S |\psi_{\beta}\rangle \langle e_{\beta}|,$$

где $c_{\alpha\beta} = \langle \varphi_{\beta} | \varphi_{\alpha} \rangle$, а $\{e_{\alpha}\}$ — стандартный базис в $\mathcal{H}_{\tilde{d}}$. Имеем $\Phi = T' \circ \tilde{\Phi}$, где

$$T'[S] = \sum_{\alpha=1}^{\tilde{d}} |\varphi_{\alpha}\rangle \langle e_{\alpha}| S |e_{\alpha}\rangle \langle \varphi_{\alpha}|.$$

Отсюда и из второго утверждения теоремы 9.3.2 вытекает следствие.

Следствие 9.3.1. *Всякий канал Φ , разрушающий сцепленность, является антидеградируемым, и, следовательно, $Q(\Phi) = 0$.*

Пример 9.3.2. Рассмотрим квантовый стирающий канал Φ_p . При $q \geq p$ имеем

$$\Phi_q = T_{(1-q)/(1-p)} \circ \Phi_p,$$

где $T_{\alpha}: \mathfrak{T}(\mathcal{H} \oplus \mathbb{C}) \rightarrow \mathfrak{T}(\mathcal{H} \oplus \mathbb{C})$ — канал, действующий по правилу

$$T_{\alpha} \left[\begin{bmatrix} S & 0 \\ 0 & s \end{bmatrix} \right] = \alpha \begin{bmatrix} S & 0 \\ 0 & s \end{bmatrix} + (1 - \alpha) \begin{bmatrix} 0 & 0 \\ 0 & \text{Tr} S + s \end{bmatrix}.$$

Используя тот факт, что $\tilde{\Phi}_p = \Phi_{1-p}$ (см. задачу 6.6.3), получаем, что канал Φ_p деградируемый при $p \in [0, 1/2]$ и антидеградируемый при $p \in [1/2, 1]$. Применяя предложение 9.3.2, получаем

$$Q(\Phi_p) = \begin{cases} (1 - 2p) \log d, & p \in [0, 1/2]; \\ 0, & p \in [1/2, 1]. \end{cases} \quad (9.55)$$

Здесь первое утверждение вытекает из соотношения (9.53) и того факта, что $H(\Phi_p[S]) = (1 - p)H(S) + h_2(p)$, следовательно,

$$I_c(S, \Phi_p) = H(\Phi_p[S]) - H(\tilde{\Phi}_p[S]) = (1 - p)H(S) - pH(S) = (1 - 2p)H(S).$$

§ 9.4. Секретная классическая пропускная способность и квантовая пропускная способность

9.4.1. Квантовый канал с перехватом

Рассмотрим ситуацию передачи классической информации, в которой имеется три участника: отправитель A , получатель B и перехватчик E . Математическая модель *квантового канала с перехватом* включает три гильбертова пространства $\mathcal{H}_A$, $\mathcal{H}_B$, $\mathcal{H}_E$ и изометрическое отображение $V: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$, при котором входное состояние S_A переходит в состояние $S_{BE} = \Phi_{BE}[S_A] \equiv VS_A V^*$ системы BE с частичными состояниями

$$S_B = \Phi_B[S_A] \equiv \text{Tr}_E VS_A V^*, \quad S_E = \Phi_E[S_A] \equiv \text{Tr}_B VS_A V^*.$$

Заметим, что ранее буква E использовалась для обозначения окружения. Если все окружение доступно перехватчику, то такое обозначение является согласованным. Предположим, что участник A выбирает состояния $\{S_A^x\}$ с вероятностями $\{\pi_x\}$; тогда участники B и E получают соответственно состояния $\{S_B^x\}$ и $\{S_E^x\}$, а верхними границами шенноновской информации для B и E являются величины $\chi(\{\pi_x\}, \{S_B^x\})$ и $\chi(\{\pi_x\}, \{S_E^x\})$. По аналогии с классическим каналом с перехватом (см. § 4.5) «секретность» передачи может быть охарактеризована величиной $\chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\})$. Предполагая, что входные состояния S_A^x являются *чистыми*, и обозначая через $\bar{S}_A = \sum_x \pi_x S_A^x$ среднее состояние входного ансамбля, из формулы (9.48) получаем ключевое соотношение

$$I_c(\bar{S}_A, \Phi_B) = \chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\}), \quad (9.56)$$

которое указывает на важную связь между когерентной информацией и секретной классической пропускной способностью; оно также подсказывает идею доказательства прямой теоремы кодирования для квантовой пропускной способности через рассмотрение канала с перехватом.

Для определения секретной классической пропускной способности рассмотрим блочное кодирование для квантового канала с перехватом. Нашей целью будет передать максимальное количество классической информации от A к B секретным образом, так, чтобы участник E смог получить лишь асимптотически исчезающее количество информации. Код $(\Sigma^{(n)}, M^{(n)})$ длины n и размера N определяется так же, как в определении 8.1.1. Таким образом, код состоит из набора состояний $\Sigma^{(n)} = \{S_{A^{(n)}}^i; i = 1, \dots, N\}$ в $\mathcal{H}_A^{\otimes n}$ вместе с наблюдаемой $M^{(n)} = \{M_j; j = 0, 1, \dots, N\}$ в $\mathcal{H}_B^{\otimes n}$. Наряду с вероятностью ошибки

$P_e(\Sigma^{(n)}, M^{(n)})$, определяемой соотношением (8.1), введем новую величину

$$v_E(\Sigma^{(n)}) = \max_{i, k=1, \dots, N} \|S_{E^{(n)}}^i - S_{E^{(n)}}^k\|_1,$$

характеризующую *изменчивость* состояния системы E , а следовательно, и количество информации, которое доступно перехватчику E . Заметим, что из неравенства треугольника для нормы вытекает, что

$$\|\bar{S}_{E^{(n)}} - S_{E^{(n)}}^i\|_1 \leq v_E(\Sigma^{(n)}) \quad \text{для всех } i,$$

где $\bar{S}_{E^{(n)}} = \frac{1}{N} \sum_{i=1}^N S_{E^{(n)}}^i$. Применяя неравенство (7.22), получаем

$$\begin{aligned} \frac{1}{n} \chi\left(\left\{\frac{1}{N}\right\}, \{S_{E^{(n)}}^i\}\right) &= \frac{1}{nN} \sum_{i=1}^N [H(\bar{S}_{E^{(n)}}) - H(S_{E^{(n)}}^i)] \leq \\ &\leq \log \dim \mathcal{H}_E \cdot v_E(\Sigma^{(n)}) + \frac{1}{n} \eta(v_E(\Sigma^{(n)})) \quad (9.57) \end{aligned}$$

в предположении, что величина $v_E(\Sigma^{(n)})$ достаточно мала. Поэтому если изменчивость мала, то мала и шенноновская взаимная информация между A и E для равновероятных сообщений.

Мы будем называть R *достижимой скоростью* для канала с перехватом, если найдется последовательность кодов $(\Sigma^{(n)}, M^{(n)})$ размера $N = 2^{nR}$ таких, что

$$\lim_{n \rightarrow \infty} P_e(\Sigma^{(n)}, M^{(n)}) = 0$$

и

$$\lim_{n \rightarrow \infty} v_E(\Sigma^{(n)}) = 0. \quad (9.58)$$

Точная верхняя грань множества достижимых скоростей называется *секретной классической пропускной способностью* $C_p(\Phi_{BE})$ канала с перехватом. Согласно соотношению (9.57) из условия (9.58) следует асимптотическое исчезновение взаимной информации между A и E . Можно показать, что на самом деле эти утверждения равносильны, однако условие (9.58) более удобно математически.

Теорема 9.4.1. *Имеет место соотношение*

$$C_p(\Phi_{BE}) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{\pi^{(n)}, \Sigma^{(n)}} [\chi(\{\pi_i^{(n)}\}, \{S_{B^{(n)}}^i\}) - \chi(\{\pi_i^{(n)}\}, \{S_{E^{(n)}}^i\})], \quad (9.59)$$

где максимум берется по всем конечным наборам состояний $\Sigma^{(n)} = \{S_{A^{(n)}}^i\}$ в $\mathcal{H}_A^{\otimes n}$ и распределениям вероятностей $\pi^{(n)} = \{\pi_i^{(n)}\}$ (мы используем обозначения $S_{B^{(n)}}^i = \Phi_B^{\otimes n}[S_{A^{(n)}}^i]$, $S_{E^{(n)}}^i = \Phi_E^{\otimes n}[S_{A^{(n)}}^i]$).

Из соотношений (9.40), (9.56) и (9.59) вытекает важное неравенство между квантовой и классической секретной пропускными способностями:

$$Q(\Phi_B) \leq C_p(\Phi_{BE}).$$

Оно следует из того, что при вычислении $C_p(\Phi_{BE})$ учитываются все ансамбли состояний, а при вычислении $Q(\Phi_B)$ — только ансамбли чистых состояний для A . В общем случае здесь возможно строгое неравенство, поэтому особый интерес представляет следующее утверждение.

Предложение 9.4.1. *Если канал Φ_B деградируемый, то*

$$C_p(\Phi_{BE}) = Q(\Phi_B) = Q_1(\Phi_B). \quad (9.60)$$

Доказательство. Используя равенство (9.48), получаем

$$\begin{aligned} & \chi(\{\pi_i^{(n)}\}, \{S_{B^{(n)}}^i\}) - \chi(\{\pi_i^{(n)}\}, \{S_{E^{(n)}}^i\}) = \\ & = H\left(\sum_i \pi_i^{(n)} S_{B^{(n)}}^i\right) - H\left(\sum_i \pi_i^{(n)} S_{E^{(n)}}^i\right) - \sum_i \pi_i^{(n)} [H(S_{B^{(n)}}^i) - H(S_{E^{(n)}}^i)] = \\ & = I_c\left(\sum_i \pi_i^{(n)} S_{A^{(n)}}^i, \Phi_B^{\otimes n}\right) - \sum_i \pi_i^{(n)} I_c(S_{A^{(n)}}^i, \Phi_B^{\otimes n}) \leq \\ & \leq I_c\left(\sum_i \pi_i^{(n)} S_{A^{(n)}}^i, \Phi_B^{\otimes n}\right), \end{aligned}$$

поскольку канал $\Phi_B^{\otimes n}$, как и Φ_B , деградируем, а значит, $I_c(S_{A^{(n)}}^i, \Phi_B^{\otimes n}) \geq 0$. Следовательно,

$$\max_{\pi^{(n)}, \Sigma^{(n)}} [\chi(\{\pi_i^{(n)}\}, \{S_B^i\}) - \chi(\{\pi_i^{(n)}\}, \{S_{E^{(n)}}^i\})] = \max_{S^{(n)}} I_c(S^{(n)}, \Phi_B^{\otimes n}),$$

а это выражение равно $nQ_1(\Phi_B)$ в силу соотношения (9.54). Подставляя в (9.59), получаем соотношение (9.60). $\square$

9.4.2. Доказательство теоремы о секретной пропускной способности

Сначала докажем неравенство $\leq$ в формуле (9.59), т. е. слабое обращение. Пусть R — достижимая скорость, тогда, используя неравенство (5.29) и границу (5.15), получаем

$$\begin{aligned} \bar{P}_e(\Sigma^{(n)}, M^{(n)}) & \geq 1 - \frac{\chi(\{1/N\}, \{S_{B^{(n)}}^i\})}{nR} - \frac{1}{nR} = \\ & = 1 - \frac{\chi(\{1/N\}, \{S_{B^{(n)}}^i\}) - \chi(\{1/N\}, \{S_{E^{(n)}}^i\})}{nR} - \frac{1 + \chi(\{1/N\}, \{S_{E^{(n)}}^i\})}{nR}. \quad (9.61) \end{aligned}$$

Согласно неравенству (9.57) имеем

$$\chi(\{1/N\}, \{S_{E^{(n)}}^i\}) \leq v_E(\Sigma^{(n)}) [n \log d_E - \log v_E(\Sigma^{(n)})],$$

где $d_E = \dim \mathcal{H}_E$, поэтому последнее слагаемое в правой части неравенства (9.61) стремится к нулю при $n \rightarrow \infty$; ошибка $\bar{P}_e$ также стремится к нулю. Отсюда получаем $0 \geq 1 - \bar{C}_p/R$, где $\bar{C}_p$ — правая часть равенства (9.59), следовательно, $C_p(\Phi_{BE}) \leq \bar{C}_p$.

Для доказательства прямого утверждения достаточно показать, что для произвольного ансамбля $\{\pi_x\}$, $\{S_A^x\}$ и $\delta > 0$ скорость $\chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\}) - \delta$ является достижимой. Тогда достижимость скорости $\bar{C}_p - \delta$ получается путем дополнительной группировки в блоки. Рассмотрим с-q-канал $x \rightarrow S_B^x$ и случайный набор кодовых слов $W^{(n)}$ размера $N = 2^{n[\chi(\{\pi_x\}, \{S_B^x\}) - c\delta]}$ с независимыми словами, имеющими распределение вероятностей

$$P\{\omega = (x_1, \dots, x_n)\} = \pi_{x_1} \cdot \dots \cdot \pi_{x_n}. \quad (9.62)$$

Константа c будет определена ниже. Согласно замечанию после доказательства прямого утверждения квантовой теоремы кодирования в конце § 5.6 для достаточно больших n найдутся наблюдаемые $M^{(n)}$ в системе B такие, что

$$E\bar{P}_e(W^{(n)}, M^{(n)}) \leq 2^{-n\beta}, \quad \beta > 0.$$

Теперь рассмотрим новый случайный код с независимыми словами, равномерно распределенными на множестве $\hat{T}^{n,\delta}$ сильно δ -типичных слов:

$$\tilde{P}(\omega) = \begin{cases} \frac{1}{|\hat{T}^{n,\delta}|}, & \omega \in \hat{T}^{n,\delta}; \\ 0, & \omega \notin \hat{T}^{n,\delta}. \end{cases}$$

Согласно задаче 8.4.3 мы имеем $|\hat{T}^{n,\delta}| \geq 2^{n[H(\pi) - \Delta_n(\delta)]}$, причем

$$\lim_{\delta \rightarrow 0} \lim_{n \rightarrow \infty} \Delta_n(\delta) = 0.$$

Так как $P(\omega) \geq 2^{-n[H(\pi) + c\delta]}$ для $\omega \in \hat{T}^{n,\delta}$, где c — константа, зависящая от $\{\pi_x\}$, мы получаем, что $\tilde{P}(\omega) \leq 2^{n[c\delta + \Delta_n(\delta)]} P(\omega)$ для всех ω , и, следовательно,

$$\tilde{E}\bar{P}_e(W^{(n)}, M^{(n)}) \leq 4^{n[c\delta + \Delta_n(\delta)]} 2^{-n\beta} \leq \varepsilon$$

для достаточно больших n , поскольку оценка (5.46) для $\bar{P}_e(W^{(n)}, M^{(n)})$ включает не более двух независимых слов. Следовательно,

$$\tilde{P}\{\bar{P}_e(W^{(n)}, M^{(n)}) \geq \sqrt{\varepsilon}\} \leq \sqrt{\varepsilon} \quad (9.63)$$

по неравенству Чебышёва.

Пока что была дана лишь некоторая модификация случайного кодирования для передачи классической информации от A к B . Чтобы сделать

код секретным, передатчик A должен пожертвовать $n[\chi(\{\pi_x\}, \{S_E^x\}) + c\delta/2]$ битами информации, дополнительно рандомизуя входные состояния. Положим

$$N_E = 2^{n[\chi(\{\pi_x\}, \{S_E^x\}) + c\delta/2]}, \quad N_B = 2^{n[\chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\}) - 3c\delta/2]},$$

так что $N_E N_B = N$; представим набор кодовых слов $W^{(n)}$ в виде прямоугольной таблицы с N_B строками и N_E столбцами. Тогда

$$W^{(n)} = \{\omega^{mj}; m = 1, \dots, N_B; j = 1, \dots, N_E\},$$

$$M^{(n)} = \{M^{mj}; m = 1, \dots, N_B; j = 1, \dots, N_E\}.$$

Пусть для каждого значения m передатчик A выбирает значение j случайным образом с равными вероятностями, что приводит к входным состояниям

$$m \rightarrow S_{A^{(n)}}^m = \frac{1}{N_E} \sum_{j=1}^{N_E} S_{A^{(n)}}^{\omega^{mj}},$$

преобразуемым в выходные состояния $S_{B^{(n)}}^m$ для B и $S_{E^{(n)}}^m$ для E . (Напомним, что $S_{A^{(n)}}^{\omega} = S_A^{x_1} \otimes \dots \otimes S_A^{x_n}$ для слова $\omega = (x_1, \dots, x_n)$.) Такая рандомизация приводит к тому, что почти вся переданная информация оказывается скрытой для E : для каждого значения m набор кодовых слов

$$\{\omega^{mj}; j = 1, \dots, N_E\}$$

с высокой вероятностью содержит почти максимально возможную информацию от A к E , при условии, что E применяет оптимальное декодирование. Поэтому взаимная информация между наборами кодовых слов с различными значениями m должна быть близка к нулю, так что рандомизация внутри каждого набора уничтожает почти всю информацию, передаваемую от A к E .

Решающим шагом в строгом обосновании этой идеи является применение следующей оценки, основанной на квантовой версии неравенства Бернштейна, которая доказывается в следующем пункте.

Предложение 9.4.2. Пусть $S_{E^{(n)}}^{\omega^{mj}}$, $m = 1, \dots, N_B$, $j = 1, \dots, N_E$, — случайные независимые одинаково распределенные операторы плотности; величины N_B, N_E определены выше. Тогда найдется число $\beta_1 > 0$ такое, что для достаточно больших n выполнено неравенство

$$\tilde{P} \left\{ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} S_{E^{(n)}}^{\omega^{mj}} - \theta \right\|_1 \geq \varepsilon \right\} \leq 2^{-2^{n\beta_1}} \quad (9.64)$$

для $m = 1, \dots, N_B$, где θ — некоторый неслучайный оператор (в действительности можно взять $\theta = \tilde{E}S_{E^{(n)}}^{w^{mj}}$, но нам это не требуется).

Из этой оценки вытекает, что

$$\begin{aligned} \tilde{P}\{\|S_{E^{(n)}}^m - \theta\|_1 < \varepsilon; m = 1, \dots, N_B\} &\geq \\ &\geq 1 - N_B 2^{-2^{n\beta_1}} = 1 - 2^n[\chi(\{\pi_x\}, \{S_B^x\}) + c\delta/2] - 2^{n\beta_1}, \end{aligned}$$

т. е. вероятность может быть сколь угодно близка к 1 для достаточно больших n . Учитывая неравенство (9.63), получаем, что найдется реализация $W^{(n)} = \{w^{mj}\}$ набора кодовых слов, для которых

$$\bar{P}_e(W^{(n)}, M^{(n)}) < \sqrt{\varepsilon}$$

и

$$\|S_{E^{(n)}}^m - S_{E^{(n)}}^l\|_1 < 2\varepsilon, \quad m, l = 1, \dots, N_B. \quad (9.65)$$

Определяя

$$\Sigma^{(n)} = \{S_{A^{(n)}}^m; m = 1, \dots, N_B\}, \quad \tilde{M}^{(n)} = \{\tilde{M}_m; m = 0, 1, \dots, N_B\},$$

где $\tilde{M}_m = \sum_{j=1}^{N_E} M_{mj}$, получаем

$$\bar{P}_e(\Sigma^{(n)}, \tilde{M}^{(n)}) \leq \bar{P}_e(W^{(n)}, M^{(n)}) < \sqrt{\varepsilon}.$$

Рассуждения, аналогичные лемме 4.4.1, показывают, что можно выбрать подкод, для которого максимальная ошибка удовлетворяет оценке $P_e(W^{(n)}, M^{(n)}) < 2\sqrt{\varepsilon}$ при $v_E(\Sigma^{(n)}) < \varepsilon'$, где $\varepsilon' \rightarrow 0$ при $\varepsilon \rightarrow 0$, что и завершает доказательство теоремы. $\square$

Доказательство предложения 9.4.2. Рассуждая как в § 5.6, рассмотрим оператор плотности

$$\bar{S}_\pi = \sum_x \pi_x S_E^x.$$

Для краткости будем использовать обозначения

$$H(\bar{S}_\pi) = H(E), \quad \sum_x \pi_x H(S_E^x) = H(E|A),$$

так что $\chi(\{\pi_x\}, \{S_E^x\}) = H(E) - H(E|A)$.

Обозначим через λ_j собственные значения оператора $\bar{S}_\pi$. Фиксируем малое положительное δ , и пусть $P = \hat{P}^{n, \delta}$ — сильно типичный проектор оператора плотности $\bar{S}_\pi^{\otimes n}$, соответствующий собственным значениям

$\lambda_J = \lambda_{j_1} \cdot \dots \cdot \lambda_{j_n}$, для которых последовательность $J = (j_1, \dots, j_n)$ является сильно типичной, т. е. частоты $N(j|J)$ появления символа j в J удовлетворяют условию

$$\left| \frac{N(j|J)}{n} - \lambda_j \right| < \delta, \quad j = 1, \dots, d_E,$$

и $N(j|J) = 0$, если $\lambda_j = 0$ (см. определение 8.4.1). Обозначим через $\lambda_j(x)$ собственные значения оператора плотности S_E^x . Для кодового слова $w = (x_1, \dots, x_n)$ длины n положим $S_w = S_E^{x_1} \otimes \dots \otimes S_E^{x_n}$ и обозначим через P_w типичный проектор оператора S_w , соответствующий собственным значениям $\lambda_J(w) = \lambda_{j_1}(x_1) \cdot \dots \cdot \lambda_{j_n}(x_n)$, для которых

$$\left| \frac{N(j, x|J, w)}{n} - \frac{N(x|w)}{n} \lambda_j(x) \right| < \delta, \quad j = 1, \dots, d_E,$$

и $N(j, x|J, w) = 0$, если $\lambda_j(x) = 0$. Нам понадобятся следующие свойства, которые являются переформулировкой соответствующих свойств типичных последовательностей.

1. Для $w \in \hat{T}^{n, \delta}$ собственные значения оператора $P_w S_w P_w$ лежат в интервале $(2^{-n[H(E|A)+c\delta]}, 2^{-n[H(E|A)-c\delta]})$, где c — некоторая константа, зависящая от $\{\lambda_j(x)\}$ (для упрощения обозначений мы используем одно и то же обозначение c для всех констант; в действительности мы можем выбрать максимальную из всех констант). В частности, $P_w S_w P_w \leq 2^{-n[H(E|A)-c\delta]} P_w$.

2. Для $\varepsilon_1 > 0$ и достаточно больших n выполняется неравенство $\text{Tr} P_w S_w \geq 1 - \varepsilon_1$. (Это является следствием закона больших чисел для распределения вероятностей, задаваемого собственными значениями оператора S_w .)

Следующее свойство является менее очевидным.

3. Для данных $\varepsilon_1, \delta > 0$ найдется такое $\delta_1 > 0$, что для $w \in \hat{T}^{n, \delta_1}$ и достаточно больших n выполняется неравенство $\text{Tr} P S_w \geq 1 - \varepsilon_1$, где $P = \hat{P}^{n, \delta}$ — сильно типичный проектор оператора $\bar{S}_\pi^{\otimes n}$.

Доказательство. Обозначим $p^{(k)}(j) = \langle e_j | S_E^{x_k} | e_j \rangle$, где $|e_j\rangle$ — собственные векторы оператора $\bar{S}_\pi$, и заметим, что $p^{(k)}(j) = 0$, если $\lambda_j = 0$, так как $\text{supp } S_E^{x_k} \subset \text{supp } \bar{S}_\pi$. Имеем

$$\begin{aligned} \text{Tr} \hat{P}^{n, \delta} S_w &= \sum_{J \in B^{n, \delta}} p^{(1)}(j_1) \cdot \dots \cdot p^{(n)}(j_n) = \\ &= \mathbf{P} \left\{ \left| \frac{N(j|J)}{n} - \lambda_j \right| < \delta, \text{ если } \lambda_j > 0 \right\}, \end{aligned} \quad (9.66)$$

где $\mathbf{P}$ — распределение вероятностей, которое приписывает вероятность $p^{(1)}(j_1) \cdot \dots \cdot p^{(n)}(j_n)$ последовательности $J = (j_1, \dots, j_n)$, $B^{n, \delta}$ — множе-

ство сильно типичных последовательностей. Тот факт, что $\omega \in \hat{T}^{n, \delta_1}$, выражается аналогичными неравенствами

$$\left| \frac{N(x|\omega)}{n} - \pi_x \right| < \delta_1, \quad \text{если } \pi_x > 0,$$

и $N(x|\omega) = 0$, если $\pi_x = 0$, откуда следует, что для $\bar{\lambda}_j = \frac{1}{n} \sum_{k=1}^n p^{(k)}(j)$ выполняется неравенство

$$\begin{aligned} |\bar{\lambda}_j - \lambda_j| &= \left| \langle e_j | \left[\frac{1}{n} \sum_{k=1}^n S_E^{x_k} - \bar{S}_\pi \right] | e_j \rangle \right| = \\ &= \left| \sum_x \left[\frac{N(x|\omega)}{n} - \pi_x \right] \langle e_j | S_E^x | e_j \rangle \right| < \delta_1 K, \end{aligned}$$

где K — количество различных символов x . Поэтому, выбирая $\delta_1 = \delta/2K$, получаем

$$\begin{aligned} \mathbf{P} \left\{ \left| \frac{N(j|J)}{n} - \lambda_j \right| < \delta; \text{ если } \lambda_j > 0 \right\} &\geq \\ &\geq \mathbf{P} \left\{ \left| \frac{N(j|J)}{n} - \bar{\lambda}_j \right| < \frac{\delta}{2}; \lambda_j > 0 \text{ для всех } j \right\} \geq \\ &\geq 1 - \sum_{j: \lambda_j > 0} \mathbf{P} \left\{ \left| \frac{N(j|J)}{n} - \bar{\lambda}_j \right| \geq \frac{\delta}{2} \right\}. \end{aligned}$$

Для распределения вероятностей $\mathbf{P}$ случайная величина $N(j|J)$ имеет среднее $\sum_{k=1}^n p^{(k)}(j) = n\bar{\lambda}_j$ и дисперсию $\sum_{k=1}^n p^{(k)}(j)(1 - p^{(k)}(j)) \leq n/4$. Применяя неравенство Чебышёва и используя соотношение (9.66), получаем свойство 3. $\square$

Далее нам понадобится следующий результат.

Лемма 9.4.1. Для любого положительного оператора X и проектора P выполняется неравенство

$$\|X - PXP\|_1 \leq 3\sqrt{\text{Tr} X \text{Tr}(I - P)X}.$$

Доказательство. Согласно неравенству треугольника и свойствам следовой нормы имеем

$$\|X - PXP\|_1 \leq \|(I - P)X(I - P)\|_1 + 2\|PX(I - P)\|_1 \leq 3\|X(I - P)\|_1.$$

Пусть U — унитарный оператор такой, что $\|X(I - P)\|_1 = \text{Tr} X(I - P)U$. По неравенству Коши—Шварца для следа (при $S = I/d$ в формуле (2.25)) имеем

$$[\text{Tr} \sqrt{X} \sqrt{X}(I - P)U]^2 \leq \text{Tr} X \text{Tr} U^*(I - P)X(I - P)U = \text{Tr} X \text{Tr}(I - P)X,$$

откуда и следует утверждение леммы. $\square$

Для упрощения обозначений в неравенстве (9.64) положим $S_{E(n)}^{\omega^{m_j}} = S_{\omega^j}$, где кодовые слова ω^j , $j = 1, \dots, N_E$, являются независимыми и равномерно распределенными на множестве $\hat{T}^{n, \delta_1}$. Мы выведем соотношение (9.64), применяя операторное неравенство типа Бернштейна (9.73), доказываемое в следующем пункте, к случайным операторам

$$X_j = 2^{n[H(E|A) - \delta]} \Pi P P_{\omega^j} S_{\omega^j} P_{\omega^j} \Pi,$$

где Π — проектор на собственное подпространство оператора

$$\theta' = \tilde{E} P P_{\omega^j} S_{\omega^j} P_{\omega^j} P,$$

соответствующий собственным значениям, не меньшим $2^{-n[H(E) + 3c\delta/2]}$. По построению $0 \leq X_j \leq I$,

$$M = \tilde{E} X_j = 2^{n[H(E|A) - c\delta]} \tilde{E} (\Pi P P_{\omega^j} S_{\omega^j} P_{\omega^j} \Pi) = 2^{n[H(E|A) - c\delta]} \Pi \theta' \Pi$$

и $\mu = 2^{n[H(E|A) - H(E) - 5c\delta/2]} = 2^{-n[\chi(\{\pi_x\}, \{S_E^x\}) + 5c\delta/2]}$, так что $N_E \mu = 2^{-2nc\delta}$ и из неравенства (9.73) следует, что

$$\begin{aligned} \tilde{P} \left\{ \omega : \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} X_j(\omega) - M \right\|_1 \geq \varepsilon_2 2^{n[H(E|A) - c\delta]} \right\} &\leq \\ &\leq 2d_E^n \exp\left(-2^{-2nc\delta} \frac{\varepsilon_2^2}{4}\right) \leq 2^{-2^{-n\beta_1}} \end{aligned} \quad (9.67)$$

для некоторого $\beta_1 > 0$ и достаточно большого n . Здесь мы использовали тот факт, что $\text{Tr } M \leq 2^{n[H(E|A) - c\delta]}$. Теперь получим неравенство (9.64) из оценки (9.67).

Вводя обозначение $\theta = \Pi \theta' \Pi$, получаем

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} S_{\omega^j} - \theta \right\|_1 \leq \frac{1}{N_E} \sum_{j=1}^{N_E} \left\| S_{\omega^j} - P S'_{\omega^j} P \right\|_1 + \quad (9.68)$$

$$+ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} P S'_{\omega^j} P - \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{\omega^j} P \Pi \right\|_1 + \quad (9.69)$$

$$+ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{\omega^j} P \Pi - \theta \right\|_1. \quad (9.70)$$

Из оценки (9.67) вытекает, что

$$\tilde{P} \left\{ \left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{\omega^j} P \Pi - \theta \right\|_1 \leq \varepsilon_2 \right\} > 1 - 2^{-2^{-n\beta_1}}.$$

Неравенство

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{\omega^j} P \Pi - \theta \right\|_1 \leq \varepsilon_2 \quad (9.71)$$

дает оценку слагаемого (9.70).

Для слагаемого (9.68) используем неравенство треугольника:

$$\|S_{\omega^j} - P S'_{\omega^j} P\|_1 \leq \|S_{\omega^j} - P_{\omega^j} S'_{\omega^j} P_{\omega^j}\|_1 + \|S'_{\omega^j} - P S'_{\omega^j} P\|_1.$$

Первое слагаемое в правой части можно сделать малым для достаточно больших n (согласно свойству 2 и лемме 9.4.1). Далее отметим, что в силу свойств 2 и 3 для $\omega^j \in T^{n, \delta_1}$ имеют место неравенства

$$\mathrm{Tr} P S'_{\omega^j} = \mathrm{Tr} S'_{\omega^j} - \mathrm{Tr}(I - P) S'_{\omega^j} \geq \mathrm{Tr} P_{\omega^j} S_{\omega^j} - \mathrm{Tr}(I - P) S_{\omega^j} \geq 1 - 2\varepsilon_1. \quad (9.72)$$

Применяя лемму, мы можем сделать второе слагаемое в правой части малым для достаточно больших n .

Слагаемое (9.69) имеет вид $\|S - \Pi S \Pi\|_1$, поэтому для доказательства его близости к нулю согласно лемме 9.4.1 достаточно доказать, что величина

$$\mathrm{Tr} \Pi S = \mathrm{Tr} \frac{1}{N_E} \sum_{j=1}^{N_E} \Pi P S'_{\omega^j} P \Pi$$

близка к 1. Но в соответствии с неравенством (9.71) это выражение не меньше, чем $\mathrm{Tr} \theta - \varepsilon_2 = \mathrm{Tr} \Pi \theta' - \varepsilon_2$. Теперь заметим, что

$$\mathrm{Tr} \Pi \theta' = \mathrm{Tr} \theta' - \mathrm{Tr}(I - \Pi) \theta' \geq \mathrm{Tr} \theta' - 2^{-nc\delta/2},$$

так как $\mathrm{Tr}(I - \Pi) \theta'$ является суммой собственных значений θ' , которые не превосходят $2^{-n[H(E)+3c\delta/2]}$, тогда как общее количество положительных собственных значений не превосходит $\dim \mathrm{supp} \theta' \leq \dim \mathrm{supp} P = 2^{n[H(E)+c\delta]}$.

Остается доказать, что $\mathrm{Tr} \theta'$ близко к 1. Мы знаем, что $\theta' = \tilde{E} P S'_{\omega^j} P$ и $\mathrm{Tr} \theta' = \tilde{E} \mathrm{Tr} P S'_{\omega^j} \geq 1 - 2\varepsilon_1$ в силу неравенств (9.72). Это означает, что при заданном ε можно выбрать $\varepsilon_1, \varepsilon_2$ такими, что неравенство (9.64) будет выполнено для достаточно большого n . $\square$

9.4.3. Большие отклонения для случайных операторов

Теорема 9.4.2 (операторное неравенство типа Бернштейна). Пусть $X_1(\omega), \dots, X_N(\omega)$ — независимые одинаково распределенные операторнозначные случайные величины в $\mathcal{H}$, $\dim \mathcal{H} = d$, такие, что $0 \leq X_i(\omega) \leq I$, $M = \mathbb{E} X_i \geq \mu I$, где $0 < \mu \leq \frac{1}{2}$. Тогда для $0 \leq \varepsilon \leq 1$ выполняется неравенство

$$\mathbb{P} \left\{ \omega : \left\| \frac{1}{N} \sum_{j=1}^N X_j(\omega) - M \right\|_1 \geq \varepsilon \mathrm{Tr} M \right\} \leq 2d \exp \left(-\frac{N\mu\varepsilon^2}{4} \right). \quad (9.73)$$

Доказательство. Доказательство состоит из нескольких шагов. Во-первых, докажем операторное обобщение неравенства Маркова: пусть X — эрмитова операторнозначная случайная величина, $t > 0$, тогда

$$P\{\omega: X(\omega) \not\leq 0\} \leq \text{Tr } E \exp tX,$$

где $\{\omega: X(\omega) \not\leq 0\} = \{\omega: X(\omega) \leq 0\}^c$. Действительно,

$$\begin{aligned} P\{\omega: X(\omega) \not\leq 0\} &= P\{\omega: \exp tX(\omega) \not\leq I\} \leq \\ &\leq E 1_{\{\exp tX \not\leq I\}} \text{Tr } \exp tX \leq \text{Tr } E \exp tX, \end{aligned}$$

где первое неравенство вытекает из того, что если $0 \leq y \not\leq I$, то $1 \leq \text{Tr } y$.

Во-вторых, обозначая $X(\omega) = \sum_{i=1}^N X_i(\omega)$, где X_i — независимые одинаково распределенные эрмитово операторнозначные случайные величины, получаем

$$\begin{aligned} P\left\{\omega: \sum_{i=1}^N X_i(\omega) \not\leq 0\right\} &\leq \text{Tr } E \exp\left(t \sum_{i=1}^N X_i\right) \leq \\ &\leq E \text{Tr } \exp\left(t \sum_{i=1}^{N-1} X_i\right) \exp tX_N = \text{Tr } E \exp\left(t \sum_{i=1}^{N-1} X_i\right) E \exp tX_N, \end{aligned}$$

где использовано неравенство Голдена—Томпсона

$$\text{Tr } \exp(A + B) \leq \text{Tr } \exp A \exp B.$$

Согласно неравенству (1.18) это выражение не превосходит

$$\text{Tr } E \exp\left(t \sum_{i=1}^{N-1} X_i\right) \|E \exp tX_N\|.$$

Применяя эту оценку последовательно, получаем

$$P\left\{\omega: \sum_{i=1}^N X_i(\omega) \not\leq 0\right\} \leq d \|E \exp tX_i\|^N. \quad (9.74)$$

В-третьих, пусть $X_1(\omega), \dots, X_N(\omega)$ — независимые операторнозначные случайные величины такие, что $0 \leq X_i(\omega) \leq I$, $E X_i = \mu I$ и $0 \leq \mu \leq a \leq 1$, тогда

$$P\left\{\omega: \frac{1}{N} \sum_{i=1}^N X_i(\omega) \not\leq aI\right\} \leq d \exp(-Nh(a; \mu)), \quad (9.75)$$

где $h(a; \mu) = a \ln \frac{a}{\mu} + (1-a) \ln \frac{1-a}{1-\mu}$. Действительно, используя неравенство (9.74) для величин $X_i(\omega) - aI$, получаем

$$\mathbf{P} \left\{ \omega: \frac{1}{N} \sum_{i=1}^N X_i(\omega) \not\leq aI \right\} \leq d \| \mathbf{E} \exp t X_i \|^N \exp(-atN).$$

Однако $\exp tx \leq 1 + x(\exp t - 1)$ для $x \in [0, 1]$, следовательно, $\exp t X_i \leq I + X_i(\exp t - 1)$, и правая часть не превосходит

$$d[1 + \mu(\exp t - 1)]^N \exp(-atN).$$

Полагая $\exp t = \frac{a}{\mu} \frac{1-\mu}{1-a} \geq 1$, получаем величину в правой части неравенства (9.75). Аналогично для $0 \leq a \leq \mu \leq 1$ получаем

$$\mathbf{P} \left\{ \omega: \frac{1}{N} \sum_{i=1}^N X_i(\omega) \not\geq aI \right\} \leq d \exp(-Nh(a; \mu)). \quad (9.76)$$

Заметим, что

$$h(\mu; \mu) = 0, \quad \frac{\partial}{\partial a} h(a; \mu)|_{\mu=a} = 0, \quad \frac{\partial^2}{\partial^2 a} h(a; \mu) = \frac{1}{a(1-a)}.$$

Отсюда следует, что

$$\frac{\partial^2}{\partial^2 \varepsilon} h(\mu(1 \pm \varepsilon); \mu) = \frac{\mu}{(1 \pm \varepsilon)(1 - \mu(1 \pm \varepsilon))} \geq \frac{\mu}{2},$$

если $\mu \leq \frac{1}{2}$, $|\varepsilon| \leq 1$, и, таким образом,

$$h(\mu(1 \pm \varepsilon); \mu) \geq \frac{\mu \varepsilon^2}{4}. \quad (9.77)$$

Наконец, пусть $X_i(\omega)$ удовлетворяют условиям теоремы 9.4.2. Рассмотрим операторные случайные величины $Y_i(\omega) = \mu M^{-1/2} X_i(\omega) M^{-1/2}$, удовлетворяющие условиям $0 \leq Y_i(\omega) \leq I$ и $\mathbf{E} Y_i = \mu I$. Имеем

$$\begin{aligned} & \left\{ \omega: \left\| \frac{1}{N} \sum_{i=1}^N X_i(\omega) - M \right\|_1 < \varepsilon \operatorname{Tr} M \right\} \supseteq \\ & \supseteq \left\{ \omega: (1 - \varepsilon)M \leq \frac{1}{N} \sum_{i=1}^N X_i(\omega) \leq (1 + \varepsilon)M \right\} = \\ & = \left\{ \omega: (1 - \varepsilon)\mu \leq \frac{1}{N} \sum_{i=1}^N Y_i(\omega) \leq (1 + \varepsilon)\mu \right\} = \\ & = \left\{ \omega: (1 - \varepsilon)\mu \leq \frac{1}{N} \sum_{i=1}^N Y_i(\omega) \right\} \cap \left\{ \omega: \frac{1}{N} \sum_{i=1}^N Y_i(\omega) \leq (1 + \varepsilon)\mu \right\}. \end{aligned}$$

Переходя к дополнениям и применяя оценки (9.75), (9.76) вместе с (9.77), получаем неравенство (9.73). $\square$

9.4.4. Прямая теорема кодирования для квантовой пропускной способности

Доказательство неравенства $Q(\Phi) \geq \bar{Q}(\Phi)$ будет основано на «когерентной» версии доказательства для классической секретной пропускной способности, т. е. на версии, использующей то же случайное кодирование, однако с заменой смесей состояний их суперпозициями. Достаточно доказать, что для данного входного состояния S величина $R = I_c(S, \Phi) - \delta$ является достижимой скоростью; достижимость величины $\bar{Q}(\Phi) - \delta$ тогда доказывается применением тех же рассуждений к каналу $\Phi^{\otimes n}$ и последующим переходом к пределу при $n \rightarrow \infty$. В этом пункте мы покажем, как следует строить кодирующие и декодирующие каналы, чтобы выполнялось условие

$$F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) \rightarrow 1, \quad (9.78)$$

где $\bar{S}^{(n)}$ — хаотическое состояние в $\mathcal{H}^{(n)}$, $d_n = \dim \mathcal{H}^{(n)} = 2^{nR}$. Применяя рассуждения, следующие за определением 9.3.1, получаем, что скорость R является достижимой для асимптотически безошибочной передачи квантовой информации.

Для канала Φ рассмотрим представление Стайнспринга (6.8) (теорема 6.2.1), а именно

$$\Phi[S] = \text{Tr}_E V S V^*,$$

где V — изометричное отображение входного пространства $\mathcal{H}_A$ в тензорное произведение $\mathcal{H}_B \otimes \mathcal{H}_E$ выходного пространства и пространства окружения.

Рассмотрим спектральное разложение $S = \sum_x \pi_x S_A^x$, где $S_A^x = |\varphi_x\rangle_A \langle \varphi_x|$ и $\{|\varphi_x\rangle_A\}$ — ортонормированный базис. Пусть $|\varphi'_x\rangle_{BE} = V|\varphi_x\rangle_A$ — векторы выходных состояний составной системы BE . Тогда состояния систем B и E равны соответственно $S_B^x = \text{Tr}_E |\varphi'_x\rangle_{BE} \langle \varphi'_x|$ и $S_E^x = \text{Tr}_B |\varphi'_x\rangle_{BE} \langle \varphi'_x|$. Напомним, что согласно соотношению (9.56) мы имеем

$$I_c(S, \Phi) = \chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\}). \quad (9.79)$$

Нашей целью является построение последовательности пространств $\mathcal{H}^{(n)}$ таких, что $\dim \mathcal{H}^{(n)} = 2^{nR}$, $R = I_c(S, \Phi) - \delta$, а также соответствующих кодирований и декодирований, для которых выполняется условие (9.78).

Рассмотрим блочный канал $\Phi^{\otimes n}$ и набор кодовых слов

$$W^{(n)} = \{\omega^{mj}; m = 1, \dots, N_B; j = 1, \dots, N_E\},$$

используемый в конструкции секретного кода, с соответствующим разложением единицы $M^{(n)} = \{M_{mj}\}$ в $\mathcal{H}_B^{\otimes n}$ такие, что

$$P_e(W^{(n)}, M^{(n)}) \equiv \max_{mj} (1 - \text{Tr} S_{B^{(n)}}^{mj} M_{mj}) < \varepsilon, \quad (9.80)$$

где $S_{B^{(n)}}^{mj} = S_B^{x_1} \otimes \dots \otimes S_B^{x_n}$, если $w^{mj} = (x_1, \dots, x_n)$,

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} S_{E^{(n)}}^{mj} - \theta \right\|_1 < \sqrt{\varepsilon}, \quad m = 1, \dots, N_B. \quad (9.81)$$

Введем пространство $\mathcal{H}^{(n)}$ с ортонормированным базисом $\{|m\rangle; m = 1, \dots, N_B\}$, где

$$N_B = 2^n [\chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_B^x\}) - \delta] = 2^n [I_c(S, \Phi) - \delta],$$

и зададим кодирующий канал $\mathcal{E}^{(n)}$ следующим изометрическим отображением $\mathcal{H}^{(n)}$ в $\mathcal{H}_A^{\otimes n}$:

$$|m\rangle \rightarrow \frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\varphi_{mj}\rangle_A,$$

где $|\varphi_{mj}\rangle_A = |\varphi_{x_1}\rangle_A \otimes \dots \otimes |\varphi_{x_n}\rangle_A$, если $w^{mj} = (x_1, \dots, x_n)$, и $\{\alpha_{mj}\} = \alpha$ — набор фаз, которые будут выбраны позднее. Изометричность этого отображения вытекает из того, что $\{|\varphi_{mj}\rangle_A\}$ — ортонормированная система, потому что она построена из ортонормированных векторов $|\varphi_x\rangle_A$.

Это и есть так называемая когерентная версия секретного кода для классической информации. Действие кодирующего канала на вторые компоненты максимально сцепленного вектора (9.42) дает вектор

$$\frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes \left[\frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\varphi_{mj}\rangle_A \right].$$

Кодирующее отображение с последующим действием канала $\Phi^{\otimes n}$ описывается формулой

$$|m\rangle \rightarrow \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes \left[\frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\varphi'_{mj}\rangle_{BE} \right],$$

где векторы $|\varphi'_{mj}\rangle_{BE} = V |\varphi_{mj}\rangle_A$ вновь образуют ортонормированную систему. Заметим, что $S_{B^{(n)}}^{mj} = \text{Tr}_E |\varphi'_{mj}\rangle_{BE} \langle \varphi'_{mj}|$, $S_{E^{(n)}}^{mj} = \text{Tr}_B |\varphi'_{mj}\rangle_{BE} \langle \varphi'_{mj}|$, где для упрощения записи мы обозначаем через Tr_E частичный след по пространству $\mathcal{H}_E^{\otimes n}$ и т.д.

Для построения декодирующего отображения $\mathcal{D}^{(n)}$ мы сначала используем наблюдаемую $M^{(n)} = \{M_{mj}\}$, которая дает значения mj с асимптотически исчезающей ошибкой. Согласно описанию процесса измерения, приводящему к соотношению (6.34), мы имеем вспомогательную систему $\mathcal{H}_0^{(n)} = \mathcal{H}^{(n)} \otimes \mathcal{H}_1^{(n)}$ с базисом $\{|m\rangle \otimes |j\rangle_1\}$, единичный вектор $|\psi_0\rangle \in \mathcal{H}_0^{(n)}$ и унитарный оператор U в $\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_0^{(n)}$ такие, что

$$M_{mj} = \text{Tr}_0(I_{B^{(n)}} \otimes |\psi_0\rangle\langle\psi_0|)U^*(I_{B^{(n)}} \otimes |mj\rangle_0\langle mj|)U,$$

где используется обозначение $|mj\rangle_0 = |m\rangle \otimes |j\rangle_1$. Определяя

$$|\psi_{mj}\rangle_{BE0} = (I_{E^{(n)}} \otimes U)(|\varphi'_{mj}\rangle_{BE} \otimes |\psi_0\rangle),$$

получаем следующий вектор состояния системы $\mathcal{H}^{(n)} \otimes \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E^{\otimes n} \otimes \mathcal{H}_0^{(n)}$:

$$|\Upsilon(\alpha)\rangle = \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes \left[\frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\psi_{mj}\rangle_{BE0} \right]$$

как результат действия на максимально сцепленный вектор композиции кодирующего канала, блочного канала и, наконец, измерения. Здесь $\{|\psi_{mj}\rangle_{BE0}\}$ вновь является ортонормированной системой. Соотношение (9.80) означает, что проекции векторов этой системы на $\mathcal{H}_0^{(n)}$ близки к $\{|mj\rangle_0\}$, а именно

$${}_0\langle mj|(\text{Tr}_{BE} |\psi_{mj}\rangle_{BE0}\langle\psi_{mj}|)|mj\rangle_0 > 1 - \varepsilon \quad \text{для всех } mj.$$

Из следующей леммы вытекает, что найдутся единичные векторы $|\chi_{mj}\rangle_{BE} \in \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E^{\otimes n}$ такие, что для $|\tilde{\psi}_{mj}\rangle_{BE0} = |\chi_{mj}\rangle_{BE} \otimes |mj\rangle_0$ выполняется неравенство

$$|{}_{BE0}\langle\psi_{mj}|\tilde{\psi}_{mj}\rangle_{BE0}|^2 > 1 - \varepsilon. \quad (9.82)$$

Лемма 9.4.2. Пусть $|\varphi\rangle_0 \in \mathcal{H}_0$, $|\psi\rangle \in \mathcal{H}_0 \otimes \mathcal{H}$ — единичные векторы, тогда

$${}_0\langle\varphi|(\text{Tr}_{\mathcal{H}} |\psi\rangle\langle\psi|)|\varphi\rangle_0 = \max_{\chi} |\langle\psi|(|\varphi\rangle_0 \otimes |\chi\rangle)|^2, \quad (9.83)$$

где максимум берется по всем единичным векторам $|\chi\rangle \in \mathcal{H}$.

Доказательство. Фиксируя ортонормированный базис $\{|e_j\rangle\}$ в $\mathcal{H}$, получаем $|\chi\rangle = \sum_j c_j |e_j\rangle$, где $\sum_j |c_j|^2 = 1$, и

$$|\langle\psi|(|\varphi\rangle_0 \otimes |\chi\rangle)|^2 = \left| \sum_j c_j \langle\psi|(|\varphi\rangle_0 \otimes |e_j\rangle) \right|^2.$$

Максимизируя по c_j , получаем равенство (9.83). □

Заметим, что $\{|\tilde{\psi}_{mj}\rangle_{BE0}\}$ также является ортонормированной системой, аппроксимирующей систему $\{|\psi_{mj}\rangle_{BE0}\}$ в смысле (9.82). Определяя вектор

$$|\Gamma(\alpha)\rangle = \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes \left[\frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i\alpha_{mj}} |\tilde{\psi}_{mj}\rangle_{BE0} \right],$$

имеем

$$\int \dots \int \langle \Upsilon(\alpha) | \Gamma(\alpha + \alpha') \rangle d\mu(\alpha) = \frac{1}{N_B N_E} \sum_{m=1}^{N_B} \sum_{j=1}^{N_E} e^{i\alpha'_{mj}} {}_{BE0}\langle \psi_{mj} | \tilde{\psi}_{mj} \rangle_{BE0},$$

где $d\mu(\alpha)$ — равномерное распределение. Всегда можно выбрать набор фаз $\alpha' = \{\alpha'_{mj}\}$ таким образом, что правая часть будет равна

$$\frac{1}{N_B N_E} \sum_{m=1}^{N_B} \sum_{j=1}^{N_E} |{}_{BE0}\langle \psi_{mj} | \tilde{\psi}_{mj} \rangle_{BE0}| > \sqrt{1 - \varepsilon}$$

согласно неравенству (9.82). Следовательно, найдется такое α , что $\text{Re}\langle \Upsilon(\alpha) | \Gamma(\alpha + \alpha') \rangle > \sqrt{1 - \varepsilon}$. Вводя дополнительную общую фазу в α'_{mj} , всегда можно сделать скалярное произведение положительным, так что

$$\langle \Upsilon(\alpha) | \Gamma(\alpha + \alpha') \rangle > \sqrt{1 - \varepsilon}. \quad (9.84)$$

В декодирующий канал следует добавить еще одно преобразование, которое приведет систему E в состояние, почти не зависящее от m . Чтобы добиться этого, заметим, что из неравенства (9.82) и соотношения (9.17) следует, что

$$\| |\psi_{mj}\rangle_{BE0} \langle \psi_{mj}| - |\tilde{\psi}_{mj}\rangle_{BE0} \langle \tilde{\psi}_{mj}| \|_1 < 2\sqrt{\varepsilon}. \quad (9.85)$$

Теперь заметим, что $S_{E^{(n)}}^{mj} = \text{Tr}_{B0} |\psi_{mj}\rangle_{BE0} \langle \psi_{mj}|$, и введем обозначение

$$\tilde{S}_{E^{(n)}}^{mj} = \text{Tr}_{B0} |\tilde{\psi}_{mj}\rangle_{BE0} \langle \tilde{\psi}_{mj}| = \text{Tr}_B |\chi_{mj}\rangle_{BE} \langle \chi_{mj}|.$$

Тогда из неравенства (9.85) и задачи 9.3.1 получаем

$$\| S_{E^{(n)}}^{mj} - \tilde{S}_{E^{(n)}}^{mj} \|_1 < 2\sqrt{\varepsilon}, \quad (9.86)$$

что в сочетании с (9.81) приводит к оценке

$$\left\| \frac{1}{N_E} \sum_{j=1}^{N_E} \tilde{S}_{E^{(n)}}^{mj} - \theta \right\|_1 < O(\sqrt{\varepsilon}), \quad m = 1, \dots, N_B. \quad (9.87)$$

Рассмотрим векторы

$$|\varphi_m\rangle_{BE1} = \frac{1}{\sqrt{N_E}} \sum_{j=1}^{N_E} e^{i(\alpha_{mj} + \alpha'_{mj})} |\chi_{mj}\rangle_{BE} \otimes |j\rangle_1,$$

являющиеся очищениями состояний $\frac{1}{N_E} \sum_{j=1}^{N_E} \tilde{S}_{E^{(n)}}^{mj}$. Пусть $|\varphi_\theta\rangle \in \mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_E^{\otimes n} \otimes \mathcal{H}_1^{(n)}$ — очищение состояния θ , тогда из неравенства (9.87) следует, что найдутся унитарные операторы W_m в $\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_1^{(n)}$ такие, что

$$|{}_{BE1}\langle\varphi_\theta|(I_{\mathcal{H}_E^{\otimes n}} \otimes W_m)\varphi_m\rangle_{BE1}| > 1 - O(\varepsilon) \quad \text{для всех } m. \quad (9.88)$$

Это вытекает из неравенства (9.33): если два состояния близки в следовой норме, то найдутся очищения этих состояний, для которых точность воспроизведения близка к 1.

Определяя «контролируемый унитарный оператор»

$$W = \sum_{m=1}^{N_B} e^{i\beta_m} W_m \otimes |m\rangle\langle m|$$

в $\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_0^{(n)}$, где β_m — фазы, которые будут подобраны ниже, получаем

$$(I_{\mathcal{H}_E^{\otimes n}} \otimes W)(|\varphi_m\rangle_{BE1} \otimes |m\rangle) = e^{i\beta_m} (I_{\mathcal{H}_E^{\otimes n}} \otimes W_m)|\varphi_m\rangle_{BE1} \otimes |m\rangle,$$

следовательно,

$$\begin{aligned} (I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W)|\Gamma(\alpha + \alpha')\rangle &= \\ &= \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes |m\rangle \otimes e^{i\beta_m} (I_{\mathcal{H}_E^{\otimes n}} \otimes W_m)|\varphi_m\rangle_{BE1}. \end{aligned}$$

Пусть $|\Omega^{(n)}\rangle = \frac{1}{\sqrt{N_B}} \sum_{m=1}^{N_B} |m\rangle \otimes |m\rangle$ — максимально сцепленный вектор в $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$. Тогда

$$\begin{aligned} (\langle\Omega^{(n)}| \otimes \langle\varphi_\theta|) (I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W) |\Gamma(\alpha + \alpha')\rangle &= \\ &= \frac{1}{N_B} \sum_{m=1}^{N_B} e^{i\beta_m} \langle\varphi_\theta| (I_{\mathcal{H}_E^{\otimes n}} \otimes W_m) |\varphi_m\rangle_{BE1}, \end{aligned}$$

а это выражение может быть сделано равным

$$\frac{1}{N_B} \sum_{m=1}^{N_B} |\langle\varphi_\theta| (I_{\mathcal{H}_E^{\otimes n}} \otimes W_m) |\varphi_m\rangle_{BE1}|$$

при соответствующем выборе фаз β_m . Последнее выражение больше, чем $1 - O(\varepsilon)$, согласно оценке (9.88). Сравнивая это с оценкой (9.84), из неравенства треугольника (9.31) получаем

$$(\langle \Omega^{(n)} | \otimes \langle \varphi_\theta |) (I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W) | \Upsilon(\alpha) \rangle > 1 - O(\varepsilon).$$

Вводя оператор плотности

$$S' = \text{Tr}_{BE1} (I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W) | \Upsilon(\alpha) \rangle \langle \Upsilon(\alpha) | (I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W)$$

в $\mathcal{H}^{(n)} \otimes \mathcal{H}^{(n)}$, получаем

$$\begin{aligned} F(|\Omega^{(n)}\rangle\langle\Omega^{(n)}|, S') &\equiv \langle\Omega^{(n)}|S'|\Omega^{(n)}\rangle \geq \\ &\geq |(\langle\Omega^{(n)}| \otimes \langle\varphi_\theta|) (I_{\mathcal{H}^{(n)}} \otimes I_{\mathcal{H}_E^{\otimes n}} \otimes W) | \Upsilon(\alpha) \rangle|^2 > 1 - O(\varepsilon). \end{aligned} \quad (9.89)$$

С другой стороны,

$$S' = (\text{Id}_{\mathcal{H}^{(n)}} \otimes \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) [|\Omega^{(n)}\rangle\langle\Omega^{(n)}|],$$

где декодирующий канал $\mathcal{D}^{(n)}$ определяется как

$$\mathcal{D}^{(n)}[S_{B(n)}] = \text{Tr}_{B1} WU(S_{B(n)} \otimes |\psi_0\rangle\langle\psi_0|)U^*W^*$$

(напомним, что $|\psi_0\rangle \in \mathcal{H}_0^{(n)} = \mathcal{H}^{(n)} \otimes \mathcal{H}_1^{(n)}$). Тогда неравенство (9.89) равносильно неравенству

$$F_e(\bar{S}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \circ \mathcal{E}^{(n)}) > 1 - O(\varepsilon),$$

и утверждение (9.78) доказано. $\square$

§ 9.5. Комментарии

1. Примеры квантовых кодов, исправляющих ошибки, были построены независимо в работах Шора [66] и Стина [148]. Многие авторы внесли вклад в последующее развитие теории, фрагменты которой представлены в этой главе, см. обзор в книге Нильсена и Чанга [22]. Необходимые и достаточные условия исправления ошибок в теореме 9.1.1 были предложены Книллом и Лафламмом; см. [115]. Проверку утверждения задачи 9.1.1 см. в книге [22, п. 10.2].

Возможность исправления ошибок является принципиальной для проблемы создания квантового компьютера, см. книгу К. А. Валиева и А. А. Кокина [2]. Была предложена архитектура квантового компьютера, исправляющего ошибки не только в квантовой памяти, но и в самой схеме, исправляющей ошибки, при условии, что вероятность ошибки не превосходит некоторого порогового значения.

По поводу квантовых вычислений, устойчивых к ошибкам, см. А. Ю. Китаев [11], и Стин [148].

На роль когерентной информации в точном исправлении ошибок указано Барнумом, Нильсеном и Шумахером; см. [54].

2. Соотношения между мерами точности исследовались Барнумом, Нильсеном и Шумахером (см. [54]), а также Вернером и Кречманом (см. [117]). Точность воспроизведения для произвольных состояний исследовалась Ульманом; см. [150]. Лемма 9.2.3 доказана в работе А. С. Холево [32].

3. Теорема кодирования для квантовой пропускной способности была впервые сформулирована Ллойдом (см. [126]) в виде $Q(\Phi) = \max_S I_c(S, \Phi)$,

но затем было показано, что величина $\bar{Q}_n$ может быть строго супераддитивна (см. работы Ди Винченцо, Шора и Смолина [78], а также Смита и Смолина [147]), следовательно, использование регуляризованного предельного выражения в (9.40) в общем случае действительно необходимо.

Неравенство $Q(\Phi) \leq \bar{Q}(\Phi)$ (т. е. обращение теоремы кодирования) было доказано Барнумом, Нильсеном и Шумахером (см. [54]), а также Барнумом, Книллом и Нильсеном [53]. Дополнительные аргументы в пользу эвристического подхода Ллойда — использования случайных подпространств — были приведены Шором. Доказательство, основанное на этом подходе, было впоследствии дано Хайденом; см. [93].

Соотношение (9.56) получено Шумахером и Вестморлендом [136], которые, основываясь на идеях классической теории информации (см. [49]), связали «секретность» передачи классической информации через квантовый канал Φ с величиной $\chi(\{\pi_x\}, \{S_B^x\}) - \chi(\{\pi_x\}, \{S_E^x\})$.

Понятие деградируемого канала введено в работе Деветака и Шора [77], где было показано, что квантовая пропускная способность деградируемого канала дается однобуквенным выражением $Q(\Phi) = \max_S I_c(S, \Phi)$.

Это напоминает понятие «ухудшенного» (stochastically degraded) канала (см. [70]) для классических широкополосных каналов, причем роль второго приемника играет окружение. Для таких каналов в теории информации получено однобуквенное выражение для области пропускных способностей. Антидеградируемые каналы рассматривались Карузо, Джованнетти и А. С. Холево; см. [67]. Следствие 9.3.1 получено в работе Кубитта, Рускаи и Смита [71].

4. Полное доказательство прямой теоремы кодирования ($Q(\Phi) \geq \bar{Q}(\Phi)$) дал Деветак; см. [76]. Оно основано на идее, связанной с соотношением между квантовой и секретной классической пропускными способностями, см. (9.56). Именно это доказательство (а также более простое доказа-

тельство обратного утверждения) излагается нами (с несколькими упрощениями). Оценка вероятностей больших отклонений типа Бернштейна, использующая операторную версию (9.75) неравенства Хёффдинга (см. [96, теорема 1]), принадлежит Винтеру; см. [157]. Другое доказательство, основанное на методе случайных подпространств, идейно близком к первоначальным соображениям Ллойда, дано Хайденом, Шором и Винтером; см. [94].

Как уже отмечалось, квантовый канал характеризуется целым спектром пропускных способностей. Помимо величин C , C_χ , C_{ea} , C_p , Q , подробно рассмотренных в настоящей книге, в квантовой теории информации изучаются классическая и квантовая пропускные способности с обратной связью (обозначаемые соответственно C_b , Q_b), а также классическая и квантовая пропускные способности с дополнительным независимым классическим двусторонним каналом (соответственно C_2 , Q_2). Отметим, что в классическом случае $C = C_b = C_2 = C_{\text{Shan}}$ и шенноновская пропускная способность остается единственной характеристикой. Для квантового канала имеет место следующая иерархия:

$$\begin{array}{ccccccc} C_\chi & \leq & C_b & \leq & C_2 & \leq & C_{ea} \\ \vee & & \vee & & \vee & & \vee \\ Q & \leq & Q_b & \leq & Q_2 & \leq & Q_{ea} \end{array},$$

где $\leq$ следует понимать как «меньше или равно для всех каналов и строго меньше для некоторых», см. работу Беннета, Деветака, Шора, Смолина [57]. Известно также, что $C_{ea} = 2Q_{ea}$ и для ряда остальных пар возможны неравенства как в ту, так и в другую стороны. Далее, оказывается возможным построить так называемый «материнский» протокол передачи через квантовый канал, который при использовании различных частных дополнительных ресурсов (таких, например, как обратная связь либо сцепленность) позволяет реализовать всевозможные способы передачи, включая упомянутые выше; см. [47].

ГЛАВА 10

Каналы с ограничениями на входе

Одним из главных вопросов, мотивировавших появление квантовой теории информации, был вопрос о пропускной способности оптического квантового канала с ограничением на среднюю энергию входного сигнала. С математической точки зрения, необходимость введения ограничений возникает, когда квантовая система, несущая информацию, описывается бесконечномерным гильбертовым пространством, что влечет необходимость использования неограниченных операторов с присущими усложнениями. Важный класс таких систем, иногда называемых системами с «непрерывными переменными», а также каналов, называемых (бозонными) гауссовскими, будет рассмотрен в следующей главе. Одной из конечных целей настоящей главы является получение общих выражений для пропускных способностей бесконечномерных каналов с ограничениями на входе, удобных для использования в случае квантовых гауссовских каналов с ограничением на среднюю энергию сигнала.

Особенностью бесконечномерного случая является разрывность и неограниченность энтропии квантовых состояний, что заставляет уделить серьезное внимание изучению непрерывности энтропийных характеристик. Другой характерной чертой является естественное появление «непрерывных» ансамблей, которые описываются вероятностными мерами на множестве квантовых состояний. Различные характеристики квантового канала, такие как пропускная способность, выражаются в виде точных верхних либо нижних граней функционалов на множестве обобщенных ансамблей, удовлетворяющих соответствующему ограничению. Эти точные грани оказываются достижимыми при выполнении определенных условий, а именно — непрерывности рассматриваемой характеристики и компактности множества, определяемого ограничением. Эти две математические проблемы и составляют основной предмет настоящей главы.

§ 10.1. О сходимости квантовых состояний

Всюду далее $\mathcal{H}$ — сепарабельное гильбертово пространство. Линейный оператор A в пространстве $\mathcal{H}$ называется *ограниченным*, если он отображает единичный шар в ограниченное по норме подмножество пространства $\mathcal{H}$. Многие определения из гл. 2 переносятся на ограниченные

операторы; там, где необходимы модификации, будут даны соответствующие пояснения. Так, норма оператора $\|A\|$ определяется выражением (1.16), в котором максимум следует заменить на точную верхнюю грань. Оператор A ограничен тогда и только тогда, когда $\|A\| < \infty$. Множество всех ограниченных операторов образует банахову алгебру $\mathfrak{B}(\mathcal{H})$. Следовая (ядерная) норма $\|T\|_1$ определяется выражением (1.14), и множество ограниченных операторов, для которых $\|T\|_1 < \infty$, образует банахово пространство $\mathfrak{T}(\mathcal{H})$ ядерных операторов. Для любых операторов $T \in \mathfrak{T}(\mathcal{H})$, $A \in \mathfrak{B}(\mathcal{H})$ имеет место неравенство

$$|\operatorname{Tr} TA| \leq \|T\|_1 \|A\|; \quad (10.1)$$

банахово пространство $\mathfrak{B}(\mathcal{H})$ является сопряженным к $\mathfrak{T}(\mathcal{H})$, т.е. любой непрерывный линейный функционал на $\mathfrak{T}(\mathcal{H})$ имеет вид $T \rightarrow \operatorname{Tr} TA$ при некотором $A \in \mathfrak{B}(\mathcal{H})$, а его норма равна $\|A\|$. Заметим также, что

$$\|A\| \leq \|A\|_1 \quad (10.2)$$

и что $\mathfrak{T}(\mathcal{H})$ является собственным подпространством пространства $\mathfrak{B}(\mathcal{H})$.

Оператором плотности (состоянием) называется положительный ядерный оператор с единичным следом (ср. определение 2.1.1). Пространство состояний $\mathfrak{S}(\mathcal{H})$ — замкнутое выпуклое подмножество банахова пространства $\mathfrak{T}(\mathcal{H})$, которое является полным сепарабельным метрическим пространством с метрикой, определяемой следовой нормой: $\rho(S_1, S_2) = \|S_1 - S_2\|_1$.

Последовательность ограниченных операторов $\{A_n\}$ в $\mathcal{H}$ сходится слабо к оператору A , если $\lim_{n \rightarrow \infty} \langle \psi | A_n | \varphi \rangle \rightarrow \langle \psi | A | \varphi \rangle$ для всех $\varphi, \psi \in \mathcal{H}$. Хотя в пространстве $\mathfrak{T}(\mathcal{H})$ такая сходимость слабее сходимости по следовой норме, на подмножестве $\mathfrak{S}(\mathcal{H})$ эти два вида сходимости оказываются эквивалентными.

Лемма 10.1.1. Пусть $\{S_n\}$ — последовательность операторов плотности в $\mathcal{H}$, слабо сходящаяся к оператору плотности S , тогда $\|S_n - S\|_1 \rightarrow 0$.

Доказательство. Для любого конечномерного проектора P имеем

$$\begin{aligned} \|S_n - S\|_1 &\leq \|P(S_n - S)P\|_1 + 2\|PS_n(I - P)\|_1 + 2\|PS(I - P)\|_1 + \\ &\quad + \|(I - P)S_n(I - P)\|_1 + \|(I - P)S(I - P)\|_1. \end{aligned}$$

Первое слагаемое в правой части стремится к нулю при любом выборе проектора P , поскольку $PS_nP \rightarrow PSP$ в силу слабой сходимости и эквивалентности всех видов сходимости в конечномерном случае. Для двух последних слагаемых имеем

$$\|(I - P)S(I - P)\|_1 = \operatorname{Tr}(I - P)S(I - P) = \operatorname{Tr}(I - P)S = 1 - \operatorname{Tr} PS$$

(это выражение можно сделать сколь угодно малым путем выбора проектора P) и

$$\|(I - P)S_n(I - P)\|_1 = 1 - \text{Tr} PS_n \rightarrow 1 - \text{Tr} PS$$

в силу слабой сходимости. Среднее слагаемое можно оценить следующим образом:

$$\|PS_n(I - P)\|_1 = \text{Tr} U^* PS_n(I - P) = \text{Tr} U^* P \sqrt{S_n} \sqrt{S_n} (I - P),$$

где U представляет собой унитарный оператор из полярного разложения оператора $PS_n(I - P)$. В силу операторного неравенства Коши—Буняковского для следа имеем

$$\begin{aligned} \text{Tr} U^* P \sqrt{S_n} \sqrt{S_n} (I - P) &\leq \\ &\leq \sqrt{\text{Tr} U^* P \sqrt{S_n} \sqrt{S_n} P U} \sqrt{\text{Tr} (I - P) \sqrt{S_n} \sqrt{S_n} (I - P)} = \\ &= \sqrt{\text{Tr} PS_n} \sqrt{1 - \text{Tr} PS_n} \rightarrow \sqrt{\text{Tr} PS} \sqrt{1 - \text{Tr} PS}, \end{aligned}$$

а это выражение также можно сделать сколь угодно малым путем выбора проектора P . $\square$

В дальнейшем, говоря о сходимости состояний, мы будем иметь в виду сходимость, о которой идет речь в этой лемме.

Теорема 10.1.1. *Замкнутое по следовой норме подмножество K множества состояний $\mathfrak{S}(\mathcal{H})$ компактно тогда и только тогда, когда для любого $\varepsilon > 0$ найдется конечномерный проектор P_ε такой, что $\text{Tr} P_\varepsilon S > 1 - \varepsilon$ для всех $S \in K$.*

Доказательство. Пусть K — компактное подмножество в $\mathfrak{S}(\mathcal{H})$. Предположим, что найдется $\varepsilon > 0$ такое, что для любого конечномерного проектора P существует состояние $S \in K$, для которого $\text{Tr} PS \leq 1 - \varepsilon$. Пусть $\{P_n\}$ — монотонно возрастающая последовательность конечномерных проекторов в $\mathcal{H}$, слабо сходящаяся к единичному оператору I , и пусть S_n — соответствующая последовательность состояний из K . В силу компактности множества K найдется ее подпоследовательность $\{S_{n_k}\}$, сходящаяся к состоянию $S_0 \in K$. По построению $\text{Tr} P_{n_l} S_{n_k} \leq \text{Tr} P_{n_k} S_{n_k} \leq 1 - \varepsilon$ при $k > l$. Следовательно,

$$\text{Tr} S_0 = \lim_{l \rightarrow +\infty} \text{Tr} P_{n_l} S_0 = \lim_{l \rightarrow +\infty} \lim_{k \rightarrow +\infty} \text{Tr} P_{n_l} S_{n_k} \leq 1 - \varepsilon,$$

что противоречит тому, что $S_0 \in K \subseteq \mathfrak{S}(\mathcal{H})$.

Обратно, пусть K — замкнутое подмножество множества $\mathfrak{S}(\mathcal{H})$, удовлетворяющее условию теоремы, и пусть $\{S_n\}$ — произвольная последовательность из K . Поскольку единичный шар в $\mathfrak{B}(\mathcal{H})$ слабо компактен,

найдется подпоследовательность $\{S_{n_k}\}$, слабо сходящаяся к ограниченному положительному оператору S_0 . Имеем

$$\mathrm{Tr} S_0 \leq \liminf_{k \rightarrow \infty} \mathrm{Tr} S_{n_k} = 1,$$

поэтому для доказательства того, что S_0 — состояние, достаточно установить, что $\mathrm{Tr} S_0 \geq 1$. Пусть $\varepsilon > 0$ и P_ε — соответствующий проектор. Имеем

$$\mathrm{Tr} S_0 \geq \mathrm{Tr} P_\varepsilon S_0 = \lim_{k \rightarrow \infty} \mathrm{Tr} P_\varepsilon S_{n_k} > 1 - \varepsilon,$$

где равенство следует из конечномерности проектора P_ε . Таким образом, S_0 имеет единичный след и является состоянием. Из леммы 10.1.1 следует сходимость подпоследовательности $\{S_{n_k}\}$ к состоянию S_0 по следовой норме. Поэтому множество K компактно в топологии следовой нормы. $\square$

Далее нам потребуется следующая частичная бесконечномерная версия спектрального разложения (1.5). Пусть $\{|e_j\rangle\}$ — ортонормированный базис в $\mathcal{H}$, $\{f_j\}$ — последовательность вещественных чисел, ограниченная снизу, тогда формула

$$F|\psi\rangle = \sum_j f_j |e_j\rangle \langle e_j|\psi\rangle \quad (10.3)$$

определяет самосопряженный полуограниченный снизу (см. § 10.8) оператор F на плотной области

$$\mathcal{D}(F) = \left\{ \psi: \sum_j |f_j|^2 |\langle e_j|\psi\rangle|^2 < \infty \right\}, \quad (10.4)$$

для которого $|e_j\rangle$ являются собственными векторами, а f_j — собственными числами.

Определение 10.1.1. Оператор с областью определения (10.4), действующий по формуле (10.3), будем называть *оператором типа $\mathfrak{F}$* .

В приложениях F является оператором энергии (системы осцилляторов). В этой связи важную роль будет играть оператор $\exp(-\theta F)$, $\theta > 0$, который определяется соотношением

$$\exp(-\theta F)|\psi\rangle = \sum_j \exp(-\theta f_j) |e_j\rangle \langle e_j|\psi\rangle \quad (10.5)$$

и является ограниченным положительным оператором типа $\mathfrak{F}$.

Пусть F — оператор типа $\mathfrak{F}$. Для произвольного оператора плотности S определим математическое ожидание

$$\mathrm{Tr} SF = \sum_{j=1}^{\infty} f_j \langle e_j|S|e_j\rangle \leq +\infty. \quad (10.6)$$

Лемма 10.1.2. *Функционал $S \rightarrow \text{Tr} SF$ является аффинным и полунепрерывным снизу на множестве $\mathfrak{S}(\mathcal{H})$.*

Доказательство. Аффинность очевидна; далее используем полунепрерывность снизу точной верхней грани семейства непрерывных функций. Имеем

$$\text{Tr} SF = \sup_n \sum_{j=1}^n f_j \langle e_j | S | e_j \rangle,$$

где все конечные суммы непрерывны. □

Лемма 10.1.3. *Пусть спектр оператора F типа $\mathfrak{F}$ состоит из собственных значений f_n конечной кратности и $\lim_{n \rightarrow \infty} f_n = +\infty$, тогда множество*

$$\mathfrak{S}_E = \{S: \text{Tr} SF \leq E\} \quad (10.7)$$

компактно.

Доказательство. Без ограничения общности можно считать, что последовательность f_n монотонно возрастает. Пусть P_n — конечномерный проектор на собственное подпространство, соответствующее первым n собственным значениям, тогда $P_n \uparrow I$. Множество $\mathfrak{S}_E$ замкнуто, поскольку $\text{Tr} SF \leq \liminf_{N \rightarrow \infty} \text{Tr} S_N F$ для любой последовательности $\{S_N\}$, сходящейся к S , в силу леммы 10.1.2. Поскольку $f_{n+1}(I - P_n) \leq F$, имеем $\text{Tr} S(I - P_n) \leq f_{n+1}^{-1} \text{Tr} SF \leq f_{n+1}^{-1} E < \varepsilon$ для достаточно больших n и для всех $S \in \mathfrak{S}_E$. В силу критерия компактности множество $\mathfrak{S}_E$ компактно. □

В приложениях, где F является оператором энергии системы осцилляторов, полученный результат означает компактность подмножества квантовых состояний с ограниченной средней энергией.

§ 10.2. Квантовая энтропия и относительная энтропия

Энтропия $H(S)$ квантового состояния S по-прежнему определяется формулой (5.7), однако в бесконечномерном случае она может принимать значение $+\infty$. Относительная энтропия корректно определяется формулой (7.2). Большинство свойств, полученных в § 4.1, обобщается на бесконечномерный случай, однако вместо непрерывности имеет место лишь полунепрерывность снизу.

Теорема 10.2.1. *Квантовая энтропия и относительная энтропия полунепрерывны снизу на множестве состояний $\mathfrak{S}(\mathcal{H})$: пусть $\{S_n\}$ (соответственно $\{S'_n\}$) — последовательность операторов плотности в $\mathcal{H}$, сходящаяся к оператору плотности S*

(соответственно S'), тогда

$$H(S) \leq \liminf_{n \rightarrow \infty} H(S_n), \quad H(S; S') \leq \liminf_{n \rightarrow \infty} H(S_n; S'_n).$$

Доказательство. В силу неравенства (10.2) имеем $\|S_n - S\| \rightarrow 0$. Функция $\eta(x) = -x \log x$ непрерывна на отрезке $[0, 1]$, следовательно, $\|\eta(S_n) - \eta(S)\| \rightarrow 0$. Действительно, функцию $\eta(x)$ можно приблизить многочленами равномерно на $[0, 1]$ и затем использовать следующую оценку.

Задача 10.2.1. Докажите, что для многочлена p и произвольных операторов A, B , норма которых не превосходит единицу, имеет место неравенство

$$\|p(A) - p(B)\| \leq c_p \|A - B\|,$$

в котором константа c_p зависит только от p . *Указание.* Используйте разложение

$$A^k - B^k = \sum_{l=0}^{k-1} A^{k-l-1} (A - B) B^l.$$

Таким образом, для любого конечномерного проектора P в силу неравенства (10.1) имеем

$$|\operatorname{Tr} P(\eta(S_n) - \eta(S))| \leq \operatorname{Tr} P \|\eta(S_n) - \eta(S)\| \rightarrow 0. \quad (10.8)$$

С другой стороны, в силу того же неравенства, для эрмитова положительного оператора A выполняется неравенство

$$\operatorname{Tr} PA \leq \|P\| \operatorname{Tr} A,$$

и, следовательно, $\operatorname{Tr} A = \sup_P \operatorname{Tr} PA$, где P пробегает множество всех конечномерных проекторов. Таким образом,

$$H(S) = \sup_P \operatorname{Tr} P \eta(S) \leq \liminf_{n \rightarrow \infty} \sup_P \operatorname{Tr} P \eta(S_n) = \liminf_{n \rightarrow \infty} H(S_n).$$

Аналогично, используя бесконечномерный аналог представления (7.20) для относительной энтропии, получаем

$$H(S; S') = \sup_{\lambda > 0} \frac{1}{\lambda} [H(\lambda S + (1 - \lambda)S') - \lambda H(S) - (1 - \lambda)H(S')],$$

следовательно,

$$\begin{aligned} H(S; S') &= \sup_{P, \lambda > 0} \frac{1}{\lambda} \operatorname{Tr} P [\eta(\lambda S + (1 - \lambda)S') - \lambda \eta(S) - (1 - \lambda)\eta(S')] \leq \\ &\leq \liminf_{n \rightarrow \infty} \sup_{P, \lambda > 0} \frac{1}{\lambda} \operatorname{Tr} P [\eta(\lambda S_n + (1 - \lambda)S'_n) - \lambda \eta(S_n) - (1 - \lambda)\eta(S'_n)] = \\ &= \liminf_{n \rightarrow \infty} H(S_n; S'_n). \end{aligned}$$

□

Лемма 10.2.1. Пусть F — оператор типа $\mathfrak{F}$, удовлетворяющий условию

$$\mathrm{Tr} \exp(-\theta F) < \infty \quad \text{для } \theta > 0, \quad (10.9)$$

тогда квантовая энтропия $H(S)$ ограничена и непрерывна на множестве $\mathfrak{S}_E$, определенном соотношением (10.7).

Заметим, что из неравенства (10.9) следует, что оператор F удовлетворяет условиям леммы 10.1.3, а значит, множество $\mathfrak{S}_E$ компактно.

Доказательство. Вводя оператор плотности $S_\theta = \exp(-\theta F - c(\theta))$, где $c(\theta) = \ln \mathrm{Tr} \exp(-\theta F)$, получаем

$$H(S) = -H(S; S_\theta) + \theta \mathrm{Tr} SF + c(\theta), \quad (10.10)$$

где $H(S; S_\theta)$ — относительная энтропия, следовательно,

$$H(S) \leq -H(S; S_\theta) + \theta E + c(\theta), \quad (10.11)$$

если $S \in \mathfrak{S}_E$. Поэтому энтропия $H(S)$ ограничена на $\mathfrak{S}_E$. Поскольку функция $H(S)$ полунепрерывна снизу в силу теоремы 10.2.1, достаточно доказать ее полунепрерывность сверху на множестве $\mathfrak{S}_E$. Пусть $\{S_n\} \subset \mathfrak{S}_E$ — последовательность состояний, сходящаяся к состоянию S . Из неравенства (10.11) в силу полунепрерывности снизу относительной энтропии следует, что

$$\limsup_{n \rightarrow \infty} H(S_n) \leq -H(S; S_\theta) + \theta E + c(\theta) \leq H(S) + \theta(E - \mathrm{Tr} SF). \quad (10.12)$$

Переходя к пределу при $\theta \rightarrow 0$, получаем полунепрерывность сверху функции $H(S)$. $\square$

Заметим, что если F — оператор энергии системы, то S_θ — оператор плотности гиббсовского равновесного состояния при обратной температуре θ , а функция $-\theta^{-1}c(\theta)$ равна свободной энергии.

§ 10.3. C-q-канал с бесконечным алфавитом

Пусть $\mathcal{X}$ — некоторое (бесконечное) множество; отображение $x \rightarrow S_x$ множества $\mathcal{X}$ в пространство состояний $\mathfrak{S}(\mathcal{H})$ будем называть *классически-квантовым (c-q) каналом* с входным алфавитом $\mathcal{X}$. Пусть $f(x)$ — функция, определенная на $\mathcal{X}$ и принимающая значения в $[0, +\infty]$. Введем класс $\mathcal{P}_E$ распределений вероятностей с конечным носителем $\pi = \{\pi_x\}$ на $\mathcal{X}$, удовлетворяющих условию

$$\sum_x f(x) \pi_x \leq E, \quad (10.13)$$

где E — положительное число. Будем считать, что множество $\mathcal{P}_E$ непусто, и предполагать, что канал удовлетворяет следующему условию:

$$\sup_{\pi \in \mathcal{P}_E} H\left(\sum_x \pi_x S_x\right) < \infty. \quad (10.14)$$

Определение 10.3.1. Определим код (W, M) размера N и длины n так же, как в определении 5.1.1, с дополнительным требованием, что все кодовые слова $\omega = (x_1, \dots, x_n) \in W$ удовлетворяют аддитивному ограничению

$$f(x_1) + \dots + f(x_n) \leq nE. \quad (10.15)$$

Средняя вероятность ошибки кода $\bar{P}_e(W, M)$ и минимальная средняя вероятность ошибки $\bar{p}_e(n, N)$ даются соответственно формулами (5.5) и (5.6). Классическая пропускная способность канала $x \rightarrow S_x$ определяется в соответствии с определением 5.1.2, т. е. как точная верхняя грань допустимых скоростей R , для которых $\lim_{n \rightarrow \infty} \bar{p}_e(n, 2^{nR}) = 0$.

Теорема 10.3.1. Классическая пропускная способность C c-q-канала $x \rightarrow S_x$, удовлетворяющего условию (10.14) с входным ограничением (10.15), равна величине

$$C_\chi = \sup_{\pi \in \mathcal{P}_E} \left[H\left(\sum_x \pi_x S_x\right) - \sum_x \pi_x H(S_x) \right]. \quad (10.16)$$

Доказательство. Пусть $\mathcal{P}_E^{(n)}$ — класс распределений вероятностей на $\mathcal{X}^n$, удовлетворяющих условию

$$\sum_{x_1, \dots, x_n} [f(x_1) + \dots + f(x_n)] \pi_{x_1, \dots, x_n} \leq nE. \quad (10.17)$$

Определим величину C_χ^n выражением (5.26), в котором точная верхняя грань по π берется по множеству $\mathcal{P}_E^{(n)}$, т. е.

$$C_\chi^n = \sup_{\pi \in \mathcal{P}_E^{(n)}} \chi(\{\pi_\omega\}; \{S_\omega\}).$$

Лемма 10.3.1. Последовательность $\{C_\chi^n\}$ аддитивна, т. е. $C_\chi^n = nC_\chi$.

Доказательство. В силу неравенства (5.27) имеем

$$\chi_n(\pi) \leq \sum_{k=1}^n \chi(\pi^{(k)}),$$

где $\pi^{(k)}$ — k -е маргинальное распределение π на $\mathcal{X}$. Далее,

$$\sum_{k=1}^n \chi(\pi^{(k)}) \leq n\chi(\bar{\pi}), \quad (10.18)$$

где $\bar{\pi} = \frac{1}{n} \sum_{k=1}^n \pi^{(k)}$, поскольку $\chi(\pi)$ — вогнутая функция распределения π (это следует из вогнутости энтропии фон Неймана). Неравенство (10.17) можно переписать следующим образом:

$$\frac{1}{n} \sum_{k=1}^n \sum_x f(x) \pi^{(k)}(x) \leq E,$$

откуда следует, что $\bar{\pi} \in \mathcal{P}_E$, если $\pi \in \mathcal{P}_E^{(n)}$. Взяв точную верхнюю грань по $\pi \in \mathcal{P}_E^{(n)}$ в соотношении (10.18), получаем $C_\chi^n \leq nC_\chi$. Обратное неравенство очевидно. $\square$

Для доказательства обращения теоремы кодирования используем следствие неравенства Фано (см. (5.29)):

$$\bar{P}_e(W, M) \geq 1 - \frac{\sup_{\pi \in \mathcal{P}_E^{(n)}} \sup_M \mathcal{I}_n(\pi, M)}{nR} - \frac{1}{nR}, \quad (10.19)$$

которое выводится следующим образом. Пусть слова в коде (W, M) берутся с входным распределением $\pi^{(N)}$, приписывающим равную вероятность $1/N$ каждому слову. Рассмотрим неравенство (4.35). Поскольку кодовые слова удовлетворяют условию (10.15), имеем $\pi^{(N)} \in \mathcal{P}_E^{(n)}$, откуда следует неравенство (10.19).

Применяя неравенство (10.19) и теорему 5.3.1, получаем

$$\bar{p}_e(n, 2^{nR}) \geq 1 - \frac{C_\chi}{R} - \frac{1}{nR},$$

где C_χ определяется выражением (10.16), откуда следует, что

$$\bar{p}_e(n, 2^{nR}) \not\rightarrow 0 \quad \text{для } R > C_\chi.$$

В классической теории информации прямая теорема кодирования для каналов с аддитивными ограничениями может быть доказана с помощью случайного кодирования с распределением вероятностей (5.42), модифицированного множителем, сконцентрированным на словах, для которых ограничение выполняется в виде приближенного равенства. Аналогичный подход можно применить и к с-q-каналу. Пусть π — распределение на $\mathcal{X}$, удовлетворяющее условию (10.13), и пусть P — распределение на множестве N слов, при котором слова независимы и имеют распределение вероятностей (5.42). Введем обозначение $\nu_n = P\left(\frac{1}{n} \sum_{k=1}^n f(x_k) \leq E\right)$ и определим модифицированное распределение вероятностей $\tilde{P}$, при котором

слова по-прежнему независимы, но

$$\tilde{P}(w = (x_1, \dots, x_n)) = \begin{cases} \nu_n^{-1} \pi_{x_1} \dots \pi_{x_n}, & \text{если } \sum_{k=1}^n f(x_k) \leq nE, \\ 0 & \text{в противном случае.} \end{cases} \quad (10.20)$$

Заметим, что, поскольку $\pi \in \mathcal{P}_E$, справедливо неравенство $Ef \leq E$ (где E — математическое ожидание относительно распределения P), и, следовательно, в силу центральной предельной теоремы имеем

$$\lim_{n \rightarrow \infty} \nu_n \geq 1/2.$$

Поэтому $\tilde{E}\xi \leq 2^m E\xi$ (где $\tilde{E}$ — математическое ожидание относительно распределения $\tilde{P}$) для любой неотрицательной случайной величины ξ , зависящей от m различных слов.

Вероятность ошибки $\bar{P}_e(W, M)$ ограничена сверху величиной (5.46). Оценим математическое ожидание этой границы относительно распределения $\tilde{P}$. Поскольку каждое слагаемое в правой части неравенства (5.46) зависит не более чем от двух различных слов, имеем

$$\tilde{E} \inf_M \bar{P}_e(W, M) \leq 4 E \inf_M \bar{P}_e(W, M),$$

и математическое ожидание относительно распределения P можно сделать сколь угодно малым при $N = 2^{nR}$, $n \rightarrow \infty$, если $R < C_X - 3\delta$. Поэтому $\tilde{E}\bar{P}_e(W, M)$ также можно сделать сколь угодно малым при тех же условиях. Поскольку распределение $\tilde{P}$ сконцентрировано на словах, удовлетворяющих условию (10.15), можно выбрать код, для которого величину $\bar{P}_e(W, M)$ можно сделать сколь угодно малой для достаточно больших n . $\square$

§ 10.4. С-q-канал с непрерывным алфавитом

Пусть теперь входной алфавит $\mathcal{X}$ является полным сепарабельным метрическим пространством с σ -алгеброй борелевских подмножеств. Рассмотрим с-q-канал, который задается *непрерывным* отображением $x \rightarrow S_x$ алфавита $\mathcal{X}$ в множество квантовых состояний $\mathfrak{S}(\mathcal{H})$ (в силу леммы 10.1.1 для этого необходимо и достаточно, чтобы все матричные элементы $\langle \psi | S_x | \varphi \rangle$, $\psi, \varphi \in \mathcal{H}$, были непрерывны на $\mathcal{X}$). Нашей целью будет получение удобного интегрального выражения для классической пропускной способности C канала $x \rightarrow S_x$ при ограничении (10.15).

Предположим, что f — неотрицательная борелевская функция на $\mathcal{X}$. Рассмотрим множество $\mathcal{P}_E^B$ борелевских вероятностных мер π на $\mathcal{X}$, удовлетворяющих условию

$$\int_{\mathcal{X}} f(x)\pi(dx) \leq E. \quad (10.21)$$

Последовательность борелевских вероятностных мер $\{\pi_n\}$ слабо сходится к мере π , если

$$\int_{\mathcal{X}} \varphi(x)\pi_n(dx) \rightarrow \int_{\mathcal{X}} \varphi(x)\pi(dx)$$

для любой ограниченной непрерывной функции φ . Нам понадобятся следующие вспомогательные результаты (см. комментарии).

Задача 10.4.1. Пусть f — полунепрерывная снизу функция, тогда функционал $\pi \rightarrow \int_{\mathcal{X}} f(x)\pi(dx)$ полунепрерывен снизу по отношению к слабой сходимости вероятностных мер. *Указание.* Используйте тот факт, что f является точной верхней гранью семейства всех ограниченных непрерывных функций $\varphi \leq f$.

Лемма 10.4.1. Пусть f — полунепрерывная снизу функция, тогда множество $\mathcal{P}_E$ всех вероятностных мер с конечным носителем, удовлетворяющих условию (10.21), слабо плотно в $\mathcal{P}_E^B$.

Приведем также удобное достаточное условие слабой компактности множества $\mathcal{P}_E^B$.

Лемма 10.4.2. Если функция f полунепрерывна снизу и для любого положительного числа k множество $\{x: f(x) \leq k\} \subset \mathcal{X}$ компактно, то подмножество вероятностных мер

$$\mathcal{P}_E^B = \left\{ \pi: \int_{\mathcal{X}} f(x)\pi(dx) \leq E \right\}$$

слабо компактно.

Доказательство. Из полунепрерывности снизу функции f следует, что функционал $\pi \rightarrow \int_{\mathcal{X}} f(x)\pi(dx)$ полунепрерывен снизу по отношению к слабой сходимости вероятностных мер (задача 10.4.1), откуда вытекает слабая замкнутость множества $\mathcal{P}_E^B$. Известно, что слабо замкнутое подмножество $\mathcal{P}$ борелевских вероятностных мер на $\mathcal{X}$ слабо компактно тогда и только тогда, когда для любого $\varepsilon > 0$ существует компакт $K \subset \mathcal{X}$ такой, что $\pi(K^c) \leq \varepsilon$ для всех $\pi \in \mathcal{P}$. Для данного $\varepsilon > 0$ рассмотрим компактное множество $K = \{x: f(x) \leq E/\varepsilon\}$. Тогда $\pi(K^c) \leq \frac{\varepsilon}{E} \int_{K^c} f(x)\pi(dx) \leq \varepsilon$ для $\pi \in \mathcal{P}_E^B$, следовательно, множество $\mathcal{P}_E^B$ слабо компактно. $\square$

Для произвольной борелевской вероятностной меры π на $\mathcal{X}$ введем среднее состояние

$$\bar{S}_\pi = \int_{\mathcal{X}} S_x \pi(dx), \quad (10.22)$$

где по предположению подынтегральная функция S_x непрерывна и интеграл определяет оператор плотности в $\mathcal{H}$.

Предполагая, что $H(\bar{S}_\pi) < \infty$, рассмотрим функционал

$$\chi(\pi) = H(\bar{S}_\pi) - \int_{\mathcal{X}} H(S_x) \pi(dx), \quad (10.23)$$

где функция $H(S_x)$ неотрицательна и полунепрерывна снизу в силу леммы 10.2.1, следовательно, интеграл от нее определен.

Теорема 10.4.1. *Пусть существует оператор F типа $\mathfrak{F}$, удовлетворяющий условию (10.9) и такой, что*

$$f(x) \geq \text{Tr } S_x F, \quad x \in \mathcal{X}. \quad (10.24)$$

Тогда выполнено условие (10.14), пропускная способность C канала $x \rightarrow S_x$ с ограничением (10.15) конечна и дается выражением (10.16).

Если, кроме того, функция f удовлетворяет условиям леммы 10.4.2, то

$$C = \max_{\pi \in \mathcal{P}_E^B} \chi(\pi). \quad (10.25)$$

Доказательство. Интегрируя неравенство (10.24), получаем

$$\text{Tr } \bar{S}_\pi F \leq E \quad (10.26)$$

для $\pi \in \mathcal{P}_E$, следовательно, согласно лемме 10.2.1 справедливо неравенство

$$H(\bar{S}_\pi) \leq \theta \text{Tr } \bar{S}_\pi F + c(\theta) \leq \theta E + c(\theta),$$

поэтому условие (10.14) выполнено, величина C конечна и определяется выражением (10.16).

Если функция f удовлетворяет условиям леммы 10.4.2, то множество $\mathcal{P}_E^B$ слабо компактно. Покажем, что функционал $\pi \rightarrow \chi(\pi)$ непрерывен и, следовательно, достигает своего максимума на $\mathcal{P}_E^B$.

Рассмотрим первое слагаемое в формуле (10.23) для $\chi(\pi)$. Поскольку матричные элементы семейства $\{S_x\}$ непрерывно зависят от x , отображение $\pi \rightarrow \bar{S}_\pi$ в множество $\mathfrak{S}_E$, снабженное слабой операторной топологией, непрерывно относительно слабой сходимости мер. В силу леммы 10.1.1 слабая операторная топология на $\mathfrak{S}(\mathcal{H})$ эквивалентна топологии ядерной нормы. Квантовая энтропия непрерывна на $\mathfrak{S}_E$ в силу леммы 10.2.1. Поэтому функционал $\pi \rightarrow H(\bar{S}_\pi)$ непрерывен на множестве $\mathcal{P}_E^B$.

Покажем, что второе слагаемое в формуле (10.23) также непрерывно. Для любой меры $\pi \in \mathcal{P}_E^B$ и $k > 0$ рассмотрим разложение

$$\int_{\mathcal{X}} H(S_x) \pi(dx) = \int_{f(x) \leq k} H(S_x) \pi(dx) + \int_{f(x) > k} H(S_x) \pi(dx). \quad (10.27)$$

Непрерывность будет следовать из того, что первое слагаемое непрерывно на $\mathcal{P}_E^B$, а второе может быть сделано равномерно малым на $\mathcal{P}_E^B$ за счет выбора достаточно большого k . В силу условия (10.24) из неравенства $f(x) \leq k$ следует, что $S_x \in \mathfrak{S}_k$, а в силу леммы 10.2.1 энтропия ограничена и непрерывна на $\mathfrak{S}_k$, поэтому функция $H(S_x)$ ограничена и непрерывна на компактном множестве $\{x : f(x) \leq k\}$, и, следовательно, первое слагаемое в разложении (10.27) непрерывно зависит от π . С другой стороны, подставляя $S = S_x$ в формулу (10.10) и вновь используя неравенство (10.24), получаем

$$H(S_x) \leq \theta f(x) + c(\theta).$$

Фиксируем $\varepsilon > 0$, и тогда, выбирая сначала достаточно малое θ , а затем достаточно большое k , для $\pi \in \mathcal{P}_E^B$ получаем

$$\begin{aligned} \int_{f(x) > k} H(S_x) \pi(dx) &\leq \theta \int_{f(x) > k} f(x) \pi(dx) + c(\theta) \int_{f(x) > k} \pi(dx) \leq \\ &\leq \theta E + c(\theta) E k^{-1} \leq \varepsilon. \end{aligned}$$

Итак, второе слагаемое, а значит, и весь функционал $\chi(\pi)$ непрерывны на $\mathcal{P}_E^B$.

Из леммы 10.4.1 и выражения (10.16) тогда вытекает, что $C = \sup_{\pi \in \mathcal{P}_E^B} \chi(\pi)$, причем точная верхняя грань достигается в силу непрерывности функционала $\chi(\pi)$ и компактности множества $\mathcal{P}_E^B$. $\square$

§ 10.5. Квантовый канал с ограничением

Пусть $\mathcal{H}_A$, $\mathcal{H}_B$ — сепарабельные гильбертовы пространства, которые будут называться соответственно входным и выходным пространством.

Определение 10.5.1. *Каналом* называется линейное, ограниченное, сохраняющее след, вполне положительное отображение $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$. Как и в конечномерном случае, полная положительность означает, что для любого $n = 1, 2, \dots$ отображение $\Phi \otimes \text{Id}_n$ положительно.

Задача 10.5.1. Докажите, что произвольное аффинное отображение $\Phi_s: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ однозначно продолжается до линейного, ограниченного, положительного, сохраняющего след отображения $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$. *Указание.* Для построения линейного продолжения исполь-

зуйте конструкцию задачи 2.2.1, а для доказательства ограниченности — оценки из леммы 9.2.2.

В этом параграфе мы изучим классическую пропускную способность канала Φ при аддитивном ограничении на входе. Пусть F — оператор типа $\mathfrak{F}$ в $\mathcal{H}_A$, представляющий величину, среднее значение которой ограничено (в приложениях это обычно средняя энергия сигнала на входе канала). Предполагается, что состояния $S^{(n)}$ на входе блочного канала $\Phi^{\otimes n}$ подчинены аддитивному ограничению

$$\mathrm{Tr} S^{(n)} F^{(n)} \leq nE, \quad (10.28)$$

где

$$F^{(n)} = F \otimes \dots \otimes I + \dots + I \otimes \dots \otimes F,$$

а E — положительная постоянная. Модифицируя определение 8.1.1 и доказательство предложения 8.1.1 на случай кодовых состояний с ограничениями (10.28), можно доказать следующий результат.

Предложение 10.5.1. *Пусть канал Φ удовлетворяет условию*

$$\sup_{S: \mathrm{Tr} SF \leq E} H(\Phi[S]) < \infty. \quad (10.29)$$

Тогда классическая пропускная способность этого канала при ограничении (10.28) конечна и дается выражением

$$C(\Phi, F, E) = \lim_{n \rightarrow \infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}, F^{(n)}, nE), \quad (10.30)$$

где

$$C_\chi(\Phi, F, E) = \sup_{\pi: \mathrm{Tr} \bar{S}_\pi F \leq E} \chi(\{\pi_i\}; \{\Phi[S_i]\}). \quad (10.31)$$

Здесь $\bar{S}_\pi = \sum_i \pi_i S_i$ — среднее состояние ансамбля $\pi = \{\pi_i, S_i\}$.

Если для канала Φ выполняется свойство аддитивности

$$C_\chi(\Phi^{\otimes n}, F^{(n)}, nE) = nC_\chi(\Phi, F, E), \quad (10.32)$$

то имеет место равенство

$$C(\Phi, F, E) = C_\chi(\Phi, F, E).$$

Это тесно связано со свойством супераддитивности выпуклого замыкания выходной энтропии (8.35), из которого следует аддитивность χ -пропускной способности при линейных ограничениях (8.39) (см. п. 8.3.2).

В любом случае величина (10.31) дает нижнюю границу для классической пропускной способности $C(\Phi, F, E)$. Получим более удобное

выражение для $C_\chi(\Phi, F, E)$, опираясь на результаты из предыдущего параграфа. Рассмотрим s - q -канал с алфавитом $\mathcal{X} = \mathfrak{S}(\mathcal{H}_A)$, определяемый отображением $S \rightarrow \Phi[S]$. Ограничение будет задаваться функцией $f(S) = \text{Tr } SF$, которая является аффинной и полунепрерывной снизу в силу леммы 10.1.2, а условие (10.14) переходит в (10.29).

Определение 10.5.2. *Обобщенным ансамблем* называется произвольная борелевская вероятностная мера π на $\mathfrak{S}(\mathcal{H}_A)$. *Среднее состояние* обобщенного ансамбля π задается барицентром

$$\bar{S}_\pi = \int_{\mathfrak{S}(\mathcal{H}_A)} S \pi(dS).$$

Обычные ансамбли соответствуют мерам с конечным носителем.

Из леммы 10.2.1 следует, в частности, что неотрицательная функция $S \mapsto H(\Phi[S])$ измерима. Следовательно, при условии $H(\Phi(\bar{S}_\pi)) < \infty$ определен функционал

$$\chi_\Phi(\pi) = H(\Phi(\bar{S}_\pi)) - \int_{\mathfrak{S}(\mathcal{H}_A)} H(\Phi(S)) \pi(dS). \quad (10.33)$$

Задача 10.5.2. Докажите, что величина $\chi_\Phi(\pi)$ является вогнутым функционалом от π .

Следствие 10.5.1. Пусть существует положительный оператор F' в $\mathcal{H}_B$ такой, что

$$\text{Tr} \exp(-\theta F') < +\infty \quad \text{для всех } \theta > 0 \quad (10.34)$$

и

$$\text{Tr} \Phi[S] F' \leq \text{Tr } S F, \quad S \in \mathfrak{S}(\mathcal{H}). \quad (10.35)$$

Тогда выполнено условие (10.29) и

$$C_\chi(\Phi, F, E) = \sup_{\pi: \text{Tr } \bar{S}_\pi F \leq E} \chi_\Phi(\pi).$$

Более того, энтропия $H(\Phi[S])$ непрерывна на компактном множестве $\mathfrak{S}_E = \{S: \text{Tr } S F \leq E\}$.

Если, кроме того, оператор F удовлетворяет условиям леммы 10.1.3, то существует оптимальный обобщенный ансамбль, т. е.

$$C_\chi(\Phi, F, E) = \max_{\pi: \text{Tr } \bar{S}_\pi F \leq E} \chi_\Phi(\pi). \quad (10.36)$$

Доказательство. Утверждение следует из теоремы 10.4.1, примененной к s - q -каналу $S \rightarrow \Phi[S]$ с функцией-ограничением $f(S) = \text{Tr } S F$, при этом роль условия (10.24) играет неравенство (10.35), а оператор F'

играет роль F . Функция $f(S) = \text{Tr} SF$ удовлетворяет условиям леммы 10.4.2 в силу лемм 10.1.2, 10.1.3.

Непрерывность энтропии $H(\Phi[S])$ следует из непрерывности отображения $S \rightarrow S' = \Phi[S]$ и леммы 10.2.1, которая гарантирует непрерывность энтропии $H(S')$ на компактном множестве $\{S' : \text{Tr} S'F' \leq E\}$. $\square$

§ 10.6. Передача классической информации с помощью сцепленного состояния через канал с ограничениями

Пусть системы A и B находятся в сцепленном чистом состоянии S_{AB} . Предположим, что имеющаяся в их распоряжении сцепленность неограничена, но конечна, т. е. состояние S_{AB} должно удовлетворять условию $H(S_A) = H(S_B) < \infty$. Обобщая результат из § 8.4, можно доказать следующее утверждение.

Предложение 10.6.1. Пусть Φ — канал, удовлетворяющий условию (10.29) с оператором F , для которого выполнено условие (10.9), тогда пропускная способность протокола передачи классической информации с помощью сцепленного состояния по каналу Φ с ограничением (10.28) конечна и дается выражением

$$C_{ea}(\Phi) = \sup_{S: \text{Tr} SF \leq E} I(S, \Phi), \quad (10.37)$$

в котором

$$I(S, \Phi) = H(S) + H(\Phi[S]) - H(S; \Phi), \quad (10.38)$$

где $H(S; \Phi)$ — обменная энтропия.

Исследуем вопрос о достижимости точной верхней грани в правой части равенства (10.37). Заметим, что из условия (10.9) следует, что оператор F удовлетворяет условию леммы 10.1.3 и, значит, множество $\mathfrak{S}_E = \{S : \text{Tr} SF \leq E\}$ компактно.

Предложение 10.6.2. Пусть ограничивающий оператор F удовлетворяет условию (10.9), и пусть существует оператор F' типа $\mathfrak{F}$, для которого выполнены условия (10.9) и (10.35). Тогда

$$C_{ea}(\Phi) = \max_{S: \text{Tr} SF \leq E} I(S, \Phi). \quad (10.39)$$

Более того, если канал Φ таков, что

$$\sup_S I(S, \Phi) = \infty, \quad (10.40)$$

то максимум в (10.39) достигается на операторе плотности S , для которого ограничение выполнено в форме равенства $\text{Tr} SF = E$.

Доказательство. Рассмотрим отдельно каждое слагаемое в формуле (10.38). Заметим, что в силу леммы 10.2.1 квантовая энтропия полунепрерывна снизу. Поскольку обменную энтропию можно представить в виде $H(S; \Phi) = H(\Phi_E[S])$, где Φ_E — комплементарный канал из пространства системы $\mathcal{H}_A$ в пространство окружения $\mathcal{H}_E$, она также полунепрерывна снизу, и поэтому последнее слагаемое в формуле (10.38) полунепрерывно сверху. Что касается первого слагаемого $H(S)$, то оно непрерывно на множестве $\mathfrak{S}_E = \{S: \text{Tr} SF \leq E\}$ в силу леммы 10.2.1, поскольку ограничивающий оператор F удовлетворяет условию (10.9). Из следствия 10.5.1 вытекает непрерывность второго слагаемого в формуле (10.38), т. е. $H(\Phi[S])$. Более того, это следствие также гарантирует выполнение условия (10.29), а значит, имеет место формула (10.37). Как следует из сказанного выше, взаимная информация (10.38) полунепрерывна сверху на компактном множестве $\mathfrak{S}_E$, а значит, достигает своего максимума.

Для доказательства второго утверждения введем обозначение

$$f_0(E) = \max_{\text{Tr} SF = E} I(S, \Phi)$$

и предположим, что существует S_1 такое, что

$$\text{Tr} S_1 F < E, \quad I(S_1, \Phi) > f_0(E).$$

Из условия (10.40) следует, что найдется S_2 такое, что

$$\text{Tr} S_2 F > E, \quad I(S_2, \Phi) > f_0(E).$$

Тогда, полагая $\lambda = \frac{\text{Tr} S_2 F - E}{\text{Tr} S_2 F - \text{Tr} S_1 F}$, получаем

$$0 < \lambda < 1, \quad \text{Tr}(\lambda S_1 + (1 - \lambda) S_2) F = E$$

и

$$I(\lambda S_1 + (1 - \lambda) S_2, \Phi) \leq f_0(E) < \lambda I(S_1, \Phi) + (1 - \lambda) I(S_2, \Phi),$$

что противоречит вогнутости функции $I(S, \Phi)$. □

§ 10.7. Каналы, разрушающие сцепленность

Состояние $S \in \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ называется *разделимым* (несцепленным), если оно принадлежит выпуклому замыканию (т. е. замыканию выпуклой оболочки) множества всех состояний-произведений $S_1 \otimes S_2 \in \mathfrak{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

Предложение 10.7.1. *Состояние S является разделимым тогда и только тогда, когда оно допускает представление*

$$S = \int_{\mathcal{X}} S_1(x) \otimes S_2(x) \pi(dx), \quad (10.41)$$

где $\pi(dx)$ — борелевская вероятностная мера, а $S_j(x)$, $j = 1, 2$, — борелевские $\mathfrak{S}(\mathcal{H}_j)$ -значные функции на некотором полном сепарабельном метрическом пространстве $\mathcal{X}$.

Доказательство. Состояние S разделимо тогда и только тогда, когда $S = \lim_{n \rightarrow \infty} S_n$, где

$$S_n = \int_{\mathfrak{S}(\mathcal{H}_1)} \int_{\mathfrak{S}(\mathcal{H}_2)} S_1 \otimes S_2 \pi_n(dS_1 dS_2), \quad (10.42)$$

$\{\pi_n\}$ — последовательность борелевских вероятностных мер с конечными носителями.

Пусть S представляется в виде (10.41), тогда, производя замену переменной интегрирования $x \rightarrow S_1(x) \otimes S_2(x)$, можно свести представление (10.41) к виду

$$S = \int_{\mathfrak{S}(\mathcal{H}_1)} \int_{\mathfrak{S}(\mathcal{H}_2)} S_1 \otimes S_2 \pi(dS_1 dS_2), \quad (10.43)$$

где мы используем то же обозначение π для образа исходной меры при данной замене переменной. Отображение $\pi \rightarrow S$ непрерывно относительно слабой сходимости вероятностных мер; это очевидно, если множество операторов плотности снабжено слабой операторной топологией, а в силу леммы 10.1.1 последняя совпадает на этом множестве с топологией ядерной нормы. В силу леммы 10.4.1 найдется последовательность $\{\pi_n\}$ борелевских вероятностных мер с конечными носителями, которая слабо сходится к π . Используя непрерывность отображения $\pi \rightarrow S$, получаем, что $S = \lim_{n \rightarrow \infty} S_n$, где S_n определяется соотношением (10.42), следовательно, состояние S разделимо.

Обратно, пусть состояние S разделимо, тогда $S = \lim_{n \rightarrow \infty} S_n$, где S_n определяется соотношением (10.42). Если мы докажем, что последовательность мер $\{\pi_n\}$ слабо относительно компактна, то отсюда будет следовать представление (10.43), где π — частичный предел этой последовательности. Сходящаяся последовательность $\{S_n\}$ относительно компактна, поэтому в силу теоремы 10.1.1 для любого $\varepsilon > 0$ найдется конечномерный проектор P такой, что $\text{Tr } S_n(I - P) \leq \varepsilon$ для всех n . Для $m = 1, 2, \dots$ обозначим через P_m проектор такой, что $\text{Tr } S_n(I - P_m) \leq 4^{-m}$ и, следовательно,

$$\int \text{Tr}(S_1 \otimes S_2)(I - P_m) \pi_n(dS_1 dS_2) \leq 4^{-m}. \quad (10.44)$$

Введем следующие подмножества в прямом произведении $\mathfrak{S}(\mathcal{H}_1) \times \mathfrak{S}(\mathcal{H}_2)$:

$$K_m = \{(S_1, S_2): \text{Tr}(S_1 \otimes S_2)(I - P_m) \leq \delta^{-1} 2^{-m}\}, \quad \mathcal{K}_\delta = \bigcap_{m \geq 1} K_m,$$

где $\delta > 0$. В силу той же теоремы 10.1.1 множество $\mathcal{K}_\delta$ компактно по построению. Для его дополнения согласно неравенству (10.44) имеем

$$\pi_n(\mathcal{K}_\delta^c) \leq \sum_m \pi_n(K_m^c) \leq \delta \sum_m 2^m \int \text{Tr}(S_1 \otimes S_2)(I - P_m) \pi_n(dS_1 dS_2) \leq \delta.$$

Таким образом, последовательность мер $\{\pi_n\}$ удовлетворяет известному критерию слабой относительной компактности (см. комментарии), что и завершает доказательство теоремы. $\square$

Определение 10.7.1. Канал $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$ называется *каналом, разрушающим сцепленность*, если для любого гильбертова пространства $\mathcal{H}_R$ и любого состояния $S \in \mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_R)$ состояние $(\Phi \otimes \text{Id}_R)[S] \in \mathfrak{S}(\mathcal{H}_B \otimes \mathcal{H}_R)$, где Id_R — тождественный канал в $\mathfrak{T}(\mathcal{H}_R)$, является разделимым.

Для описания структуры таких каналов нам потребуется обобщение понятия наблюдаемой (определение 2.2.1) на случай произвольного множества исходов.

Определение 10.7.2. Пусть $\mathcal{X}$ — измеримое пространство с σ -алгеброй измеримых подмножеств $\mathfrak{B}$. *Наблюдаемой* со значениями в $\mathcal{X}$ называется вероятностная операторнозначная мера на $\mathcal{X}$, т. е. семейство $M = \{M(B), B \in \mathfrak{B}\}$ эрмитовых операторов в $\mathcal{H}$, удовлетворяющее условиям

- 1) $M(B) \geq 0; B \in \mathfrak{B}$;
- 2) $M(\mathcal{X}) = I$;
- 3) для любого счетного разбиения $B = \cup B_j$ ($B_i \cap B_j = \emptyset, i \neq j$) выполняется условие $M(B) = \sum_j M(B_j)$ в смысле слабой сходимости операторов.

Вероятностная операторнозначная мера E называется *спектральной мерой*, если

$$E(B_1 \cap B_2) = E(B_1)E(B_2), \quad B_1, B_2 \in \mathfrak{B}.$$

В этом случае все операторы $E(B)$ являются проекторами, причем проекторы, отвечающие непересекающимся подмножествам, взаимно ортогональны. Соответствующая наблюдаемая называется *четкой*.

Распределение вероятностей наблюдаемой M в состоянии S задается вероятностной мерой

$$\mu_S^M(B) = \text{Tr} SM(B), \quad B \in \mathfrak{B}. \quad (10.45)$$

Отметим, что линейное продолжение аффинного отображения $S \rightarrow \mu_S^M$ можно рассматривать как обобщение понятия квантово-классического (q-c) канала (см. § 6.4).

Задача 10.7.1. Докажите, что формула (10.45) задает вероятностную меру на $\mathfrak{B}$.

Теорема 10.7.1. Канал Φ разрушает сцепленность тогда и только тогда, когда найдутся полное сепарабельное метрическое пространство $\mathcal{X}$, борелевская $\mathfrak{S}(\mathcal{H}_B)$ -значная функция $S_B(x)$ и наблюдаемая M в $\mathcal{H}_A$ с множеством исходов $\mathcal{X}$, задаваемая вероятностной операторнозначной мерой $M(dx)$, такие, что

$$\Phi[S] = \int_{\mathcal{X}} S_B(x) \mu_S^M(dx). \quad (10.46)$$

Соотношение (10.46) является континуальной версией представления (6.27), а утверждение можно рассматривать как бесконечномерное обобщение предложения 6.4.1. Таким образом, и в бесконечномерном случае квантовый канал, разрушающий сцепленность, является композицией q -с-канала (измерение наблюдаемой M) и s - q -канала (приготавливающего состояние $S_B(x)$ в зависимости от исхода измерения).

Набросок доказательства. Предположим, что канал имеет вид (10.46). Рассмотрим состояние $\omega \in \mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_R)$. Тогда

$$(\Phi \otimes \text{Id}_R)(\omega) = \int_{\mathcal{X}} S_B(x) \otimes m_\omega(dx), \quad (10.47)$$

где

$$m_\omega(B) = \text{Tr}_A \omega(M(B) \otimes I_R), \quad B \subseteq \mathcal{X}.$$

Любой матричный элемент операторнозначной меры m_ω (в фиксированном базисе) является комплексной мерой на $\mathcal{X}$, абсолютно непрерывной относительно вероятностной меры $\mu_\omega(B) = \text{Tr} m_\omega(B)$, $B \subseteq \mathcal{X}$. Из теоремы Радона—Никодима вытекает представление

$$m_\omega(B) = \int_B \sigma_\omega(x) \mu_\omega(dx),$$

где $\sigma_\omega(x)$ — функция на $\mathcal{X}$ со значениями в $\mathfrak{S}(\mathcal{K})$. Используя это представление, мы можем переписать равенство (10.47) в виде

$$(\Phi \otimes \text{Id}_\mathcal{K})(\omega) = \int_{\mathcal{X}} S'(x) \otimes \sigma_\omega(x) \mu_\omega(dx), \quad (10.48)$$

а это разделимое состояние согласно предложению 10.7.1.

Обратно, пусть Φ — канал, разрушающий сцепленность. Фиксируем невырожденное состояние S_A в $\mathfrak{S}(\mathcal{H}_A)$, и пусть $\{|e_j\rangle, j = 1, \dots\}$ — базис собственных векторов оператора S_A с соответствующими (положительными) собственными значениями $\{\lambda_j\}$. Рассмотрим единичный вектор

$$|\Omega\rangle = \sum_{j=1}^{+\infty} \sqrt{\lambda_j} |e_j\rangle \otimes |e_j\rangle$$

в пространстве $\mathcal{H}_A \otimes \mathcal{H}_A$, тогда $|\Omega\rangle\langle\Omega|$ является очищением состояния S_A . Поскольку Φ разрушает сцепленность, состояние

$$S_{AB} = (\text{Id}_A \otimes \Phi)[|\Omega\rangle\langle\Omega|] \quad (10.49)$$

в $\mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ является разделимым. В силу представления (10.41) найдется вероятностная мера π на $\mathfrak{S}(\mathcal{H}_A) \times \mathfrak{S}(\mathcal{H}_B)$ такая, что

$$(\text{Id}_A \otimes \Phi)(|\Omega\rangle\langle\Omega|) = \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} S_A \otimes S_B \pi(dS_A dS_B). \quad (10.50)$$

Отсюда вытекает, что

$$\begin{aligned} \sigma &= \text{Tr}_B(\text{Id}_{\mathcal{H}_A} \otimes \Phi)(|\Omega\rangle\langle\Omega|) = \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} S_A \pi(dS_A dS_B) = \\ &= \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} \bar{S}_A \pi(dS_A dS_B), \end{aligned} \quad (10.51)$$

где черта обозначает комплексное сопряжение в базисе $\{|e_i\rangle\}$. В силу этого равенства для любого борелевского множества $B \subseteq \mathfrak{S}(\mathcal{H}_B)$ оператор

$$M(B) = \sigma^{-1/2} \left[\int_{\mathfrak{S}(\mathcal{H}_A)} \int_B \bar{S}_A \pi(dS_A dS_B) \right] \sigma^{-1/2} \quad (10.52)$$

может быть корректно определен как ограниченный положительный оператор в $\mathcal{H}_A$ такой, что $M(B) \leq M(\mathcal{X}) = I_A$. Нетрудно убедиться, что M является наблюдаемой с исходами в $\mathcal{X} = \mathfrak{S}(\mathcal{H}_B)$.

Теперь рассмотрим канал, разрушающий сцепленность,

$$\widehat{\Phi}(S) = \int_{\mathfrak{S}(\mathcal{H}_B)} S_B \mu_S^M(dS_B),$$

и покажем, что $\Phi(S) = \widehat{\Phi}(S)$. Для этого достаточно проверить, что

$$\widehat{\Phi}(|e_i\rangle\langle e_j|) = \Phi(|e_i\rangle\langle e_j|)$$

для всех i, j . Однако

$$\begin{aligned} \widehat{\Phi}(|e_i\rangle\langle e_j|) &= \int_{\mathfrak{S}(\mathcal{H}_B)} S_B \langle e_j | M(dS_B) | e_i \rangle = \\ &= \lambda_i^{-1/2} \lambda_j^{-1/2} \int_{\mathfrak{S}(\mathcal{H}_A)} \int_{\mathfrak{S}(\mathcal{H}_B)} \langle e_i | S_A | e_j \rangle S_B \pi(dS_A dS_B) = \Phi(e_{ij}), \end{aligned}$$

где

$$e_{ij} = \lambda_i^{-1/2} \lambda_j^{-1/2} \text{Tr}_A(|e_j\rangle\langle e_i| \otimes I_A) |\Omega\rangle\langle\Omega| = |e_i\rangle\langle e_j|.$$

□

Как было показано в п. 8.3.3, в конечномерном случае каналы, разрушающие сцепленность, образуют обширный класс, для которого выполняется гипотеза аддитивности. Этот факт обобщается и на бесконечномерный случай.

Предложение 10.7.2. Пусть имеются два канала Φ_1, Φ_2 с соответствующими ограничениями F_1, F_2 , удовлетворяющие условиям следствия 10.5.1, причем Φ_1 — канал, разрушающий сцепленность. Тогда выполняются все свойства аддитивности (8.35), (8.33) и (8.39). В частности, классическая пропускная способность канала Φ , разрушающего сцепленность, равна

$$C(\Phi, F, E) = C_\chi(\Phi, F, E).$$

Доказательство этого предложения получается обобщением рассуждений в конечномерном случае (предложение 8.3.4) с заменой сумм на интегралы и ансамблей на обобщенные ансамбли и с учетом того обстоятельства, что условия следствия 10.5.1 гарантируют конечность всех входящих в рассмотрение энтропий. Приведем также без доказательства обобщение следствия 9.3.1, касающегося квантовой пропускной способности.

Предложение 10.7.3. Всякий канал в сепарабельном гильбертовом пространстве, разрушающий сцепленность, является антидеградируемым и, следовательно, имеет нулевую квантовую пропускную способность.

§ 10.8. Приложение: спектральное разложение

Пусть $\mathcal{H}$ — сепарабельное гильбертово пространство, и пусть $\{E(B); B \in \mathcal{B}(\mathbb{R})\}$ — спектральная мера на $\mathbb{R}$, где $\mathcal{B}(\mathbb{R})$ — σ -алгебра борелевских подмножеств. Согласно определению 10.7.2 спектральная мера E задает четкую вещественную наблюдаемую. Как объясняется ниже, такие наблюдаемые находятся во взаимно однозначном соответствии с самосопряженными операторами в $\mathcal{H}$.

Для любого единичного вектора $\psi \in \mathcal{H}$ соотношение

$$\mu_\psi(B) = \langle \psi | E(B) | \psi \rangle$$

определяет борелевскую вероятностную меру на $\mathbb{R}$. Если $f(x)$ — борелевская функция на $\mathbb{R}$, то интеграл $X_f = \int_{-\infty}^{\infty} f(x) E(dx)$ сходится сильно на плотной области

$$\mathcal{D}(X_f) = \left\{ \psi : \int_{-\infty}^{\infty} |f(x)|^2 \mu_\psi(dx) < \infty \right\}$$

и, таким образом, однозначно определяет линейный оператор с областью определения $\mathcal{D}(X_f)$. (Напомним, что сильная сходимость последовательности операторов $\{X_n\}$ к оператору X на области $\mathcal{D}$ означает, что $\lim_{n \rightarrow \infty} \|X_n \psi - X \psi\| = 0$ для $\psi \in \mathcal{D}$, а если $\mathcal{D} = \mathcal{H}$, то такая сходимость называется сильной сходимостью операторов.)

В самом деле, если $f(x) = \sum_{i=1}^{\infty} f_i 1_{B_i}(x)$ — функция с конечным или счетным множеством значений (здесь $\{B_i\}$ — измеримое разбиение пространства $\mathbb{R}$), то полагаем

$$X_f = \sum_{i=1}^{\infty} f_i E(B_i),$$

так что

$$\|X_f \psi\|^2 = \sum_{i=1}^{\infty} |f_i|^2 \mu_{\psi}(B_i).$$

Это определение можно расширить на произвольную борелевскую функцию $f(x)$, равномерно приближая ее функциями со счетным множеством значений. В частности, для функции $f(x) = x$ получаем оператор

$$X = \int_{-\infty}^{\infty} x E(dx) \quad (10.53)$$

с областью определения

$$\mathcal{D}(X) = \left\{ \psi: \int_{-\infty}^{\infty} |x|^2 \mu_{\psi}(dx) < \infty \right\},$$

для которого

$$\langle \psi | X | \psi \rangle = \int_{-\infty}^{\infty} x \mu_{\psi}(dx), \quad \|X \psi\|^2 = \int_{-\infty}^{\infty} |x|^2 \mu_{\psi}(dx), \quad \psi \in \mathcal{D}(X). \quad (10.54)$$

Часто приходится иметь дело с *существенно самосопряженными* операторами, которые заданы не на максимальной области определения, но однозначно продолжаются до самосопряженных [24]. *Спектральная теорема* утверждает, что для любого самосопряженного оператора X существует единственная спектральная мера E на $\mathbb{R}$, для которой имеют место соотношения (10.53), (10.54). Таким образом, самосопряженные операторы — это в точности те, которые имеют спектральное разложение со спектром в $\mathbb{R}$ и поэтому естественно ассоциируются с (четкими) вещественными наблюдаемыми в бесконечномерном случае. Мера μ_{ψ} дает

распределение вероятностей наблюдаемой X в чистом состоянии $|\psi\rangle\langle\psi|$, а формулы (10.54) — первый и второй моменты наблюдаемой X .

В определенном смысле, который мы не будем здесь подробно раскрывать, имеют место соотношения $X_f = f(X)$ и $X_{fg} = X_f X_g$. Рассмотрим случай экспоненты:

$$V_t = \int_{-\infty}^{\infty} \exp(itx) E(dx) = \exp itX.$$

Тогда семейство $\{V_t; t \in \mathbb{R}\}$ является (сильно непрерывной) группой унитарных операторов с инфинитезимальным генератором X :

$$\lim_{t \rightarrow 0} t^{-1}(V_t - I)|\psi\rangle = iX|\psi\rangle, \quad \psi \in \mathcal{D}(X).$$

Если оператор X ограничен, то $\exp itX$ определяется соответствующим степенным рядом, сходящимся по норме к V_t .

Обратно, всякая сильно непрерывная группа унитарных операторов $\{V_t; t \in \mathbb{R}\}$ имеет вид $V_t = \exp itX$, где X — однозначно определенный самосопряженный оператор. Это утверждение составляет содержание *теоремы Стоуна*.

Задача 10.8.1. 1. Пусть $\mathcal{H} = L^2(\mathbb{R})$ — гильбертово пространство квадратично интегрируемых функций $\psi(\xi)$, $\xi \in \mathbb{R}$, и семейство $E = \{E(B); B \in \mathcal{B}(\mathbb{R})\}$ определено соотношением

$$(E(B)\psi)(\xi) = 1_B(\xi)\psi(\xi), \quad \psi \in \mathcal{H}.$$

Докажите, что E — спектральная мера оператора X умножения на ξ , V_t — оператор умножения на $\exp it\xi$ и, вообще, X_f — оператор умножения на $f(\xi)$.

2. Рассмотрим унитарный оператор в $\mathcal{H}$, определяемый преобразованием Фурье

$$(\tilde{F}\psi)(\lambda) = \frac{1}{\sqrt{2\pi}} \int \exp(-i\lambda\xi)\psi(\xi)d\xi.$$

Докажите, что $\tilde{E}(B) = \tilde{F}^* E(B) \tilde{F}$ — спектральная мера на $\mathbb{R}$, которой отвечает самосопряженный оператор $\tilde{X} = \frac{1}{i} \frac{d}{d\xi}$, порождающий группу унитарных операторов

$$(\tilde{V}_t\psi)(\xi) = \psi(\xi + t).$$

Самосопряженные операторы A_j , $j = 1, \dots, s$, называются *коммутирующими*, если коммутируют их спектральные меры. Имеет место следующее многомерное обобщение теоремы Стоуна.

Теорема 10.8.1. Пусть V_x , $x = [x_1, \dots, x_s] \in \mathbb{R}^s$, — сильно непрерывная группа унитарных операторов в сепарабельном гильбертовом пространстве $\mathcal{H}$. Тогда существует такое семейство A_j , $j = 1, \dots, s$, коммутирующих самосопряженных операторов в $\mathcal{H}$, что

$$V_x = \exp\left(i \sum_{j=1}^s x_j A_j\right). \quad (10.55)$$

Обратно, для всякого семейства A_j , $j = 1, \dots, s$, коммутирующих самосопряженных операторов в $\mathcal{H}$ формула (10.55) определяет сильно непрерывную унитарную группу в $\mathcal{H}$.

§ 10.9. Комментарии

1. Первая попытка математически строгого рассмотрения основных понятий квантовой механики в сепарабельном гильбертовом пространстве была сделана в классической монографии фон Неймана [21]. В частности, было подчеркнуто различие между эрмитовыми (симметрическими) и самосопряженными операторами, на которое не обращалось внимания в предшествующих работах физиков, и отмечена ключевая роль самосопряженности для спектрального разложения операторов. Другой важный круг вопросов связан с понятием следа и ядерных операторов. Современное рассмотрение этих вопросов в связи с приложениями к квантовой теории имеется в книгах [24, 37, 73].

Лемма 10.1.1 получена Дель'Антонио в работе [74], см. также приложение в книге Дэвиса [73]. Критерий компактности для подмножеств квантовых состояний представляет собой модификацию результата, полученного Т. А. Сарымсаковым (см. [26]) и названного им «некоммутативной теоремой Прохорова». Последняя дает критерий слабой компактности семейств вероятностных мер на метрических пространствах (см. [131]) и используется в § 10.4. По поводу компактности единичного шара в $\mathfrak{B}(\mathcal{H})$ в слабой операторной топологии см., например, книгу [24].

2. Хорошо известно, что свойства энтропии в бесконечномерном случае существенно отличаются от конечномерного: в последнем случае энтропия — ограниченная непрерывная функция на $\mathfrak{S}(\mathcal{H})$, тогда как в бесконечномерном случае она разрывна всюду и бесконечна «почти всюду» в том смысле, что множество состояний с конечной энтропией является подмножеством первой категории в $\mathfrak{S}(\mathcal{H})$, см. обзор Верля [152], где получен ряд полезных свойств энтропии и относительной энтропии, включая теорему 10.2.1 и лемму 10.2.1. В этом обзоре можно также найти ссылки на оригинальные работы Либа, Рускаи, Саймона и других авторов, кото-

рые внесли значительный вклад в изучение свойств квантовой энтропии. Новые результаты о свойствах квантовой энтропии, в частности удобные условия непрерывности, получены в работе М. Е. Широкова [45].

3. Важность рассмотрения входных ограничений для квантовых каналов была понятна с момента появления идеи квантовых коммуникаций; подробное физическое обсуждение вопроса об определении пропускной способности квантовых оптических каналов с ограничением на среднюю энергию входного сигнала см. в обзоре [68]. Исследование классической пропускной способности s - q -канала с ограничением основано на работах А. С. Холево [35, 42]. В них используется модификация случайного кодирования (10.20), которая была предложена для соответствующей классической задачи. Другие подходы рассматривались Винтером (см. [156]) и Хайаши (см. [90]).

4. Каналы с непрерывным алфавитом рассматривались в работах А. С. Холево [42], а также А. С. Холево и М. Е. Широкова [43], где систематически использовалось понятие обобщенного ансамбля. Доказательства необходимых фактов из теории вероятностных мер на метрических пространствах, таких как задача 10.4.1 и лемма 10.4.1, можно найти в монографии Партасарати [131].

5. Доказательство ограниченности отображения Φ в задаче 10.5.1 см. в книге [73, лемма 2.2.1]. Рассмотрение χ -пропускной способности квантовых каналов с ограничениями основано на работах [42, 43]. обстоятельное исследование свойств χ -пропускной способности и других энтропийных характеристик бесконечномерных каналов без предположений типа конечности выходной энтропии было проведено М. Е. Широковым в работах [46, 140].

6. Этот параграф основан на результатах работы [42].

7. Концепция квантовой наблюдаемой как вероятностной операторнозначной меры подробно излагается в книгах [36, 37]. Теорема 10.7.1 доказана в работе А. С. Холево, М. Е. Широкова и Р. Ф. Вернера [39]. По поводу доказательства предложений 10.7.2, 10.7.3 см. статью [105].

8. Спектральная теорема для самосопряженных операторов в сепарабельном гильбертовом пространстве, теорема Стоуна и связанные с этим вопросы подробно рассматриваются в книге Рида и Саймона [24].

ГЛАВА 11

Гауссовские системы

Фундаментальным физическим носителем информации является электромагнитное поле, в частности свет и радиоволны. С математической точки зрения излучение эквивалентно ансамблю осцилляторов. В квантовой оптике рассматриваются квантованные поля и, следовательно, квантовые осцилляторы. Это типичная бозонная квантовая система с «непрерывными переменными», в которой основные наблюдаемые (амплитуды осцилляторов) удовлетворяют каноническим коммутационным соотношениям (ККС). Многие из современных экспериментов по обработке квантовой информации реализованы именно в таких системах.

Имеется особенно важный класс состояний бозонной системы, которые естественно соответствуют классическим гауссовским распределениям. С физической точки зрения этот класс содержит состояния теплового равновесия, а также когерентные и сжатые состояния, реализуемые в лазерах и «нелинейных» квантовых оптических приборах. С математической точки зрения эти состояния полностью характеризуются, аналогично классическим гауссовским распределениям, средним значением и матрицей ковариаций. При рассмотрении конечного числа осцилляторных мод, что является обычным приближением в квантовой оптике, возможно описание таких состояний с помощью методов конечномерной линейной алгебры.

В связи с бозонными системами и ККС неизбежно возникают аналитические сложности, связанные с бесконечной размерностью и неограниченностью некоторых операторов. Мы будем уделять основное внимание тем вопросам, которые имеют первостепенное значение с точки зрения квантовой теории информации, иногда обращаясь с неограниченными операторами достаточно бегло. Более детальное математическое рассмотрение таких вопросов можно при желании найти в соответствующей литературе (см. комментарии).

§ 11.1. Операторы, ассоциированные с коммутационным соотношением Гейзенберга

В гильбертовом пространстве $\mathcal{H} = L^2(\mathbb{R})$ рассмотрим операторы

$$(q\psi)(\xi) = \xi\psi(\xi), \quad (p\psi)(\xi) = \frac{\hbar}{i} \frac{d}{d\xi}\psi(\xi),$$

заданные на общей области определения $\mathcal{D}$, в качестве которой можно взять пространство $\mathcal{S}(\mathbb{R})$ бесконечно дифференцируемых функций, все производные которых убывают на бесконечности быстрее, чем любая степень функции $|\xi|$. Эти операторы являются существенно самосопряженными, следовательно, представляют (четкие) вещественные наблюдаемые (см. § 10.8).

На указанной области определения операторы q и p удовлетворяют коммутационному соотношению Гейзенберга

$$[q, p] = i\hbar I. \quad (11.1)$$

Рассмотрим чистое состояние $|\psi\rangle\langle\psi|$, $\psi \in \mathcal{D}$, и введем обозначения

$$x = \langle\psi|q|\psi\rangle, \quad y = \langle\psi|p|\psi\rangle,$$

$$D_\psi(q) = \|(q - x)\psi\|^2, \quad D_\psi(p) = \|(p - y)\psi\|^2$$

для средних значений и дисперсий наблюдаемых q , p . Для любого вещественного числа ω имеем

$$\begin{aligned} \omega^2 D_\psi(q) - \omega\hbar + D_\psi(p) &= \omega^2 D_\psi(q) + i\omega\langle\psi|[q, p]|\psi\rangle + D_\psi(p) = \\ &= \|[\omega(q - x) + i(p - y)]\psi\|^2 \geq 0, \end{aligned}$$

следовательно,

$$D_\psi(q)D_\psi(p) \geq \frac{\hbar^2}{4}, \quad (11.2)$$

причем равенство достигается тогда и только тогда, когда найдется ω такое, что ψ является решением дифференциального уравнения

$$\left[\omega(\xi - x) + \left(\hbar \frac{d}{d\xi} - iy \right) \right] \psi(\xi) = 0, \quad (11.3)$$

нормированное решение которого существует при $\omega > 0$ и имеет вид

$$\psi(\xi) = \frac{k}{\sqrt[4]{\pi\hbar/\omega}} \exp \left[\frac{iy\xi}{\hbar} - \frac{\omega(\xi - x)^2}{2\hbar} \right], \quad (11.4)$$

где $|k| = 1$.

Неравенство (11.2) есть *соотношение неопределенностей Гейзенберга*, а формула (11.4) описывает векторы состояний *минимальной*

неопределенности, для которых $D_\psi(q) = \frac{\hbar}{2\omega}$, $D_\psi(p) = \frac{\omega\hbar}{2}$. Далее полагаем $k = \exp\left(-\frac{ixy}{2\hbar}\right)$, что приводит к равенству

$$\psi(\xi) = \sqrt[4]{\frac{\omega}{\pi\hbar}} \exp\left[\frac{iy}{\hbar}\left(\xi - \frac{x}{2}\right) - \frac{\omega(\xi - x)^2}{2\hbar}\right]. \quad (11.5)$$

Вводя комплексные комбинации

$$a = \frac{1}{\sqrt{2\hbar\omega}}(\omega q + ip), \quad \zeta = \frac{1}{\sqrt{2\hbar\omega}}(\omega x + iy)$$

и обозначая соответствующий вектор состояния (11.5) через $|\zeta\rangle$, можно переписать определяющее уравнение (11.3) в виде

$$a|\zeta\rangle = \zeta|\zeta\rangle, \quad \zeta \in \mathbb{C}. \quad (11.6)$$

В частности,

$$a|0\rangle = 0, \quad (11.7)$$

где $|0\rangle$ — вектор, соответствующий функции

$$\psi(\xi) = \sqrt[4]{\frac{\omega}{\pi\hbar}} \exp\left[-\frac{\omega\xi^2}{2\hbar}\right].$$

Оператор $a = \frac{1}{\sqrt{2\hbar\omega}}(\omega q + ip)$ имеет сопряженный $a^\dagger = \frac{1}{\sqrt{2\hbar\omega}}(\omega q - ip)$, а коммутационное соотношение (11.1) принимает вид

$$[a, a^\dagger] = I.$$

Рассмотрим оператор

$$\mathcal{N} = a^\dagger a = aa^\dagger - I, \quad (11.8)$$

который является симметричным и существенно самосопряженным на $\mathcal{D}$. В силу соотношения (11.7) имеем

$$\mathcal{N}|0\rangle = 0.$$

Задача 11.1.1. Последовательно применяя равенство (11.8), покажите, что векторы

$$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle \quad (11.9)$$

образуют ортонормированную систему собственных векторов оператора $\mathcal{N}$:

$$\mathcal{N}|n\rangle = n|n\rangle, \quad n = 0, 1, \dots$$

Соответствующие собственные функции в $L^2(\mathbb{R})$ с точностью до нормировки имеют вид

$$\left[\omega\xi - \hbar\frac{d}{d\xi}\right]^n \exp\left[-\frac{\omega\xi^2}{2\hbar}\right] \simeq H_n\left(\sqrt{\frac{\omega}{\hbar}}\xi\right) \exp\left[-\frac{\omega\xi^2}{2\hbar}\right],$$

где H_n , $n=0, 1, \dots$, — полиномы Эрмита, которые образуют полную систему в $L^2(\mathbb{R})$. Следовательно, $\{|n\rangle; n=0, 1, \dots\}$ — ортонормированный базис в $\mathcal{H}$,

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = I$$

и $\mathcal{N}$ имеет спектральное разложение

$$\mathcal{N} = \sum_{n=0}^{\infty} n|n\rangle\langle n|. \quad (11.10)$$

Задача 11.1.2. Покажите, что $\mathcal{N}$ — самосопряженный оператор типа $\mathfrak{F}$ с областью определения

$$\mathcal{D}(\mathcal{N}) = \left\{ \psi: \sum_{n=0}^{\infty} n^2 |\langle n|\psi\rangle|^2 < \infty \right\}$$

и соотношение (11.10) выполнено в смысле сильной сходимости на $\mathcal{D}(\mathcal{N})$.

Имеют место соотношения

$$a|n\rangle = \sqrt{n}|n-1\rangle, \quad a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle.$$

Вводя группу унитарных операторов $\{e^{iN\omega t}; t \in \mathbb{R}\}$, получаем

$$e^{iN\omega t} a e^{-iN\omega t} = a e^{-i\omega t}, \quad e^{iN\omega t} a^\dagger e^{-iN\omega t} = a^\dagger e^{i\omega t}. \quad (11.11)$$

Возвращаясь к операторам q , p , видим, что

$$\hbar\omega\left(\mathcal{N} + \frac{1}{2}\right) = \frac{1}{2}(\omega^2 q^2 + p^2) \equiv \hbar H \quad (11.12)$$

— оператор энергии квантового гармонического осциллятора с частотой ω и уравнения (11.11) описывают динамику осциллятора с гамильтонианом H . Оператор $\mathcal{N}$ называется оператором числа квантов, $|n\rangle$ — вектором состояния с n квантами, $|0\rangle$ — вектором вакуумного состояния, оператор a (соответственно $a^\dagger$) — оператором уничтожения (соответственно рождения) квантов. В квантовой оптике операторы a , $a^\dagger$ описывают одну гармонику (моду) поля, соответствующую определенной частоте ω (а также определенной поляризации).

Состояния $|\zeta\rangle\langle\zeta|$, $\zeta \in \mathbb{C}$, называются в квантовой оптике *когерентными*. Из соотношений (11.9), (11.6) получаем

$$\langle n|\zeta\rangle = \frac{1}{\sqrt{n!}}\langle 0|a^n\zeta\rangle = \frac{\zeta^n}{\sqrt{n!}}\langle 0|\zeta\rangle = \frac{\zeta^n}{\sqrt{n!}}\exp\left(-\frac{|\zeta|^2}{2}\right),$$

где также была использована формула

$$\langle\zeta_1|\zeta_2\rangle = \exp\left[-\frac{1}{2}(|\zeta_1|^2 + |\zeta_2|^2 - 2\bar{\zeta}_1\zeta_2)\right]. \quad (11.13)$$

Задача 11.1.3. Докажите равенство (11.13), используя вещественную параметризацию (11.5) векторов $|\zeta\rangle$.

Задача 11.1.4. Докажите, что система векторов $\{|\zeta\rangle; \zeta \in \mathbb{C}\}$ является переполненной в том смысле, что

$$\frac{1}{\pi} \int |\zeta\rangle\langle\zeta| d^2\zeta = I,$$

где $d^2\zeta = \frac{1}{2\hbar} dx dy$. *Указание.* Матричные элементы интеграла в базисе $\{|n\rangle\}$ имеют вид

$$\frac{1}{\pi} \int \frac{\zeta^n}{\sqrt{n!}} \frac{\bar{\zeta}^m}{\sqrt{m!}} \exp(-|\zeta|^2) d^2\zeta = \delta_{nm}.$$

Пусть $p(\zeta)$ — плотность распределения вероятностей на $\mathbb{C}$. Тогда

$$S = \int |\zeta\rangle\langle\zeta| p(\zeta) d^2\zeta \quad (11.14)$$

— оператор плотности в $\mathcal{H}$, который соответствует *квазиклассическому* состоянию. В частности, для комплексного гауссовского распределения с нулевым средним и дисперсией N получаем оператор плотности

$$S_0 = \frac{1}{\pi N} \int |\zeta\rangle\langle\zeta| \exp\left(-\frac{|\zeta|^2}{N}\right) d^2\zeta \quad (11.15)$$

с матричными элементами

$$\langle n|S_0|m\rangle = \frac{1}{\pi N} \int \frac{\zeta^n}{\sqrt{n!}} \frac{\bar{\zeta}^m}{\sqrt{m!}} \exp\left(-\frac{(N+1)|\zeta|^2}{N}\right) d^2\zeta = \delta_{nm} \frac{1}{N+1} \left(\frac{N}{N+1}\right)^n.$$

Поэтому S_0 имеет спектральное разложение

$$S_0 = \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1}\right)^n |n\rangle\langle n|. \quad (11.16)$$

Это выражение имеет смысл и при $N=0$, когда S_0 определяется вырожденным распределением, сосредоточенным в точке $\zeta=0$.

Учитывая спектральное разложение (11.10) и равенство (11.12), последнее соотношение можно переписать в виде

$$S_0 = \frac{\exp[-\theta H]}{\text{Tr} \exp[-\theta H]}, \quad (11.17)$$

а это есть оператор плотности гиббсовского состояния квантового гармонического осциллятора, т. е. равновесного состояния при обратной температуре $\theta/\hbar = \frac{1}{\hbar\omega} \ln \frac{N+1}{N}$. Величина $N = \text{Tr} S_0 \mathcal{N} = \text{Tr} S_0 a^\dagger a$ интерпретируется как среднее число квантов энергии осциллятора.

Другой важный оператор плотности соответствует смещенной плотности распределения

$$S_\mu = \frac{1}{\pi N} \int |\zeta\rangle\langle\zeta| \exp\left(-\frac{|\zeta-\mu|^2}{N}\right) d^2\zeta, \quad (11.18)$$

где $\mu = \frac{1}{\sqrt{2\hbar\omega}}(\omega m_q + i m_p)$. Введем унитарные операторы

$$D(\zeta)\psi(\xi) = \exp\left[\frac{iy}{\hbar}\left(\xi - \frac{x}{2}\right)\right]\psi(\xi - x). \quad (11.19)$$

Очевидно, что

$$|\zeta\rangle = D(\zeta)|0\rangle, \quad D(\zeta_2)|\zeta_1\rangle = \exp(i \text{Im} \bar{\zeta}_1 \zeta_2)|\zeta_1 + \zeta_2\rangle,$$

т. е. действие этих операторов приводит к смещению средних значений наблюдаемых q , p . В физическом эксперименте такое смещение происходит при внешнем воздействии, осуществляемом идеальным лазером, которое преобразует вакуум $|0\rangle\langle 0|$ в когерентное состояние $|\zeta\rangle\langle\zeta|$. Квазиклассическое состояние (11.14) представляет собой статистическую смесь когерентных состояний, тогда как

$$S_\mu = D(\mu)S_0D(\mu)^* \quad (11.20)$$

есть преобразование равновесного состояния S_0 при внешнем воздействии. Заметим, что состояние S_μ является чистым тогда и только тогда, когда $N = 0$, причем в этом случае оно совпадает с когерентным состоянием $|\mu\rangle\langle\mu|$.

Задача 11.1.5. Докажите, что операторы смещения удовлетворяют коммутационному соотношению

$$D(\zeta_2)D(\zeta_1) = \exp(i \text{Im} \bar{\zeta}_1 \zeta_2)D(\zeta_1 + \zeta_2), \quad (11.21)$$

из которого следует равенство

$$D(\mu)^*D(\zeta)D(\mu) = \exp(2i \text{Im} \bar{\mu}\zeta)D(\zeta). \quad (11.22)$$

В дальнейшем нам понадобится некоммутативный аналог характеристической функции для состояния S_μ :

$$\mathrm{Tr} S_\mu D(\zeta) = \exp \left[2i \operatorname{Im} \bar{\mu} \zeta - \left(N + \frac{1}{2} \right) |\zeta|^2 \right]. \quad (11.23)$$

Доказательство формулы (11.23). В силу соотношений (11.20), (11.22) имеем

$$\mathrm{Tr} S_\mu D(\zeta) = \exp(2i \operatorname{Im} \bar{\mu} \zeta) \mathrm{Tr} S_0 D(\zeta),$$

и достаточно доказать равенство (11.23) для $\mu = 0$. Имеем

$$\begin{aligned} \mathrm{Tr} S_0 D(\zeta) &= \int \langle \zeta_1 | D(\zeta) | \zeta_1 \rangle \frac{1}{\pi N} \exp \left(-\frac{|\zeta_1|^2}{N} \right) d^2 \zeta_1 = \\ &= \int \langle 0 | D(\zeta_1)^* D(\zeta) D(\zeta_1) | 0 \rangle \frac{1}{\pi N} \exp \left(-\frac{|\zeta_1|^2}{N} \right) d^2 \zeta_1 = \\ &= \int \exp(i \operatorname{Im} \bar{\zeta}_1 \zeta) \langle 0 | D(\zeta) | 0 \rangle \frac{1}{\pi N} \exp \left(-\frac{|\zeta_1|^2}{N} \right) d^2 \zeta_1. \end{aligned} \quad (11.24)$$

Используя равенство (11.13), получаем

$$\langle 0 | D(\zeta) | 0 \rangle = \langle 0 | \zeta \rangle = \exp \left(-\frac{1}{2} |\zeta|^2 \right).$$

Подставляя это выражение в формулу (11.24) и используя выражение для характеристической функции гауссовского распределения, получаем

$$\mathrm{Tr} S_0 D(\zeta) = \exp \left(-\left(N + \frac{1}{2} \right) |\zeta|^2 \right). \quad \square$$

§ 11.2. Канонические коммутационные соотношения

В квантовой механике канонические коммутационные соотношения (ККС) возникают при квантовании классической системы с конечным либо бесконечным числом степеней свободы, т. е. поля. В квантовой оптике обычно имеют дело только с конечным набором существенных частот, что сводит проблему к рассмотрению системы с конечным числом s степеней свободы.

Рассмотрим гильбертово пространство $\mathcal{H} = L^2(\mathbb{R}^s)$ комплексных квадратично интегрируемых функций вещественных переменных ξ_j , $j = 1, \dots, s$, где $\mathbb{R}^s$ является координатным пространством рассматриваемой классической системы. В пространстве $\mathcal{H}$ зададим две группы унитарных операторов

$$V_x \psi(\xi) = \exp(i \xi^\top x) \psi(\xi), \quad U_y \psi(\xi) = \psi(\xi + \hbar y), \quad (11.25)$$

где $\xi, x, y \in \mathbb{R}^s$ рассматриваются как вектор-столбцы, а $^\top$ обозначает транспонирование. Эти группы удовлетворяют каноническим коммутационным соотношениям (ККС) Вейля

$$U_y V_x = \exp(i\hbar y^\top x) V_x U_y. \quad (11.26)$$

Отметим аналогию с дискретными операторами Вейля, определенными соотношениями (6.47). Операторы U_y, V_x описывают изменение квантового состояния при смещении координаты (соответственно импульса), а соотношения Вейля задают кинематику квантовомеханической системы.

Чтобы использовать очевидную симметрию между x, y , введем вектор-столбец вещественных параметров $z = [x_1, y_1, \dots, x_s, y_s]^\top$ и унитарные операторы

$$W(z) = \exp\left(\frac{i}{2}\hbar y^\top x\right) V_x U_y. \quad (11.27)$$

Из соотношений (11.27) и (11.26) следует, что операторы $W(z)$ удовлетворяют *ККС Вейля—Сигала*

$$W(z)W(z') = \exp\left[\frac{i}{2}\Delta(z, z')\right] W(z + z'), \quad (11.28)$$

где

$$\Delta(z, z') = \hbar \sum_{j=1}^s (x'_j y_j - x_j y'_j) \quad (11.29)$$

— каноническая *симплектическая форма*. Из равенства (11.28) и унитарности операторов $W(z)$, в частности, следует, что

$$W(-z) = W(z)^* \quad z \in Z.$$

Из равенства (11.28) следует, что

$$W(z')^* W(z) W(z') = \exp[i\Delta(z, z')] W(z). \quad (11.30)$$

Сходство коммутационных соотношений (11.21) и (11.28) не случайно: на самом деле операторы $W(z)$ с точностью до параметризации представляют собой многомодовое обобщение унитарных операторов смещения.

Задача 11.2.1. Покажите, что в случае одной степени свободы

$$D(\mu) = W(m_p/\hbar, -m_q/\hbar), \quad (11.31)$$

так что

$$D(\mu)^* W(z) D(\mu) = \exp i(m_q x + m_p y) W(z). \quad (11.32)$$

Поскольку $\Delta(z, z) \equiv 0$, из равенства (11.28) вытекает, что для любого фиксированного z однопараметрическое семейство $\{W(tz); t \in \mathbb{R}\}$ является унитарной группой. Согласно теореме Стоуна (см. § 10.8) существует самосопряженный оператор $R(z)$ такой, что

$$W(z) = \exp i R(z). \quad (11.33)$$

Задача 11.2.2. С использованием равенства (11.30) докажите соотношение

$$W(z')^* R(z) W(z') = R(z) + \Delta(z, z') I. \quad (11.34)$$

Задача 11.2.3. Проверьте, что соответствие $z \rightarrow R(z)$ является линейным и что операторы $R(z)$ удовлетворяют коммутационным соотношениям

$$[R(z), R(z')] = -i \Delta(z, z') I. \quad (11.35)$$

Указание. В соотношении (11.28) замените z, z' на tz, sz' и рассмотрите первые и вторую смешанную производные по s, t при $s = t = 0$.

Пространство $Z = \mathbb{R}^{2s}$, снабженное невырожденной кососимметричной формой $\Delta(z, z')$, является *симплектическим пространством*. Симплектическое пространство (Z, Δ) описывает фазовое пространство классической механической системы, квантование которой дается семейством унитарных операторов $W(z)$ в гильбертовом пространстве $\mathcal{H}$. Такое квантование в существенном единственно: всякое неприводимое семейство унитарных операторов $W(z)$ в каком-либо гильбертовом пространстве, удовлетворяющих ККС Вейля—Сигала, унитарно эквивалентно описанному выше представлению в $L^2(\mathbb{R}^s)$, называемому представлением Шрёдингера (теорема единственности Стоуна—фон Неймана, см. комментарии). В дальнейшем считаем, что $W(z), z \in Z$, — некоторое неприводимое представление ККС.

Базис $\{e_j, h_j; j = 1, \dots, s\}$ в Z называется *симплектическим*, если

$$\Delta(e_j, h_k) = -\hbar \delta_{jk}, \quad \Delta(e_j, e_k) = \Delta(h_j, h_k) = 0, \quad j, k = 1, \dots, s. \quad (11.36)$$

В таком базисе симплектическая форма $\Delta(z, z')$ имеет стандартный вид (11.29) и

$$R(z) = Rz = \sum_{j=1}^s (x_j q_j + y_j p_j),$$

где

$$R = [q_1, p_1, \dots, q_s, p_s]$$

— вектор-строка самосопряженных операторов — *канонических наблюдаемых*, удовлетворяющих ККС Гейзенберга

$$[q_j, p_k] = i\delta_{jk}\hbar I, \quad [q_j, q_k] = 0, \quad [p_j, p_k] = 0. \quad (11.37)$$

Представление Шрёдингера ККС (11.37) дается самосопряженными операторами

$$q_j = \xi_j, \quad p_j = \frac{\hbar}{i} \frac{\partial}{\partial \xi_j}$$

в гильбертовом пространстве $L^2(\mathbb{R}^s)$. Операторы q_j, p_j не ограничены, поэтому соотношения (11.37) следует рассматривать только на общей плотной области определения, в качестве которой удобно выбрать пространство $\mathcal{S}(\mathbb{R})$. Мы уже видели, что подход, основанный на использовании ККС Вейля, является более фундаментальным с физической точки зрения. С другой стороны, он также позволяет избежать ряда не относящихся к делу математических патологий, связанных с областями определения неограниченных операторов.

В дальнейшем в пространстве $Z = \mathbb{R}^{2s}$ будут рассматриваться различные билинейные формы $\Delta, \alpha, \dots$, при этом матрицы форм будут обозначаться тем же символом, т.е. $\alpha(z, z') = z^\top \alpha z'$ и т.д. В частности, $\Delta(z, z') = z^\top \Delta z'$, где

$$\Delta = \begin{bmatrix} 0 & -\hbar & & \\ \hbar & 0 & & \\ & & \ddots & \\ & & & 0 & -\hbar \\ & & & \hbar & 0 \end{bmatrix} \equiv \text{diag} \begin{bmatrix} 0 & -\hbar \\ \hbar & 0 \end{bmatrix}. \quad (11.38)$$

Лемма 11.2.1. Пусть $\alpha(z, z') = z^\top \alpha z'$ — произвольное скалярное произведение в симплектическом пространстве (Z, Δ) . Существует симплектический базис $\{e_j, h_j; j = 1, \dots, s\}$ в Z , в котором форма α имеет диагональный вид с матрицей

$$\tilde{\alpha} = \text{diag} \begin{bmatrix} \alpha_j & 0 \\ 0 & \alpha_j \end{bmatrix},$$

причем $\alpha_j > 0$.

Доказательство. Рассмотрим матрицу $\hat{\alpha} = \Delta^{-1}\alpha$, которая является матрицей оператора (обозначаемого тем же символом), связывающего две формы:

$$\alpha(z, z') = \Delta(z, \hat{\alpha} z').$$

Оператор $\hat{\alpha}$ является кососимметричным в евклидовом пространстве (Z, α) : $\hat{\alpha}^* = -\hat{\alpha}$. По известной теореме из линейной алгебры существуют

ортогональный базис $\{e_j, h_j\}$ в (Z, α) и положительные числа $\{\alpha_j\}$ такие, что

$$\hat{\alpha}e_j = -\hbar^{-1}\alpha_j h_j, \quad \hat{\alpha}h_j = \hbar^{-1}\alpha_j e_j.$$

Выбирая нормировку $\alpha(e_j, e_j) = \alpha(h_j, h_j) = \alpha_j$, получаем симплектический базис в (Z, Δ) с требуемыми свойствами. $\square$

Обозначая через T матрицу перехода от исходного симплектического базиса в Z к новому симплектическому базису, т. е. матрицу со столбцами $\{e_j, h_j; j = 1, \dots, s\}$, получаем

$$\Delta = T^\top \Delta T, \quad \tilde{\alpha} = T^\top \alpha T.$$

Канонические наблюдаемые в новом базисе даются соотношениями

$$\tilde{q}_j = R(e_j), \quad \tilde{p}_j = R(h_j), \quad j = 1, \dots, s,$$

так что $RT = \tilde{R}$, где $\tilde{R} = [\tilde{q}_1, \tilde{p}_1, \dots, \tilde{q}_s, \tilde{p}_s]$. Матрица T задает *симплектическое преобразование* в (Z, Δ) , которое характеризуется свойством

$$\Delta(Tz, Tz') = \Delta(z, z'), \quad z, z' \in Z.$$

§ 11.3. Динамика, квадратичные операторы и комплексные структуры

Для любого симплектического преобразования T в Z существует *каноническое унитарное преобразование* U_T в $\mathcal{H}$ такое, что

$$U_T^* W(z) U_T = W(Tz).$$

Это следует из теоремы единственности, поскольку операторы $W(Tz)$, $z \in Z$, также образуют (неприводимое) представление ККС (11.28) в пространстве $\mathcal{H}$. В терминах канонических наблюдаемых имеем

$$U_T^* R U_T = RT. \quad (11.39)$$

Для получения явного выражения для операторов U_T рассмотрим однопараметрическую группу

$$T_t = e^{tD}, \quad t \in \mathbb{R},$$

симплектических преобразований в Z , которая описывает линейную динамику в классическом фазовом пространстве. Здесь D — генератор, который удовлетворяет условию

$$\Delta(T_t z, T_t z') \equiv \Delta(z, z').$$

Будем предполагать, что оператор D является строго Δ -положительным, т. е. $\Delta(z, Dz')$ является скалярным произведением в Z . Отсюда получаем, в матричных обозначениях,

$$\Delta D = -D^\top \Delta \geq 0. \quad (11.40)$$

Квантование линейной динамики T_t дается следующей теоремой.

Теорема 11.3.1. *Рассмотрим оператор энергии $H = \frac{1}{\hbar} R \varepsilon R^\top$ в $\mathcal{H}$, квадратичный относительно канонических наблюдаемых R , где $\varepsilon = -\frac{\hbar}{2} D \Delta^{-1}$. Тогда H — положительный самосопряженный оператор в $\mathcal{H}$, порождающий унитарную группу $\{e^{itH}\}$ в $\mathcal{H}$ такую, что*

$$W(T_t z) = e^{itH} W(z) e^{-itH}. \quad (11.41)$$

Доказательство (набросок). Рассмотрим билинейную форму

$$\varepsilon(z, z') = -z^\top \Delta \varepsilon \Delta z' = \frac{\hbar}{2} \Delta(z, Dz'),$$

которая является скалярным произведением в силу предположения об операторе D . Согласно лемме 11.2.1 существует симплектический базис $\{e_j, h_j\}$, в котором матрица этой формы имеет диагональный вид

$$-\Delta \tilde{\varepsilon} \Delta = \hbar^2 \operatorname{diag} \begin{bmatrix} \omega_j/2 & 0 \\ 0 & \omega_j/2 \end{bmatrix},$$

где $\omega_j > 0$, следовательно,

$$\tilde{\varepsilon} = \operatorname{diag} \begin{bmatrix} \omega_j/2 & 0 \\ 0 & \omega_j/2 \end{bmatrix}.$$

Вводя канонические наблюдаемые $\tilde{q}_j = R(e_j)$, $\tilde{p}_j = R(h_j)$, $j = 1, \dots, s$, получаем

$$H = \sum_{j=1}^s \frac{\omega_j}{2\hbar} (\tilde{q}_j^2 + \tilde{p}_j^2), \quad (11.42)$$

откуда видно, что H — положительный самосопряженный оператор, как сумма операторов типа (11.12), относящихся к разным модам. Определяя операторы рождения-уничтожения

$$\tilde{a}_j^\dagger = \frac{1}{\sqrt{2\hbar}} (\tilde{q}_j - i\tilde{p}_j), \quad \tilde{a}_j = \frac{1}{\sqrt{2\hbar}} (\tilde{q}_j + i\tilde{p}_j),$$

удовлетворяющие коммутационным соотношениям

$$[\tilde{a}_j, \tilde{a}_k^\dagger] = \delta_{jk} I, \quad (11.43)$$

получаем

$$H = \sum_{j=1}^s \omega_j (\tilde{a}_j^\dagger \tilde{a}_j + I/2). \quad (11.44)$$

В терминах генераторов канонических наблюдаемых соотношение (11.41) сводится к уравнению

$$Re^{tD} = e^{-it\frac{1}{2}RD\Delta^{-1}R^\top} Re^{it\frac{1}{2}RD\Delta^{-1}R^\top}, \quad (11.45)$$

где $D = -2\varepsilon\Delta/\hbar$. В базисе $\{e_j, h_j\}$ матрица оператора D имеет вид

$$\tilde{D} = -2\hbar^{-1}\varepsilon\Delta = \text{diag} \begin{bmatrix} 0 & \omega_j \\ -\omega_j & 0 \end{bmatrix},$$

следовательно, соотношение (11.45) сводится к уравнениям типа (11.11)

$$\tilde{a}_j e^{-i\omega_j t} = e^{i\omega_j t \tilde{a}_j^\dagger \tilde{a}_j} \tilde{a}_j e^{-i\omega_j t \tilde{a}_j^\dagger \tilde{a}_j}, \quad j = 1, \dots, s, \quad (11.46)$$

описывающим динамику квантовых гармонических осцилляторов с частотами ω_j . $\square$

Подход, использующий представление матрицы энергии ε в диагональной форме, называется в квантовой оптике разложением на нормальные моды.

Оператор J в (Z, Δ) называется *оператором комплексной структуры*, если он Δ -положителен и

$$J^2 = -1, \quad (11.47)$$

где 1 — единичный оператор в Z . В частности,

$$\Delta J = -J^\top \Delta \geq 0. \quad (11.48)$$

Задача 11.3.1. Докажите, что оператор J порождает в Z структуру комплексного унитарного пространства (размерности s), если положить по определению $iz = Jz$ и ввести скалярное произведение

$$h(z, z') = j(z, z') + i\Delta(z, z') = \Delta(z, Jz') + i\Delta(z, z').$$

С любой комплексной структурой можно связать циклическую однопараметрическую группу $\{e^{\varphi J}\}$ симплектических преобразований, которую мы будем называть *калибровочной группой*. Согласно доказанной теореме калибровочная группа в Z порождает унитарную группу *калибровочных преобразований* в $\mathcal{H}$ по формуле

$$W(e^{\varphi J} z) = e^{-i\varphi G} W(z) e^{i\varphi G}, \quad (11.49)$$

где $G = -\frac{1}{2}RJ\Delta^{-1}R^\top$ — самосопряженный положительный оператор в $\mathcal{H}$. В терминах канонических наблюдаемых соотношение (11.49) сводится к линейному преобразованию

$$Re^{\varphi J} = e^{-i\varphi G} R e^{i\varphi G}, \quad (11.50)$$

которое является частным случаем преобразования (11.45).

Из доказательства теоремы в случае $D = J$ с учетом дополнительного свойства (11.47) вытекает существование симплектического базиса $\{e_j, h_j; j = 1, \dots, s\}$, ассоциированного со скалярным произведением $j(z, z') = \Delta(z, Jz')$, в котором оператор J имеет матрицу

$$\tilde{J} = \text{diag} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \quad (11.51)$$

В этом базисе

$$G = \sum_{j=1}^s \frac{1}{2\hbar} (\tilde{q}_j^2 + \tilde{p}_j^2) = \sum_{j=1}^s (\tilde{a}_j^\dagger \tilde{a}_j + I/2), \quad (11.52)$$

что с точностью до несущественного слагаемого совпадает с оператором полного числа квантов

$$\mathcal{N} = \sum_{j=1}^s \tilde{a}_j^\dagger \tilde{a}_j.$$

Соотношение (11.50) сводится к (11.46) с заменой $\omega_j t$ на φ .

Оператор A в $\mathcal{H}$ называется калибровочно инвариантным, если

$$e^{-i\varphi G} A e^{i\varphi G} = A$$

для всех вещественных φ . Используя соотношение (11.50), получаем, что квадратичный оператор $A = R\varepsilon R^\top$, где ε — симметричная положительная матрица, является калибровочно инвариантным, если $e^{\varphi J} \varepsilon e^{\varphi J^\top} = \varepsilon$, или, что эквивалентно, $J\varepsilon + \varepsilon J^\top = 0$, что с учетом (11.48) равносильно условию

$$[J, \varepsilon \Delta] = 0.$$

Для любой энергетической матрицы ε существует оператор комплексной структуры, удовлетворяющий этому условию: это оператор $J = T\tilde{J}T^{-1}$, который имеет матрицу (11.51) в симплектическом базисе, ассоциированном со скалярным произведением $\varepsilon(z, z') = \Delta(z, \varepsilon \Delta z')$.

Пример 11.3.1. Пусть $\omega_j, j = 1, \dots, s$, — положительные числа и

$$H = \sum_{j=1}^s \frac{1}{2\hbar} (\omega_j^2 q_j^2 + p_j^2)$$

— гамильтониан ансамбля осцилляторов с частотами ω_j , тогда $\tilde{q}_j = \sqrt{\omega_j} q_j$, $\tilde{p}_j = \sqrt{\omega_j}^{-1} p_j$, так что

$$\tilde{a}_j^\dagger = \frac{1}{\sqrt{2\hbar\omega_j}}(\omega_j q_j - i p_j), \quad \tilde{a}_j = \frac{1}{\sqrt{2\hbar\omega_j}}(\omega_j q_j + i p_j)$$

и

$$H = \sum_{j=1}^s \frac{\omega_j}{2\hbar} (\tilde{q}_j^2 + \tilde{p}_j^2) = \sum_{j=1}^s \omega_j (\tilde{a}_j^\dagger \tilde{a}_j + I/2).$$

Соответствующий оператор комплексной структуры имеет вид

$$J = \text{diag} \begin{bmatrix} 0 & \omega_j \\ -\omega_j^{-1} & 0 \end{bmatrix},$$

что соответствует умножению на i операторов уничтожения $\tilde{a}_j$, при этом калибровочный оператор в пространстве $\mathcal{H}$ дается формулой (11.52), т. е. равен $\mathcal{N} + \frac{S}{2}I$.

§ 11.4. Гауссовские состояния

11.4.1. Характеристическая функция

Характеристическая функция квантового состояния S определяется соотношением

$$\varphi(z) = \text{Tr} SW(z), \quad z \in Z.$$

Для произвольного ядерного оператора S это выражение можно рассматривать как некоммутативный аналог преобразования Фурье, однозначно определяющий оператор S .

Из положительности оператора S следует неотрицательная определенность $(n \times n)$ -матриц с элементами

$$\varphi(z_r - z_s) \exp \left[-\frac{i}{2} \Delta(z_r, z_s) \right] = \text{Tr} W(z_s)^* SW(z_r) \quad (11.53)$$

для всех $n = 1, 2, \dots$ и всевозможных наборов $\{z_1, \dots, z_n\} \in Z$.

Оператор плотности S имеет *конечные вторые моменты*, если $\text{Tr} S q_j^2 < \infty$, $\text{Tr} S p_j^2 < \infty$ для всех j , где след определяется как в соотношении (10.6). В этом случае определены *вектор средних значений* $m = \text{Tr} SR$ и *матрица ковариаций* $B_S(R) = \alpha$ (ср. п. 2.2.3). В силу ККС (11.35) коммутационная матрица имеет вид $C_S(R) = \Delta$, так что

$$\alpha - \frac{i}{2} \Delta = \text{Tr}(R - m)^\top S(R - m). \quad (11.54)$$

Отсюда вытекает неравенство

$$\alpha \geq \frac{i}{2} \Delta, \quad (11.55)$$

которое есть не что иное, как соотношение неопределенностей (2.21) для канонических наблюдаемых R . Далее будет показано (теорема 11.4.1), что условие (11.55) не только необходимо, но и достаточно для того, чтобы матрица α была матрицей ковариаций некоторого состояния. В дальнейшем мы будем обозначать через $\Sigma(m, \alpha)$ множество всех состояний с фиксированным вектором средних значений m и матрицей ковариаций α .

Как и в классическом случае, компоненты m, α (как и моменты более высокого порядка) можно выразить через производные характеристической функции.

Задача 11.4.1. Предполагая существование моментов соответствующего порядка, докажите, что

$$\text{Tr } SR(z)^n = i^{-n} \frac{d^n}{dt^n} \varphi(tz) \Big|_{t=0}.$$

11.4.2. Определение и свойства гауссовских состояний

Состояние S называется *гауссовским*, если его характеристическая функция $\varphi(z) = \text{Tr } SW(z)$ имеет вид

$$\varphi(z) = \exp \left(i m(z) - \frac{1}{2} \alpha(z, z) \right), \quad (11.56)$$

где $m(z) = mz$ — линейная форма, а $\alpha(z, z) = z^\top \alpha z$ — билинейная форма на (Z, Δ) . Здесь m — вещественная $(2s)$ -вектор-строка, а α — вещественная симметричная $(2s) \times (2s)$ -матрица.

Задача 11.4.2. Найдите первые и вторые производные функции (11.56) при $z = 0$ и покажите, используя результат задачи 11.4.1, что m — вектор средних значений, а α — матрица ковариаций состояния S .

Теорема 11.4.1. Для того чтобы соотношение (11.56) определяло квантовое состояние, необходимо и достаточно, чтобы матрица α удовлетворяла условию (11.55). При выполнении этого условия формула (11.56) определяет единственное гауссовское состояние в $\Sigma(m, \alpha)$.

Доказательство. Как уже было отмечено, необходимость вытекает из соотношения (11.54). Альтернативное доказательство вытекает из следующей леммы, которая понадобится и в дальнейшем.

Лемма 11.4.1. Пусть α — скалярное произведение и Δ — косо-симметричная форма в Z такие, что для всех $n = 1, 2, \dots$ и всевозможных наборов $\{z_1, \dots, z_n\} \in Z$ эрмитовы матрицы с элементами

$$\exp\left\{\alpha(z_r, z_s) - \frac{i}{2}\Delta(z_r, z_s)\right\} \quad (11.57)$$

неотрицательно определены. Тогда матрицы форм α, Δ удовлетворяют условию (11.55).

Доказательство. Пусть $t > 0$. Записывая условие неотрицательной определенности для набора $\{0, \sqrt{t}z_1, \dots, \sqrt{t}z_n\}$ с переменными $\{c_0, c_1, \dots, c_n\} \in \mathbb{C}$, удовлетворяющими условию $c_0 = -\sum_{j=1}^n c_j$, получаем

$$\sum_{r,s=1}^n \bar{c}_r c_s \left(\exp t \left[\alpha(z_r, z_s) - \frac{i}{2}\Delta(z_r, z_s) \right] - 1 \right) \geq 0.$$

Деля на t и переходя к пределу при $t \rightarrow 0$, получаем, что матрицы с элементами $\alpha(z_r, z_s) - \frac{i}{2}\Delta(z_r, z_s)$ неотрицательно определены для всевозможных наборов $z_1, \dots, z_n$, что равносильно условию (11.55). $\square$

Подставляя в формулу (11.53) гауссовское выражение (11.56), можно видеть, что

$$\varphi(z_r - z_s) \exp\left[-\frac{i}{2}\Delta(z_r, z_s)\right] = \varphi(z_r) \overline{\varphi(z_s)} \exp\left\{\alpha(z_r, z_s) - \frac{i}{2}\Delta(z_r, z_s)\right\},$$

таким образом, условие леммы выполнено, откуда следует неравенство (11.55).

Пусть теперь матрица α удовлетворяет неравенству (11.55). Из леммы 11.2.1 следует, что существует симплектическое преобразование T такое, что

$$\tilde{\alpha} = T^\top \alpha T = \text{diag} \begin{bmatrix} \alpha_j & 0 \\ 0 & \alpha_j \end{bmatrix}, \quad (11.58)$$

где $\alpha_j > 0$, причем неравенство (11.55) равносильно тому, что $\alpha_j \geq \frac{\hbar}{2}$, $j = 1, \dots, s$. Полагая $\alpha_j = \hbar\left(N_j + \frac{1}{2}\right)$, получаем $N_j \geq 0$.

Из соотношения (11.58) следует, что

$$\varphi(Tz) = \exp\left(i\tilde{m}z - \frac{1}{2}z^\top \tilde{\alpha}z\right) = \exp\sum_{j=1}^s \left[i(\tilde{m}_{jq}x_j + \tilde{m}_{jp}y_j) - \frac{1}{2}\alpha_j(x_j^2 + y_j^2)\right],$$

где $\tilde{m} = mT$. Однако в силу соотношений (11.23), (11.31) функция

$$\varphi_j(z) = \exp\left[i(\tilde{m}_{jq}x + \tilde{m}_{jp}y) - \frac{\alpha_j}{2}(x^2 + y^2)\right] \quad (11.59)$$

является характеристической функцией оператора плотности типа (11.18) для одной степени свободы (при $\omega = 1$) в канонических наблюдаемых $\tilde{R} = RT$. Обозначая соответствующее состояние $S^{(i)}$ и полагая

$$S = \bigotimes_{j=1}^s S^{(j)}, \quad (11.60)$$

получаем

$$\varphi(Tz) = \text{Tr } S \exp i \tilde{R} z = \text{Tr } S W(Tz),$$

откуда следует, что состояние S имеет характеристическую функцию $\varphi(z)$. $\square$

В квантовой оптике представление гауссовского состояния в виде (11.60) обычно связано с разложением на нормальные моды.

Пусть J — оператор комплексной структуры в Z и $\{e^{i\varphi G}\}$ — соответствующая калибровочная группа в $\mathcal{H}$. Из соотношения (11.49) следует, что гауссовский оператор плотности S является калибровочно инвариантным, $e^{-i\varphi G} S e^{i\varphi G} = S$, $\varphi \in \mathbb{R}$, тогда и только тогда, когда его характеристическая функция удовлетворяет условию $\varphi(e^{i\varphi J} z) = \varphi(z)$, что равносильно условиям $m = 0$ и $J^\top \alpha + \alpha J = 0$. Используя (11.48), последнее равенство можно переписать в виде

$$[J, \Delta^{-1} \alpha] = 0. \quad (11.61)$$

Напомним, что $\hat{\alpha} = \Delta^{-1} \alpha$ является матрицей кососимметричного оператора. Для любой матрицы ковариаций α найдется по крайней мере один оператор комплексной структуры в Z , коммутирующий с оператором $\Delta^{-1} \alpha$, а именно ортогональный оператор J из полярного разложения

$$\hat{\alpha} = |\Delta^{-1} \alpha| J = J |\Delta^{-1} \alpha| \quad (11.62)$$

в евклидовом пространстве (Z, α) . Пусть T — симплектическое преобразование, диагонализующее α , тогда $J = T \tilde{J} T^{-1}$, где $\tilde{J}$ определено соотношением (11.51). Более того, $|\Delta^{-1} \alpha| = T \tilde{A} T^{-1}$, где

$$\tilde{A} = \text{diag} \begin{bmatrix} \alpha_j / \hbar & 0 \\ 0 & \alpha_j / \hbar \end{bmatrix} = \text{diag} \begin{bmatrix} N_j + \frac{1}{2} & 0 \\ 0 & N_j + \frac{1}{2} \end{bmatrix}.$$

Задача 11.4.3. Докажите, что гауссовское состояние S является чистым тогда и только тогда, когда выполняется одно из следующих равносильных условий:

- 1) $N_j = 0$, $j = 1, \dots, s$;
- 2) $|\det(2\Delta^{-1} \alpha)| = 1$;
- 3) $\alpha = \frac{1}{2} \Delta J$, где J — оператор комплексной структуры.

При выполнении этих условий множество $\Sigma(m, \alpha)$ состоит из одного чистого гауссовского состояния.

Пусть S — гауссовское состояние с параметрами $(0, \alpha)$, J — оператор комплексной структуры из полярного разложения (11.62) и S_0 — чистое гауссовское состояние с параметрами $(0, \frac{1}{2}\Delta J)$. Таким образом, оба этих состояния калибровочно инвариантны.

Задача 11.4.4. Докажите следующее многомерное обобщение формулы (11.15):

$$S = \int W(z) S_0 W(z)^* P(d^{2s} z) = \int W(Jz) S_0 W(Jz)^* P(d^{2s} z), \quad (11.63)$$

где P — гауссовское распределение вероятностей с симплектической характеристической функцией

$$\int e^{i\Delta(w, z)} P(d^{2s} z) = \exp\left[-w^\top \left(\alpha - \frac{1}{2}\Delta J\right) w\right].$$

Это распределение калибровочно инвариантно, т. е. инвариантно относительно действия оператора комплексной структуры J_A в Z_A . Заметим также, что состояния $W(Jz) S_0 W(Jz)^*$ являются когерентными относительно рассматриваемой комплексной структуры.

11.4.3. Оператор плотности гауссовского состояния

Заметим, что $\Delta^{-1}\alpha = T(\Delta^{-1}\tilde{\alpha})T^{-1}$, где

$$\Delta^{-1}\tilde{\alpha} = \text{diag} \begin{bmatrix} 0 & \alpha_j/\hbar \\ -\alpha_j/\hbar & 0 \end{bmatrix}. \quad (11.64)$$

Следовательно, числа $\pm i\alpha_j/\hbar$, $j = 1, \dots, s$, являются собственными значениями оператора $\Delta^{-1}\alpha$.

Задача 11.4.5. Докажите, что оператор $-(\Delta^{-1}\alpha)^2 - \frac{1}{4}I$ является положительным в евклидовом пространстве (Z, α) , причем состояние S является чистым тогда и только тогда, когда этот оператор равен 0, т. е.

$$(\Delta^{-1}\alpha)^2 = -\frac{1}{4}I. \quad (11.65)$$

Спектральное разложение произвольного гауссовского состояния (11.60) можно получить как тензорное произведение спектральных разложений одномодовых состояний $S^{(j)}$. Следующая теорема обобщает представление (11.17) на случай произвольных гауссовских состояний, разложение которых не содержит «чистой» моды.

Теорема 11.4.2. *Предположим, что оператор $-(\Delta^{-1}\alpha)^2 - \frac{1}{4}I$ невырожден, тогда гауссовский оператор плотности с нулевым средним и матрицей ковариаций α представляется в виде*

$$S_0 = c \exp\left(-\frac{1}{\hbar} R \varepsilon R^\top\right), \quad (11.66)$$

где

$$c = \left[\det\left(-(\Delta^{-1}\alpha)^2 - \frac{1}{4}I\right)\right]^{-\frac{1}{4}} = \left[\det\left(-4 \sin^2 \frac{\varepsilon \Delta}{\hbar}\right)\right]^{\frac{1}{4}}, \quad (11.67)$$

α ε находится из соотношения

$$2\Delta^{-1}\alpha = \operatorname{ctg} \frac{\varepsilon \Delta}{\hbar}. \quad (11.68)$$

Доказательство. Переписывая представление (11.17) (при $\omega = 1$) в виде

$$(e^{\theta/2} - e^{-\theta/2}) \exp\left(-\frac{\theta}{2\hbar}(q^2 + p^2)\right)$$

и используя разложение (11.58), диагонализующее матрицу α , получаем

$$S_0 = c \exp\left(-\frac{1}{\hbar} \tilde{R} \tilde{\varepsilon} \tilde{R}^\top\right),$$

где

$$c = \prod_{j=1}^s (e^{\theta_j/2} - e^{-\theta_j/2}), \quad \tilde{\varepsilon} = \operatorname{diag} \begin{bmatrix} \theta_j/2 & 0 \\ 0 & \theta_j/2 \end{bmatrix}$$

и $\theta_j = \ln \left(\frac{\frac{\alpha_j}{\hbar} + \frac{1}{2}}{\frac{\alpha_j}{\hbar} - \frac{1}{2}} \right)$, так что

$$e^{\theta_j/2} - e^{-\theta_j/2} = \left[\left(\frac{\alpha_j}{\hbar} \right)^2 - \frac{1}{4} \right]^{-\frac{1}{2}}. \quad (11.69)$$

Оператор $\Delta^{-1}\alpha$ имеет собственные значения $\pm i \frac{\alpha_j}{\hbar}$, откуда следует первая из формул (11.67). Переходя к исходным каноническим наблюдаемым R , получаем формулу (11.66), где $\varepsilon = T \tilde{\varepsilon} T^\top$.

Обращая соотношение (11.69), получаем

$$\frac{\alpha_j}{\hbar} = \frac{1}{2} \operatorname{cth} \frac{\theta_j}{2}. \quad (11.70)$$

Имеем

$$\frac{\tilde{\varepsilon} \Delta}{\hbar} = \operatorname{diag} \begin{bmatrix} 0 & -\theta_j/2 \\ \theta_j/2 & 0 \end{bmatrix}.$$

Заметим, что $\varepsilon \Delta = T \tilde{\varepsilon} \Delta T^{-1}$ и $\Delta^{-1}\alpha = T \Delta^{-1} \tilde{\alpha} T^{-1}$ — матрицы операторов, причем $\Delta^{-1} \tilde{\alpha}$ дается соотношением (11.64). Операторы $-\frac{\tilde{\varepsilon} \Delta}{\hbar}$ и $\tilde{\Delta}^{-1} \tilde{\alpha}$ имеют одинаковые собственные векторы с собственными значениями $\pm i \theta_j/2$ и $\pm i \alpha_j/\hbar$ соответственно, поэтому из соотношения (11.70) следует равенство (11.68). $\square$

11.4.4. Энтропия гауссовского состояния

Для вычисления энтропии произвольного гауссовского состояния используем разложение на нормальные моды. Для одной моды ($s = 1$) оператор плотности $S^{(j)}$ унитарно эквивалентен оператору (11.16). Поэтому энтропия фон Неймана равна

$$H(S_0) = \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1} \right)^n [(n+1) \log(N+1) - n \log N] = g(N),$$

где введено обозначение

$$\begin{aligned} g(x) &= (x+1) \log(x+1) - x \log x, \quad x > 0; \\ g(0) &= 0. \end{aligned}$$

Для гауссовского состояния общего вида (11.60) суммированием по нормальным модам получаем

$$H(S) = \sum_{j=1}^s g(N_j), \quad (11.71)$$

где $N_j = \alpha_j / \hbar - 1/2$.

Чтобы получить общее выражение, не зависящее от выбора базиса, заметим, что в силу соотношения (11.64) оператор $\Delta^{-1}\alpha$ имеет собственные значения $\pm i \frac{\alpha_j}{\hbar}$, и, следовательно, он диагонализуем (в поле комплексных чисел). Для любой диагонализуемой матрицы $M = U \operatorname{diag}(m_j) U^{-1}$ по аналогии с другими непрерывными функциями на комплексной плоскости введем функцию $\operatorname{abs}(M) = U \operatorname{diag}(|m_j|) U^{-1}$. Тогда выражение (11.71) можно переписать в виде

$$H(S) = \frac{1}{2} \operatorname{Sp} g \left(\operatorname{abs}(\Delta^{-1}\alpha) - \frac{I}{2} \right), \quad (11.72)$$

где Sp — след матрицы (который следует отличать от следа Tr оператора в гильбертовом пространстве).

Другое выражение для энтропии гауссовского состояния можно получить из представления (11.66). По определению энтропии имеем

$$H(S) = -\log c + \frac{1}{\hbar} \operatorname{Sp} \varepsilon \alpha,$$

а в силу соотношений (11.67) и (11.68) это выражение равно

$$\begin{aligned} \frac{1}{4} \operatorname{Sp} \log \left[-(\Delta^{-1}\alpha)^2 - \frac{1}{4} I \right] + \operatorname{Sp}(\Delta^{-1}\alpha) \operatorname{arc} \operatorname{ctg}(2\Delta^{-1}\alpha) = \\ = -\frac{1}{4} \operatorname{Sp} \log \left(-\sin^2 \frac{\varepsilon \Delta}{\hbar} \right) + \frac{1}{2\hbar} \operatorname{Sp} \varepsilon \Delta \operatorname{ctg} \frac{\varepsilon \Delta}{\hbar}. \end{aligned} \quad (11.73)$$

Задача 11.4.6. Используя соотношение

$$g\left(\alpha - \frac{1}{2}\right) = \frac{1}{2} \log\left(\alpha^2 - \frac{1}{4}\right) + \alpha \log \frac{\alpha + \frac{1}{2}}{\alpha - \frac{1}{2}},$$

докажите совпадение выражений (11.72) и (11.73).

Пример 11.4.1. В случае одномодового гауссовского оператора плотности общего вида имеем $\alpha = \begin{bmatrix} \alpha^{qq} & \alpha^{qp} \\ \alpha^{qp} & \alpha^{pp} \end{bmatrix}$, причем $\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2 \geq \frac{\hbar^2}{4}$ (это неравенство равносильно условию (11.55)). Тогда

$$-(\Delta^{-1}\alpha)^2 = \frac{\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2}{\hbar^2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

следовательно,

$$|\Delta^{-1}\alpha| = \frac{\sqrt{\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2}}{\hbar} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

и

$$H(S) = g\left(\sqrt{\frac{\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2}{\hbar^2}} - \frac{1}{2}\right).$$

Геометрически величина $\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2$ равна квадрату площади эллипса рассеяния

$$\pi \hbar z^\top \alpha^{-1} z = 1, \quad z = [x, y]^\top,$$

для двумерного гауссовского распределения с матрицей ковариаций α .

Заметим, что в соответствии с соотношением (11.65) гауссовское состояние является чистым тогда и только тогда, когда оно имеет минимальную неопределенность $\alpha^{qq}\alpha^{pp} - (\alpha^{qp})^2 = \frac{\hbar^2}{4}$. Это соотношение имеет место как для когерентных состояний, для которых

$$\alpha^{qq} = \alpha^{pp} = \frac{\hbar}{2}, \quad \alpha^{qp} = 0,$$

так и для *сжатых* состояний, для которых последнее условие не выполняется (в отличие от квантовой оптики, мы используем здесь вещественную, а не комплексную параметризацию). Заметим, что состояние, которое является «сжатым» относительно данной комплексной структуры, всегда можно сделать «когерентным», используя комплексную структуру, ассоциированную с матрицей ковариаций. В многомодовом случае используется разложение на нормальные моды. В квантовой оптике выделяется та комплексная структура, для которой гамильтониан осциллятора

имеет канонический вид (11.42), и когерентные/сжатые состояния определяются относительно этой комплексной структуры.

Тогда как чистые гауссовские состояния являются состояниями минимальной неопределенности канонических наблюдаемых, произвольные гауссовские состояния характеризуются следующим свойством максимальной энтропийной неопределенности при фиксированных моментах канонических наблюдаемых.

Лемма 11.4.2. *Гауссовское состояние имеет максимальную энтропию среди всех состояний с фиксированными средним t и матрицей ковариаций α . Поэтому для любого множества состояний, заданного ограничениями на первые и вторые моменты, при нахождении максимальной энтропии достаточно ограничиться рассмотрением гауссовских состояний.*

Доказательство. Пусть $S \in \Sigma(m, \alpha)$, и пусть $\tilde{S}$ — единственное гауссовское состояние в $\Sigma(m, \alpha)$. Без ограничения общности можно считать, что состояние $\tilde{S}$ невырожденно. Общий случай можно свести к этому посредством отделения чистых компонент в разложении $\tilde{S}$ в тензорное произведение. Действительно, рассматривая разложение на нормальные моды, можно считать, что $Z = Z_1 + Z_2$ при $\Delta = \Delta_1 + \Delta_2$, $\alpha = \alpha_1 + \alpha_2$, где α_1 удовлетворяет аналогу условия (11.65) и поэтому соответствует единственному, обязательно гауссовскому, состоянию в Z_1 , в то время как α_2 соответствует невырожденному оператору плотности. Имеем

$$H(\tilde{S}) - H(S) = H(S; \tilde{S}) + \text{Tr}(S - \tilde{S}) \log \tilde{S},$$

где последнее слагаемое равно нулю, поскольку для невырожденного гауссовского состояния $\tilde{S}$ оператор $\log \tilde{S}$ является многочленом второго порядка от канонических наблюдаемых в силу теоремы 11.4.2, а первые и вторые моменты состояний $S, \tilde{S}$ совпадают. Поэтому $H(\tilde{S}) - H(S) = H(S; \tilde{S}) \geq 0$. $\square$

Аналогичный результат имеет место для условной квантовой энтропии.

Лемма 11.4.3. *Гауссовское состояние имеет максимальную условную энтропию среди всех состояний составной бозонной системы AB с данными средним t и матрицей ковариаций α .*

Доказательство. Пусть $S_{AB} \in \Sigma(m_{AB}, \alpha_{AB})$, и пусть $\tilde{S}_{AB}$ — единственное гауссовское состояние в $\Sigma(m_{AB}, \alpha_{AB})$. Тогда $S_A \in \Sigma(m_A, \alpha_A)$ и $\tilde{S}_A$ — гауссовское состояние в $\Sigma(m_A, \alpha_A)$. Мы вновь можем считать, что состояние $\tilde{S}_{AB}$ невырожденно. Обозначая

$$H(A|B) = H(S_{AB}) - H(S_B), \quad H(\tilde{A}|\tilde{B}) = H(\tilde{S}_{AB}) - H(\tilde{S}_B),$$

получаем

$$H(\tilde{A}|\tilde{B}) - H(A|B) = H(S_{AB}; \tilde{S}_{AB}) - H(S_A; \tilde{S}_A) + \\ + \text{Tr}(S_{AB} - \tilde{S}_{AB}) \log \tilde{S}_{AB} - \text{Tr}(S_A - \tilde{S}_A) \log \tilde{S}_A = H(S_{AB}; \tilde{S}_{AB}) - H(S_A; \tilde{S}_A),$$

поскольку $\log \tilde{S}_{AB}, \log \tilde{S}_A$ — многочлены второго порядка от канонических переменных. В силу монотонности относительной энтропии $H(S_{AB}; \tilde{S}_{AB}) - H(S_A; \tilde{S}_A) \geq 0$. $\square$

11.4.5. Очищение гауссовского состояния

Рассмотрим две бозонные системы, описываемые ККС с симплектическими пространствами (Z_1, Δ_1) , (Z_2, Δ_2) . Симплектическим пространством составной системы является прямая сумма $Z_{12} = Z_1 \oplus Z_2$, состоящая из пар (z_1, z_2) с компонентами $z_i \in Z_i$, причем $\Delta_{12} = \Delta_1 + \Delta_2$. По определению симплектическая матрица Δ_{12} является блочно-диагональной по отношению к разложению $Z_{12} = Z_1 \oplus Z_2$. Операторы Вейля для составной системы определяются как $W_{12}(z_1, z_2) = W_1(z_1) \otimes W_2(z_2)$.

Пусть S_{12} — гауссовское состояние составной системы с матрицей ковариаций α_{12} . Сужение гауссовского состояния S_{12} на первую подсистему определяется математическим ожиданием операторов Вейля $W_1(z_1) \otimes I_2 = W_{12}(z_1, 0)$, а значит, в соответствии с соотношением (11.56) оно имеет матрицу ковариаций α_1 , которая является первым диагональным блоком в блочно-матричном разложении

$$\alpha_{12} = \begin{bmatrix} \alpha_1 & \beta \\ \beta^\top & \alpha_2 \end{bmatrix}, \quad \Delta_{12} = \begin{bmatrix} \Delta_1 & 0 \\ 0 & \Delta_2 \end{bmatrix}. \quad (11.74)$$

Матрица ковариаций α_{12} состояния S_{12} составной системы блочно-диагональна тогда и только тогда, когда это состояние является состоянием-произведением.

Пусть S_1 — гауссовское состояние с матрицей ковариаций $\alpha_1 = \alpha$ на симплектическом пространстве Z_1 с формой $\Delta_1 = \Delta$. Рассмотрим пространство $Z_2 = Z_1$ с формой $\Delta_2 = -\Delta$, тогда

$$\Delta_{12} = \begin{bmatrix} \Delta & 0 \\ 0 & -\Delta \end{bmatrix}. \quad (11.75)$$

Задача 11.4.7. Рассмотрим симплектическое пространство $Z_{12} = Z_1 \oplus Z_2$ и гауссовское состояние S_{12} с матрицей ковариаций

$$\alpha_{12} = \begin{bmatrix} \alpha & \Delta \sqrt{-(\Delta^{-1}\alpha)^2 - I/4} \\ -\Delta \sqrt{-(\Delta^{-1}\alpha)^2 - I/4} & \alpha \end{bmatrix}. \quad (11.76)$$

Докажите, что S_{12} является очищением состояния S_1 .

Указание. Проверьте, что матрица

$$\Delta_{12}^{-1} \alpha_{12} = \begin{bmatrix} \frac{\Delta^{-1} \alpha}{\sqrt{-(\Delta^{-1} \alpha)^2 - I/4}} & \sqrt{-(\Delta^{-1} \alpha)^2 - I/4} \\ -\Delta^{-1} \alpha & \end{bmatrix} \quad (11.77)$$

удовлетворяет условию (11.65) для чистого гауссовского состояния.

В случае элементарных одномодовых гауссовских состояний (11.16) из этой конструкции получаем

$$\Delta_{12} = \hbar \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\alpha_{12} = \begin{bmatrix} N+1/2 & 0 & 0 & \sqrt{N^2+N} \\ 0 & N+1/2 & -\sqrt{N^2+N} & 0 \\ 0 & -\sqrt{N^2+N} & N+1/2 & 0 \\ \sqrt{N^2+N} & 0 & 0 & N+1/2 \end{bmatrix}$$

и

$$\Delta_{12}^{-1} \alpha_{12} = \begin{bmatrix} 0 & -(N+1/2) & \sqrt{N^2+N} & 0 \\ N+1/2 & 0 & 0 & \sqrt{N^2+N} \\ \sqrt{N^2+N} & 0 & 0 & N+1/2 \\ 0 & \sqrt{N^2+N} & -(N+1/2) & 0 \end{bmatrix}. \quad (11.78)$$

§ 11.5. Гауссовские каналы

11.5.1. Классически-квантовый гауссовский канал

Как отмечалось в конце § 11.1, состояние S_μ , определенное соотношением (11.18), описывает в квантовой оптике когерентный сигнал лазера в одномодовом равновесном электромагнитном поле. Отображение $\mu \rightarrow S_\mu$ можно рассматривать как классически-квантовый (с-к) канал, осуществляющий передачу классического сигнала μ на фоне аддитивного квантового гауссовского шума. Вводя вещественную параметризацию $m = [m_q, m_p]$ вместо комплексной $\mu = \frac{1}{\sqrt{2\hbar}}(m_q + im_p)$, получаем канал $m \rightarrow S_m$ с непрерывным алфавитом $\mathcal{X} = \mathbb{R}^2$, для которого

$$\text{Tr } S_m q = m_q, \quad \text{Tr } S_m p = m_p, \quad \text{Tr } S_m a^\dagger a = N + \frac{1}{2\hbar} \|m\|^2, \quad (11.79)$$

где $\|m\|^2 = m_q^2 + m_p^2$. Для нахождения его пропускной способности используем общий подход из § 10.4.

Предполагая, что слова $\omega = (m_1, \dots, m_n)$ передаются посредством независимой передачи букв, введем аддитивное энергетическое ограничение типа (10.15):

$$\frac{1}{2\hbar}(\|m_1\|^2 + \dots + \|m_n\|^2) \leq nE, \quad (11.80)$$

которое соответствует функции ограничения $f(m) = \frac{1}{2\hbar}\|m\|^2$. Тогда условия теоремы 10.4.1 выполнены при выборе оператора $F = a^\dagger a$ и классическая пропускная способность канала $m \rightarrow S_m$ с энергетическим ограничением (11.80) на входе равна

$$C = \max_{\pi \in \mathcal{P}_E} \left[H(\bar{S}_\pi) - \int H(S_m) \pi(d^2 m) \right], \quad (11.81)$$

где $\mathcal{P}_E$ определяется как множество входных распределений $\pi(d^2 m)$, удовлетворяющих условию

$$\frac{1}{2\hbar} \int \|m\|^2 \pi(d^2 m) \leq E, \quad (11.82)$$

а

$$\bar{S}_\pi = \int S_m \pi(d^2 m).$$

Заметим, что состояния S_m унитарно эквивалентны в силу соотношения (11.20) и поэтому имеют одинаковую энтропию $H(S_m) = H(S_0) = g(N)$. Следовательно, для любого входного распределения $\pi(d^2 m)$ выполняется равенство

$$\chi(\pi) = H(\bar{S}_\pi) - H(S_0),$$

и задача сводится к максимизации энтропии $H(\bar{S}_\pi)$ при ограничении (11.82). В силу соотношений (11.79) из неравенства (11.82) следует, что

$$\text{Tr} \bar{S}_\pi a^\dagger a \leq N + E. \quad (11.83)$$

Это неравенство является ограничением на второй момент состояния $\bar{S}_\pi$; в соответствии с леммой 11.4.2 максимум энтропии, равный

$$H(\bar{S}_\pi) = g(N + E), \quad (11.84)$$

достигается на гауссовском операторе плотности

$$\bar{S}_\pi = \frac{1}{N + E + 1} \sum_{n=0}^{\infty} \left(\frac{N + E}{N + E + 1} \right)^n |n\rangle \langle n|, \quad (11.85)$$

для которого имеет место равенство в формуле (11.83). Такое состояние соответствует оптимальному распределению

$$\pi(d^2 m) = \frac{1}{2\pi\hbar E} \exp\left(-\frac{\|m\|^2}{2\hbar E}\right) d^2 m. \quad (11.86)$$

Окончательно получаем, что пропускная способность гауссовского s - q -канала задается выражением

$$C = C_\chi = g(N + E) - g(N) = \\ = \log\left(1 + \frac{E}{N+1}\right) + (N + E) \log\left(1 + \frac{1}{N+E}\right) - N \log\left(1 + \frac{1}{N}\right), \quad (11.87)$$

которое при $N \rightarrow \infty$, $E/N \rightarrow \text{const}$ асимптотически ведет себя как $\log\left(1 + \frac{E}{N+1}\right)$. Таким образом, соотношение (11.87) можно рассматривать как квантовое обобщение знаменитой формулы Шеннона (4.48) с гауссовским шумом мощности N . Отсутствие множителя $1/2$ в формуле (11.87) объясняется наличием двух независимых вещественных амплитуд m_q , m_p для одной квантовой моды.

11.5.2. Открытые бозонные системы

В этом пункте рассматриваются каналы, которые естественно порождаются взаимодействием бозонной системы с бозонным окружением (шумом). Пусть Z_A , Z_B — симплектические пространства, описывающие вход и выход канала, а Z_D , Z_E — соответствующие окружения, так что

$$Z_A \oplus Z_D = Z_B \oplus Z_E = Z, \quad (11.88)$$

и пусть $W_A(z_A)$, ... — операторы Вейля в гильбертовых пространствах $\mathcal{H}_A$, ... соответствующих бозонных систем. Предположим, что составная система, находящаяся в исходном состоянии $S_A \otimes S_D$, эволюционирует согласно каноническому унитарному преобразованию U_T , которое отвечает симплектическому преобразованию T в Z . В соответствии с разложениями (11.88) в прямые суммы преобразование T можно записать в блочно-матричной форме:

$$T = \begin{bmatrix} K & L \\ K_D & L_D \end{bmatrix}, \quad (11.89)$$

где

$$K: Z_B \rightarrow Z_A, \quad L: Z_E \rightarrow Z_A, \quad K_D: Z_B \rightarrow Z_D, \quad L_D: Z_E \rightarrow Z_D.$$

Характеристическая функция состояния системы после взаимодействия, описываемого унитарным преобразованием U_T , имеет вид

$$\varphi_B(z_B) = \text{Tr } U_T(S_A \otimes S_D) U_T^*(W_B(z_B) \otimes I_E) = \\ = \text{Tr}(S_A \otimes S_D) U_T^*(W_B(z_B) \otimes W_E(0)) U_T = \\ = \text{Tr}(S_A \otimes S_D)(W_A(Kz_B) \otimes W_D(K_D z_B)) = \varphi_A(Kz_B) \varphi_D(K_D z_B),$$

где $\varphi_D(z_D) = \text{Tr } S_D W_D(z_B)$ — характеристическая функция исходного состояния окружения. Это преобразование можно переписать в виде

$$\varphi_B(z_B) = \varphi_A(Kz_B) f(z_B), \quad (11.90)$$

где

$$f(z_B) = \varphi_D(K_D z_B). \quad (11.91)$$

Если исходное состояние окружения является гауссовским с параметрами (m_D, α_D) , то f имеет вид гауссовской характеристической функции

$$f(z_B) = \exp \left[i l(z_B) - \frac{1}{2} \alpha(z_B, z_B) \right], \quad (11.92)$$

где $l(z_B) = m_D(K_D z_B)$ и

$$\alpha(z_B, z'_B) = \alpha_D(K_D z_B, K_D z'_B). \quad (11.93)$$

Задача 11.5.1. Докажите, что преобразование состояний согласно формуле (11.90) задает квантовый канал $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$. *Указание.* Преобразование представляет собой композицию унитарной эволюции и частичного следа, которые являются каналами в смысле определения 10.5.1.

Определение 11.5.1. Канал, преобразующий состояния согласно формуле (11.90), называется *линейным бозонным каналом*. Если, кроме того, f — гауссовская характеристическая функция (11.92), где l — линейная форма, а α — скалярное произведение на Z_B , то линейный бозонный канал называется *гауссовским с параметрами* (K, l, α) .

Пусть $R_A, \dots$ — векторы канонических наблюдаемых в $\mathcal{H}_A, \dots$ с коммутационными матрицами $\Delta_A, \dots$. Согласно соотношению (11.39) действие оператора U_T описывается линейным преобразованием

$$[R'_B R'_E] \equiv U_T^* [R_A R_D] U_T = [R_A R_D] T, \quad (11.94)$$

где T — блочная матрица (11.89), и для упрощения обозначений мы пишем $R_A, \dots$ вместо $R_A \otimes I_D, \dots$. В частности,

$$R'_B = R_A K + R_D K_D. \quad (11.95)$$

Коммутационная матрица и матрица ковариаций канонических наблюдаемых R_B на выходе канала даются выражением

$$\alpha_B - \frac{i}{2} \Delta_B = \text{Tr} (R'_B)^\top S R'_B,$$

где $S = S_A \otimes S_D$ и S_A, S_D — операторы плотности в $\mathcal{H}_A$ и $\mathcal{H}_D$ с матрицами ковариаций α_A и α_D соответственно. Используя соотношение (11.95),

получаем

$$\Delta_B = K^\top \Delta_A K + K_D^\top \Delta_D K_D, \quad (11.96)$$

$$\alpha_B = K^\top \alpha_A K + K_D^\top \alpha_D K_D. \quad (11.97)$$

Заметим, что в гауссовском случае $\alpha = K_D^\top \alpha_D K_D$ является матрицей соответствующей формы, входящей в выражение для функции (11.92), определяющей канал. Поскольку $\alpha_D \geq \frac{i}{2} \Delta_D$, из соотношения (11.96) вытекает неравенство

$$\alpha \geq \frac{i}{2} [\Delta_B - K^\top \Delta_A K], \quad (11.98)$$

которое в дальнейшем будет играть ключевую роль.

Конечное состояние окружения определяется аналогичным уравнением для канонических наблюдаемых R_E после взаимодействия:

$$R'_E = R_A L + R_D L_D.$$

Слабо комплементарный канал $\Phi_E: S_A \rightarrow S_E$ (см. § 6.6) определяется соотношением

$$\varphi_E(z_E) = \varphi_A(L z_E) \cdot \varphi_D(L_D z_E)$$

и, следовательно, также является линейным бозонным каналом, причем гауссовским, если состояние S_D гауссовское. Если исходное состояние окружения чистое, $S_D = |\psi_D\rangle\langle\psi_D|$, то канал Φ_E является комплементарным к каналу Φ , причем изометрия Стайнспринга задается формулой $V = U_T |\psi_D\rangle$.

Теорема 11.5.1. *Неравенство (11.98) является необходимым и достаточным условием для того, чтобы набор (K, l, α) определял гауссовский канал.*

Доказательство. Необходимость условия (11.98) была установлена выше. Покажем, что при выполнении этого условия можно построить симплектическое преобразование T , определяющее динамику открытой бозонной системы. Прежде всего заметим, что для данных операторов K, K_D , удовлетворяющих соотношению (11.96), всегда возможно расширить преобразование (11.95) до симплектического преобразования T . Соотношение (11.96) означает, что преобразование $z_B \rightarrow \begin{bmatrix} K z_B \\ K_D z_B \end{bmatrix}$ является симплектическим вложением Z_B в $Z_A \oplus Z_D = Z$, т. е. столбцы матрицы $\begin{bmatrix} K \\ K_D \end{bmatrix}$ образуют систему, которая может быть расширена до симплектического базиса в Z , формирующего матрицу T . Таким образом,

проблема сводится к следующей: для данных K, α , удовлетворяющих неравенству (11.98), найти симплектическое пространство (Z_D, Δ_D) , оператор $K_D: Z_B \rightarrow Z_D$ и скалярное произведение в Z_D , задаваемое симметричной матрицей $\alpha_D \geq \frac{i}{2} \Delta_D$, удовлетворяющие условиям

$$K_D^\top \Delta_D K_D = \Delta_B - K^\top \Delta_A K \equiv \tilde{\Delta}_D; \quad (11.99)$$

$$K_D^\top \alpha_D K_D = \alpha. \quad (11.100)$$

Сначала предположим, что матрица α невырожденна. Рассмотрим евклидово пространство (Z_B, α) с кососимметричной формой $\tilde{\Delta}_D$. Пусть $2n = \dim Z_B$. По условию $\alpha \geq \frac{i}{2} \tilde{\Delta}_D$. Рассмотрим кососимметричный оператор S , определяемый соотношением

$$\tilde{\Delta}_D(z_B, z'_B) = \alpha_D(z_B, S z'_B), \quad z_B, z'_B \in Z_B.$$

Согласно теореме из линейной алгебры найдется ортонормированный базис $\tilde{e}_j, j = 1, \dots, 2n - l, \tilde{h}_j, j = 1, \dots, l$, в (Z_B, α) такой, что

$$\begin{aligned} S \tilde{e}_j &= s_j \tilde{h}_j, & S \tilde{h}_j &= -s_j \tilde{e}_j, & j &= 1, \dots, l, \\ S \tilde{e}_j &= 0, & & & j &= l + 1, \dots, 2n - l. \end{aligned}$$

Из условия $\alpha \geq \frac{i}{2} \tilde{\Delta}_D$ следует, что $l - \frac{i}{2} S \geq 0$, поэтому $0 < s_j \leq 2$.

Пусть (Z_D, Δ_D) — стандартное симплектическое пространство размерности $2l + 2(2n - 2l) = 2(2n - l)$ с базисом $e_j, h_j, j = 1, \dots, 2n - l$. Определим α_D как форму с диагональной матрицей

$$\begin{aligned} \alpha_D e_j &= s_j^{-1} e_j, & \alpha_D h_j &= s_j^{-1} h_j, & j &= 1, \dots, l, \\ \alpha_D e_j &= e_j, & \alpha_D h_j &= \frac{1}{4} h_j, & j &= l + 1, \dots, 2n - l, \end{aligned}$$

тогда $\alpha_D \geq \frac{i}{2} \Delta_D$. Определим оператор $K_D: Z_B \rightarrow Z_D$ формулами

$$\begin{aligned} K_D \tilde{e}_j &= \sqrt{s_j} e_j, & K_D \tilde{h}_j &= \sqrt{s_j} h_j, & j &= 1, \dots, l, \\ K_D \tilde{e}_j &= e_j, & & & j &= l + 1, \dots, 2n - l. \end{aligned} \quad (11.101)$$

Тогда соотношения (11.99), (11.100) вытекают из рассмотрения значений соответствующих квадратичных форм на базисных векторах $\tilde{e}_j, j = 1, \dots, 2n - l, \tilde{h}_j, j = 1, \dots, l$ в Z_B . Отметим, что по построению α_D является матрицей ковариаций чистого состояния тогда и только тогда, когда $s_j = 2, j = 1, \dots, l$.

Если же форма α обращается в нуль на нетривиальном подпространстве $Z_0 \subset Z_B$, то форма $\tilde{\Delta}_D$ также равна нулю на Z_0 в силу условия $\alpha \geq \frac{i}{2} \tilde{\Delta}_D$. Поэтому векторы $\tilde{e}_j$, $j = l + 1, \dots, 2n - l$, можно выбрать таким образом, что часть из них будет образовывать базис в Z_0 . Тогда можно модифицировать определение (11.101), потребовав, чтобы выполнялось условие $K_D \tilde{e}_j = 0$ для $\tilde{e}_j \in Z_0$; при этом будут выполнены соотношения (11.99), (11.100). $\square$

11.5.3. Основные свойства гауссовских каналов

Формула (11.90) равносильна следующему соотношению для двойственного канала:

$$\Phi^*[W_B(z_B)] = W(Kz_B)f(z_B), \quad (11.102)$$

которое показывает, что операторы Вейля с точностью до множителя переходят в операторы Вейля. В случае гауссовского канала

$$\Phi^*[W_B(z_B)] = W(Kz_B) \exp\left[il(z_B) - \frac{1}{2}\alpha(z_B, z_B)\right]. \quad (11.103)$$

Следующее утверждение показывает, что гауссовские каналы могут быть определены соотношениями (11.90), (11.103) безотносительно к картине взаимодействия с окружением, рассмотренной в предыдущем пункте.

Предложение 11.5.1. *Для того чтобы отображение (11.103) было вполне положительным, необходимо и достаточно выполнения условия (11.98).*

Доказательство. Достаточность была установлена в теореме 11.5.1. Для доказательства необходимости заметим, что из полной положительности отображения (11.102) следует неотрицательная определенность матриц с операторными элементами

$$\begin{aligned} W(Kz_s)\Phi^*[W(z_s)^*W(z_r)]W(Kz_r)^* = \\ = f(z_r - z_s) \exp \frac{i}{2} [\Delta(z_r, z_s) - \Delta(K^\top z_r, K^\top z_s)], \end{aligned} \quad (11.104)$$

где $z_1, \dots, z_n$ — произвольные конечные наборы элементов из Z . В гауссовском случае (11.103) это равносильно неотрицательной определенности эрмитовых матриц с элементами

$$\exp\left\{\alpha(z_r, z_s) - \frac{i}{2}\Delta(z_r, z_s) + \frac{i}{2}\Delta(Kz_r, Kz_s)\right\}, \quad (11.105)$$

и условие (11.98) вытекает из леммы 11.4.1. $\square$

Отметим следующие свойства.

1. Гауссовский канал преобразует гауссовские состояния в гауссовские состояния.

2. Канал, двойственный к линейному бозонному каналу, преобразует любой многочлен от канонических наблюдаемых R_B в многочлен от R_A того же порядка при условии, что функция f имеет производные достаточно высокого порядка. Это проверяется дифференцированием соотношения (11.102) в точке $z_B = 0$.

3. Композиция гауссовских каналов является гауссовским каналом. Действительно, пусть Φ_j , $j = 1, 2$, — два гауссовских канала с параметрами K_j , l_j , α_j , тогда, используя определение (11.103), получаем гауссовский канал $\Phi_2 \circ \Phi_1$ с параметрами

$$K = K_1 K_2, \quad l = K_2^\top l_1 + l_2, \quad \alpha = K_2^\top \alpha_1 K_2 + \alpha_2. \quad (11.106)$$

4. Линейный бозонный (в частности гауссовский) канал ковариантен в следующем смысле:

$$\Phi[W(z)^* S W(z)] = W(K'z)^* \Phi[S] W(K'z), \quad (11.107)$$

где $K' = \Delta^{-1} K^\top \Delta$ — симплектически сопряженное преобразование.

11.5.4. Гауссовские наблюдаемые

Пусть заданы два симплектических пространства Z_A , Z_B с соответствующими системами Вейля в гильбертовых пространствах $\mathcal{H}_A$, $\mathcal{H}_B$. Пусть M — наблюдаемая в $\mathcal{H}_A$ с множеством исходов Z_B , которая задается вероятностной операторнозначной мерой $M(d^{2n}z)$. Далее в этом пункте мы будем опускать индекс B , так что $z = z_B$ и т. д. Наблюдаемая полностью определяется *операторной характеристической функцией*

$$\varphi_M(w) = \int e^{i\Delta(w, z)} M(d^{2n}z).$$

Отметим следующее очевидное свойство характеристической функции наблюдаемой: для любого конечного подмножества $\{\omega_j\} \subset Z_B$ блочная матрица с операторными элементами $\varphi(\omega_j - \omega_k)$ является неотрицательно определенной.

Наблюдаемая M называется *гауссовской*, если ее операторная характеристическая функция имеет вид

$$\begin{aligned} \varphi_M(w) &= W_A(Kw) \exp\left(-\frac{1}{2}\alpha(w, w)\right) = \\ &= \exp\left(iR_A^\top Kw - \frac{1}{2}\alpha(w, w)\right), \end{aligned} \quad (11.108)$$

где $K: Z_B \rightarrow Z_A$ — линейный оператор, а α — билинейная форма на Z_B .

Теорема 11.5.2. *Для того чтобы соотношение (11.108) определяло наблюдаемую, необходимо и достаточно выполнения матричного неравенства*

$$\alpha \geq \frac{i}{2} K^\top \Delta_A K. \quad (11.109)$$

Доказательство. Для операторной функции, заданной соотношением (11.108), выполняется соотношение

$$\begin{aligned} \varphi(\omega_j - \omega_k) = W(K\omega_k)^* W(K\omega_j) \exp \left[-\frac{i}{2} \Delta(K\omega_j, K\omega_k) - \right. \\ \left. - \frac{1}{2} \alpha(\omega_j - \omega_k, \omega_j - \omega_k) \right] = C_k^* C_j \exp \left[\alpha(\omega_j, \omega_k) - \frac{i}{2} \Delta(K\omega_j, K\omega_k) \right], \end{aligned}$$

где

$$C_j = W(K\omega_j) \exp \left[-\frac{1}{2} \alpha(\omega_j, \omega_j) \right],$$

и согласно лемме 11.4.1 из неотрицательной определенности матриц со скалярными коэффициентами $\exp \left[\alpha(\omega_j, \omega_k) - \frac{i}{2} \Delta(K\omega_j, K\omega_k) \right]$ следует неравенство (11.109).

Достаточность условия (11.109) будет доказана прямым построением расширения Наймарка наблюдаемой M в духе следствия 3.1.1. $\square$

Предложение 11.5.2. *Предположим, что выполняется условие (11.109), тогда найдутся бозонная система в пространстве $\mathcal{H}_C$ с каноническими наблюдаемыми R_C , для которой $\mathcal{H}_B \subseteq \mathcal{H}_A \otimes \mathcal{H}_C$, и гауссовское состояние $S_C \in \mathfrak{S}(\mathcal{H}_C)$ такие, что*

$$M(U) = \text{Tr}_C(I_A \otimes S_C) E_{AC}(S), \quad U \subseteq Z_B; \quad (11.110)$$

здесь E_{AC} — четкая наблюдаемая в пространстве $\mathcal{H}_A \otimes \mathcal{H}_C$, задаваемая спектральной мерой коммутирующих самосопряженных операторов

$$X_B = \Delta_B^{-1}(R_A K + R_C K_C)^\top, \quad (11.111)$$

где $K_C: Z_B \rightarrow Z_C$ — оператор такой, что

$$K_C^\top \Delta_C K_C = -K^\top \Delta_A K. \quad (11.112)$$

Доказательство. Условие (11.112) означает, что

$$K_C^\top \Delta_C K_C + K^\top \Delta_A K = 0,$$

т. е. имеет место коммутативность операторов (11.111). Модифицируя доказательство предложения 11.5.1, построим симплектическое пространство (Z_C, Δ_C) , оператор $K_C: Z_B \rightarrow Z_C$ и скалярное произведение в Z_C ,

задаваемое симметричной матрицей $\alpha_C \geq \frac{i}{2}\Delta_C$, так, чтобы выполнялось соотношение (11.112) вместе с условием

$$K_C^\top \alpha_C K_C = \alpha.$$

Тогда характеристическая функция наблюдаемой E_{AC} равна

$$\begin{aligned} \varphi_{E_{AC}}(\omega_B) &= \int \exp[i\Delta(\omega_B, z_B)] E_{AC}(d^{2n}z_B) = \\ &= \exp i\omega_B^\top \Delta_B X_B = \exp i(R_A K + R_C K_C)\omega_B = W_A(K\omega_B) W_C(K_C\omega_B), \end{aligned}$$

откуда следуют равенство

$$\begin{aligned} \text{Tr}_C(I_A \otimes S_C) \varphi_{E_{AC}}(\omega_B) &= W_A(K\omega_B) \exp\left(-\frac{1}{2}\alpha_C(K_C\omega_B, K_C\omega_B)\right) = \\ &= W_A(K\omega_B) \exp\left(-\frac{1}{2}\alpha(\omega_B, \omega_B)\right) = \varphi_M(\omega_B) \end{aligned}$$

и соотношение (11.110). $\square$

Наблюдаемая M является четкой тогда и только тогда, когда $\alpha = 0$, при этом она является спектральной мерой коммутирующих самосопряженных операторов $R_A K$.

11.5.5. Гауссовские каналы, разрушающие сцепленность

Теорема 11.5.3. *Гауссовский канал Φ с параметрами $(K, 0, \alpha)$ является каналом, разрушающим сцепленность, тогда и только тогда, когда α допускает разложение*

$$\alpha = \alpha_A + \alpha_B, \quad \text{где} \quad \alpha_A \geq \frac{i}{2}K^\top \Delta_A K, \quad \alpha_B \geq \frac{i}{2}\Delta_B. \quad (11.113)$$

В этом случае Φ имеет представление

$$\Phi[S] = \int_{Z_B} W_B(z) \sigma_B W_B(z)^* \mu_S(d^{2n}z), \quad (11.114)$$

где σ_B — гауссовское состояние с параметрами $(0, \alpha_B)$, а $\mu_S(U) = \text{Tr} S M_A(U)$, $U \subseteq Z_B$, — распределение вероятностей гауссовской наблюдаемой M_A с характеристической функцией

$$\varphi_{M_A}(\omega) = W_A(K\omega) \exp\left(-\frac{1}{2}\alpha_A(\omega, \omega)\right). \quad (11.115)$$

Доказательство. Предположим сначала, что α допускает указанное разложение, и рассмотрим канал, определяемый соотношением (11.114); надо показать, что

$$\Phi^*[W_B(\omega)] = W_A(K\omega) \exp\left[-\frac{1}{2}\alpha(\omega, \omega)\right]. \quad (11.116)$$

В самом деле, для произвольного состояния S имеем

$$\begin{aligned}
 \text{Tr } S \Phi^* [W_B(\omega)] &= \\
 &= \text{Tr } \Phi[S] W_B(\omega) = \int_{Z_B} \text{Tr } W_B(z) \sigma_B W_B(z)^* W_B(\omega) \mu_S(d^{2n}z) = \\
 &= \int_{Z_B} \text{Tr } \sigma_B W_B(z)^* W_B(\omega) W_B(z) \mu_S(d^{2n}z) = \\
 &= \text{Tr } \sigma_B W_B(\omega) \int_{Z_B} \exp[i\Delta(\omega, z)] \mu_S(d^{2n}z) = \\
 &= \exp\left[-\frac{1}{2}\alpha_B(\omega, \omega)\right] \text{Tr } S \varphi_{M_A}(\omega) = \\
 &= \text{Tr } S W_A(K\omega) \exp\left[-\frac{1}{2}\alpha_B(\omega, \omega) - \frac{1}{2}\alpha_A(\omega, \omega)\right], \quad (11.117)
 \end{aligned}$$

откуда и следует соотношение (11.116).

Обратно, пусть канал Φ гауссовский и разрушает сцепленность. Мы используем гауссовскую версию доказательства теоремы 10.7.1. Фиксируем гауссовское невырожденное состояние S_A в $\mathfrak{S}(\mathcal{H}_A)$, и пусть $\{|e_j\rangle\}_{j=1}^{+\infty}$ — базис собственных векторов оператора S_A с соответствующими (положительными) собственными значениями $\{\lambda_j\}_{j=1}^{+\infty}$. Рассмотрим единичный вектор

$$|\Omega\rangle = \sum_{j=1}^{+\infty} \sqrt{\lambda_j} |e_j\rangle \otimes |e_j\rangle$$

в пространстве $\mathcal{H}_A \otimes \mathcal{H}_A$, тогда $|\Omega\rangle\langle\Omega|$ является гауссовским очищением состояния S_A . Поскольку Φ разрушает сцепленность, гауссовское состояние

$$S_{AB} = (\text{Id}_A \otimes \Phi)[|\Omega\rangle\langle\Omega|] \quad (11.118)$$

в $\mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ является разделимым. Отсюда вытекает представление

$$S_{AB} = \int_{Z_A} \int_{Z_B} W_A(z_A) \sigma_A W_A(z_A)^* \otimes W_B(z_B) \sigma_B W_B(z_B)^* P(d^{2m}z_A d^{2n}z_B), \quad (11.119)$$

где σ_A, σ_B — гауссовские состояния, а P — гауссовское распределение вероятностей. В самом деле, из представления (10.41) для разделимого состояния следует, что матрица ковариаций α_{AB} состояния S_{AB} удовлетворяет неравенству

$$\alpha_{AB} \geq \begin{bmatrix} \alpha_A & 0 \\ 0 & \alpha_B \end{bmatrix} \equiv \hat{\alpha}_{AB},$$

где α_A, α_B — матрицы ковариаций некоторых квантовых состояний в системах A, B . Обозначая через σ_A, σ_B гауссовские состояния с такими

матрицами ковариаций и через P — гауссовское распределение вероятностей с симплектическим преобразованием Фурье, соответствующим матрице ковариаций $\alpha_{AB} - \hat{\alpha}_{AB}$, получаем (11.119).

Взяв частичный след по системе B , получаем

$$\begin{aligned} S_A &= \text{Tr}_B(\text{Id}_A \otimes \Phi)[|\Omega\rangle\langle\Omega|] = \int_{Z_A} \int_{Z_B} W_A(z_A) \sigma_A W_A(z_A)^* P(d^{2m} z_A d^{2n} z_B) = \\ &= \int_{Z_A} \int_{Z_B} \overline{W_A(z_A) \sigma_A W_A(z_A)^*} P(d^{2m} z_A d^{2n} z_B), \end{aligned}$$

где черта означает комплексное сопряжение в базисе из собственных значений оператора S_A . Тогда аналогично формуле (10.52) получаем, что соотношение

$$M_A(U) = S_A^{-1/2} \left[\int_{Z_A} \int_U \overline{W_A(z_A) \sigma_A W_A(z_A)^*} P(d^{2m} z_A d^{2n} z_B) \right] S_A^{-1/2}$$

задает ограниченный положительный оператор такой, что $M_A(U) \leq M_A(Z_B) = I_A$. Нетрудно показать, что $M_A(U)$ является вероятностной операторнозначной мерой на борелевских подмножествах $U \subseteq Z_B$.

Покажем, что имеет место представление (11.114) для канала Φ с определенными таким образом M_A и σ_B . Рассмотрим канал, разрушающий сцепленность,

$$\hat{\Phi}[S] = \int_{Z_B} W_B(z) \sigma_B W_B(z)^* \mu_S(d^{2n} z),$$

где $\mu_S(U) = \text{Tr} S M_A(U)$, $U \subseteq Z_B$. Чтобы доказать, что $\Phi = \hat{\Phi}$, достаточно показать, что $\hat{\Phi}[|e_j\rangle\langle e_k|] = \Phi[|e_j\rangle\langle e_k|]$ для всех j, k . Однако

$$\begin{aligned} \hat{\Phi}[|e_j\rangle\langle e_k|] &= \int_{Z_B} W_B(z) \sigma_B W_B(z)^* \langle e_k | M_A(d^{2n} z) | e_j \rangle = \\ &= \lambda_j^{-1/2} \lambda_k^{-1/2} \int_{Z_A} \int_{Z_B} \langle e_j | W_A(z_A) \sigma_A W_A(z_A)^* | e_k \rangle \times \\ &\quad \times W_B(z_B) \sigma_B W_B(z_B)^* P(d^{2m} z_A d^{2n} z_B) = \\ &= \lambda_j^{-1/2} \lambda_k^{-1/2} \text{Tr}_A(|e_k\rangle\langle e_j| \otimes I_B) S_{AB} = \Phi[|e_j\rangle\langle e_k|] \end{aligned}$$

в силу соотношений (11.118), (11.119).

Остается доказать, что M_A — гауссовская наблюдаемая с характеристической функцией (11.115), где $\alpha_A = \alpha - \alpha_B$, а α_B — корреляционная функция состояния σ_B ; не ограничивая общности, мы можем предположить, что среднее равно нулю, так как его всегда можно устранить действием операторов Вейля. Однако из соотношения (11.117) следует, что

$$\Phi^*[W_B(w)] = \exp\left[-\frac{1}{2}\alpha_B(w, w)\right] \varphi_{M_A}(w)$$

для любого канала Φ с представлением (11.114), откуда, принимая во внимание равенство (11.116), получаем соотношение (11.115) с $\alpha_A = \alpha - \alpha_B$. $\square$

Условие теоремы автоматически выполнено в частном случае, когда

$$K^\top \Delta_A K = 0.$$

В этом случае компоненты векторного оператора $R_A K$ коммутируют, поэтому M_A — четкая наблюдаемая, задаваемая их спектральной мерой, и распределение вероятностей $\mu_S(d^{2n}z)$ может быть сколь угодно сильно сконцентрировано в любой точке z при надлежащем выборе состояния S . Таким образом, в этом случае естественно отождествить Φ с классически-квантовым (с-к) каналом, определяемым семейством состояний $z \rightarrow W(z)\sigma_B W(z)^*$.

§ 11.6. Пропускные способности гауссовских каналов

11.6.1. Максимизация квантовой взаимной информации

Мы начнем с рассмотрения классической пропускной способности с использованием сцепленного состояния, поскольку она находится наиболее эффективно в гауссовском случае. Если состояние S и канал Φ являются гауссовскими, то величины $H(S)$, $H(\Phi[S])$, $H(S, \Phi)$ и $I(S, \Phi)$ могут быть вычислены с использованием формул (11.72), (11.97), (11.77). В частности, энтропия $H(\Phi[S])$ дается формулой (11.72) с заменой α на матрицу α' , вычисленную по формуле (11.97). Производя очищение входного состояния и используя формулу (7.41), получаем

$$H(S, \Phi) = \frac{1}{2} \text{Sp } g \left(\text{abs}(\Delta_{12}^{-1} \alpha'_{12}) - \frac{I}{2} \right),$$

где матрица

$$\alpha'_{12} = \begin{bmatrix} \alpha' & K\beta \\ \beta^\top K^\top & \alpha \end{bmatrix} \quad (11.120)$$

с $\beta = \Delta \sqrt{-(\Delta^{-1} \alpha)^2 - I/4}$ получается подстановкой уравнения (11.95) в соотношение

$$\alpha'_{12} - \frac{i}{2} \Delta'_{12} = \text{Tr}[R' R_2]^\top S[R' R_2],$$

в котором R_2 обозначает неизменяемые канонические наблюдаемые эталонной системы. С другой стороны, если имеется явное описание комплемментарного канала $\tilde{\Phi}$, то обменную энтропию можно найти как выходную энтропию $H(\tilde{\Phi}[S])$.

Следующий результат существенно упрощает вычисление пропускной способности гауссовских каналов для передачи классической информации с помощью сцепленного состояния, сводя вычисления к случаю гауссовских входных состояний.

Теорема 11.6.1. Пусть Φ — гауссовский канал. Максимум взаимной информации $I(S, \Phi)$ на множестве состояний $\Sigma(m, \alpha)$ с фиксированными первыми и вторыми моментами достигается на гауссовском состоянии.

Доказательство. Используя представление (7.46) для квантовой взаимной информации, можно записать

$$I(S, \Phi) = H(B|E) + H(B),$$

где B — выход канала и E — окружение. Для гауссовского канала первые и вторые моменты преобразуются одинаково для всех состояний из $\Sigma(m, \alpha)$. Применяя лемму 11.4.2, получаем

$$H(B) = H(\Phi[S]) \leq H(\widetilde{\Phi[S]}) = H(\Phi[\tilde{S}]) = H(\tilde{B}),$$

где $\widetilde{\Phi[S]}$ (соответственно $\tilde{S}$) — гауссовское состояние с теми же первыми и вторыми моментами, что и $\Phi[S]$ (соответственно S). Канал $S \rightarrow S_{BE} = VSV^*$, где V — изометрия Стайнспринга для Φ , также является гауссовским, поскольку он осуществляется каноническим унитарным преобразованием с гауссовским состоянием окружения, а именно

$$\text{Tr } S_{BE} W(z_B) \otimes W(z_E) = \varphi_A(Kz_B + Lz_E) \varphi_D(K_D z_B + L_D z_E). \quad (11.121)$$

Поэтому аналогичное рассуждение, основанное на лемме 11.4.3, показывает, что $H(B|E) \leq H(\tilde{B}|\tilde{E})$. Таким образом, $I(S, \Phi) \leq I(\tilde{S}, \Phi)$. $\square$

Из этого результата вытекает, что если максимум информации $I(S, \Phi)$ на некотором множестве состояний, задаваемом ограничениями на первые и вторые моменты, вообще достигается, то он достигается на гауссовском состоянии. Рассмотрим энергетическое ограничение

$$\text{Tr } SF \leq E, \quad (11.122)$$

где $F = R\epsilon R^\top$ — квадратичный оператор с положительной невырожденной матрицей энергии ϵ . Заметим, что

$$\text{Tr } SF = \text{Sp}(\epsilon\alpha_A) + m_A \epsilon m_A^\top,$$

где m_A — вектор-строка средних значений и α_A — матрица ковариаций состояния S . Предложение 10.6.2 дает выражение для классической пропускной способности передачи с использованием сцепленного состояния $C_{ea}(\Phi, F, E)$ в виде максимума квантовой взаимной информации $I(S, \Phi)$

на множестве всех состояний S , удовлетворяющих ограничению (11.122). Покажем, что оператор $F = R\varepsilon R^\top$ удовлетворяет условиям этого предложения. Действительно, в силу теоремы 11.4.2 оператор F удовлетворяет условию (10.9). Выбирая $\tilde{F} = c[RR^\top - (\text{Sp } \alpha_E K_E^\top K_E)I]$, получаем $\Phi^*[\tilde{F}] = cRK^\top KR^\top$, и всегда можно подобрать такое положительное c , что $\Phi^*[\tilde{F}] \leq F$. Более того, $\tilde{F}$ удовлетворяет условию (10.9). Поэтому максимум величины $I(S, \Phi)$ достигается и имеет место формула (10.39). Поскольку энергетическое ограничение выражается через первые и вторые моменты m_A , α_A , значение $C_{ea}(\Phi, F, E)$ достигается на гауссовском состоянии.

Дальнейшее упрощение максимизации получается в калибровочно инвариантном случае.

11.6.2. Калибровочно ковариантные каналы

Рассмотрим канал $\Phi: \mathfrak{I}(\mathcal{H}_A) \rightarrow \mathfrak{I}(\mathcal{H}_B)$. Предположим, что в Z_A, Z_B фиксированы некоторые операторы комплексной структуры J_A, J_B , и пусть G_A, G_B — операторы, порождающие унитарные группы калибровочных преобразований в $\mathcal{H}_A, \mathcal{H}_B$ согласно формуле (11.49). Канал называется *калибровочно ковариантным*, если

$$\Phi[e^{i\varphi G_A} S e^{-i\varphi G_A}] = e^{i\varphi G_B} \Phi[S] e^{-i\varphi G_B} \quad (11.123)$$

для всех входных состояний S и вещественных чисел φ . В случае линейного бозонного канала Φ в силу соотношений (11.49), (11.90) это равносильно следующему условию:

$$\varphi(e^{\varphi J_A} K z_B) f(z_B) = \varphi(K e^{\varphi J_B} z_B) f(e^{\varphi J_B} z_B),$$

где $\varphi(z_A)$ — характеристическая функция состояния S . Для гауссовского канала с параметрами $(K, 0, \alpha)$ это условие сводится к соотношениям

$$KJ_B - J_A K = 0, \quad [\Delta_B^{-1} \alpha, J] = 0.$$

Таким образом, естественный выбор комплексной структуры в Z_B дается любым оператором J_B , коммутирующим с оператором $\Delta_B^{-1} \alpha$. Существование такой комплексной структуры доказывается аналогично формуле (11.61) с той разницей, что матрица α может быть вырожденной.

В задачах максимизации с ограниченной средней энергией естественная комплексная структура в Z_A определяется оператором энергии $F = R\varepsilon R^\top$, а именно, J_A — оператор комплексной структуры в Z_A , коммутирующий с оператором $\varepsilon \Delta_A$, так что

$$J_A \varepsilon + \varepsilon J_A^\top = 0. \quad (11.124)$$

В случае обычного гамильтониана системы осцилляторов $H = \frac{1}{\hbar} F$ действие оператора J_A сводится к умножению на i в соответствующей комплексификации.

Пусть теперь гауссовский канал Φ ковариантен по отношению к указанным естественным комплексным структурам. Тогда

$$I(e^{i\varphi G_A} S e^{-i\varphi G_A}, \Phi) \equiv I(S, \Phi),$$

что вытекает из аналогичного свойства всех трех слагаемых, составляющих $I(S, \Phi)$. Для $H(S)$ это просто следствие унитарной инвариантности энтропии, для $H(\Phi[S])$ дополнительно используется ковариантность канала Φ , а для $H(S, \Phi) = H(\tilde{\Phi}[S])$ это следует из ковариантности комплементарного канала $\tilde{\Phi}$ (задача 6.7.2). Определяя усредненное G_A -инвариантное состояние

$$\bar{S} = \frac{1}{2\pi} \int_0^{2\pi} e^{i\varphi G_A} S e^{-i\varphi G_A} d\varphi,$$

получаем

$$\text{Tr } SF = \text{Sp}(\varepsilon\alpha_A) + m_A \varepsilon m_A^\top \geq \text{Sp}(\varepsilon\alpha_A) = \text{Tr } \bar{S}F,$$

где m_A , α_A — первые и вторые моменты состояния S и последнее равенство вытекает из соотношения (11.124):

$$\begin{aligned} \text{Tr } \bar{S}F &= \frac{1}{2\pi} \int_0^{2\pi} \text{Tr } e^{i\varphi G_A} S e^{-i\varphi G_A} \text{Sp}(R \varepsilon R^\top) d\varphi = \\ &= \frac{1}{2\pi} \int_0^{2\pi} \text{Sp}(e^{\varphi J_A} \varepsilon e^{\varphi J_A^\top} \alpha_A) d\varphi = \text{Sp}(\varepsilon\alpha_A). \end{aligned}$$

Теперь, используя вогнутость взаимной информации $I(S, \Phi)$, мы заключаем, что $I(S, \Phi) \leq I(\bar{S}, \Phi)$. Таким образом, максимум квантовой взаимной информации при энергетическом ограничении $\text{Tr } SF \leq E$ достигается на калибровочно инвариантном (G_A -инвариантном) состоянии. Первые и вторые моменты такого состояния с необходимостью удовлетворяют соотношениям $m_A = 0$, $[J_A, \Delta^{-1}\alpha_A] = 0$. Рассматривая гауссовское состояние с этими же первыми и вторыми моментами, в итоге получаем такой результат.

Следствие 11.6.1. Пусть Φ — гауссовский канал, калибровочно ковариантный относительно естественных комплексных структур J_A, J_B (где структура J_A ассоциирована с оператором энергии). Тогда максимум квантовой взаимной информации на множестве состояний с ограниченной средней энергией достигается на калибровочно инвариантном (G_A -инвариантном) гауссовском состоянии.

11.6.3. Максимизация когерентной информации

Рассмотрим когерентную информацию

$$I_c(S, \Phi) = H(\Phi[S]) - H(S, \Phi).$$

Предложение 11.6.1. Пусть Φ — гауссовский деградируемый канал, так что

$$\tilde{\Phi} = T \circ \Phi, \quad (11.125)$$

где T — также гауссовский канал, тогда квантовая пропускная способность канала Φ равна

$$Q(\Phi) = \sup_{\tilde{S}} I_c(\tilde{S}, \Phi),$$

где точная верхняя грань берется по множеству гауссовских состояний $\tilde{S}$. Если, кроме того, все каналы калибровочно ковариантны относительно некоторых комплексных структур, то точную верхнюю грань достаточно брать только по множеству калибровочно инвариантных (G_A -инвариантных) гауссовских состояний.

Доказательство. Если канал Φ является деградируемым, т. е. имеет место равенство (11.125), где $\tilde{\Phi}$ — комплементарный канал и T — некоторый канал, то (см. п. 9.3.3)

$$I_c(S, \Phi) = H(E'|E) = H(S_{E'E}) - H(S_E), \quad (11.126)$$

где $S_{E'E} = V'S_B V'^*$ и $V': \mathcal{H}_B \rightarrow \mathcal{H}_E \otimes \mathcal{H}_{E'}$ — изометрия Стайнспринга для канала T . Если же канал T можно выбрать гауссовским, то канал $S_B \rightarrow S_{E'E}$ также гауссовский и, значит, применимо рассуждение с использованием леммы 11.4.3. Поэтому $I_c(S, \Phi) = H(E'|E) \leq H(\tilde{E}'|\tilde{E}) = I_c(\tilde{S}, \Phi)$. Следовательно, квантовая пропускная способность канала Φ равна

$$Q(\Phi) = \sup_S I_c(S, \Phi) = \sup_{\tilde{S}} I_c(\tilde{S}, \Phi),$$

где точная верхняя грань берется по множеству гауссовских состояний $\tilde{S}$.

Если, кроме того, канал Φ калибровочно ковариантен, то из вогнутости условной квантовой энтропии (11.126) следует, что эту точную верхнюю грань можно брать только по множеству калибровочно инвариантных гауссовских состояний аналогично рассуждениям из предыдущего пункта. $\square$

11.6.4. Классическая пропускная способность

Классическую пропускную способность гауссовского канала Φ естественно рассматривать при аддитивном входном ограничении (10.28), соответствующем оператору

$$F^{(n)} = F \otimes I \otimes \dots \otimes I + \dots + I \otimes \dots \otimes I \otimes F,$$

где $F = R^\top \varepsilon R$ — квадратичный оператор энергии с положительно определенной матрицей ε . Однако нахождение значения пропускной способности $C(\Phi, F, E)$ зависит от решения до сих пор открытой проблемы аддитивности для гауссовских каналов. Естественной оценкой для $C(\Phi, F, E)$ является величина $C_\chi(\Phi, F, E)$, определяемая выражением (10.31), которая совпадает с $C(\Phi, F, E)$ в случае аддитивности, например для каналов, разрушающих сцепленность. Во всяком случае, эта величина дает нижнюю границу для $C(\Phi, F, E)$.

Однако даже вычисление величины $C_\chi(\Phi, F, E)$ для гауссовских каналов остается в общем случае открытым вопросом (за исключением с- q -каналов и специального случая, который будет рассмотрен в предложении 11.7.1). Отметим, что по крайней мере в рассматриваемой ситуации оптимальный обобщенный ансамбль всегда существует, поскольку набор условий в следствии 10.5.1 выполнен для $F = R^\top \varepsilon R$, как было показано в п. 11.6.1. Таким образом, максимум величины $\chi_\Phi(\pi)$ достигается, и для $C_\chi(\Phi, F, E)$ имеет место формула (10.36).

Выдвигается следующая **гипотеза о гауссовских оптимальных ансамблях**. Для гауссовского канала Φ с квадратичным энергетическим ограничением максимум величины $\chi_\Phi(\pi)$ в выражении (10.36) для $C_\chi(\Phi, F, E)$ достигается на гауссовском обобщенном ансамбле π , который состоит из обобщенных когерентных состояний $W(z)S_0W(z)^*$, где S_0 — чистое гауссовское состояние, с гауссовским распределением $P(d^{2n}z)$.

Для ансамбля описанного типа в силу свойства ковариантности (11.107) гауссовских каналов имеем $H(\Phi[W(z)S_0W(z)^*]) = H(\Phi[S_0])$, поэтому

$$\chi_\Phi(\pi) = H(\Phi[\bar{S}_\pi]) - H(\Phi[S_0]), \quad (11.127)$$

что приводит к **гипотезе о гауссовской минимальной энтропии**: для гауссовского канала Φ минимум выходной энтропии достигается на (чистом) гауссовском состоянии S_0 .

Рассмотрим калибровочные преобразования в $\mathcal{H}_A$, ассоциированные с оператором комплексной структуры. Определим действие калибровочных преобразований на обобщенные ансамбли состояний соотношением

$$\pi_\varphi(U) = \pi(\{S: e^{i\varphi G_A} S e^{-i\varphi G_A} \in U\}), \quad \varphi \in [0, 2\pi],$$

для борелевских подмножеств $U \in \mathfrak{S}(\mathcal{H}_A)$. Обобщенный ансамбль калибровочно инвариантен, если $\pi_\varphi \equiv \pi$. Используя вогнутость функционала $\chi_\Phi(\pi)$ (задача 10.5.2) и рассуждая, как в п. 11.6.1, нетрудно доказать, что если гауссовский канал Φ калибровочно ковариантен относительно комплексной структуры, ассоциированной с матрицей энергии ε , то максимум в соотношении (10.36) достигается на калибровочно инвариантном обобщенном ансамбле. Отсюда также следует, что среднее состояние $\bar{S}_\pi$ такого оптимального ансамбля является калибровочно инвариантным.

Однако в том же предположении можно доказать следующее условное утверждение, связывающее две гипотезы, сформулированные выше.

Предложение 11.6.2. Пусть гауссовский канал Φ калибровочно ковариантен относительно естественных комплексных структур J_A, J_B . Предположим также, что минимум выходной энтропии достигается на G_A -инвариантном гауссовском состоянии S_0 . Тогда выполняется гипотеза о гауссовских оптимальных ансамблях, причем оптимальный ансамбль π может быть выбран так, что выходное состояние $\bar{S}_B = \Phi[\bar{S}_\pi]$ является G_B -инвариантным гауссовским состоянием.

Доказательство. Выше было отмечено, что оптимальный ансамбль π существует. Обозначим $\bar{S}_B = \Phi[\bar{S}_\pi]$, тогда $\text{Tr } \bar{S}_\pi F \leq E$ и

$$\begin{aligned} C_\chi(\Phi, F, E) &= \chi_\Phi(\pi) = H(\bar{S}_B) - \hat{H}_\Phi(\bar{S}_B) \leq \\ &\leq H(\bar{S}_B) - \check{H}(\Phi) = H(\bar{S}_B) - H(\Phi[S_0]) \end{aligned} \quad (11.128)$$

в силу общего неравенства $\hat{H}_\Phi(\bar{S}_B) \geq \check{H}(\Phi)$ и предположения о том, что $H(\Phi[S_0]) = \check{H}(\Phi)$.

Рассмотрим G_A -инвариантное состояние

$$\bar{S}_A = \frac{1}{2\pi} \int_0^{2\pi} e^{i\varphi G_A} \bar{S}_\pi e^{-i\varphi G_A} d\varphi,$$

тогда $\text{Tr } \bar{S}_A F = \text{Tr } \bar{S}_\pi F$. Пусть теперь $\tilde{S}_A$ — гауссовское состояние с теми же первыми и вторыми моментами, что и $\bar{S}_A$, тогда вновь выполняется равенство

$$\text{Tr } \tilde{S}_A F = \text{Tr } \bar{S}_A F = \text{Tr } \bar{S}_\pi F. \quad (11.129)$$

Более того, $\tilde{S}_A$ является G_A -инвариантным гауссовским состоянием, а $\tilde{S}_B = \Phi[\tilde{S}_A]$ — G_B -инвариантным гауссовским состоянием, причем

$$H(\tilde{S}_B) \geq H(\Phi[\tilde{S}_A]) \geq H(\bar{S}_B). \quad (11.130)$$

Здесь первое неравенство следует из леммы 11.4.2, а второе — из вогнутости энтропии. Поскольку S_0 — чистое G_A -инвариантное гауссовское состояние, согласно формуле (11.63) имеет место разложение

$$\tilde{S}_A = \int W(z) S_0 W(z)^* P(d^{2s} z).$$

Обозначим через $\tilde{\pi}$ ансамбль когерентных состояний $W(z) S_0 W(z)^*$ с гауссовским распределением $P(d^{2s} z)$. Тогда

$$\tilde{S}_B = \Phi[\tilde{S}_A] = \int \Phi[W(z) S_0 W(z)^*] P(d^{2s} z) = \int W(K'z) \Phi[S_0] W(K'z)^* P(d^{2s} z)$$

в силу свойства ковариантности (11.107) гауссовских каналов, поэтому

$$\hat{H}_\Phi(\tilde{S}_B) \leq H(\Phi[S_0]) = \check{H}(\Phi).$$

В силу равенства (11.129) ансамбль $\tilde{\pi}$ удовлетворяет энергетическому ограничению. Более того,

$$\chi_\Phi(\tilde{\pi}) = H(\tilde{S}_B) - \hat{H}_\Phi(\tilde{S}_B) \geq H(\tilde{S}_B) - H(\Phi[S_0]). \quad (11.131)$$

Сопоставляя неравенства (11.128), (11.130) и (11.131), получаем $\chi_\Phi(\tilde{\pi}) \geq \chi_\Phi(\pi) = C_\chi(\Phi, F, E)$, поэтому $\tilde{\pi}$ является оптимальным ансамблем с требуемыми свойствами. $\square$

§ 11.7. Случай одной моды

11.7.1. Классификация гауссовских каналов

В этом пункте нас будет интересовать задача о приведении произвольного квантового гауссовского канала к простейшему виду путем подходящих канонических унитарных преобразований на входе и выходе канала:

$$\Phi^{*'}[V(z)] = U_{T_1}^* \Phi^*[U_{T_2}^* V(z) U_{T_2}] U_{T_1},$$

т. е.

$$\Phi^{*'}[V(z)] = V(T_1 K T_2 z) f(T_2 z).$$

Здесь мы дадим полное решение этой задачи в случае $s = 1$.

Пусть Z — двумерное симплектическое пространство, т. е. линейное пространство векторов $z = [x, y]^T$ с симплектической формой

$$\Delta(z, z') = x'y - xy'. \quad (11.132)$$

(Для упрощения обозначений в этом пункте полагаем $\hbar = 1$.) Базис e, h в Z является симплектическим, если $\Delta(e, h) = -1$, т. е. если площадь ориентированного параллелограмма со сторонами e, h равна -1 . Линейное

преобразование T в Z является симплектическим, если оно отображает симплектический базис в симплектический базис.

В соответствии с формулой (11.103) гауссовский канал характеризуется параметрами K , l , α , удовлетворяющими условию

$$\alpha \geq \frac{i}{2} [\Delta - K^\top \Delta K]. \quad (11.133)$$

Используя преобразование смещения (11.32), всегда можно получить $l = 0$, что мы и будем подразумевать далее. Поэтому

$$\Phi^*[W(z')] = W(Kz') \exp \left[-\frac{1}{2} \alpha(z', z') \right]. \quad (11.134)$$

Теорема 11.7.1. Пусть e, h — некоторый симплектический базис; в зависимости от значения

- A) $\Delta(Ke, Kh) = 0$; B) $\Delta(Ke, Kh) = 1$;
 C) $\Delta(Ke, Kh) = k^2 > 0, k \neq 1$; D) $\Delta(Ke, Kh) = -k^2 < 0$

найдутся такие симплектические преобразования T_1, T_2 , что канал $\Phi^{*'}$ имеет вид (11.90), где

$$A_1) K[x, y]^\top = [0, 0]^\top, \quad f(z) = \exp \left[-\frac{1}{2} \left(N_0 + \frac{1}{2} \right) (x^2 + y^2) \right], \quad N_0 \geq 0;$$

$$A_2) K[x, y]^\top = [x, 0]^\top, \quad f(z) = \exp \left[-\frac{1}{2} \left(N_0 + \frac{1}{2} \right) (x^2 + y^2) \right],$$

$$B_1) K[x, y]^\top = [x, y]^\top, \quad f(z) = \exp \left[-\frac{1}{4} y^2 \right],$$

$$B_2) K[x, y]^\top = [x, y]^\top, \quad f(z) = \exp \left[-\frac{1}{2} N_c (x^2 + y^2) \right], \quad N_c \geq 0,$$

$$C) K[x, y]^\top = [kx, ky]^\top, \quad k > 0, k \neq 1, \\ f(z) = \exp \left[-\frac{1}{2} \left(N_c + \frac{|k^2 - 1|}{2} \right) (x^2 + y^2) \right],$$

$$D) K[x, y]^\top = [kx, -ky]^\top, \quad k > 0, \\ f(z) = \exp \left[-\frac{1}{2} \left(N_c + \frac{(k^2 + 1)}{2} \right) (x^2 + y^2) \right].$$

Очевидно, что в случаях A, B₂, C канал является калибровочно инвариантным по отношению к естественной комплексной структуре, ассоциированной с умножением на i в комплексной плоскости x, y .

Доказательство. А. Пусть $\Delta(Ke, Kh) = 0$. Тогда $\Delta(Kz, Kz') \equiv 0$ и либо $K = 0$, либо K имеет ранг 1. Тогда неравенство (11.133) есть просто

условие, характеризующее корреляционную матрицу квантового гауссовского состояния. Из леммы 11.2.1 следует, что найдется симплектическое преобразование T_2 такое, что

$$\alpha(T_2 z, T_2 z) = (N_0 + \frac{1}{2})(x^2 + y^2). \quad (11.135)$$

Если $K = 0$, то мы получаем случай A_1 .

Пусть теперь K имеет ранг 1, тогда и KT_2 имеет ранг 1, значит, найдется такой вектор e' , что $KT_2[x, y]^T = (k_1 x + k_2 y)e'$. Тогда найдется симплектическое преобразование T_1 такое, что $T_1 e' = [1, 0]$ и, следовательно, $T_1 KT_2[x, y]^T = [k_1 x + k_2 y, 0]^T$. Производя поворот T'_2 , который оставляет форму α инвариантной, мы можем преобразовать этот вектор к виду $[k'_1 x, 0]^T$, $k'_1 \neq 0$, и, производя затем симплектическое масштабное преобразование T'_1 , мы приходим к случаю A_2 .

В. С. Пусть $\Delta(Ke, Kh) = k^2 > 0$. Тогда $T = k^{-1}K$ — симплектическое преобразование и $\Delta(Kz, Kz') = k^2 \Delta(z, z')$. Положим $T_1 = (TT_2)^{-1}$, где T_2 будет выбрано позднее, так что $T_1 KT_2 = kI$. Отображение T_2 выбирается следующим образом.

В случае В имеем $k = 1$, и условие (11.133) означает неотрицательную определенность матрицы α . Тогда имеем следующие подслучаи.

V_2 . Если форма α невырожденна, то согласно лемме 11.2.1 найдется симплектическое преобразование T_2 такое, что

$$\alpha(T_2 z, T_2 z) = N_c(x^2 + y^2),$$

где $N_c > 0$. Также если $\alpha = 0$, то получаем аналогичную формулу с $N_c = 0$.

V_1 . С другой стороны, если форма α вырожденна и имеет ранг 1, то $\alpha(z, z) = (k_1 x + k_2 y)^2$ при некоторых k_1, k_2 , не равных нулю одновременно, тогда для произвольного $N_c > 0$ найдется симплектическое преобразование T_2 такое, что

$$\alpha(T_2 z, T_2 z) = N_c y^2,$$

в частности, можно взять $N_c = \frac{1}{2}$.

В случае С имеем $k \neq 1$, и из условия (11.133) следует, что $\alpha/|k^2 - 1|$ является корреляционной матрицей квантового гауссовского состояния, поэтому найдется симплектическое преобразование T_2 такое, что

$$\alpha(T_2 z, T_2 z) = |k^2 - 1| \left(N_0 + \frac{1}{2} \right) (x^2 + y^2) = \left(N_c + \frac{|k^2 - 1|}{2} \right) (x^2 + y^2),$$

где $N_0 \geq 0$, $N_c = |k^2 - 1|N_0$.

Д. Пусть $\Delta(Ke, Kh) = -k^2 < 0$. Тогда $T = k^{-1}K$ — антисимплектическое преобразование ($\Delta(Tz, Tz') = -\Delta(z, z')$) и $\Delta(Kz, Kz') = -k^2 \Delta(z, z')$.

Аналогично случаям В, С получаем

$$\alpha(T_2 z, T_2 z) = (k^2 + 1) \left(N_0 + \frac{1}{2} \right) (x^2 + y^2) = \left(N_c + \frac{(k^2 + 1)}{2} \right) (x^2 + y^2),$$

где $N_0 \geq 0$, $N_c = (k^2 + 1)N_0$. Полагая $T_1 = \Lambda(TT_2)^{-1}$, где $\Lambda[x, y]^T = [x, -y]^T$, мы получаем первое уравнение в случае D. Заметим, что T_1 — симплектическое преобразование, поскольку как T , так и Λ антисимплектические. $\square$

Как показано в п. 11.5.2, гауссовский канал Φ можно расширить до линейной динамики открытой бозонной системы, описываемой каноническими наблюдаемыми q , p и каноническими наблюдаемыми окружения q_E , p_E , ... в гауссовском состоянии S_E ; более того, эта линейная динамика также дает описание слабо комплементарного канала Φ_E , отображающего исходное состояние системы q , p в конечное состояние окружения q'_E , p'_E , ...; если состояние S_E чистое, то Φ_E — комплементарный канал $\tilde{\Phi}$, который определяется каналом Φ однозначно с точностью до унитарной эквивалентности. Заметим, что окружение может быть многомодовым, что отражается символом ... в обозначении вспомогательных переменных.

Дадим описание в терминах открытой системы в каждом из случаев предыдущей теоремы.

A_1 . Это есть полностью деполяризующий канал

$$q' = q_E, \quad p' = p_E,$$

где наблюдаемые q_E , p_E описывают окружение в равновесном состоянии S_E со средним числом квантов N_0 . Слабо комплементарным является идеальный канал Id .

A_2 . Линейное преобразование канонических переменных моды имеет вид

$$q' = q + q_E, \quad p' = p_E, \quad (11.136)$$

где мода q_E , p_E снова находится в равновесном состоянии S_E со средним числом квантов N_0 . Слабо комплементарным к этому каналу является канал, который задается преобразованием

$$q'_E = q, \quad p'_E = p - p_E, \quad (11.137)$$

где p_E может рассматриваться как классическая случайная величина с дисперсией $N_0 + \frac{1}{2}$.

B_1 . Уравнение канала имеет вид (11.137), где p_E имеет дисперсию $\frac{1}{2}$, так что мода q_E , p_E находится в чистом (вакуумном) состоянии, при этом комплементарный канал задается преобразованием (11.136).

В₂. Канал с аддитивным комплексным гауссовским шумом интенсивности N_c :

$$q' = q + \xi, \quad p' = p + \eta.$$

Задача 11.7.1. Докажите, что расширение Стайнспринга для этого канала дается окружением с двумя бозонными модами $q_j, p_j, j = 1, 2$, в чистом гауссовском состоянии, которое имеет нулевые средние, нулевые ковариации и дисперсии

$$Dq_1 = Dq_2 = N_c, \quad Dp_1 = Dp_2 = \frac{1}{4N_c},$$

так что $\xi = q_1, \eta = q_2$, причем динамика составной системы описывается уравнениями

$$\begin{aligned} q' &= q + q_1, & p' &= p + q_2, \\ q'_1 &= q_1, & p'_1 &= p_1 - p - q_2/2, \\ q'_2 &= q_2, & p'_2 &= p_2 + q + q_1/2. \end{aligned}$$

С. Аттенюатор/усилитель с коэффициентом k и квантовым шумом со средним числом квантов N_0 . В случае аттенюатора ($k < 1$) уравнение канала имеет вид

$$\begin{aligned} q' &= kq + \sqrt{1 - k^2}q_E, \\ p' &= kp + \sqrt{1 - k^2}p_E, \end{aligned}$$

где мода q_E, p_E находится в равновесном состоянии S_E со средним числом квантов N_0 . Слабо комплементарный канал задается уравнениями

$$q'_E = \sqrt{1 - k^2}q - kq_E, \quad (11.138)$$

$$p'_E = \sqrt{1 - k^2}p - kp_E \quad (11.139)$$

и также является аттенюатором (с коэффициентом $k' = \sqrt{1 - k^2}$).

В случае усилителя ($k > 1$) имеем

$$\begin{aligned} q' &= kq + \sqrt{k^2 - 1}q_E, \\ p' &= kp - \sqrt{k^2 - 1}p_E \end{aligned}$$

со слабо комплементарным каналом

$$\begin{aligned} q'_E &= \sqrt{k^2 - 1}q + kq_E, \\ p'_E &= -\sqrt{k^2 - 1}p + kp_E, \end{aligned}$$

см. случай D.

D. Уравнение канала имеет вид

$$\begin{aligned} q' &= kq + \sqrt{k^2 + 1}q_E, \\ p' &= -kp + \sqrt{k^2 + 1}p_E, \end{aligned}$$

т. е. этот канал является слабо комплементарным к усиливающему каналу с коэффициентом $k' = \sqrt{k^2 + 1}$ и квантовым шумом со средним числом квантов N_0 .

11.7.2. Каналы, разрушающие сцепленность

Применим теорему 11.5.3 к случаю одной бозонной моды $A = B$, где

$$\Delta_A(z, z') = \Delta_B(z, z') = \Delta(z, z') = x'y - xy'.$$

Как было показано выше, произвольный одномодовый гауссовский канал приводится к одной из нормальных форм.

Нам остается только найти форму $K^\top \Delta_A K$ и проверить разложимость (11.113) в каждом из этих случаев. Мы опираемся на следующий простой факт.

Задача 11.7.2. Проверьте, что неравенство

$$\left(N + \frac{1}{2}\right)I \geq \frac{i}{2}\Delta,$$

выполняется тогда и только тогда, когда $N \geq 0$.

В случае A имеем $K^\top \Delta K = 0$, поэтому Φ является с-q-каналом (фактически классическим каналом).

В случае B имеем $K^\top \Delta K = \Delta$, поэтому из необходимого условия разложимости (11.113) следует, что $\alpha \geq i\Delta$. Это не может быть выполнено в случае B₁ в силу вырожденности формы α , следовательно, канал не является разрушающим сцепленность. С другой стороны, в случае B₂ условие (11.113) выполняется при $\alpha_B = \alpha_A = \alpha/2$ тогда и только тогда, когда $N_c \geq 1$, и Φ является каналом, разрушающим сцепленность.

В случае C имеем $K^\top \Delta K = k^2\Delta$. Ясно, что в этом случае условие разложимости выполняется тогда и только тогда, когда $\alpha \geq \frac{i}{2}(1 + k^2)\Delta$,

что равносильно неравенству $N_c + \frac{|1 - k^2|}{2} \geq \frac{(1 + k^2)}{2}$, или

$$N_c \geq \min(1, k^2). \quad (11.140)$$

Отсюда следует условие разрушения сцепленности (которое также формально включает случай B₂).

В случае D имеем $K^\top \Delta K = -k^2 \Delta$. Условие разложимости выполняется тогда и только тогда, когда $\alpha \geq \frac{i}{2}(1 + k^2)\Delta$, что выполнено всегда, поэтому канал является разрушающим сцепленность для всех $N_c \geq 0$.

Таким образом, свойство аддитивности (10.32) выполняется для одномодовых гауссовских каналов вида A, D с произвольными значениями параметров, и B₂, C с параметрами, удовлетворяющими условию (11.140). В общем случае каналы, разрушающие сцепленность, имеют нулевую квантовую пропускную способность, $Q(\Phi) = 0$, см. следствие 9.3.1. Однако в п. 11.7.4 на основе анализа деградируемости будет найдена более широкая область нулевой квантовой пропускной способности.

11.7.3. Аттенюатор/усилитель

Рассмотрим подробно случай C. Введя параметр $N_c = |k^2 - 1|N_0 \geq 0$, можно представить действие канала Φ следующим образом:

$$\text{Tr } \Phi[S]W(z) = \text{Tr } SW(kz) \cdot \exp\left[-\frac{1}{2}(|k^2 - 1|/2 + N_c)\|z\|^2\right]. \quad (11.141)$$

Как отмечалось, этот канал является калибровочно инвариантным по отношению к естественной комплексной структуре, ассоциированной с умножением на i в комплексной плоскости x, y . Поэтому далее, опираясь на результаты § 11.6, мы ограничимся рассмотрением калибровочно инвариантных состояний.

Пусть входное состояние $S = S(N)$ системы является гауссовским с характеристической функцией

$$\text{Tr } S(N)W(z) = \exp\left[-\frac{1}{2}\left(N + \frac{1}{2}\right)\|z\|^2\right],$$

где параметр N представляет мощность (среднее число квантов) сигнала

$$\text{Tr } S(N)a^\dagger a = N, \quad (11.142)$$

$a = \frac{1}{\sqrt{2}}(q + ip)$. Энтропия состояния $S(N)$ равна

$$H(S(N)) = g(N). \quad (11.143)$$

Из соотношения (11.141) следует, что выходное состояние $\Phi[S]$ является гауссовским состоянием $S(N')$, где

$$N' = k^2 N + N'_0, \quad (11.144)$$

а

$$N'_0 = \max\{0, (k^2 - 1)\} + N_c$$

— среднее число фотонов на выходе, соответствующем входному вакуумному состоянию $S(0)$. Тогда

$$H(\Phi[S(N)]) = g(N'). \quad (11.145)$$

Найдем обменную энтропию $H(S(N), \Phi)$. Чистое входное состояние S_{12} расширенной системы $\mathcal{H} \otimes \mathcal{H}_0$ характеризуется (2×2) -матрицей ковариаций (11.78). В соответствии с соотношением (11.120) действие расширенного канала $\Phi \otimes \text{Id}$ преобразует эту матрицу к виду

$$\Delta_{12}^{-1} \alpha'_{12} = \begin{bmatrix} 0 & -(N' + 1/2) & 0 & k\sqrt{N^2 + N} \\ N' + 1/2 & 0 & k\sqrt{N^2 + N} & 0 \\ 0 & -k\sqrt{N^2 + N} & 0 & N + 1/2 \\ -k\sqrt{N^2 + N} & 0 & -(N + 1/2) & 0 \end{bmatrix}.$$

Из формулы (11.72) получаем $H(S(N), \Phi) = g(|\lambda_1| - \frac{1}{2}) + g(|\lambda_2| - \frac{1}{2})$, где $\pm \lambda_1, \pm \lambda_2$ — собственные значения матрицы в правой части. Решая характеристическое уравнение, находим

$$\lambda_{1,2} = \frac{i}{2}((N' - N) \pm D), \quad (11.146)$$

где

$$D = \sqrt{(N + N' + 1)^2 - 4k^2N(N + 1)}.$$

Следовательно,

$$H(S(N), \Phi) = g\left(\frac{D + N' - N - 1}{2}\right) + g\left(\frac{D - N' + N - 1}{2}\right). \quad (11.147)$$

Зависимость энтропий $H(\Phi[S(N)])$, $H(S(N), \Phi)$ от k для случая $N_c = 0$ показана на рис. 11.1. Заметим, что для всех N когерентная информация $H(\Phi[S(N)]) - H(S(N), \Phi)$ оказывается положительной при $k > 1/\sqrt{2}$ и отрицательной при остальных значениях k . Она стремится к $-H(S(N))$ при $k \rightarrow 0$, равна $H(S(N))$ при $k = 1$ и быстро убывает к нулю при $k \rightarrow \infty$.

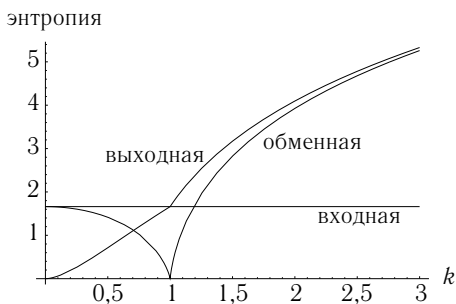


Рис. 11.1. Энтропии: выходная энтропия (11.145), обменная энтропия (11.147) в случае $N_c = 0$

Рассмотрим классические пропускные способности канала Φ при аддитивных входных энергетических ограничениях, соответствующих оператору $F = a^\dagger a$. В соответствии с теоремой 11.6.1 и следствием из нее классическая пропускная способность с использованием сцепленного состояния равна

$$C_{ea}(\Phi, F, E) = \max_{S: \text{Tr } S a^\dagger a \leq E} I(S, \Phi),$$

и она достигается на калибровочно инвариантном гауссовском состоянии S . Поскольку условие (10.40), очевидно, выполнено для данного канала, для этого состояния $\text{Tr } S a^\dagger a = E$. Поэтому $S = S(E)$, и для энтропий имеют место выражения (11.143), (11.145) и (11.147). Следовательно, указанный выше максимум равен

$$C_{ea}(\Phi, F, E) = I(S(E), \Phi) = H(S(E)) + H(\Phi[S(E)]) - H(S(E), \Phi).$$

Рассматривая величину $C_{ea}(\Phi, F, E)$ как функцию параметров E , k , N_c , интересно сравнить ее с величиной $C_\chi(\Phi, F, E)$, которая является нижней границей для классической пропускной способности $C(\Phi, F, E)$ (возможно, совпадающей с ней). Если верна гипотеза о гауссовских оптимальных ансамблях, то оптимальным является ансамбль, состоящий из когерентных состояний $S_\zeta = |\zeta\rangle\langle\zeta|$, $\zeta \in \mathbb{C}$, с гауссовской плотностью вероятности $p(\zeta) = (\pi E)^{-1} \exp(-|\zeta|^2/E)$, что приводит к значению

$$C_\chi(\Phi, F, E) = g(k^2 E + N'_0) - g(N'_0).$$

Отношение

$$G = \frac{C_{ea}(\Phi, F, E)}{C_\chi(\Phi, F, E)} \quad (11.148)$$

дает по крайней мере верхнюю границу для *выигрыша* за счет использования сцепленных состояний при передаче классических сообщений. В частности, если среднее число квантов E сигнала стремится к нулю, тогда как $N'_0 > 0$, то

$$C_\chi(\Phi, F, E) \sim Ek^2 \log\left(\frac{N'_0 + 1}{N'_0}\right),$$

$$C_{ea}(\Phi, F, E) \sim -Ek^2 \log E/(N'_0 + 1)$$

и G стремится к бесконечности как $-\log E$. График отношения G как функции аргумента k при $N_c = 0$ показан на рис. 11.2.

Гипотеза о гауссовских оптимальных ансамблях верна в частном случае аттенюатора Φ с вакуумным шумом $N_c = 0$, $k < 1$. Более того, в этом случае выполняется и гипотеза аддитивности, так что величина $C_\chi(\Phi, F, E)$ дает классическую пропускную способность канала.

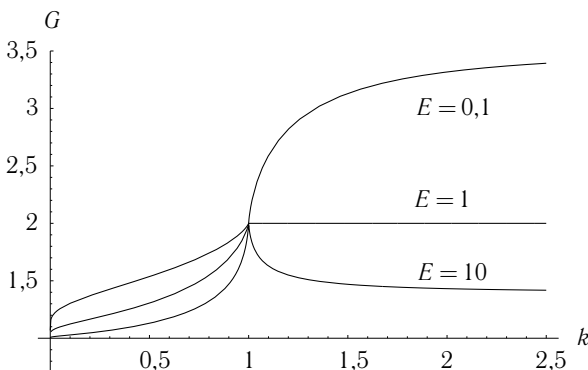


Рис. 11.2. Выигрыш (11.148) за счет использования сцепленного состояния как функция k при $N_c = 0$. Параметр = входная мощность E

Предложение 11.7.1. Для аттенюатора Φ с вакуумным шумом

$$C(\Phi, F, E) = C_\chi(\Phi, F, E) = g(k^2 E). \quad (11.149)$$

Доказательство. Докажем свойство аддитивности

$$C_\chi^{(n)}(\Phi, H^{(n)}, nE) = nC_\chi(\Phi, F, E). \quad (11.150)$$

Действительно, для этого канала $N'_0 = 0$, $N' = k^2 E$ и $H(\Phi[S(E)]) = g(k^2 E)$. Следовательно,

$$H(\Phi[S_z]) = 0 \quad (11.151)$$

для произвольного когерентного состояния S_z , для которого $E = 0$, и поэтому минимальная выходная энтропия равна нулю:

$$\min_S H(\Phi[S]) = 0.$$

Следовательно, $\min_{S^{(n)}} H(\Phi^{\otimes n}[S^{(n)}]) = 0$, и аддитивность выходной энтропии очевидна. Подставляя ансамбль когерентных состояний и используя соотношение (11.151), получаем

$$C_\chi(\Phi, F, E) \geq g(k^2 E) = \max_{S: \text{Tr } S a^\dagger a \leq E} H(\Phi[S]).$$

С другой стороны, используя субаддитивность выходной энтропии, получаем

$$nC_\chi(\Phi, F, E) \leq C_\chi^{(n)}(\Phi, F, E) \leq n \max_{S: \text{Tr } S a^\dagger a \leq E} H(\Phi[S]).$$

Сравнивая эти неравенства, мы приходим к соотношениям (11.150) и (11.149). $\square$

11.7.4. Квантовая пропускная способность

В этом пункте мы вычислим квантовую пропускную способность ряда одномодовых гауссовских каналов, опираясь на свойства (анти)деградируемости (п. 9.3.3, 11.6.3). При этом мы используем тот факт, что композиция одномодовых гауссовских каналов является одномодовым гауссовским каналом. В частности, из общих правил (11.106) вытекают следующие соотношения.

Пусть $\Phi_{C,k}$ (соответственно $\Phi_{D,k}$) — канал класса C (соответственно D) с коэффициентом k и фиксированным значением параметра N_c . Тогда

$$\Phi_{C,k_2} \circ \Phi_{C,k_1} = \Phi_{C,k_1 k_2}, \quad \text{если } k_1, k_2 < 1, \quad (11.152)$$

$$\Phi_{D,k_2} \circ \Phi_{C,k_1} = \Phi_{D,k_1 k_2}, \quad \text{если } k_1 > 1. \quad (11.153)$$

Предложение 11.7.2. Для аттенюатора с коэффициентом k , не превосходящим $\frac{1}{\sqrt{2}}$, квантовая пропускная способность $Q(\Phi_{C,k})$ равна 0. Для аттенюатора/усилителя с $k \geq \frac{1}{\sqrt{2}}$ и $N_c = 0$ выполняется равенство

$$Q(\Phi_{C,k}) = Q_G(\Phi_{C,k}) = \log \frac{k^2}{|k^2 - 1|}. \quad (11.154)$$

Здесь

$$Q_G(\Phi) = \sup_{N \geq 0} I_c(S(N), \Phi),$$

где точная верхняя грань когерентной информации $I_c(S, \Phi) = H(\Phi[S]) - H(S, \Phi)$ берется по всем гауссовским калибровочно инвариантным входным состояниям вида $S(N)$.

Доказательство. Достаточно доказать, что аттенюатор с $k < \frac{1}{\sqrt{2}}$ — антидеградируемый канал, тогда как аттенюатор/усилитель с $k \geq \frac{1}{\sqrt{2}}$ и $N_c = 0$ деградируем.

Если $k < \frac{1}{\sqrt{2}}$, то $k_1 = \frac{k}{\sqrt{1-k^2}} < 1$. Принимая во внимание, что слабо комплементарным к каналу $\Phi_{C,k}$ является канал

$$\tilde{\Phi}_{C,k}^{\omega} = \Phi_{C, \sqrt{1-k^2}}, \quad (11.155)$$

см. (11.138), соотношение (11.152) можно записать в виде

$$\Phi_{C,k} = \Phi_{C, \frac{k}{\sqrt{1-k^2}}} \circ \tilde{\Phi}_{C,k}^{\omega}, \quad (11.156)$$

откуда следует, что $\Phi_{C,k}$ — антидеградируемый канал, и, значит, в силу теоремы 9.3.2 его квантовая пропускная способность равна нулю.

В случае $N_c = 0$, когда состояние окружения чистое, комплементарный канал совпадает со слабо комплементарным: $\tilde{\Phi}_{C,k} = \tilde{\Phi}_{C,k}^{\omega} = \Phi_{C,k'}$, где $k' = \sqrt{1 - k^2} > \frac{1}{\sqrt{2}}$, и соотношение (11.156) приобретает вид

$$\tilde{\Phi}_{C,k'} = \Phi_{C, \frac{k}{\sqrt{1-k^2}}} \circ \Phi_{C,k'},$$

откуда следует, что $\Phi_{C,k'}$ — деградируемый канал при $\frac{1}{\sqrt{2}} < k' < 1$. Поэтому из предложения 11.6.1 следует, что

$$Q(\Phi_{C,k}) = Q_G(\Phi_{C,k}). \quad (11.157)$$

Аналогично в случае усилителя ($k > 1$, $N_c = 0$) из соотношения (11.153) следует, что

$$\tilde{\Phi}_{C,k} = \Phi_{D, \frac{\sqrt{k^2-1}}{k}} \circ \Phi_{C,k},$$

поэтому $\Phi_{C,k}$ — деградируемый канал, и снова имеет место равенство (11.157). Остается найти величину $Q_G(\Phi_{C,k})$.

В случае $N_c \geq 0$ когерентная информация

$$I_c(S(N), \Phi) = g(N') - g\left(\frac{D + N' - N - 1}{2}\right) - g\left(\frac{D - N' + N - 1}{2}\right) \quad (11.158)$$

сложным образом зависит от входной мощности N . Имеем $I_c(S(0), \Phi) = 0$ и

$$\lim_{N \rightarrow \infty} I_c(S(N), \Phi) = \log k^2 - \log |k^2 - 1| - g(N_c/|k^2 - 1|), \quad k \neq 1.$$

Пусть теперь $N_c = 0$. В случае $k < 1$ находим

$$N' = k^2 N, \quad D = (1 - k^2)N + 1$$

и

$$I_c(S(N), \Phi) = g(k^2 N) - g((1 - k^2)N).$$

Задача 11.7.3. Покажите, что $I_c(S(N), \Phi)$ — выпуклая убывающая функция параметра N при $k^2 < \frac{1}{2}$ (соответственно вогнутая возрастающая функция при $k^2 > \frac{1}{2}$) и, следовательно,

$$\sup_N I_c(S(N), \Phi) = \begin{cases} I_c(S(N), \Phi)|_{N=0} = 0, & k^2 < \frac{1}{2}, \\ \lim_{N \rightarrow \infty} I_c(S(N), \Phi) = \log \frac{k^2}{1 - k^2}, & k^2 > \frac{1}{2}. \end{cases}$$

В случае $k > 1$, используя соотношение (11.144), получаем $N' = k^2(N + 1) - 1$, $D = k^2(N + 1) - N$ и

$$I_c(S(N), \Phi) = g(k^2(N + 1) - 1) - g((k^2 - 1)(N + 1)).$$

Задача 11.7.4. Покажите, что $I_c(S(N), \Phi)$ — вогнутая возрастающая функция аргумента N и, следовательно,

$$\sup_N I_c(S(N), \Phi) = \lim_{N \rightarrow \infty} I_c(S(N), \Phi) = \log \frac{k^2}{k^2 - 1}.$$

Окончательно получаем общее выражение (11.154) для квантовой пропускной способности аттенюатора/усилителя при $N_c = 0$. $\square$

Обширная область нулевой квантовой пропускной способности, перекрывающая область (11.140) каналов, разрушающих сцепленность, дается следующим предложением.

Предложение 11.7.3. Пусть $k \geq \frac{1}{\sqrt{2}}$, тогда $Q(\Phi_{C,k}) = 0$ при

$$N_c \geq \frac{1}{2}(k^2 - |k^2 - 1|) = \min\{k^2, 1\} - \frac{1}{2}. \quad (11.159)$$

Доказательство. Рассмотрим композицию $\Phi = \Phi_2 \circ \Phi_1$, где

$$\Phi_1^*[W(z)] = W(\sqrt{2}kz) \exp\left[-\frac{(2k^2 - 1)}{2}\left(N_1 + \frac{1}{2}\right)\right],$$

$$\Phi_2^*[W(z)] = W\left(\frac{z}{\sqrt{2}}\right) \exp\left[-\frac{1}{4}\left(N_2 + \frac{1}{2}\right)\right],$$

так что $Q(\Phi_2) = 0$ в силу предложения 11.7.2 и, значит, $Q(\Phi_2 \circ \Phi_1) = 0$ в силу неравенства (9.45). Тогда

$$\Phi_1^* \circ \Phi_2^*[W(z)] = W(kz) \exp\left[-\frac{1}{2}\left(\frac{|k^2 - 1|}{2} + N_c\right)\right],$$

где

$$\frac{|k^2 - 1|}{2} + N_c = \frac{1}{2}\left(N_2 + \frac{1}{2}\right) + \frac{(2k^2 - 1)}{2}\left(N_1 + \frac{1}{2}\right).$$

Варьируя числа $N_1, N_2 \geq 0$, можно получить все значения N_c , удовлетворяющие условию (11.159). $\square$

Задача 11.7.5. Докажите, что в случае А выполняется равенство

$$\Phi = \Phi \circ \tilde{\Phi},$$

где $\tilde{\Phi}$ — комплементарный канал, и, следовательно, канал Φ антидеградируемый, а значит, $Q(\Phi) = 0$.

Задача 11.7.6. Докажите, что в случае В₁ выполняется равенство $Q(\Phi) = \infty$. Для этого рассмотрите когерентную информацию $I_c(S, \Phi) = H(\Phi[S]) - H(\tilde{\Phi}[S])$, где S — гауссовское состояние с дисперсиями

$\sigma_q^2 = DQ$, $\sigma_p^2 = DP$ и нулевыми средними и ковариацией. Покажите, что

$$H(\Phi[S]) = g\left(\sqrt{\sigma_Q^2\left(\sigma_P^2 + \frac{1}{2}\right)} - \frac{1}{2}\right),$$

$$H(\tilde{\Phi}[S]) = g\left(\sqrt{\left(\sigma_Q^2 + \frac{1}{2}\right)\frac{1}{2}} - \frac{1}{2}\right).$$

В частности, выбирая состояния, для которых $\sigma_Q^2 \sigma_P^2 \rightarrow \infty$, $\sigma_Q^2 \rightarrow 0$, получаем $I_c(S, \Phi) \rightarrow \infty$.

Задача 11.7.7. Докажите, что в случае D канал Φ является антидеградируемым и, следовательно, $Q(\Phi) = 0$.

Поскольку $I_c(S, \Phi) = H(\Phi[S]) - H(\tilde{\Phi}[S])$, для пропускной способности $Q(\tilde{\Phi})$ имеет место выражение, аналогичное (9.40), в котором I_c заменено на $-I_c$. Следовательно,

$$\sup_S I_c(S, \Phi) \leq Q(\Phi), \quad \sup_S [-I_c(S, \Phi)] \leq Q(\tilde{\Phi}).$$

Таким образом, если когерентная информация $I_c(S, \Phi)$ принимает значения разных знаков, то обе пропускные способности положительны и, следовательно, канал Φ не является ни деградируемым, ни антидеградируемым.

Задача 11.7.8. Рассмотрим канал с аддитивным классическим гауссовским шумом интенсивности N_c (случай B₂, $k = 1$). Покажите, что

$$F(N) \equiv I_c(S(N), \Phi) = g\left(N + N_c\right) - g\left(\frac{D + N_c - 1}{2}\right) - g\left(\frac{D - N_c - 1}{2}\right),$$

где $D = \sqrt{(N_c + 1)^2 + 4N_c N}$. При этом $F(0) = 0$,

$$\lim_{N \rightarrow \infty} F(N) = -\log e N_c,$$

где использована асимптотика $g(x) \simeq \log ex$ при $x \rightarrow \infty$, следовательно, $\lim_{N \rightarrow \infty} F(N) = 0$, если $N_c = e^{-1}$. Рассматривая функцию $F(N)$ при $N_c = 0,99e^{-1}$, покажите, что она принимает значения разных знаков и, следовательно, канал Φ не является ни деградируемым, ни антидеградируемым.

§ 11.8. Комментарии

1. Квантовый гармонический осциллятор, впервые исследованный Дираком [8], лежит в основе многих математических моделей квантовой

оптики и квантовой электроники. В частности, полезное символическое исчисление, позволяющее получить алгебраические тождества, вытекающие из канонических коммутационных соотношений, такие как (11.46), развито в книге Люиселла [15]. Анализ, основанный на когерентных состояниях, разработан Глаубером; см. [7]. Формула (11.14) — это знаменитое P -представление операторов плотности, широко используемое в квантовой оптике. Представление поля излучения в виде ансамбля квантовых осцилляторов, также предложенное Дираком, в подходящей для приложений в квантовой оптике форме рассмотрено, например, в книгах Клаудера и Сударшана [12] и Хелстрема [30].

Используя переполненность системы когерентных векторов (задача 11.1.4), можно определить нечеткую наблюдаемую со значениями в $\mathbb{C} \equiv \mathbb{R}^2$:

$$M(B) = \frac{1}{\pi} \int_B |\zeta\rangle \langle \zeta| d^2\zeta. \quad (11.160)$$

Она играет ключевую роль в описании «приближенного совместного измерения» наблюдаемых q и p . Подробное обсуждение этого вопроса и дальнейшие ссылки см. в книгах А. С. Холево [37] и Дэвиса [73].

2. На полезность представления ККС в симметричной форме (11.28) указал Сигал; см. [27]. Доказательство следующей теоремы можно найти, например, в работе [37].

Теорема (единственности Стоуна—фон Неймана). Пусть $V_x, U_y, x, y \in \mathbb{R}^s$, — сильно непрерывные группы унитарных операторов в сепарабельном гильбертовом пространстве $\mathcal{H}$, удовлетворяющие ККС Вейля (11.26). Тогда V_x, U_y унитарно эквивалентны прямой сумме не более чем счетного числа копий представления Шрёдингера (11.25). В частности, любое неприводимое представление ККС унитарно эквивалентно представлению Шрёдингера.

Работа Вильямсона [155] содержит общую классификацию классических квадратичных гамильтонианов (необязательно положительных). Доказательство леммы 11.2.1 см. также в гл. V книги [37].

3. Многочисленные физические приложения линейной динамики систем с квадратичным гамильтонианом рассматриваются в книге И. А. Малкина и В. И. Манько [18].

4. Рассмотрение квантовых гауссовских состояний основано на гл. V книги А. С. Холево [37], где можно найти доказательства утверждений задач 11.4.1—11.4.3, 11.4.5. Условие (11.53) является не только необходимым, но и достаточным для положительности оператора S . Подход к квантовым гауссовским состояниям, основанный на характеристической функции, опирается на очевидные аналогии с классической теорией

вероятностей и является, по-видимому, наиболее прямым и аналитически прозрачным.

Формулы для энтропии квантовых состояний общего вида были получены А. С. Холево, Сома и Хирота [100]. Характеризация гауссовского состояния как состояния с максимальной энтропией (лемма 11.4.2) тесно связана с принципом максимальной энтропии в статистической физике, см., например, [15, раздел 6.6]; аналогичное свойство для условной квантовой энтропии (лемма 11.4.3) было установлено Айсертом и Вольфом; см. [79].

Очищение произвольного гауссовского состояния построено в работе А. С. Холево [32].

5. Формула для пропускной способности гауссовского s - q -канала была предугадана Гордоном; см. [87]. Приведенное доказательство следует работе А. С. Холево [35], где рассмотрен и случай многомодового гауссовского s - q -канала, в частности реалистичная модель временного классического сигнала на фоне окрашенного квантового шума. Пропускная способность для канала со сжатым гауссовским шумом вычислена в работе А. С. Холево, Сома и Хирота [100]. Более детальную информацию о скорости сходимости вероятности ошибки для гауссовских каналов с чистыми состояниями можно получить, модифицируя оценки функции надежности из § 5.7 на случай каналов с бесконечным алфавитом и входными ограничениями; см. [101].

Общее описание бозонных гауссовских каналов было дано в работе А. С. Холево и Р. Ф. Вернера [103] (см. также обзор [79]); при этом авторы следовали работе [31]. Используя общее описание бозонного гауссовского канала, можно показать, что в квантовой оптике такие каналы могут быть реализованы из блоков, соответствующих линейным многоканальным смесителям и основным одномодовым преобразователям, таким как параметрический усилитель; см. [65].

С другой стороны, гауссовские каналы представляют собой вполне положительные отображения C^* -алгебры ККС; Демон, Ванеувертвин и Вербер (см. [75]) показали, что неотрицательная определенность матриц (11.104) необходима и достаточна для полной положительности отображения Φ .

Гауссовские наблюдаемые фактически соответствуют гауссовским q - s -каналам; они рассматриваются в гл. VI книги [37]. В частности, там показано, что расширение Наймарка для нечеткой наблюдаемой (11.160) дается спектральной мерой коммутирующих операторов $q + q_C$, $p - p_C$, где мода C находится в вакуумном состоянии.

Гауссовские каналы, разрушающие сцепленность, исследованы в работе А. С. Холево [105].

6. Принцип «пропускная способность гауссовского канала достигается для гауссовского сигнала» выполняется в классической теории информации; см. [70]. Гипотеза об оптимальных гауссовских ансамблях экстраполирует аналогичный принцип на квантовые гауссовские каналы, однако в этом направлении пока получены лишь частичные результаты. Имеются основания полагать, что подтверждение этой гипотезы для классической пропускной способности квантового гауссовского канала по крайней мере частично зависит от решения проблемы аддитивности. В работе Вольфа, Гидке и Сирака [159] показано, что если гипотеза аддитивности верна, то среднее состояние $\bar{S}_\pi$ оптимального ансамбля должно быть гауссовским.

Теорема 11.6.1, доказанная в статье А. С. Холево и Р. Ф. Вернера [103], означает выполнение «гауссовского» принципа для классической пропускной способности с использованием сцепленного состояния. Предложение 11.6.1, подтверждающее этот принцип для квантовой пропускной способности деградируемых гауссовских каналов, основано на результатах Вольфа, Перес-Гарсиа и Гидке; см. [160].

7. Классификация одномодовых гауссовских каналов была получена А. С. Холево; см. [105], а также [67].

Пропускные способности аттенюатора/усилителя изучались в работе [103]. Предложение 11.7.1 для аттенюатора с вакуумным шумом доказано в статье Джованнетти, Гуха, Ллойда, Макконе, Шапиро и Юна [86].

Утверждение о том, что квантовая пропускная способность аттенюатора/усилителя дается гауссовским выражением, полученным в работе [103], было установлено Вольфом и Перес-Гарсиа в работе [160]. Области нулевой квантовой пропускной способности описаны в статье Карузо, Джованнетти и А. С. Холево [67]. Решения задач из п. 11.7.4, в частности подробное описание канала, комплементарного к каналу с аддитивным классическим гауссовским шумом, см. в работе А. С. Холево [41].

Литература

1. *Бурнашев М. В., Холево А. С.* О функции надежности квантового канала связи // Пробл. передачи информ. 1998. Т. 34. С. 1—13; e-print quant-ph/9703013, 1997.
2. *Валиев К. А., Кокин А. А.* Квантовые компьютеры: надежды и реальность. М.; Ижевск: РХД, 2001.
3. *Вейль Г.* Теория групп и квантовая механика. М.: Наука, 1986.
4. *Вигнер Э. П.* Теория групп и ее приложения к квантовомеханической теории атомных спектров. М.: Физматгиз, 1961.
5. *Галлагер Р.* Теория информации и надежная связь. М.: Советское радио, 1974.
6. *Глазман И. М., Любич Ю. И.* Конечномерный линейный анализ в задачах. М.: Наука, 1969.
7. *Глаубер Р.* Оптическая когерентность и статистика фотонов // Квантовая оптика и квантовая радиофизика. М.: Мир, 1966.
8. *Дирак П. А. М.* Принципы квантовой механики. М.: Наука, 1970.
9. *Кадомцев Б. Б.* Динамика и информация. М.: УФН, 1999.
10. *Китаев А. Ю., Шень А., Вьялый М. Н.* Классические и квантовые вычисления. М.: МЦНМО, 1999.
11. *Китаев А. Ю.* Квантовые вычисления: алгоритмы и исправление ошибок // УМН. 1997. Т. 52, № 6. С. 53—112.
12. *Клаудер Дж., Сударшан Э.* Основы квантовой оптики. М.: Мир, 1970.
13. *Кострикин А. И., Манин Ю. И.* Линейная алгебра и геометрия. М.: Наука, 1986.
14. *Курикса А. А.* Квантовая оптика и оптическая локация. М.: Советское радио, 1973.
15. *Люиселл У.* Излучение и шумы в квантовой оптике. М.: Наука, 1972.
16. *Макки Дж.* Лекции по математическим основам квантовой механики. М.: Мир, 1965.
17. *Магарил-Ильяев Г. Г., Тихомиров В. М.* Выпуклый анализ и его приложения. М.: УРСС, 2003.
18. *Малкин И. А., Манько В. И.* Динамические симметрии и когерентные состояния квантовых систем. М.: Наука, 1979.
19. *Митюгов В. В.* Физические основы теории информации. М.: Советское радио, 1976.
20. *Морозова Е. А., Ченцов Н. Н.* Марковская инвариантная геометрия на многообразиях состояний. Итоги науки и техники // Совр. пробл. матем. Новейшие достижения. ВИНТИ, 1990. Т. 36. С. 69—102.
21. *фон Нейман Дж.* Математические основы квантовой механики. М.: Наука, 1964.
22. *Нильсен М. А., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир, 2006.
23. *Наймарк М. А.* Спектральные функции симметричного оператора // Изв. АН СССР. Сер. матем. 1940. Т. 4, № 3. С. 277—318.

24. Рид М., Саймон Б. Методы современной математической физики / Пер. с англ. Т. 1. М.: Мир, 1985.
25. Рокафеллар Р. Выпуклый анализ / Пер. с англ. М.: Мир, 1973.
26. Сарымсаков Т. А. Введение в квантовую теорию вероятностей. Ташкент: ФАН, 1985.
27. Сигал И. Математические проблемы релятивистской физики. М.: Мир, 1968.
28. Стратонович Р. Л., Ванцян А. Г. Об асимптотически безошибочном декодировании в чистых квантовых каналах // Пробл. управл. и теор. информ. 1978. Т. 7, № 3. С. 161—174.
29. Фаддеев Л. Д., Якубовский О. А. Лекции по квантовой механике для студентов-математиков. Изд-во ЛГУ, 1980.
30. Хелстром К. Квантовая теория проверки гипотез и оценивания / Пер. с англ. М.: Мир, 1978.
31. Холево А. С. К математической теории квантовых каналов связи // Пробл. передачи информ. 1972. Т. 8, № 1. С. 63—71.
32. Холево А. С. О квазиэквивалентности локально-нормальных состояний // ТМФ. 1972. Т. 13, № 2. С. 184—199.
33. Холево А. С. Информационные аспекты квантовых измерений // Пробл. передачи информ. 1973. Т. 9, № 2. С. 31—42.
34. Холево А. С. Некоторые оценки для количества информации, передаваемого квантовым каналом связи // Пробл. передачи информ. 1973. Т. 9, № 3. С. 3—11.
35. Холево А. С. Квантовые теоремы кодирования // УМН. 1998. Т. 53. С. 193—230; arXiv: quant-ph/9809023
36. Холево А. С. Статистическая структура квантовой теории. М.; Ижевск: 2003.
37. Холево А. С. Вероятностные и статистические аспекты квантовой теории. 2-е изд. М.; Ижевск: ИКИ, 2004.
38. Холево А. С. Введение в квантовую теорию информации. М.: МЦНМО, 2003.
39. Холево А. С., Широков М. Е., Вернер Р. Ф. О понятии сцепленности в гильбертовых пространствах // УМН. 2005. Т. 60, № 2. С. 153—154; Separability and entanglement-breaking in infinite dimensions, e-print quant-ph/0504204
40. Холево А. С. Комплементарные каналы и проблема аддитивности // ТВП. 2006. Т. 51. С. 133—134; e-print quant-ph/0509101
41. Холево А. С. Одномодовые квантовые гауссовские каналы: структура и квантовая пропускная способность // Проблемы передачи информации. 2007. Т. 43. С. 1—11; e-print quant-ph/0607051
42. Холево А. С. Классические пропускные способности квантового канала // ТВП. 2003. Т. 48. С. 359—374; e-print quant-ph/0211170
43. Холево А. С., Широков М. Е. Непрерывные ансамбли и пропускная способность квантовых каналов бесконечной размерности // ТВП. 2005. Т. 50, № 1. С. 98—114; e-print quant-ph/0408176
44. Чисар И., Кёрнер Я. Теория информации. М.: Мир, 1985.

45. *Широков М.Е.* Энтропийные характеристики подмножеств состояний: I // Известия РАН. Серия математическая. 2006. Т. 70, № 6. С. 193—222.
46. *Широков М.Е.* О свойствах квантовых каналов, связанных с классической пропускной способностью // Теория вероятностей и ее применения. 2007. Т. 52, № 2. С. 301—335.
47. *Abeyesinghe A., Devetak I., Hayden P., Winter A.* The mother of all protocols: Restructuring quantum information's family tree quant-ph/0606225
48. *Adami C., Cerf N.J.* Capacity of noisy quantum channels // Phys. Rev. A. 1997. Vol. 56. P. 3470—3485.
49. *Ahlsvede R., Csiszár I.* Common randomness in information theory and cryptography. P. II: CR capacity // IEEE Trans. Inform. Theory. 1998. Vol. 44. P. 225—240.
50. *Alber G., Beth T., Horodecki M., Horodecki P., Horodecki R., Rötteler M., Weinfurter H., Werner R.F.* Quantum information. An introduction to basic theoretical concepts and experiments. Berlin: Springer, 2001.
51. *Araki H.* On a characterization of the state space in quantum mechanics // Commun. Math. Phys. 1980. Vol. 75, № 1. P. 1—24.
52. *Audenaert K.M.R.* A sharp Fannes-type inequality for the von Neumann entropy; e-print quant-ph/0610146
53. *Barnum H., Knill E., Nielsen M.A.* On quantum fidelities and channel capacities // IEEE Trans. Inform. Theory. 1998. Vol. 46, № 4. P. 1317—1329; e-print quant-ph/9809010
54. *Barnum H., Nielsen M.A., Schumacher B.* Information transmission through a noisy quantum channel // Phys. Rev. A. 1998. Vol. 57. P. 4153—4175.
55. *Bell J.S.* On the Einstein—Podolsky—Rosen paradox // Physics. 1964. Vol. 1. P. 195—200.
56. *Bennett C.H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W.K.* Teleporting an unknown quantum state via dual classical and EPR channels // Phys. Rev. Lett. 1993. Vol. 70. P. 1895—1899.
57. *Bennett C.H., Devetak I., Shor P.W., Smolin J.A.* Inequalities and separations among assisted capacities of quantum channels; quant-ph/0406086
58. *Bennett C.H., Di Vincenzo D.P., Smolin J.A., Wootters W.K.* Mixed state entanglement and quantum error correction; quant-ph/9604024
59. *Bennett C.H., Fuchs C.A., Smolin J.A.* Entanglement-enhanced classical communication on a noisy quantum channel // Quantum Communication, Computing and Measurement. Proc. QCM96 / Ed. O. Hirota, A. S. Holevo, C. M. Caves. New York: Plenum 1997. P. 79—88; e-print quant-ph/9611006
60. *Bennett C.H., Shor P.W.* Quantum Information Theory // IEEE Trans. Inform. Theory. 1998. Vol. 44, № 6. P. 2724—2742.
61. *Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V.* Entanglement-assisted capacity and the reverse Shannon theorem // IEEE Trans. Inform. Theory; e-print quant-ph/0106052

62. *Bennett C.H., Wiesner S.J.* Communication via one- and two-particle operators on Einstein—Podolsky—Rosen states // *Phys. Rev. Lett.* 1992. Vol. 69. P. 2881—2884.
63. *Bhatia R.* Matrix Analysis. New York: Springer, 1997.
64. *Bjelaković I., Siegmund-Schultze R.* A new proof of the monotonicity of quantum relative entropy for finite quantum systems; e-print quant-ph/0307170
65. *Braunstein S.L.* Squeezing as an irreducible resource; e-print quant-ph/9904002
66. *Calderbank R., Shor P.W.* Good quantum error-correcting codes exist // *Phys. Rev. A.* 1996. Vol. 54. P. 1098—1105; Good Quantum Error-Correcting Codes Exist // *Phys. Rev. A.* 1996. Vol. 54, № 2. P. 1098—1106; quant-ph/9512032
67. *Caruso F., Giovannetti V., Holevo A.S.* One-mode Bosonic Gaussian channels: a full weak-degradability classification // *New Journal of Physics.* 2006. Vol. 8, № 310; quant-ph/0609013
68. *Caves C.M., Drummond P.B.* Quantum limits of bosonic communication rates // *Rev. Mod. Phys.* 1994. Vol. 66. P. 481—538.
69. *Choi M.-D.* Completely positive maps on complex matrices // *Linear Alg. and Its Appl.* 1975. Vol. 10. P. 285—290.
70. *Cover T.M., Thomas J.A.* Elements of Information Theory. New York: Wiley Series in Telecommunications, John Wiley & Sons, 1991.
71. *Cubitt T.S., Ruskai M.-B., Smith G.* The structure of degradable quantum channels; arXiv:0802.1360
72. *Davies E.B.* Information and quantum measurement // *IEEE Trans. Inform. Theory.* 1978. Vol. 24, № 6. P. 596—599.
73. *Davies E.B.* Quantum theory of open systems. London: Academic Press, 1976.
74. *Dell'Antonio G.F.* On the limits of sequences of normal states // *Commun. Pure Appl. Math.* 1967. Vol. 20. P. 413—430.
75. *Demoen B., Vanheuverzwijn P., Verbeure A.* Completely positive quasi-free maps on the CCR algebra // *Rep. Math. Phys.* 1979. Vol. 15. P. 27—39.
76. *Devetak I.* The private classical information capacity and quantum information capacity of a quantum channel; e-print quant-ph/0304127, 2003.
77. *Devetak I., Shor P.* The capacity of a quantum channel for simultaneous transition of classical and quantum information; quant-ph/0311131
78. *Di Vincenzo D., Shor P.W., Smolin J.* Quantum channel capacities of very noisy channels // *Phys. Rev. A.* 1998. Vol. 57. P. 830—839.
79. *Eisert J., Wolf M.M.* Gaussian quantum channels; quant-ph/0505151
80. *Effros E.G.* A matrix convexity approach to some celebrated quantum inequalities; math-ph/0802.1234
81. *Fannes M.* A continuity property of quantum entropy for spin lattice systems // *Commun. Math. Phys.* 1973. Vol. 31. P. 291—294.
82. Foundations of quantum mechanics and ordered linear spaces / Ed. A. Hartkammer, H. Neumann. New York; Heidelberg; Berlin: Springer-Verlag, 1974. (Lect. Notes Phys; Vol. 29).

83. *Fuchs C.A.* Quantum mechanics as quantum information (and only a little more); e-print quant-ph/0205039
84. *Fukuda M., Wolf M.M.* Simplifying additivity problems using direct sum constructions // *J. Math. Phys.* 2007. Vol. 48, № 072101.
85. *Fukuda M., King C., Moser D.* Comments on Hastings' additivity counter-examples; e-print arXiv:0905.3697
86. *Giovannetti V., Guha S., Lloyd S., Maccone L., Shapiro J.H., Yuen H.P.* Classical capacity of the lossy bosonic channel: the exact solution; e-print quant-ph/0308012
87. *Gordon J.P.* Noise at optical frequencies; information theory // *Quantum Electronics and Coherent Light, Proc. Int. School Phys. «Enrico Fermi», Course XXXI / Ed. P.A.Miles. New York: Academic Press, 1964. P. 156—181.*
88. *Hastings M.B.* A counterexample to additivity of minimum output entropy; quant-ph/0809.3972
89. *Hausladen P., Jozsa R., Schumacher B., Westmoreland M., Wootters W.* Classical information capacity of a quantum channel // *Phys. Rev. A.* 1996. Vol. 54. P. 1869—1876.
90. *Hayashi M.* Quantum information: an introduction. Berlin: Springer, 2006.
91. *Hayashi M., Nagaoka H.* General formulas for capacity of classical-quantum channels; e-print quant-ph/0206186
92. *Hayden P.* The maximal p-norm multiplicativity conjecture is false; quant-ph/0707.3291
93. *Hayden P.* Entanglement in Random Subspaces // *Proc. of QCMC04. AIP conference proceedings. 2004. Vol. 734. P. 226—229; quant-ph/0409157*
94. *Hayden P., Shor P.W., Winter A.* Random quantum codes from Gaussian ensembles and an uncertainty relation // *Open Syst. Inf. Dyn.* 2008. Vol. 15. P. 71—89; quant-ph/0712.0975
95. *Hiroshima T.* Additivity and multiplicativity properties of some Gaussian channels for Gaussian inputs // *Phys. Rev. A* 2006. Vol. 73, № 012330; quant-ph/0511006
96. *Hoeffding W.* Probability inequalities for sums of bounded random variables // *J. Amer. Statist. Assoc.* 1963. Vol. 58, № 31. P. 13—30.
97. *Holevo A.S.* Statistical definition of observable and the structure of statistical models // *Rep. Math. Phys.* 1985. Vol. 22, № 3. P. 385—407.
98. *Holevo A.S.* The capacity of quantum communication channel with general signal states; e-print quant-ph/9611023, 1996; *IEEE Trans. Inform. Theory.* 1998. Vol. 44. P. 269—272.
99. *Holevo A.S.* On entanglement-assisted classical capacity // *J. Math. Phys.* 2002. Vol. 43; e-print quant-ph/0106075
100. *Holevo A.S., Shohma M., Hirota O.* Capacity of quantum Gaussian channels // *Phys. Rev. A.* 1999. Vol. 59. P. 1820—1828.
101. *Holevo A.S., Shohma M., Hirota O.* Error exponents for quantum channels with constrained inputs // *Rep. Math. Phys.* 2000. Vol. 46. P. 343—358.

102. *Holevo A. S., Shirokov M. E.* On Shor's channel extension and constrained channels // Commun. Math. Phys. 2004. Vol. 249. P. 417—430; arxiv e-print quant-ph/0306196
103. *Holevo A. S., Werner R. F.* Evaluating capacities of Bosonic Gaussian channels // Phys. Rev. A. 2001. Vol. 63, № 032312; LANL e-print quant-ph/9912067, 1999.
104. *Holevo A. S.* The additivity problem in quantum information theory. Madrid, Spain: Proc. ICM, 2006. P. 999—1018.
105. *Holevo A. S.* Entanglement-breaking channels in infinite dimensions; quant-ph/0802.0235
106. *Horodecki M., Oppenheim J., Winter A.* Quantum state merging and negative information // Comm. Math. Phys. 2006. Vol. 269, № 107; quant-ph/0512247
107. *Horodecki M., Shor P. W., Ruskai M. B.* General entanglement breaking channels // Rev. Math. Phys. 2003. Vol. 15. P. 629—641; quant-ph/0302031
108. *Josza R., Schumacher B.* A new proof of the quantum noiseless coding theorem / J. Modern Optics. 1994. Vol. 41. P. 2343—2349.
109. *Kato K., Osaki M., Hirota O.* Derivation of classical capacity of quantum channels for discrete information sources; e-print quant-ph/9811085
110. *Kato K., Osaki M., Suzuki T., Ban M., Hirota O.* Upper bound of the accessible information and lower bound of the Bayes cost in quantum signal detection processes // Phys. Rev. A. 1996. Vol. 54. P. 2718—2727.
111. *Keyl M.* Fundamentals of Quantum Information; e-print quant-ph/0202122. Feb. 2002.
112. *King C.* Additivity for a class of unital qubit channels; e-print quant-ph/0103156
113. *King C.* The capacity of quantum depolarizing channel; e-print quant-ph/0204172
114. *King C., Matsumoto K., Natanson M., Ruskai M. B.* Properties of conjugate channels with applications to additivity and multiplicativity; quant-ph/0509126
115. *Knill E., Laflamme R.* Theory of quantum error-correcting codes // Phys. Rev. A. 1997. Vol. 55. P. 900—911.
116. *Kraus K.* States, Effects and Operations. Springer, 1983. (Lecture Notes in Physics; Vol. 190).
117. *Kretschmann D., Werner R.* Tema con variazioni: quantum channel capacities; e-print quant-ph/0311037
118. *Kretschmann D., Werner R.* Quantum channels with memory; e-print quant-ph/0502106
119. *Lesniewski A., Ruskai M. B.* Monotone Riemannian metrics and relative entropy on noncommutative probability spaces // J. Math. Phys. 1999. Vol. 40. P. 5702—5724.
120. *Levitin L. B.* Optimal quantum measurement for two pure and mixed states // Quantum Communications and Measurement, Proc. QCM94 / Ed. V. P. Belavkin, O. Hirota, R. L. Hudson. New York: Plenum, 1995. P. 439—448.

121. *Lieb E. H., Ruskai M. B.* Proof of the strong subadditivity of quantum mechanical entropy // J. Math. Phys. 1973. Vol. 14. P. 1938—1941.
122. *Lindblad G.* Entropy, information and quantum measurements // Commun. Math. Phys. 1973. Vol. 33. P. 305—322.
123. *Lindblad G.* Expectations and entropy inequalities for finite quantum systems // Commun. Math. Phys. 1974. Vol. 39. P. 111—119.
124. *Lindblad G.* Completely positive maps and entropy inequalities // Commun. Math. Phys. 1975. Vol. 40. P. 147—151.
125. *Lindblad G.* Quantum entropy and quantum measurements // Quantum Aspects of Optical Communication / Ed. C. Benjaballah, O. Hirota, S. Reynaud. 1991. (Lect. Notes Phys.; Vol. 378). P. 71—80.
126. *Lloyd S.* Capacity of noisy quantum channel // Phys. Rev. 1997. Vol. A 55. P. 1613—1622.
127. *Ludwig G.* Foundations of Quantum Mechanics. Vol. I. Berlin; Heidelberg; New York: Springer, 1983.
128. *Ohya M., Petz D.* Quantum Entropy and Its Use // Texts and Monographs in Physics. New York: Springer, 1993.
129. *Ozawa M.* On information gain by quantum measurement of continuous observable // J. Math. Phys. 1986. Vol. 27. P. 759—763.
130. *Ozawa M.* Quantum measuring process of continuous observables // J. Math. Phys. 1987. Vol. 18. P. 412—421.
131. *Parthasarathy K. R.* Probability measures on metric spaces, New York; London: Academic Press, 1967.
132. *Petz D.* Quantum information theory and quantum statistics. Berlin: Springer, 2008.
133. *Ruskai M. B., Szarek S., Werner E.* A characterization of completely-positive trace-preserving maps on $\mathcal{M}_2$; e-print quant-ph/0005004
134. *Sasaki M., Barnett S. M., Jozsa R., Osaki M., Hirota O.* Accessible information and optimal strategies for real symmetric quantum sources // Phys. Rev. A. 1999. Vol. 59, № 3325; e-print quant-ph/9812062
135. *Schumacher B., Westmoreland M. D.* Sending classical information via noisy quantum channel // Phys. Rev. A. 1997. Vol. 56. P. 131—138.
136. *Schumacher B., Westmoreland M. D.* Quantum privacy and quantum coherence // Phys. Rev. Lett. 1998. Vol. 80. P. 5695—5697; e-print quant-ph/9709058
137. *Schumacher B., Westmoreland M. D.* Optimal signal ensembles; e-print quant-ph/9912122
138. *Schumacher B., Westmoreland M. D.* Approximate quantum error correction; e-print quant-ph/0112106
139. *Shannon C., Weaver W.* The mathematical theory of communication. Urbana Ill.: Univ. Illinois Press, 1949. [Имеется русский перевод: Шеннон К. Математическая теория связи // Теория передачи электрических сигналов при наличии помех. М.: ИЛ, 1953.]

140. *Shirokov M. E.* The Holevo capacity of infinite dimensional channels and the additivity problem // Commun. Math. Phys. 2006. Vol. 262, № 2. P. 137—159; e-print quant-ph/0408009
141. *Shor P. W.* Introduction to quantum algorithms; e-print quant-ph/0005003
142. *Shor P. W.* On the number of elements needed in a POVM attaining the accessible information; e-print quant-ph/0009077
143. *Shor P. W.* Additivity of the classical capacity of entanglement-breaking quantum channels // J. Math. Phys. 2002. Vol. 43. P. 4334—4340; e-print quant-ph/0201149
144. *Shor P. W.* The adaptive classical capacity of a quantum channel, or information capacity of 3 symmetric pure states in three dimensions; e-print quant-ph/0206058
145. *Shor P. W.* Equivalence of additivity questions in quantum information theory // Commun. Math. Phys. 2004. Vol. 246. P. 453—472; arXiv: quant-ph/0305035
146. *Shor P. W.* The classical capacity achievable by a quantum channel assisted by limited entanglement // Quantum Information, Statistics, Probability / Ed. O. Hirota. New Jersey: Rinton Press, Inc., Princeton, 2004; quant-ph/0402129
147. *Smith G., Smolin J. A.* Degenerate quantum codes for Pauli channels // Phys. Rev. Lett. 2007. Vol. 98. 030501.
148. *Steane A.* Quantum computing // Rept. Prog. Phys. 1997. Vol. 61. P. 117—173.
149. *Stinespring W. F.* Positive functions on C^* -algebras // Proc. Amer. Math. Soc. 1955. Vol. 6. P. 211—316.
150. *Uhlmann A.* The «transition probability» in the state space of a $*$ -algebra // Rept. Math. Phys. 1976. Vol. 9. P. 273—279.
151. *Uhlmann A.* Relative entropy and the Wigner—Yanase—Dyson—Lieb concavity in an interpolation theory // Commun. Math. Phys. 1977. Vol. 54. P. 21—32.
152. *Wehrl A.* General properties of entropy // Rev. Mod. Phys. 1978. Vol. 50. P. 221—260.
153. *Werner R. F., Wolf M. M.* Bound entangled Gaussian states; e-print quant-ph/0009118
154. *Wightman A. S.* Hilbert's sixth problem: mathematical treatment of the axioms of physics // Proc. Symp. in pure math. Vol. 28. 1977. Pt. 1. C. 147—240.
155. *Williamson J.* On the algebraic problem concerning the normal forms of linear dynamical systems // Am. J. Math. 1936. Vol. 58, № 141; 1937. Vol. 59, № 599; 1939. Vol. 61, № 897.
156. *Winter A.* Coding theorem and strong converse for quantum channels // IEEE Trans. Inform. Theory. 1999. Vol. 45. P. 2481—2485.
157. *Winter A.* Compression of sources of probability distributions and density operators; e-print quant-ph/0208131
158. *Winter A.* The maximum output p -norm of quantum channels is not multiplicative for any $p > 2$; e-print quant-ph/ 0707.0402

-
159. *Wolf M., Giedke G., Cirac J.I.* Extremality of Gaussian quantum states; quant-ph/0509154
160. *Wolf M., Pérez-García D., Giedke G.* Quantum Capacities of Bosonic Channels // Phys. Rev. Lett. 2007. Vol. 98, № 130501; quant-ph/0606132

Предметный указатель

- ансамбль 147, 159
 - обобщенный 244
- асимптотическая
 - равнораспределенность 68, 99
- аттенуатор/усилитель 303
- базис
 - Белла 60
 - Паули 27
 - симплектический 264
- бит 21
- q-бит 27
- вероятностная операторнозначная мера 29, 248
- вероятностное распределение 29
- вероятность ошибки 75, 85, 158
- вполне положительное отображение 116
- выпуклая оболочка 147, 160
- выпуклая комбинация 18
- гипотеза аддитивности 163
- *-гомоморфизм 117
- дисперсия наблюдаемой 33
- дополнительность 31
- достижимая скорость 76, 80, 85, 201
- инструмент 126
- информация
 - квантовая 61, 185
 - — взаимная 153
 - —, невозможность копирования 61
 - классическая (шенноновская) 70
 - когерентная 190
- канал
 - антидеградируемый 207
 - бистохастический 122
 - восстанавливающий 188
 - гауссовский 283
 - деградируемый 207
 - деполяризующий 132
 - диагональный 130
 - калибровочно ковариантный 294
 - квантово-классический 123
 - квантовый 122, 242
 - — с перехватом 210
 - — стирающий 124
 - классически-квантовый 123, 236
 - классический 70
 - — с перехватом 80
 - ковариантный 133
 - комплементарный 127
 - линейный бозонный 283
 - полностью деполяризующий 124
 - , разрушающий сцепленность 124, 248
 - точно обратимый 191
- канонические коммутационные соотношения Вейля—Сигала 263
 - — — дискретная версия 131
- канонические наблюдаемые 265
- картина Гейзенберга 114, 122
 - Шрёдингера 114, 122
- код 75, 85, 158
 - квантовый, исправляющий ошибки 188
- коммутатор 30
- компактность
 - множества вероятностных мер 240
 - — квантовых состояний 232
- косвенное измерение 126
- крайняя точка 19
- Куна—Таккера условия 73
- максимальной удаленности условие 161
- матрица ковариаций 33, 270
 - коммутационная 33
- наблюдаемая 22
 - вещественная 30

- наблюдаемая гауссовская 287
— квантовая 29, 248
— классическая 21
— нечеткая 21
— четкая 21, 29, 248
— экстремальная 35
наблюдаемые
— совместимые 24
— стохастически совместимые 25
неравенство
— Белла—Клаузера—Хорна—Шимони 55
— Кэдисона 116
— Линдблада—Озавы 170
— Линдблада—Озавы 183
— Фано 76
норма операторная 17, 231
— следовая 17, 231
оператор
— антиунитарный 114
— калибровочно инвариантный 269
— комплексной структуры 268
— ограниченный 230
— плотности 25, 231
— положительный 16
— самосопряженный 252
— сопряженный 14
— унитарный 15
— частичной изометрии 15
— числа квантов 259, 269
— энергии 259
— эрмитов 15
— ядерный 231
операторы Вейля 263
— — дискретные 131
— рождения-уничтожения 259, 267
операции локальные 58
ортогональная выпуклая комбинация 131
очищение состояния 51
переполненная система 35
поляризационное тождество 14
полярное разложение 16
представление Крауса 119
— — минимальное 120
— Стайнспринга 118
— — минимальное 119
принцип максимального правдоподобия 40
проектор 15
— δ -типичный 98
— сильно типичный 180
— условно типичный 101
проекционный постулат
фон Неймана—Людерса 125
произведение йорданово 33
— тензорное 46
пропускная способность 201
— — классическая 85, 158
— — протокола передачи классической информации с помощью сцепленного состояния 173
— — секретная 81, 211
— — шенноновская 72, 95, 165
 χ -пропускная способность 160
разделимость 56
разложение единицы 29
— — ортогональное 15, 29
разложение Шмидта 50
распределение вероятностей наблюдаемой 22
расстояние Бюреса 199
сжатие
— данных 69
— квантовой информации 99
симплектическая форма 263
симплектическое преобразование 266
— пространство 264
след 16
— частичный 47
слово (последовательность)
— δ -типичное 68
— сильно типичное 181
— условно типичное 78
соответствие Чоя—Ямилковского 123

соотношение неопределенностей 33
— — Гейзенберга 257
состояние 22
— апостериорное 59, 125
— вакуумное 259
— гауссовское 271
— квантовое 25
— классическое 21
— когерентное 260
— максимально сцепленное 50
— минимальной неопределенности 257
— разделимое (несцепленное) 124, 246
— с n квантами 259
— сжатое 277
— статистическое 21
— сцепленное 50
— чистое 21, 26
спектр оператора 15
спектральная мера 248
спектральное разложение 15, 233, 251
статистическая модель 23
— — квантовая
— — — максимальная 29
— — — фон Неймана 30
— — классическая 24
— — — Вальда 25
— — — Колмогорова 24
— — — отделимая 23
статистическая формула
Борна—фон Неймана 30
статистический ансамбль 23
— —, смесь 26
сцепленность формирования 146

теорема
— единственности Стоуна—фон Неймана 264, 313
— Каратеодори 19
— Наймарка 48
— Стайнспринга 117
— Стоуна 253
тест 35
точность воспроизведения
— — подпространства 195
— — состояния 198
— — средняя 99
— — сцепленности 195
— — чистого состояния 194

укрупнение 23
унитарное отображение 114

функция
— аффинная 19
— вогнутая 19
— выпуклая 19
— надежности 105
— операторно-монотонная 155
— характеристическая 270

шар Блоха 27

энтропия
— квантовая 86
— — обменная 151
— — относительная 137
— — условная 150
— случайной величины 67
— — условная 70
— совместная 70
эталонная система 122

Магазин «Математическая книга»

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга» в Москве по адресу: Б. Власьевский пер., д. 11; тел. (499) 241-72-85; biblio.mccme.ru

Книга — почтой: <http://biblio.mccme.ru/shop/order>

Книги в электронном виде: <http://www.litres.ru/mcnmo/>

Мы сотрудничаем с интернет-магазинами

- Книготорговая компания «Абрис»; тел. (495) 229-67-59, (812) 327-04-50; www.umlit.ru, www.textbook.ru, абрис.рф
- Интернет-магазин «Книга.ру»; тел. (495) 744-09-09; www.kniga.ru

Наши партнеры в Москве и Подмоскowie

- Московский Дом Книги и его филиалы (работает интернет-магазин); тел. (495) 789-35-91; www.mdk-arbat.ru
- Магазин «Молодая Гвардия» (работает интернет-магазин): ул. Б. Полянка, д. 28; тел. (499) 238-50-01, (495) 780-33-70; www.bookmg.ru
- Магазин «Библио-Глобус» (работает интернет-магазин): ул. Мясницкая, д. 6/3, стр. 1; тел. (495) 781-19-00; www.biblio-globus.ru
- Спорткомплекс «Олимпийский», 5-й этаж, точка 62; тел. (903) 970-34-46
- Сеть киосков «Аргумент» в МГУ; тел. (495) 939-21-76, (495) 939-22-06; www.arg.ru
- Сеть магазинов «Мир школьника» (работает интернет-магазин); тел. (495) 715-31-36, (495) 715-59-63, (499) 182-67-07, (499) 179-57-17; www.uchebnik.com
- Сеть магазинов «Шаг к пятерке»; тел. (495) 728-33-09, (495) 346-00-10; www.shkolkniga.ru
- Издательская группа URSS, Нахимовский проспект, д. 56, Выставочный зал «Науку — Всем», тел. (499) 724-25-45, www.urss.ru
- Книжный магазин издательского дома «Интеллект» в г. Долгопрудный: МФТИ (новый корпус); тел. (495) 408-73-55

Наши партнеры в Санкт-Петербурге

- Санкт-Петербургский Дом книги: Невский пр-т, д. 62; тел. (812) 314-58-88
- Магазин «Мир науки и медицины»: Литейный пр-т, д. 64; тел. (812) 273-50-12
- Магазин «Новая техническая книга»: Измайловский пр-т, д. 29; тел. (812) 251-41-10
- Информационно-книготорговый центр «Академическая литература»: Васильевский остров, Менделеевская линия, д. 5
- Киоск в здании физического факультета СПбГУ в Петергофе; тел. (812) 328-96-91, (812) 329-24-70, (812) 329-24-71
- Издательство «Петроглиф»: Фарфоровская, 18, к. 1; тел. (812) 560-05-98, (812) 943-80-76; k_i_@bk.ru, k_i_@petroglyph.ru
- Сеть магазинов «Учебная литература»; тел. (812) 746-82-42, тел. (812) 764-94-88, тел. (812) 235-73-88 (доб. 223)

Наши партнеры в Челябинске

- Магазин «Библио-Глобус», ул. Молдавская, д. 16, www.biblio-globus.ru

Наши партнеры в Украине

- Александр Елисаветский. Рассылка книг наложенным платежом по Украине: тел. 067-136-37-35; df-al-el@bk.ru