Летняя школа «Современная математика»
Дубна, июль 2008

А. М. Райгородский

Системы общих представителей в комбинаторике и их приложения в геометрии

Москва
Издательство МЦНМО
2009

УДК 519.1
ББК 22.15
Р18

Райгородский А. М.

Р18 Системы общих представителей в комбинаторике и их приложения в геометрии. — М.: МЦНМО, 2009. — 136 с.

ISBN 978-5-94057-524-5

Настоящая книга посвящена различным аспектам задачи о системах общих представителей в комбинаторике. Рассказывается о многочисленных приложениях в комбинаторной геометрии, геометрии чисел, математической статистике и др. Книга написана по лекциям, которые ее автор читал в 2007 году на школе «Современная математика» в Дубне. Поэтому материал в ней изложен так, чтобы бóльшая его часть оказалась доступной первокурсникам. Однако материала много, и в конечном счете в книге возникает весьма нетривиальная техника, в том числе вероятностная. Книга будет интересна всем, кто интересуется современной комбинаторикой и ее приложениями.

УДК 519.1

ISBN 978-5-94057-524-5

Предисловие

Посвящается моей жене Ире

В настоящей книге мы расскажем об одном из красивейших разделов современной комбинаторики. Речь пойдет о так называемых системах общих представителей для совокупностей подмножеств конечного множества. Грубо говоря, система представителей — это любое множество, которое содержит хотя бы по одному «представителю» (элементу) из каждого множества, принадлежащего данной совокупности. Отыскание таких систем (в особенности минимальных) — это исключительно важная проблема дискретного анализа, которая имеет массу приложений в самых разнообразных областях знания. Так, имеются целые классы известных проблем в геометрии, решение которых напрямую зависит от того, как на данном этапе развития науки обстоят дела с построением оптимальных систем представителей для тех или иных совокупностей множеств. Среди этих проблем и классическая задача К. Борсука о разбиении множеств на части меньшего диаметра, и знаменитая задача Нелсона—Эрдёша—Хадвигера о раскрасках пространств, и задача Грюнбаума о покрытии множеств шарами. Имеются также красивые приложения систем общих представителей в геометрии чисел, которая является ярким и активно развивающимся разделом теории чисел. Имеется, наконец, и глубокая связь с понятием размерности Вапника—Червоненкиса — одним из центральных понятий в теории сложности и в математической статистике.

В этой книге мы подробно расскажем как о чисто комбинаторных свойствах систем общих представителей, так и об упомянутых выше приложениях этих объектов в геометрии, статистике и пр. Начнем мы с самых азов, но затем разовьем достаточно нетривиальную технику. Впрочем, для понимания материала будет абсолютно достаточным знание предметов, которые преподаются, скажем, на первых двух курсах механико-математического факультета МГУ им. М. В. Ломоносова. Более того, по гамбургскому счету нам необходимы лишь основы математического анализа на уровне пределов, асимптотик, производных и пр., линейной алгебры на уровне понимания того, что такое, скажем, базис в пространстве $\mathbb{R}^n$, и высшей алгебры на уровне приблизительного владения понятием группы и факторгруппы. Ничего больше нам и не требуется. В этой связи практически весь материал будет доступен сильному старшекласснику. Заметим, кстати, что в сокращенном виде он излагался на школе «Современная математика» в Дубне, где лекции автора этой книги посещали

ученики 10-х и 11-х классов, а также студенты первых и вторых курсов различных вузов.

Правда, есть одна небольшая оговорка. Зачастую для решения тех или иных комбинаторных задач мы будем применять соображения теории вероятностей. Все базовые объекты и схемы, которые нам понадобятся и которые, по счастью, будут носить абсолютно элементарный характер, мы по ходу введем. Разве что один раз мы прибегнем к помощи столь «продвинутых» понятий, как математическое ожидание и дисперсия. Это будет верхом вероятностной нетривиальности в рамках книги. Но и это всего лишь раз.

В целом, книга имеет следующую структуру. Она подразделяется на главы (всего их девять). Некоторые главы разбиваются, в свою очередь, на параграфы, каковые при необходимости делятся еще и на пункты. Теоремы, леммы, утверждения и пр. нумеруются сообразно тому, в каком пункте (параграфе, главе) они располагаются: так проще их искать. Скажем, если в текущем параграфе пунктов нет, а сам он имеет номер 7.1, то соответствующие теоремы будут названы теоремами 7.1.1, 7.1.2 и т. д. Некоторые главы, параграфы и пункты будут сопровождаться задачами. Сложные задачи мы, как обычно, пометим звездочкой, а нерешенные проблемы — двумя звездочками. Нумерация задач будет сквозной.

Автору очень приятно вспомнить, как в 1994 г. он впервые познакомился с тематикой систем общих представителей на спецкурсе по геометрической теории диофантовых приближений, которую на механико-математическом факультете МГУ читал Н. Г. Мощевитин. В конечном счете, именно благодаря тому замечательному спецкурсу и появилась данная книга.

Оглавление

Глава 1

Введение и постановка типичной задачи

Представим себе такую ситуацию. В аудитории 16-24 механико-математического факультета МГУ, где читается популярная лекция по математике, сидят сто школьников. Некоторые из них одинаково хорошо и лучше всех остальных умеют решать задачи по геометрии, некоторым точно так же легко дается комбинаторика, некоторые в равной мере превосходят других еще в какой-нибудь области математики, и т. д. Допустим, самих областей двадцать, и нам хочется из наших школьников создать команду для выступления на международной олимпиаде. Естественно, мы желаем добиться высочайшего результата, причем затратив на это, по возможности, минимум средств. Что это значит? По-видимому, разумнее всего взять в команду хотя бы одного школьника, «специализирующегося» в геометрии, хотя бы одного, блестяще владеющего комбинаторикой, и так в конечном итоге поступить с *представителями* всех «профессий». Однако если мы будем действовать неосмотрительно, то нам вряд ли удастся соблюсти условие минимальности средств, затраченных на поездку. В самом деле, мы же не знаем априори, какие именно школьники являются «великими» геометрами, а какие — «великими комбинаторами». Это могут оказаться вообще одни и те же люди, а может быть, множества таких школьников, напротив, не пересекаются: все комбинаторы слабы в геометрии, и всем геометрам абсолютно чужда комбинаторика. Что делать? Нужно, стало быть, постараться осуществить выбор наименьшего количества школьников и, тем не менее, добиться того, чтобы для каждой из наших двадцати областей среди выбранных нами олимпиадников нашелся хотя бы один дока в этой области.

Вот пример вполне конкретной и вместе с тем весьма практической задачи о *системах общих представителей*. Понятно, почему задача так называется, и нет сомнений, что ее постановку можно сделать совершенно абстрактной. В последнем случае мы, с одной стороны, дадим строгую математическую формализацию проблемы, а с другой стороны, нам проще будет в дальнейшем выводить из получающихся результатов многочисленные и разнообразные конкретные следствия — вовсе не обязательно связанные с формированием «олимпийской сборной». Ведь на самом деле — и в этом мы до некоторой степени убедимся — задача о системах общих представителей крайне многогранна и в конечном счете нетриви-

альна; ее различные варианты широко используются почти во всех областях комбинаторики, комбинаторной геометрии и пр. (Словосочетание «комбинаторная геометрия» особенно забавно смотрится в связи с нашими недавними рассуждениями о «великих геометрах» и «комбинаторах», но так уж вышло. В действительности комбинаторная геометрия — это очень красивая и важная дисциплина современной математики, о которой мы уже не раз писали в серии брошюр (см. [23,25,29]) и о которой здесь также пойдет речь.) Итак, в следующей главе мы сформулируем задачу в общем виде и в дальнейшем станем ее изучать.

Глава 2

Абстрактная постановка задачи

Пусть $\mathcal{R}_n$ — некоторое множество, состоящее из n элементов. Например, можно считать, что $\mathcal{R}_n = \{1, \ldots, n\}$, хотя это не всегда будет удобно. Рассмотрим произвольные *сочетания* элементов множества $\mathcal{R}_n$. Скажем, $M_1 \subseteq \mathcal{R}_n$ — это какое-то k_1-сочетание, $M_2 \subseteq \mathcal{R}_n$ — какое-то k_2-сочетание, и так далее вплоть до $M_s \subseteq \mathcal{R}_n$, являющегося каким-нибудь k_s — сочетанием. В результате образуется совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$, состоящая из всех указанных сочетаний. Слово «сочетание» мы употребили с одной единственной целью — подчеркнуть, что порядок элементов в множествах M_1, $\ldots$, M_s для нас значения не имеет (см. [3, 41]). Оно и естественно: если вспомнить задачу про олимпиаду, там уж точно нам было все равно, в какой последовательности вызывать будущих «олимпийцев» из аудитории 16-24; главное было составить команду. В дальнейшем однако, мы не станем больше говорить о сочетаниях, заменяя этот термин словом «подмножество». Итак, у нас есть совокупность каких-то s подмножеств множества $\mathcal{R}_n$. В принципе, некоторые их этих подмножеств могут даже совпадать между собой («специалисты в комбинаторике и в геометрии оказались одними и теми же людьми»), некоторые могут быть пустыми ($k_i = 0$, т. е., если угодно, «комбинаторов в аудитории 16-24 нет»), некоторые вправе совпасть со всем $\mathcal{R}_n$, и пр., и пр. Иными словами, изначально величина s сколь угодно большая (в первой главе она была ограничена лишь числом различных математических дисциплин, доступных школьнику), а величины k_i суть любые (возможно, одинаковые) неотрицательные целые числа, заключенные в пределах от нуля до n.

Рассмотрим произвольное подмножество $S \subseteq \mathcal{R}_n$, обладающее тем свойством, что $S \bigcap M_j \neq \varnothing$ для каждого $j \in \{1, \ldots, s\}$. Таким образом, S содержит хотя бы по одному элементу — представителю — из каждого множества $M_j \in \mathcal{M}$. Такое множество S называется *системой общих представителей* (*с. о. п.*) для совокупности $\mathcal{M}$. Ясно, что для данной совокупности систем общих представителей можно придумать, вообще говоря, кучу. Одна из многих подобных ситуаций изображена на рис. 1. Между прочим, каждая из указанных на рисунке с. о. п. минимальна в том смысле, что для приведенной совокупности множеств с. о. п. с меньшей мощностью не существует. Тем самым, осмысленно определение понятия

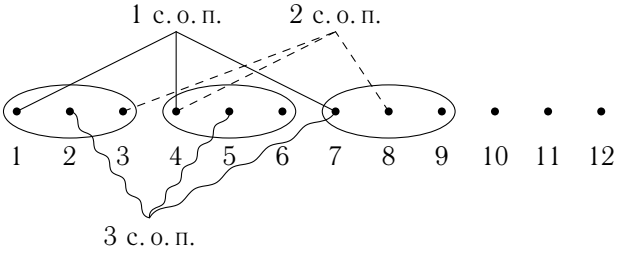

Рис. 1

минимальной с. о. п. (она, как мы поняли, не обязана быть единственной) и, главное, ее мощности, которую мы обозначим через $\tau(\mathcal{M})$:

$$\tau(\mathcal{M}) = \min\bigl\{|S|\colon S \text{ является с. о. п. для } \mathcal{M}\bigr\}.$$

Именно величина $\tau(\mathcal{M})$ и представляет наибольший интерес для нас. В частности, в задаче про олимпиаду речь шла как раз о ней.

Различных совокупностей $\mathcal{M}$ исключительно (если не бесконечно) много, даже если фиксирована часть параметров (чисел n, s, k_1, …, k_s). Прежде всего хотелось бы осознать, как мы со всем этим собираемся работать. Наверное, более или менее ясно, что начать исследование нужно с попытки отыскания величины

$$Z = Z(n, s, k_1, \ldots, k_s) = \max_{\mathcal{M}} \tau(\mathcal{M}),$$

где максимум берется по всем совокупностям $\mathcal{M}$ с данными параметрами. В самом деле, если величина Z окажется маленькой, то в любом случае (скажем, как бы хитро ни пересекались между собой множества «комбинаторов», «геометров» и пр.) мы с гарантией извлечем «экономную» с. о. п. («команду»); если Z велико, то возможны ситуации, когда как ни крути, а затрат избежать не удастся. Это уже потом возникнет вопрос о реальном поиске в каждом конкретном случае надлежащих систем общих представителей. Пока же и сам факт их наличия или отсутствия, безусловно, важен. Итак, будем возиться с $Z(n, s, k_1, \ldots, k_s)$.

Давайте еще немного упростим себе задачу. Заметим, что если какие-то множества $M_i, M_j \in \mathcal{M}$ совпадают, то об одном из них без потери общности можно легко забыть: любой представитель M_i есть автоматически и представитель M_j. Такое наблюдение позволяет нам, по крайней мере, считать, что различных совокупностей заведомо конечное число, т. е. что s точно не может равняться бесконечности (см. задачу 6).

Иногда полезно облегчить себе жизнь, полагая

$$k_1 = k_2 = \ldots = k_s = k.$$

Иными словами, зачастую интересно рассматривать только совокупности, которым принадлежат лишь подмножества $\mathcal{R}_n$, имеющие одинаковую мощность. В таком случае вместо величины $Z(n, s, k_1, \ldots, k_s)$ мы будем рассматривать величину $\zeta(n, s, k)$. Естественно, с «дзетой» иметь дело проще, но мы обсудим впоследствии и «зед» тоже.

Прежде чем переходить к формулировкам и доказательствам различных нетривиальных результатов, приведем в качестве задач несколько более простых фактов.

Задачи

1. Приведите пример совокупности с единственной минимальной с. о. п. При каких значениях параметров вам удается это сделать?

2. Пусть $u \in \{0, 1, \ldots, n\}$. Приведите пример совокупности $\mathcal{M}$ с $\tau(\mathcal{M}) = u$. При каких значениях параметров вам удается это сделать?

3. а) Докажите, что

$$\min\left\{s, \left[\frac{n}{k}\right]\right\} \leqslant \zeta(n, s, k) \leqslant \min\{n, s\}$$

($[x]$ — это целая часть вещественного числа x).

б) Проверьте справедливость неравенства $\zeta(n, s, k) \leqslant n - k + 1$. При каких значениях параметров такая оценка неулучшаема?

4. Докажите, что

$$Z(n, s, k_1, \ldots, k_s) \leqslant \zeta\bigl(n, s, \min_{i=1,\ldots,s} k_i\bigr).$$

5. а) Докажите, что $\zeta(20, 18, 5) \in \{4, 13\}$.

б) Докажите, что $\zeta(20, 18, 5) \in \{6, 7\}$.

в*) Найдите точное значение $\zeta(20, 18, 5)$ (можно ли составить команду для игры «Что? Где? Когда?», если претендентов 20, областей знания, которые должны быть представлены в команде, 18, а специалистов в каждой из областей ровно 5?).

6. а) Докажите, что совокупностей с параметрами

$$n,\ s,\ k_1 = k_2 = \ldots = k_s = k$$

ровно $C_{C_n^k}^s$ штук.

б) Найдите число различных совокупностей с произвольными параметрами $n,\ s,\ k_1,\ \ldots,\ k_s$.

7. Сколько есть различных с. о. п. для совокупности, изображенной на рис. 1?

Глава 3

Верхняя оценка для мощности минимальной с. о. п.

В разделе задач предыдущей главы уже были приведены простые примеры некоторых верхних оценок мощности минимальной с. о. п. для произвольной совокупности $\mathcal{M}$ с данными параметрами n, s, k. Нетрудно понять, глядя, скажем, на задачу 5, что все эти оценки, вообще-то, крайне далеки от идеальных. В самом деле, в задаче 5 дано $n = 20$, $s = 18$. Однако там же мы постулируем справедливость неравенства $\zeta(20, 18, 5) \leqslant 7$, хотя, окажись оценки из задачи 3 по существу неулучшаемыми, вряд ли бы стали мы утверждать подобное: $\min\{n - k + 1, s\} = 16$, а это куда больше семи! Таким образом, возникает проблема получения нетривиальных (а по возможности, в разумном смысле точных) верхних оценок для $\zeta(n, s, k)$. Естественно, такая же проблема актуальна и для величины Z. Да нам бы с более простой ситуацией сперва разобраться и результат задачи 4 на худой конец применить.

Следующая теорема в более или менее одинаковом виде доказывалась множество раз различными авторами, натыкавшимися на необходимость что-нибудь «экономно представлять» (как мы уже говорили, приложений у задачи много, и люди, занимавшиеся подчас совершенно непохожими науками, убеждались в важности изучения с. о. п.), и потому мы не станем приписывать ее утверждение какому-либо конкретному человеку. Просто сформулируем ее, прокомментируем и докажем.

Теорема 3.1. *Для любых n, s, k имеет место неравенство*

$$\zeta(n, s, k) \leqslant G(n, s, k) = \max\left\{\frac{n}{k}, \frac{n}{k}\ln\frac{sk}{n}\right\} + \frac{n}{k} + 1.$$

На взгляд неискушенного читателя, оценка, приведенная в формулировке теоремы, выглядит, наверное, довольно устрашающе. Попробуем понять, что же она означает. Во-первых, с самого начала может возникнуть недоразумение. Читатель спросит: «Как же так? Очевидно ведь, что вторая величина, стоящая под знаком максимума, больше первой. Если первая есть всего лишь дробь $\frac{n}{k}$, то вторая в логарифм от некой другой дроби раз ее заведомо превосходит. Зачем же нужно тогда максимум брать?» А дело все в том, что логарифм взят именно что от дроби, и дроби этой, в принципе, ничто не мешает быть меньше $e = 2{,}71\ldots$ и, более

того, меньше единицы. В последнем же случае и вовсе наш натуральный логарифм отрицательным сделается. Так что от максимума избавиться не удастся. В то же время доля правды в вопросе читателя есть. При условии, что $s \geqslant e\frac{n}{k}$, о максимизации можно спокойно забыть. При этом с ростом значения логарифма слагаемые $\frac{n}{k}+1$ тоже станут пренебрежимо малы по сравнению с величиной $\frac{n}{k}\ln\frac{sk}{n}$. В результате вся соль будет как раз в указанной величине, а она уже гораздо приятнее смотрится.

Сильно ли ограничительно условие $s \geqslant e\frac{n}{k}$? Отнюдь нет. Если $s \leqslant \frac{n}{k}$, то в силу задачи 3 имеем $\zeta(n, s, k) \leqslant s \leqslant \frac{n}{k}$, так что и теорема никакая не нужна. К тому же из той же задачи вытекает неуточняемость упомянутой оценки, а значит, здесь говорить буквально не о чем. Реальный интерес представляет ситуация, когда s значительно больше известной дроби, и в этом случае, как мы только что поняли, главной составляющей длинного неравенства из теоремы является величина $\frac{n}{k}\ln\frac{sk}{n}$. Хорошо бы еще на примерах пощупать, какими в действительности бывают n, s и k.

Зачастую удобно считать, что параметры s и k сами суть функции, зависящие от n. Пусть, скажем, $s = n$, а $k = [\ln n]$. Тогда легко понять, что выражение $\frac{n}{k}\ln\frac{sk}{n}$ устроено приблизительно так же, как и функция $\frac{n}{\ln n}\ln\ln n$. Разница ничтожна, и ничего не стоит строго обосновать асимптотическое равенство указанных формул. Вместе с тем ни у кого, пожалуй, не вызовет сомнений тот факт, что $\frac{n}{k} = \frac{n}{[\ln n]}$ — это величина, значительно, пренебрежимо меньшая обеих величин, упомянутых выше. Так что наши соображения еще раз подтверждаются. Впрочем, иногда теорема все-таки вырождается. Возьмем $n = 100$, $k = 10$, $s = C_{100}^{10}$. Лобовой счет показывает, что тут $\frac{n}{k}\ln\frac{sk}{n} > n$. Но оценка $\zeta(n, s, k) \leqslant n$ уже тривиальна, и потому здесь теоремы не хватает. Тем не менее, — и это мы увидим позднее, — теорема в большинстве случаев «почти» точна. А о вырожденных ситуациях и разговор особый. Пора, стало быть, переходить к доказательству.

Доказательство теоремы 3.1. Возможны три (быть может, пересекающихся) случая: $s \leqslant \frac{2n}{k}$; $\frac{n}{k}\ln\frac{sk}{n} \geqslant n-k+1$; $s > \frac{2n}{k}$ и $\frac{n}{k}\ln\frac{sk}{n} < n-k+1$. Рассуждения, предшествующие доказательству теоремы, свидетельствуют о том, что нетривиален лишь последний случай. Два остальных мы рассматриваем для пущей аккуратности, и по ходу дела мы поясним, зачем это нужно. Итак, изучим каждую ситуацию отдельно.

Случай 1. Пусть $s \leqslant \frac{2n}{k}$. Тогда, очевидно, $\zeta(n, s, k) \leqslant s \leqslant \frac{2n}{k}$. В то же время $\frac{n}{k} \ln \frac{sk}{n} \leqslant \frac{n}{k} \ln 2 < \frac{n}{k}$. Значит,

$$\zeta(n, s, k) \leqslant \max\left\{\frac{n}{k}, \frac{n}{k} \ln \frac{sk}{n}\right\} + \frac{n}{k} + 1 = \frac{2n}{k} + 1,$$

и все в порядке.

Случай 2. Пусть $\frac{n}{k} \ln \frac{sk}{n} \geqslant n - k + 1$. Тогда опять-таки легко видеть, что

$$\zeta(n, s, k) \leqslant n - k + 1 \leqslant \frac{n}{k} \ln \frac{sk}{n} \leqslant \max\left\{\frac{n}{k}, \frac{n}{k} \ln \frac{sk}{n}\right\} + \frac{n}{k} + 1.$$

Случай 3. Пусть, наконец, $s > \frac{2n}{k}$ и $\frac{n}{k} \ln \frac{sk}{n} < n - k + 1$. Зафиксируем произвольную совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$, состоящую из k-элементных подмножеств множества $\mathcal{R}_n$. Будем постепенно набирать искомую с. о. п. для $\mathcal{M}$, кладя в нее элемент за элементом. Всякий раз мы будем стараться выбрать очередной элемент так, чтобы он являлся представителем как можно большего числа множеств, которые не были «представлены» на предыдущих шагах процедуры. Такая процедура (и мы сейчас ее аккуратно распишем) по праву называется *жадным алгоритмом*: мы последовательно извлекаем из $\mathcal{R}_n$ элементы, жадно захватывая (т. е. представляя каждым из них) максимум того, что до тех пор захвачено не было. Еще этот алгоритм иногда называют *градиентным*, и он весьма широко используется в математике.

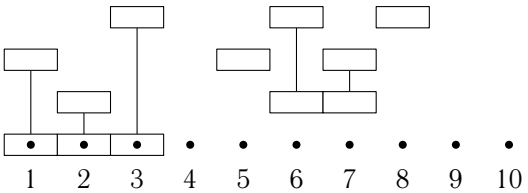

Рис. 2

Теперь формально положим

$$\rho_1 = \max_{\nu \in \mathcal{R}_n} |\{M \in \mathcal{M} \colon \nu \in M\}|$$

и возьмем любой элемент $\nu_1 \in \mathcal{R}_n$, на котором достигается значение ρ_1 (такой элемент не обязан быть единственным, но это не страшно; см., впрочем, рис. 2, на котором $\rho_1 = 2$, а ν_1 — любой из элементов 1, 2, 3, 6, 7). Этот элемент действительно «жаден». С его помощью мы

заведомо извлекли представителей из некоторых ρ_1 множеств, и ничего лучшего мы сходу сделать, в принципе, не могли. В результате непредставленными остались $s_1 = s - \rho_1$ множеств. Обозначим совокупность этих множеств через $\mathcal{M}^1 = \{M_1^1, \ldots, M_{s_1}^1\} \subset \mathcal{M}$. Заметим, что $|M_i^1| = k$ для любого i, причем каждое M_i^1 лежит в множестве $\mathcal{R}_n \setminus \{\nu_1\}$, которое, в свою очередь, мы вполне можем отождествить с $\mathcal{R}_{n-1}$ (см. рис. 2 и 3). Далее действуем аналогично, полагая

$$\rho_2 = \max_{\nu \in \mathcal{R}_{n-1}} |\{M \in \mathcal{M}^1 \colon \nu \in M\}|$$

и выбирая произвольный элемент $\nu_2 \in \mathcal{R}_{n-1}$, на котором достигается значение ρ_2. Остается совокупность $\mathcal{M}^2 = \{M_1^2, \ldots, M_{s_2}^2\} \subset \mathcal{M}^1$, где $s_2 = s_1 - \rho_2$, $|M_i^2| = k$ и $M_i^2 \subseteq \mathcal{R}_{n-2}$ $(i = 1, \ldots, s_2)$. Вообще, если уже проделано $r \geqslant 1$ шагов процедуры, то у нас на руках имеется совокупность $\mathcal{M}^r = \{M_1^r, \ldots, M_{s_r}^r\}$, у которой $s_r = s_{r-1} - \rho_r$, $|M_i^r| = k$ и $M_i^r \subseteq \mathcal{R}_{n-r}$ $(i = 1, \ldots, s_r)$. (Здесь $s_0 = s$.) Снова обозначим

$$\rho_{r+1} = \max_{\nu \in \mathcal{R}_{n-r}} |\{M \in \mathcal{M}^r \colon \nu \in M\}|,$$

после чего понятно, как устроен ν_{r+1} и пр. Правда, нужно еще следить за выполнением тривиального условия $n - r \geqslant k$ или $r \leqslant n - k$ (иначе процесс, очевидно, вырождается, ведь не может же k-элементное множество M_i^r лежать в $\mathcal{R}_{n-r}$ при $n - r < k$).

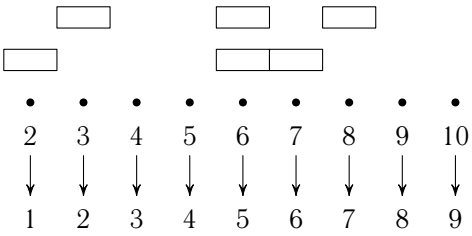

Рис. 3

Покажем, что $\rho_{r+1} \geqslant \dfrac{s_r k}{n - r}$. Для этого посмотрим на величину $\sum\limits_{i=1}^{s_r} |M_i^r|$. С одной стороны, эта величина есть, конечно же, $s_r k$. С другой стороны,

$$\sum_{i=1}^{s_r} |M_i^r| = \sum_{\nu \in \mathcal{R}_{n-r}} |\{M \in \mathcal{M}^r \colon \nu \in M\}| \leqslant (n - r)\rho_{r+1}.$$

Тем самым, $s_r k \leqslant (n - r)\rho_{r+1}$, и утверждение установлено.

Пусть $N = \left[\frac{n}{k}\ln\frac{sk}{n}\right] + 1$. Если $N = n - k + 1$ (формально такое возможно), то мы возвращаемся ко второму случаю и обсуждать нечего. Иначе $N \leqslant n - k$, и мы вольны проделать N шагов жадного алгоритма. Нами уже набраны представители $\nu_1, \ldots, \nu_N$. Непредставленными остались s_N множеств. Оценим величину s_N:

$$s_N = s_{N-1} - \rho_N \leqslant s_{N-1} - \frac{s_{N-1}k}{n-N+1} = \\ = s_{N-1}\left(1 - \frac{k}{n-N+1}\right) \leqslant s_{N-1}\left(1 - \frac{k}{n}\right).$$

Здесь важно, что $1 \leqslant N \leqslant n - k$, а это обусловлено выбором текущей ситуации. Аналогично $s_{N-1} \leqslant s_{N-2}\left(1 - \frac{k}{n}\right)$ и т. д. В конечном итоге

$$s_N \leqslant s\left(1 - \frac{k}{n}\right)^N \leqslant s\left(1 - \frac{k}{n}\right)^{\frac{n}{k}\ln\frac{sk}{n}} = se^{\left(\frac{n}{k}\ln\frac{sk}{n}\right)\ln\left(1-\frac{k}{n}\right)}.$$

Тут опять использован тот факт, что у нас $\frac{n}{k}\ln\frac{sk}{n} > \frac{n}{k}\ln 2 > 0$, а стало быть, $N \geqslant \frac{n}{k}\ln\frac{sk}{n}$. Правда, некоторая неаккуратность возникает при $n = k$, но этот случай даже рассматривать отдельно нелепо, настолько в его рамках все очевидно. Итак, заметим, что $\ln(1-x) \leqslant -x$, и в результате получим неравенство

$$se^{\left(\frac{n}{k}\ln\frac{sk}{n}\right)\ln\left(1-\frac{k}{n}\right)} \leqslant se^{-\frac{k}{n}\frac{n}{k}\ln\frac{sk}{n}} = \frac{n}{k}.$$

Последняя выкладка свидетельствует о том, что $\tau(\mathcal{M}^N) \leqslant s_N \leqslant \frac{n}{k}$. Добавим элементы из минимальной с. о. п. для $\mathcal{M}^N$ к $\nu_1, \ldots, \nu_N$. Получится система мощности не более чем $N + \frac{n}{k}$, и она есть с. о. п. для исходной совокупности $\mathcal{M}$. Таким образом, и здесь

$$\tau(\mathcal{M}) \leqslant N + \frac{n}{k} \leqslant \max\left\{\frac{n}{k}, \frac{n}{k}\ln\frac{sk}{n}\right\} + \frac{n}{k} + 1.$$

Теорема доказана.

Задачи

8. Приведите пример ситуации (набора параметров n, s, k), в рамках которой оценка из теоремы 3.1 допускает уточнение хотя бы на единицу.

9. Пусть $k = k(n)$ и $s = s(n)$, причем $G(n, s, k) \to \infty$ при $n \to \infty$. Приведите пример ситуации, в рамках которой оценка из теоремы 3.1 допускает уточнение на некоторую величину $\varphi(n) \to \infty$.

Глава 4

Нижние оценки для мощности минимальной с. о. п.

В этой главе мы займемся получением и обсуждением результатов, которые будут в некотором смысле обратны по отношению к результатам предыдущей главы.

§ 4.1. Формулировки результатов

В предыдущей главе мы получили универсальную верхнюю оценку величины минимальной с. о. п. для совокупности подмножеств конечного множества. Сразу же встает вопрос: а насколько это оценка точна? Можно ли рассчитывать на ее улучшение и если да, то будет ли подобное улучшение существенным? Разумеется, само понятие «существенного улучшения» довольно размыто, но ближе к делу станет ясно, о чем речь (ср. задачу 8).

В этой главе мы докажем следующие три теоремы и одно следствие.

Теорема 4.1.1. *Пусть* $n \geqslant 32$, $k \leqslant \frac{n}{32}$, *а* s *таково, что* $4 \leqslant \ln \frac{sk}{n} \leqslant k$. *Тогда имеет место неравенство*

$$\zeta(n, s, k) \geqslant \frac{1}{64} \frac{n}{k} \ln \frac{sk}{n}.$$

Теорема 4.1.2. *Пусть* n, s, k *и* $l \leqslant n - k$ *таковы, что*

$$G(C_n^k, C_n^l, C_{n-l}^k) \leqslant s.$$

Тогда справедлива оценка $\zeta(n, s, k) \geqslant l$.

Не правда ли, неожиданное утверждение? Загадочным образом для доказательства *нижней* оценки функции $\zeta(n, s, k)$ используется величина, стоящая в правой части *верхней* оценки той же функции!

Следствие 4.1.1. *Предположим, что* $n \to \infty$, $s = s(n) \to \infty$, $k = k(n) \to \infty$, *причем* $\frac{sk}{n}$ *также неограниченно возрастает с увеличением* n. *Пусть, далее,* $k = o(\sqrt{n})$, $\ln k = o\left(\frac{sk}{n}\right)$ *и* $\ln \frac{sk}{n} = o(\sqrt{k})$. *Положим*

$$l = \left[\frac{n}{k} \ln \frac{sk}{n} - \frac{n}{k} \ln \ln \frac{sk}{n} - \frac{n}{k} \ln \ln k - \frac{10n}{k}\right].$$

Тогда при достаточно больших n *выполнена оценка* $\zeta(n, s, k) \geqslant l$.

Теорема 4.1.3. *Пусть n, s, k и $l \leqslant n-k$ таковы, что*

$$C_n^l \frac{C^s_{C_n^k - C_{n-l}^k}}{C^s_{C_n^k}} < 1.$$

Тогда справедлива оценка $\zeta(n, s, k) \geqslant l$.

Теорема 4.1.3 имеет следствие, аналогичное следствию 4.1.1. Однако в целях уменьшения громоздкости книги мы соответствующее утверждение здесь не приводим. Зато читатель сможет самостоятельно попробовать отыскать при данных n, s, k как можно большее значение параметра l, фигурирующего в формулировке теоремы 4.1.3.

Вообще, теоремы выглядят довольно страшно, и потому очевидно, что, прежде чем переходить к их доказательствам, необходимо дать подробный комментарий к их утверждениям. Мы займемся этим в §4.2. В §4.3—4.6 мы приведем собственно доказательства теорем, а в §4.7 наметим пути улучшения доказанных результатов.

§4.2. Соотношения между результатами теорем 3.1 и 4.1.1—4.1.3

Сперва посмотрим на теорему 4.1.1. Ее утверждение, очевидно, уже не столь универсально, как это было с утверждением теоремы 3.1: некоторые ограничения на значения параметров мы все-таки здесь накладываем. Тем не менее, сейчас мы покажем, что эти ограничения практически ничего не ограничивают. Во-первых, техническое условие $n \geqslant 32$ означает лишь, что в худшем случае нам не удастся применить теорему 4.1.1 к *конечному* множеству ситуаций (мощность этого множества есть в некотором смысле 31, и это, в общем, мелочь). Это условие нужно только для того, чтобы корректным стало неравенство $k \leqslant \frac{n}{32}$, которое тривиализуется, коль скоро $n < 32$. Более того, само неравенство для k допускает уточнения (ср. §4.7), хотя и в нынешнем виде (удобном для дальнейшего доказательства) оно не производит впечатления чересчур значимого. Что же тогда за условие $4 \leqslant \ln \frac{sk}{n} \leqslant k$? А это тоже условие нетривиальности параметров. Действительно, если, напротив, $\ln \frac{sk}{n} > k$, то даже теорема 3.1 интереса не представляет. Если же $\ln \frac{sk}{n} < 4$, то теорема 3.1 повлечет оценку $\zeta(n, s, k) \leqslant \frac{cn}{k}$, которая элементарна (см. гл. 3). Таким образом, мы попросту отделяем ту нишу, где максимум, фигурирующий в определении функции $G(n, s, k)$, достигается на второй, гораздо более интересной, величине. Сама оценка $\ln \frac{sk}{n} \geqslant 4$ достаточно произвольна: ее можно уточнять, но большого смысла в этом нет. Наконец, итоговый

результат теоремы 4.1.1 весьма примечателен. Он свидетельствует о том, что во всех нетривиальных ситуациях теорема 3.1 практически точна: она, как принято говорить, точна по порядку. Иными словами, если ее и можно улучшить, то не более чем в постоянное число раз. Разумеется, величина $\frac{1}{64}$ здесь также не является принципиальной (см. § 4.7); однако техника, используемая при доказательстве теоремы 4.1.1, не позволяет заменить указанную дробь единицей или чем-либо асимптотически равным одному (коль скоро вообще уместно говорить об асимптотиках). Итак, теорема 4.1.1 почти столь же универсальна, как и теорема 3.1; небольшой минус состоит в том, что в результате мы по-прежнему имеем некоторый зазор между верхними и нижними оценками для $\zeta(n, s, k)$.

Перейдем к обсуждению теоремы 4.1.2, следствия 4.1.1 и теоремы 4.1.3. Сразу понятно, что ограничения $l \leqslant n - k$ никакой реальной роли в формулировках обеих теорем не играют (ср. задачу 3). В то же время осознать, как соотносятся, скажем, теоремы 4.1.2, 4.1.1 и 3.1, можно по большому счету, только глядя на следствие 4.1.1. Отметим, что следствие не равносильно, конечно, соответствующей теореме, но оно достаточно полно покрывает множество ситуаций, в рамках которых эта теорема применима (читателю стоит попытаться самостоятельно убедиться в этом). Существенная разница состоит в том, что теорема 4.1.2, в отличие от следствия 4.1.1, не говорит об асимптотиках; ее можно использовать, отнюдь не предполагая, что какой-либо из параметров неограниченно растет. Тем не менее, при всех преимуществах общей теоремы перед частным следствием, именно в последнем заключена суть происходящего: доказано, что при определенных условиях теорема 3.1 точна уже не по порядку, а асимптотически. Иначе говоря, вкупе с теоремой 3.1 теорема 4.1.2 при указанных условиях влечет асимптотику $\zeta(n, s, k) \sim \frac{n}{k} \ln \frac{sk}{n}$. Сами условия уже куда более ограничительны, нежели их предшественники из теоремы 4.1.1. В результате теорема 4.1.1, безусловно, превосходит теорему 4.1.2 широтой своей применимости; однако она же и уступает теореме 4.1.2 по аккуратности оценки. Есть еще один важный момент. И теорема 4.1.1, и теорема 4.1.2 говорят о нижних оценках для $\zeta(n, s, k)$. Стало быть, в каждой из них утверждается существование совокупности множеств с параметрами n, s, k, у которой минимальная с. о. п. весьма велика. В теореме 4.1.1 такая совокупность строится явно (см. следующий параграф), а в теореме 4.1.2 используется некий трюк, который лишь показывает, что с необходимостью искомая совокупность и впрямь найдется; как устроена совокупность из теоремы 4.1.2 — вопрос отдельный и вовсе не тривиальный (см. § 4.4, 4.6).

Скажем несколько слов о степени ограничительности условий следствия 4.1.1 и об их смысле. Смысл очень простой. Требование стремления к бесконечности величин n, s, k, $\frac{sk}{n}$ нужно для того, чтобы корректно говорить об асимптотиках, бесконечно малых величинах и пр. Условие $\ln k = o\left(\frac{sk}{n}\right)$ показывает, что $\frac{n}{k}\ln\ln k = o\left(\frac{n}{k}\ln\frac{sk}{n}\right)$, т. е. что первое слагаемое в выражении для l главное, а остальные слагаемые в том же выражении суть остаточные члены асимптотики. Ограничение $\ln\frac{sk}{n} = o(\sqrt{k})$ можно рассматривать, например, как свидетельство того, что $l = o(n)$ и, стало быть, в частности, $l \leqslant n - k$ при достаточно больших n. Здесь мы не забываем, что, наконец, $k = o(\sqrt{n})$, хотя изначально это просто техническое условие, от которого, по-видимому, нетрудно избавиться. Что касается широты применимости следствия, то она, несмотря на перечисленные условия, довольно велика. Например, ситуация, описанная непосредственно перед доказательством теоремы 3.1, вполне следствием 4.1.1 покрывается:

$$\zeta(n, n, [\ln n]) \sim \frac{n}{\ln n}\ln\ln n.$$

Есть и много других примеров, которые читатель наверняка придумает сам.

Теперь скажем несколько слов по поводу теоремы 4.1.3. Ее доказательство столь же неявно, как и доказательство теоремы 4.1.2 (см. § 4.5). Однако трюк принципиально иной — на сей раз вероятностный. Следствие, аналогичное следствию 4.1.1, можно вывести и из теоремы 4.1.3, но мы на этом не задерживаемся, оставляя это в качестве упражнения читателю. Подчеркнем, впрочем, что, как и в случае с теоремой 4.1.2, снова зачастую возникнет асимптотика $\zeta(n, s, k) \sim \frac{n}{k}\ln\frac{sk}{n}$; только остаточные члены будут другими. Таким образом, конструктивная теорема 4.1.1 страдает отсутствием асимптотических следствий, а теоремы 4.1.2 и 4.1.3, приводящие к асимптотическим формулам для $\zeta(n, s, k)$, напротив, не дают ни малейшего намека на явный вид совокупностей, существование которых в них фактически постулируется.

Отметим, наконец, что из литературных источников здесь полезно использовать книгу [34], статьи [20] и [15].

§ 4.3. Доказательство теоремы 4.1.1

Для удобства введем обозначение $\mathcal{R}_{i,j} = \{i, \ldots, j\}$. Разумеется, мы всегда вольны отождествить $\mathcal{R}_{i,j}$ с $\mathcal{R}_{j-i+1}$, но в данном случае полезно

уметь различать два упомянутых множества. Положим $m = \left[\frac{1}{2}\ln\frac{sk}{n}\right]$. Ввиду условий теоремы $m \geqslant 1$. Рассмотрим разбиение

$$\mathcal{R}_{2qm} = \mathcal{R}_{1,2qm} = \mathcal{R}_{1,2m} \sqcup \mathcal{R}_{2m+1,4m} \sqcup \ldots \sqcup \mathcal{R}_{2(q-1)m+1,2qm} \subset \mathcal{R}_n,$$

где $q = \left[\frac{2k}{m}\right]$. Заметим, что разбиение определено корректно. Во-первых, из неравенства $\ln\frac{sk}{n} \leqslant k$ вытекает оценка

$$\frac{2k}{m} \geqslant \frac{2k}{\frac{1}{2}\ln\frac{sk}{n}} = \frac{4k}{\ln\frac{sk}{n}} \geqslant 4,$$

означающая, что $q > 1$ и $q \geqslant \frac{k}{m}$ (мы используем неравенство $[x] \geqslant \frac{x}{2}$ при $x \geqslant 1$). Во-вторых, $2qm \leqslant 4k \leqslant \frac{n}{8}$, так что на самом деле $\mathcal{R}_{2qm} \subset \mathcal{R}_n$.

Занумеруем в определенном порядке все m-элементные подмножества множества $\mathcal{R}_{1,2m}$. Получится совокупность $\mathcal{N}^1 = \left\{N_1^1, \ldots, N_{C_{2m}^m}^1\right\}$. В том же порядке запишем все m-элементные подмножества в множествах

$$\mathcal{R}_{2m+1,4m}, \quad \ldots, \quad \mathcal{R}_{2(q-1)m+1,2qm}.$$

Образуются совокупности $\mathcal{N}^i = \left\{N_1^i, \ldots, N_{C_{2m}^m}^i\right\}$, $i = 1, \ldots, q$. Заметим, что

$$|\mathcal{N}^i| = C_{2m}^m < 2^{2m} \leqslant 2^{\ln\frac{sk}{n}} < \frac{sk}{n}$$

и что $\tau(\mathcal{N}^i) = m + 1 > m$ (ср. задачу 3) для любого i.

Пусть $\mathcal{M}^1 = \{M_1^1, \ldots, M_{C_{2m}^m}^1\}$ — это совокупность, состоящая из множеств

$$M_j^1 = N_j^1 \cup N_j^2 \cup \ldots \cup N_j^q, \quad j = 1, \ldots, C_{2m}^m.$$

Теперь уже ясно, что $|\mathcal{M}^1| < \frac{sk}{n}$ и что $\tau(\mathcal{M}^1) > m$. Более того,

$$|M_j^1| = qm \geqslant \frac{mk}{m} = k, \quad j = 1, \ldots, C_{2m}^m.$$

Положим $t = \left[\frac{n}{2mq}\right]$. Рассмотрим разбиение

$$\mathcal{R}_{2qmt} = \mathcal{R}_{1,2qmt} = \mathcal{R}_{1,2qm} \sqcup \mathcal{R}_{2qm+1,4qm} \sqcup \ldots \sqcup \mathcal{R}_{2qm(t-1)+1,2qmt} \subset \mathcal{R}_n.$$

И снова разбиение задано корректно. Прежде всего, стандартные выкладки показывают, что $t > 1$. Кроме того, очевидно, $2qmt \leqslant n$.

В каждый элемент последнего разбиения поместим копию совокупности $\mathcal{M}^1$. Появятся совокупности $\mathcal{M}^2, \ldots, \mathcal{M}^t$. Соберем все совокупности воедино:

$$\mathcal{M}' = \mathcal{M}^1 \cup \ldots \cup \mathcal{M}^t.$$

Понятно, что

$$|\mathcal{M}'| < t\frac{sk}{n} \leqslant \frac{n}{2mq}\frac{sk}{n} \leqslant \frac{n}{2k}\frac{sk}{n} < s.$$

Далее, мощность каждого множества $M \in \mathcal{M}'$ не меньше k. Наконец,

$$\tau(\mathcal{M}') > tm \geqslant \frac{n}{4mq}\frac{1}{4}\ln\frac{sk}{n} \geqslant \frac{n}{64k}\ln\frac{sk}{n}.$$

Если какое-то множество в $\mathcal{M}'$ имеет строго больше чем k элементов, то удалим из него любой такой кусок, чтобы размер оставшегося множества оказался в точности равным k. Получится совокупность $\mathcal{M}''$. Если $|\mathcal{M}''| < s$, то добавим к $\mathcal{M}''$ произвольные k-элементные подмножества множества $\mathcal{R}_n$ так, чтобы окончательная совокупность $\mathcal{M}$ имела мощность s и состояла только из k-элементных множеств в $\mathcal{R}_n$. Поскольку $\mathcal{M} \supseteq \mathcal{M}''$, получаем неравенство $\tau(\mathcal{M}) \geqslant \tau(\mathcal{M}'')$. Верно и неравенство $\tau(\mathcal{M}'') \geqslant \tau(\mathcal{M}')$. Таким образом,

$$\zeta(n, s, k) \geqslant \tau(\mathcal{M}) \geqslant \tau(\mathcal{M}'') \geqslant \tau(\mathcal{M}') \geqslant \frac{n}{64k}\ln\frac{sk}{n},$$

и теорема доказана.

§ 4.4. Доказательство теоремы 4.1.2

Наша задача — показать существование совокупности $\mathcal{M}$ с параметрами n, s, k и с $\tau(\mathcal{M}) \geqslant l$. Положим $\bar{n} = C_n^k$, $\bar{s} = C_n^l$, $\bar{k} = C_{n-l}^k$. Рассмотрим совокупность $\mathcal{K} = \{K_1, \ldots, K_{\bar{n}}\}$, состоящую из всех возможных k-элементных подмножеств множества $\mathcal{R}_n$. Сопоставляя каждому множеству из $\mathcal{K}$ его номер, получаем взаимно однозначное соответствие между совокупностью $\mathcal{K}$ и множеством $\mathcal{R}_{\bar{n}}$. Пусть, далее, $\mathcal{L} = \{L_1, \ldots, L_{\bar{s}}\}$ — совокупность, которая образована всеми l-элементными подмножествами множества $\mathcal{R}_n$. Учитывая, что $l \leqslant n - k$, положим

$$\Lambda_i = \{\nu \in \mathcal{R}_{\bar{n}} \colon K_\nu \cap L_i = \varnothing\} \subset \mathcal{R}_{\bar{n}}, \quad i = 1, \ldots, \bar{s}.$$

Имеем совокупность $\mathfrak{L} = \{\Lambda_1, \ldots, \Lambda_{\bar{s}}\}$. Это совокупность с параметрами $\bar{n}$, $\bar{s}$, $\bar{k}$, поскольку, очевидно, $\bar{k} = |\Lambda_i|$ для любого i. Возьмем произвольную минимальную с. о. п. для $\mathfrak{L}$ и обозначим ее элементы $\sigma_1, \ldots, \sigma_{\bar{\tau}}$, где

$$\bar{\tau} = \tau(\mathfrak{L}) \leqslant G(\bar{n}, \bar{s}, \bar{k}) \leqslant s.$$

Рассмотрим совокупность $\mathcal{M}' = \{K_{\sigma_1}, \ldots, K_{\sigma_{\bar{\tau}}}\}$. Понятно, что $\mathcal{M}'$ состоит из не более чем s подмножеств множества $\mathcal{R}_n$, каждое из которых имеет мощность k. Докажем, что $\tau(\mathcal{M}') > l$. Предположим противное. Тогда существует такое $L_i \in \mathcal{L}$, что $L_i \cap K_{\sigma_j} \neq \varnothing$ для всех $j \in \{1, \ldots, \bar{\tau}\}$. Последнее свойство равносильно утверждению о том, что $\sigma_j \notin \Lambda_i$ при любом j.

Но это противоречит определению множества $\{\sigma_1, \ldots, \sigma_{\bar{\tau}}\}$ как с. о. п. уже для $\mathfrak{L}$, ведь нашлось множество $\Lambda_i \in \mathfrak{L}$, которое ни одним из элементов $\sigma_1, \ldots, \sigma_{\bar{\tau}}$ не представлено. Значит, в самом деле, $\tau(\mathcal{M}') > l$. Если теперь добавить в $\mathcal{M}'$ произвольные k-элементные подмножества $\mathcal{R}_n$, чтобы возникла совокупность $\mathcal{M}$ мощности s, то теорема будет доказана, ведь мы помним, что при наращивании совокупности размер ее минимальной с. о. п. заведомо не убывает.

Приведенное доказательство напоминает какой-то фокус, и из него не видно, как именно могла бы быть устроена совокупность $\mathcal{M}$, найденная в нем. В этом и состоит специфика неконструктивных рассуждений. Зачастую они куда проще своих конструктивных аналогов (ср. доказательство теоремы 4.1.1), и даже результат получается подчас куда более сильным; однако пощупать его, материализовать совсем не просто. И что делать, когда все упирается в полный перебор? Хорошо, если на помощь приходят теоремы типа теоремы 4.1.1. К несчастью, так бывает отнюдь не всегда.

§ 4.5. Доказательство теоремы 4.1.3

Можно сказать, что в доказательстве теоремы 4.1.2 мы использовали некий «двойственный переход». На сей раз мы прибегнем к помощи классического вероятностного метода в комбинаторике (см. [28, 44, 46]). Выберем *случайную* совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$ из множества всех совокупностей с параметрами n, s, k. Это означает, что мы возьмем совокупность $\mathcal{K}$, состоящую из всех k-элементных подмножеств множества $\mathcal{R}_n$ (ср. § 4.4), и «наугад» извлечем из нее некоторое s-сочетание, полагая все потенциальные исходы равновероятными. Такое случайное s-сочетание и будет представлять собой искомую случайную совокупность. Если говорить более формально, то мы вводим *вероятностное пространство* (см. [8, 35, 37]), т. е. «тройку» $(\Omega, \mathcal{B}, P)$, в которой пространство элементарных событий имеет вид

$$\Omega = \{\mathcal{M} = \{M_1, \ldots, M_s\}\colon M_i \subset \mathcal{R}_n,\ |M_i| = k,\ i = 1, \ldots, s\},$$

σ-алгебра событий есть $\mathcal{B} = 2^{\Omega}$ (множество всех подмножеств множества Ω), а вероятность задается формулой $P(\mathcal{M}) = \dfrac{1}{|\Omega|}$, коль скоро $\mathcal{M} \in \Omega$. Ясно, что $|\Omega| = C^s_{C^k_n}$ (см. задачу 6 а).

Пусть $\mathfrak{A} \in \mathcal{B}$ — это событие, состоящее в том, что для случайной совокупности $\mathcal{M}$ выполнено неравенство $\tau(\mathcal{M}) \leqslant l$:

$$\mathfrak{A} = \{\mathcal{M} \in \Omega\colon \tau(\mathcal{M}) \leqslant l\}.$$

Очевидно, $\mathfrak{A} = \bigcup\limits_{i=1}^{C_n^l} \mathfrak{A}_i$, где

$$\mathfrak{A}_i = \{\mathcal{M} \in \Omega\colon L_i \in \mathcal{L} \text{ — с. о. п. для } \mathcal{M}\}.$$

(Здесь $\mathcal{L}$ — совокупность из предыдущего параграфа.) Значит,

$$P(\mathfrak{A}) = P\left(\bigcup_{i=1}^{C_n^l} \mathfrak{A}_i\right) \leqslant \sum_{i=1}^{C_n^l} P(\mathfrak{A}_i) = C_n^l P(\mathfrak{A}_i) \quad \forall i \in \{1, \ldots, C_n^l\}.$$

Замечаем, что

$$P(\mathfrak{A}_i) = \frac{|\mathfrak{A}_i|}{|\Omega|} = \frac{C^s_{C_n^k - C_{n-l}^k}}{C^s_{C_n^k}}.$$

Следовательно,

$$P(\mathfrak{A}) \leqslant C_n^l \frac{C^s_{C_n^k - C_{n-l}^k}}{C^s_{C_n^k}} < 1,$$

т. е. вероятность отрицания события $\mathfrak{A}$ положительна. Стало быть, $\{\mathcal{M} \in \Omega\colon \tau(\mathcal{M}) > l\} \neq \varnothing$, и теорема доказана.

Любопытно еще такое обстоятельство. Нетрудно показать, что при минимальном ослаблении условий теоремы «почти всякая» совокупность обладает очень «жирной» наименьшей с. о. п. Выражение «почти всякая» применительно к совокупности означает, например, что при $n \to \infty$ ($s = s(n)$, $k = k(n)$) вероятность извлечь такую совокупность стремится к единице. Для выполнения указанного свойства достаточно считать, что

$$C_n^l \frac{C^s_{C_n^k - C_{n-l}^k}}{C^s_{C_n^k}} \to 0 \quad \text{при } n \to \infty.$$

Скучные выкладки показывают, что и в этих предположениях можно взять $l = l(n, s, k) \sim \frac{n}{k} \ln \frac{sk}{n}$. Иными словами, вероятностный метод свидетельствует о том, что «почти наверное» оценка в теореме 3.1 асимптотически точна. Это особенно удивительно, если вспомнить, каких усилий требовало доказательство теоремы 4.1.1. Почти всякая совокупность обладает асимптотически максимальным возможным τ, и так трудно предъявить хотя бы один пример подобной совокупности! Впрочем, в математике часто возникают аналогичные странные казусы. Достаточно вспомнить про трансцендентные числа (см. [6,38,43]): почти все числа на вещественной прямой трансцендентны, а вот пойди докажи, что трансцендентно число $e = 2{,}71\ldots$ или число $\pi = 3{,}14\ldots$ О $e + \pi$ же и зарекаться не стоит (до сих пор неизвестно даже, иррационально ли такое число).

§ 4.6. Доказательство следствия 4.1.1

Нам нужно проверить, что в условиях следствия выполняется неравенство

$$G(C_n^k, C_n^l, C_{n-l}^k) = \max\Big\{\frac{C_n^k}{C_{n-l}^k}, \frac{C_n^k}{C_{n-l}^k}\ln\frac{C_n^l C_{n-l}^k}{C_n^k}\Big\} + \frac{C_n^k}{C_{n-l}^k} + 1 \leqslant s.$$

Итак,

$$\frac{C_n^k}{C_{n-l}^k} = \frac{n(n-1)\dots(n-k+1)}{k!}\cdot\frac{k!}{(n-l)(n-l-1)\dots(n-l-k+1)} =$$

$$= \Big(\frac{n-l}{n}\cdot\frac{n-l-1}{n-1}\cdot\dots\cdot\frac{n-l-k+1}{n-k+1}\Big)^{-1} = \Big(\Big(1-\frac{l}{n}\Big)\Big(1-\frac{l}{n-1}\Big)\dots$$

$$\dots\Big(1-\frac{l}{n-k+1}\Big)\Big)^{-1} \leqslant \Big(1-\frac{l}{n-k+1}\Big)^{-k} = e^{-k\ln\left(1-\frac{l}{n-k+1}\right)}.$$

За счет условия $k = o(n)$ и формулы Тейлора (см. [39]) получаем

$$e^{-k\ln\left(1-\frac{l}{n-k+1}\right)} = e^{\frac{kl}{n-k+1}+O\left(\frac{kl^2}{n^2}\right)}.$$

Опять-таки по формуле Тейлора выполняется неравенство

$$\frac{kl}{n-k+1} \leqslant \frac{kl}{n-k} = \frac{kl}{n}\Big(1-\frac{k}{n}\Big)^{-1} = \frac{kl}{n}\Big(1+O\Big(\frac{k}{n}\Big)\Big) = \frac{kl}{n}+O\Big(\frac{k^2l}{n^2}\Big).$$

Здесь ввиду условий $\ln\dfrac{sk}{n} = o(k)$ и $k = o(\sqrt{n})$ имеем

$$\frac{k^2l}{n^2} \sim \frac{k}{n}\ln\frac{sk}{n} = o\Big(\frac{k^2}{n}\Big) = o(1).$$

Таким образом, $\dfrac{kl}{n-k+1} = \dfrac{kl}{n} + o(1)$. В то же время,

$$\frac{kl^2}{n^2} \sim \frac{\ln^2\frac{sk}{n}}{k} = o(1),$$

так как $\ln\dfrac{sk}{n} = o(\sqrt{k})$. В итоге

$$\frac{C_n^k}{C_{n-l}^k} \leqslant e^{\frac{kl}{n}+o(1)} \leqslant 2e^{\frac{kl}{n}}$$

при достаточно больших n. Продолжая оценку, получаем

$$\frac{C_n^k}{C_{n-l}^k} \leqslant 2e^{\frac{kl}{n}} \leqslant 2\frac{sk}{n}\frac{1}{\ln\frac{sk}{n}}\frac{1}{\ln k}e^{-10} = o(s) < s$$

при больших n.

Далее, при больших n имеем

$$\ln \frac{C_n^l C_{n-l}^k}{C_n^k} \leqslant \ln C_n^l \leqslant \ln \frac{n^l}{l!} \leqslant \ln\Big(\frac{en}{l}\Big)^l \leqslant l \ln \frac{2en}{\frac{n}{k}\ln\frac{sk}{n}} \leqslant l \ln k \leqslant \frac{n}{k} \cdot \ln \frac{sk}{n} \cdot \ln k.$$

Вместе с тем очевидно, что

$$\ln \frac{C_n^l C_{n-l}^k}{C_n^k} \to \infty \quad \text{при } n \to \infty.$$

Значит,

$$G(C_n^k, C_n^l, C_{n-l}^k) = \max\Big\{\frac{C_n^k}{C_{n-l}^k}, \frac{C_n^k}{C_{n-l}^k} \ln \frac{C_n^l C_{n-l}^k}{C_n^k}\Big\} + \frac{C_n^k}{C_{n-l}^k} + 1 \leqslant$$
$$\leqslant 4 \frac{sk}{n} \frac{1}{\ln \frac{sk}{n}} \frac{1}{\ln k} e^{-10} \times \frac{n}{k} \cdot \ln \frac{sk}{n} \cdot \ln k < s.$$

Следствие 4.1.1 доказано.

§ 4.7. Возможные уточнения теорем 4.1.1—4.1.3

В этом параграфе мы скажем несколько слов о возможности улучшения оценок, полученных в теоремах 4.1.1—4.1.3. Ведь при всей их (подчас даже асимптотической) точности, явных формул для величины $\zeta(n, s, k)$ они не дают.

Начнем с теоремы 4.1.1. Нетрудно видеть, что неравенство $\zeta(n, s, k) \geqslant \geqslant \frac{n}{64k} \ln \frac{sk}{n}$ допускает значительные уточнения. Например, легкая модификация рассуждений из § 4.3 позволяет заменить константу 64 константой 4. Вообще, оптимальную константу в теореме 4.1.1 никто не считал, равно как никто не пытался оптимизировать ограничения из формулировки теоремы. В этой связи интересно, например, отыскать минимальное значение c в следующем утверждении.

Утверждение 4.7.1. *Пусть* $n \geqslant n_0$, $k \leqslant \frac{n}{n_0}$, *а* s *таково, что* $u_0 \leqslant \leqslant \ln \frac{sk}{n} \leqslant k$. *Тогда*

$$\zeta(n, s, k) \geqslant \frac{n}{ck} \ln \frac{sk}{n}.$$

Здесь $c = c(n_0, u_0)$.

Результат получился бы особенно сильным, если бы с ростом ограничений n_0, u_0 величина c стремилась к единице. Подчеркнем, что теоремы 4.1.2 и 4.1.3 фактически о таком поведении c и свидетельствуют, но

нас же сейчас именно явные конструкции привлекают. А в теоремах 4.1.2 и 4.1.3 никакого рецепта построения искомых совокупностей не дано.

Что касается теоремы 4.1.2 (вернее, следствия из нее), то там наиболее неприятным является наличие слишком большого множества ограничений, накладываемых на значения параметров n, s, k. Частично эту проблему удается решить. В работе [20] доказан, например, такой факт.

Утверждение 4.7.2. *Предположим, что* $n \to \infty$, $s = s(n) \to \infty$, $k = k(n) \to \infty$, *причем* $\dfrac{sk}{n}$ *также неограниченно возрастает с увеличением* n. *Пусть, далее,* $k = o(\sqrt{n})$ *и* $\ln \dfrac{sk}{n} = o(\sqrt{k})$. *Тогда*

$$\zeta(n, s, k) \geqslant \frac{n}{k} \ln \frac{sk}{n} + O\left(\frac{n}{k} \ln \ln \frac{sk}{n}\right).$$

Иными словами, утверждение 4.7.2 практически повторяет следствие 4.1.1, только в утверждении пропадает условие $\ln k = o\left(\dfrac{sk}{n}\right)$. Наверняка возможны и дальнейшие продвижения на указанном пути. g

§ 4.8. Несколько слов про $Z(n, s, k_1, \ldots, k_s)$

Величина $Z(n, s, k_1, \ldots, k_s)$ в самом общем случае устроена как-то совсем уж сложно и неприятно. Поэтому мы не станем здесь делать обширный экскурс в соответствующую науку. Мы лишь отошлем заинтересованного читателя к статьям [15] и [50].

Однако один аспект проблематики мы не преминем осветить в этом параграфе.

Предположим, величины k_1, $\ldots$, k_s могут, в принципе, принимать любые значения из множества $\{1, \ldots, n\}$. Будем считать, впрочем, что в той или иной интересующей нас совокупности $\mathcal{M}$ количество множеств мощности i не превосходит Ci^m, где C и m — заранее фиксированные константы. Рассмотрим максимум $\tau(\mathcal{M})$ по всем таким $\mathcal{M}$ и обозначим его $g(n, C, m)$.

Отдельно рассмотрим величину $g(n) = \max\limits_{\mathcal{M}} \tau(\mathcal{M})$, беря на сей раз максимум по всем совокупностям, состоящим из множеств попарно различной мощности. Понятно, что в этом случае $s \leqslant n$, но, как мы знаем, такое ограничение вовсе не является тривиальным.

Обе указанные выше величины достаточно хорошо изучены. На данный момент наилучшие результаты принадлежат авторам статьи [48], которые показали, в частности, что

$$g(n, C, m) \leqslant (Cm! + 1)n^{(m+1)/(m+2)}.$$

Формально полагая в последнем неравенстве $C = 1$, $m = 0$, очевидно, получаем $g(n) \leqslant 2\sqrt{n}$. Для достаточно больших n эта оценка допускает улучшение: $g(n) \leqslant 1{,}98\sqrt{n}$. Вместе с тем слишком на многое тут тоже рассчитывать не приходится. Доказано, что $g(n) \geqslant 1{,}5338\sqrt{n}$, если n достаточно велико.

Задачи

10. а) Оптимизируя выбор параметров в §4.3, уточните константу $\frac{1}{64}$ в теореме 4.1.1 (ср. §4.2, 4.7).

б*) Покажите, что техника из параграфа 4.3 не позволяет заменить величину $\frac{1}{64}$ величиной $1 - \varepsilon$ со сколь угодно малым ε (ср. §4.2).

в**) Опишите явную конструкцию совокупности $\mathcal{M}$ с какими-либо нетривиальными параметрами n, $s = s(n)$, $k = k(n)$, у которой $\tau(\mathcal{M}) \sim \sim \frac{n}{k} \ln \frac{sk}{n}$ (ср. §4.2, 4.7).

11. а) Можно ли избавиться в формулировках следствия 4.1.1 и утверждения 4.7.2 от условия $k = o(\sqrt{n})$?

б*) Можно ли в предположениях следствия 4.1.1 получить верхнюю оценку величины $\zeta(n, s, k)$ вида $\zeta(n, s, k) \leqslant \frac{n}{k} \ln \frac{sk}{n} - \varphi(n)$ с каким-либо $\varphi(n) \to \infty$, $n \to \infty$ (ср. задачу 9)? А с $\varphi(n) \geqslant c \frac{n}{k} \ln \ln \frac{sk}{n}$, $c > 0$?

12. Выведите из теоремы 4.1.3 следствие, аналогичное следствию 4.1.1. Сравните результаты обоих следствий.

13*. В §4.4 мы построили совокупность $\mathfrak{L}$ и для получения верхней оценки размера ее минимальной с. о. п. применили общую теорему 3.1. Нельзя ли уточнить оценку за счет специфики конструкции? Приведите какую-нибудь нетривиальную нижнюю оценку для $\tau(\mathfrak{L})$.

14*. С помощью вероятностной техники (см. §4.5) найдите как можно более точные верхние оценки мощности минимальной с. о. п. «почти всякой» совокупности с теми или иными параметрами n, s, k.

15.** Пусть параметры n, $s = s(n)$ и $k = k(n)$ таковы, что $\frac{n}{k} \ln \frac{sk}{n} > n$. Как в этом случае уточнить верхнюю оценку $\zeta(n, s, k) \leqslant n - k + 1$ (см. задачу 3б) и что можно сказать про нижние оценки? Для примера рассмотрите $k = [\sqrt{n}]$, $s = \left[\frac{C_n^k}{\sqrt{n}}\right] = o(C_n^k)$.

Глава 5

Проблема Турана и лотерея «Спортлото»

В этой главе мы расскажем о некоторых важных обобщениях задачи о системах общих представителей. Кроме того, мы обсудим довольно забавное приложение этих обобщений к известной лотерее «Спортлото».

§ 5.1. Постановки двух основных задач

Зафиксируем натуральное число n и два других натуральных числа k, l. Допустим, $k \leqslant l \leqslant n$. Рассмотрим в $\mathcal{R}_n$ совокупности

$$\mathcal{K} = \{K_1, \ldots, K_{C_n^k}\}, \quad \mathcal{L} = \{L_1, \ldots, L_{C_n^l}\},$$

состоящие из всевозможных k-элементных подмножеств (k-сочетаний) и l-элементных подмножеств (l-сочетаний) в $\mathcal{R}_n$ соответственно. Сейчас мы введем два очень естественных и важных обобщения понятия с. о. п. Речь, по сути, пойдет о покрытии k-элементных множеств l-элементными и наоборот.

Итак, мы скажем, что совокупность $\mathcal{S} \subseteq \mathcal{K}$ *покрывает* совокупность $\mathcal{L}$, если для любого $L_i \in \mathcal{L}$ найдется некоторое (хотя бы одно) $K_j \in \mathcal{S}$, которое обладает свойством $K_j \subseteq L_i$. Заметим, что, конечно же, K_j может совпадать с L_i лишь в одном вырожденном случае, когда $k = l$. С другой стороны, при $k = 1$ мы возвращаемся к задаче о системах общих представителей, так что нынешняя постановка действительно обобщает прежнюю. Правда, теперь мы ищем покрытие не для произвольной совокупности подмножеств $\mathcal{R}_n$, имеющих заданную наперед мощность, а только для совокупности, состоящей из всех возможных таких подмножеств. В случае $k = 1$, т. е. в случае с. о. п., подобная задача не слишком осмысленна, ведь, как мы помним (см. задачу 3 б и § 4.3), в ней минимальная совокупность $\mathcal{S}$ (являющаяся, вообще-то, обычным множеством $S \subseteq \mathcal{R}_n$) имеет мощность $n - l + 1$, и говорить тут более не о чем. Удивительным образом, сложность задачи при переходе от $k = 1$ к $k = 2$ и тем более к $k > 2$ катастрофически возрастает. Сама же задача, разумеется, состоит в отыскании наиболее экономного покрытия, т. е. величины

$$m(n, k, l) = \min\{|\mathcal{S}| : \mathcal{S} \text{ покрывает } \mathcal{L}\}.$$

Обратная задача сводится к нахождению числа

$$M(n, k, l) = \min\{|\mathcal{S}|: \mathcal{S} \subseteq \mathcal{L},\ \mathcal{S} \text{ покрывает } \mathcal{K}\}.$$

Здесь покрытие понимается в том смысле, что для каждого $K_i \in \mathcal{K}$ имеется такое $L_j \in \mathcal{S}$, что $L_j \supseteq K_i$. Употребление слова «покрытие» в рамках данной задачи кажется чуть более мотивированным, чем в первом случае. Однако задачи тесно связаны друг с другом, и они в равной мере посвящены покрытию.

О связи между задачами (обе они носят, как читатель уже, конечно, догадался, название *проблем Турана*) и о трудностях, возникающих при их решении, мы поговорим в следующем параграфе. В § 5.3 мы обсудим связь проблемы Турана с известной лотереей «Спортлото».

§ 5.2. Обзор известных результатов

В этом параграфе мы приведем ряд важнейших результатов, касающихся проблемы Турана. Разумеется, мы не станем претендовать на энциклопедичность изложения; мы лишь наметим основные направления исследований. Уже сейчас мы заранее можем сослаться на книгу [34] и на статьи [15, 50], которые в существенной мере дополнят создаваемую нами картину. В дальнейшем мы еще не раз вернемся к этим ссылкам.

Итак, прежде всего практически очевидным является следующее утверждение.

Теорема 5.2.1. *Для любых n, k, l имеет место тождество*

$$m(n, n-l, n-k) = M(n, k, l).$$

Теорема 5.2.1 устанавливает несложную связь между двумя величинами. Доказательство ее действительно под силу всякому, и потому не имеет смысла здесь его приводить. Важно то, что отныне мы вольны работать с любой из двух интересующих нас величин: коль скоро есть какой-либо факт, справедливый для одной из них, мы без труда транслируем его на язык второй величины.

Как мы уже говорили в предыдущем параграфе, задача отыскания величин $m(n, k, l)$, $M(n, k, l)$ крайне нетривиальна даже в случае, когда $k = 2$. Например, теорема, которую мы сформулируем ниже, доказана в книге [34] на четырех страницах, что отнюдь не мало. А ведь насколько частным кажется ее утверждение!

Теорема 5.2.2. *Выполнена формула*

$$M(n,2,3)=\begin{cases}\dfrac{n^2}{6}, & n\equiv 0 \pmod 6,\\ \dfrac{n(n-1)}{6}, & n\equiv 1,3 \pmod 6,\\ \dfrac{n^2+2}{6}, & n\equiv 2,4 \pmod 6,\\ \dfrac{n^2-n+4}{6}, & n\equiv 5 \pmod 6.\end{cases}$$

Это один из немногих случаев, когда в задаче получен точный ответ. Заметим, что о ряде подобных ситуаций также рассказано в книге [34] и статье [50]; мы же перейдем к общим оценкам.

Наиболее универсальными и простыми являются следующие две теоремы.

Теорема 5.2.3. *Для любых n, k, l имеет место неравенство*

$$M(n,k,l)\geqslant \frac{n}{l}M(n-1,k-1,l-1).$$

Теорема 5.2.4. *Для любых n, k, l имеет место неравенство*

$$M(n,k,l)\leqslant M(n-1,k,l)+M(n-1,k-1,l-1).$$

Иными словами, установлены рекуррентные оценки, причем ясно, что $M(n,k,k)=C_n^k$ (нельзя покрыть k-элементные множества k-элементными множествами, не задействовав их все). Доказательства теорем см. в [34].

Еще один любопытный аспект проблематики связан с использованием техники, практически идентичной той, которую мы применяли в § 4.4.

Теорема 5.2.5. *Для любых n, k, l имеют место неравенства*

$$M(n,k,l)\leqslant G\bigl(C_n^l, C_n^k, C_{n-k}^{l-k}\bigr),\quad m(n,k,l)\leqslant G\bigl(C_n^k, C_n^l, C_l^k\bigr),$$

где $G(\bar n,\bar s,\bar k)$ — функция из теоремы 3.1.

Понятно, что второе неравенство в теореме 5.2.5 эквивалентно первому ввиду теоремы 5.2.1. Тем не менее, мы явно докажем каждую из оценок, дабы сделать максимально прозрачной методику, которая пригодится нам в гл. 7.

Доказательство первого неравенства в теореме 5.2.5. Не погнушаемся почти дословно повторить рассуждение из § 4.4 (правда, с новыми параметрами). Положим $\bar n=C_n^l$, $\bar s=C_n^k$, $\bar k=C_{n-k}^{l-k}$. Рассмотрим совокупность $\mathcal{L}=\{L_1,\ldots,L_{\bar n}\}$, введенную фактически в начале § 5.1. Сопоставляя каждому множеству из $\mathcal{L}$ его номер, получаем взаимно однозначное соответствие между совокупностью $\mathcal{L}$ и множеством $\mathcal{R}_{\bar n}$. Пусть, далее,

$\mathcal{K} = \{K_1, \ldots, K_{\bar{s}}\}$ также совокупность из начала § 5.1. Положим

$$\Lambda_i = \{\nu \in \mathcal{R}_{\bar{n}} \colon L_\nu \supseteq K_i\} \subset \mathcal{R}_{\bar{n}}, \quad i = 1, \ldots, \bar{s}.$$

Имеем совокупность $\mathfrak{L} = \{\Lambda_1, \ldots, \Lambda_{\bar{s}}\}$. Это совокупность с параметрами $\bar{n}$, $\bar{s}$, $\bar{k}$, поскольку, очевидно, $\bar{k} = |\Lambda_i|$ для любого i. Возьмем произвольную минимальную с. о. п. для $\mathfrak{L}$ и обозначим ее элементы $\sigma_1, \ldots, \sigma_{\bar{\tau}}$, где

$$\bar{\tau} = \tau(\mathfrak{L}) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Рассмотрим совокупность $\mathcal{S} = \{L_{\sigma_1}, \ldots, L_{\sigma_{\bar{\tau}}}\}$. Понятно, что $\mathcal{S}$ покрывает $\mathcal{K}$. В самом деле, условие «для любого i найдется такое ν, что $\sigma_\nu \in \Lambda_i$» равносильно условию «для любого i найдется такое ν, что $L_{\sigma_\nu} \supseteq K_i$». Неравенство доказано.

Доказательство второго неравенства в теореме 5.2.5. Что называется, повторение — мать учения... Положим $\bar{n} = C_n^k$, $\bar{s} = C_n^l$, $\bar{k} = C_l^k$. Рассмотрим совокупность $\mathcal{K} = \{K_1, \ldots, K_{\bar{n}}\}$. Сопоставляя каждому множеству из $\mathcal{K}$ его номер, получаем взаимно однозначное соответствие между совокупностью $\mathcal{K}$ и множеством $\mathcal{R}_{\bar{n}}$. Пусть, далее, $\mathcal{L} = \{L_1, \ldots, L_{\bar{s}}\}$. Положим

$$\Lambda_i = \{\nu \in \mathcal{R}_{\bar{n}} \colon K_\nu \subseteq L_i\} \subset \mathcal{R}_{\bar{n}}, \quad i = 1, \ldots, \bar{s}.$$

Имеем совокупность $\mathfrak{L} = \{\Lambda_1, \ldots, \Lambda_{\bar{s}}\}$. Это совокупность с параметрами $\bar{n}$, $\bar{s}$, $\bar{k}$, поскольку, очевидно, $\bar{k} = |\Lambda_i|$ для любого i. Возьмем произвольную минимальную с. о. п. для $\mathfrak{L}$ и обозначим ее элементы $\sigma_1, \ldots, \sigma_{\bar{\tau}}$, где

$$\bar{\tau} = \tau(\mathfrak{L}) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Рассмотрим совокупность $\mathcal{S} = \{K_{\sigma_1}, \ldots, K_{\sigma_{\bar{\tau}}}\}$. Понятно, что $\mathcal{S}$ покрывает $\mathcal{L}$. В самом деле, условие «для любого i найдется такое ν, что $\sigma_\nu \in \Lambda_i$» равносильно условию «для любого i найдется такое ν, что $K_{\sigma_\nu} \subseteq L_i$». Неравенство доказано.

§ 5.3. Несколько слов о стратегии игры в лотерею «Спортлото»

Многие знают, в чем состоит лотерея «Спортлото». Конечно, во времена Советского Союза эта лотерея была куда более известна, нежели сегодня, когда розыгрыши плодятся, как грибы после дождя, и каким-нибудь «джек-потом» в миллион «у. е.» никого не удивить. Однако и сейчас небезынтересно попытаться понять, что могло бы помочь увеличить вероятность выигрыша в данной лотерее. Подчеркнем, что речь не может идти о построении беспроигрышной стратегии. Это было бы просто нелепо. Речь идет именно о попытках, действуя не совсем наугад, повысить шансы на успех.

1	~~7~~	13	19	25	31
2	8	14	20	26	32
3	9	~~15~~	21	27	33
4	10	16	22	28	~~34~~
5	11	17	~~23~~	29	35
~~6~~	12	18	24	30	36

1	7	~~13~~	19	25	31
2	8	14	20	26	32
3	9	15	21	27	~~33~~
~~4~~	10	16	22	28	34
5	11	17	~~23~~	29	35
6	~~12~~	18	24	30	36

Рис. 4

Напомним, в чем состоит лотерея. Листок бумаги разделен на две одинаковые части, в каждой из которых написаны числа от 1 до 36 (или до 49, но мы для определенности остановимся лишь на первой ситуации). Нужно в каждой из частей зачеркнуть любые пять чисел (см. рис. 4). Если хотя бы одна из полученных пятерок совпадет с той, которая возникнет в результате розыгрыша, то играющий сорвет банк. Более того, даже совпадение некоторых четырех или некоторых трех чисел принесет игроку приличную сумму денег. Иными словами, если он вычеркнул, скажем, числа 1, 7, 23, 29, 32, а во время розыгрыша выпали номера 29, 32, 1, 5, 34, то это успех, ведь в обоих случаях имеется серия из трех номеров 1, 29, 32.

Тут важно еще напомнить, как именно осуществляется розыгрыш. В большом прозрачном «барабане» хаотически крутятся, прыгают 36 шаров с номерами 1, 2 и т. д. Через равные промежутки времени один из шаров проваливается в на миг открывающееся отверстие, и таким образом мы узнаем очередной выигрышный номер. Именно поэтому мы не стали упорядочивать выше числа в примере: как правило, порядок их как раз неправильный. Главное следствие для нас состоит, стало быть, в том, что и пятерку вычеркнутых чисел, и любую тройку потенциально совпадающих номеров мы вольны рассматривать как сочетание (без повторений); вместе с тем пятерку номеров, выпавших из барабана, мы обязаны интерпретировать, напротив, как размещение (тоже без повторений).

Предположим, в результате розыгрыша выпало некоторое размещение номеров. Мы же, допустим, стремились угадать хотя бы три цифры. Какова вероятность того, что, вычеркивая наугад числа, мы добились нашей цели? Очевидно, всего есть C_{36}^5 способов осуществить выбор интересующего нас сочетания без повторений. Выигрышных же троек в любом

случае $C_5^3 = 10$. Пусть A — это количество сочетаний, каждое из которых содержит хотя бы одну выигрышную тройку. Тогда искомую вероятность естественно считать равной $\dfrac{A}{C_{36}^5}$.

С другой стороны, пусть $n = 36$, $k = 3$, $l = 5$ и мы знаем значение величины $M(n, k, l)$, а также систему l-элементных множеств (пятерок), на которой оно достигается. Тогда, выбирая случайную пятерку в этой системе, мы отлавливаем выигрышную тройку с вероятностью не меньше $\dfrac{1}{M(n, k, l)}$. Проблема лишь в том (см. предыдущий параграф), что отыскание $M(n, k, l)$ — пока дело будущего. Тем не менее, любопытные стратегии игры в Спортлото были предложены. Здесь техника чуть более специальная, и она выходит за рамки данной книги. Зато в книге [34] об этом сказано весьма подробно. Так или иначе, речь по-прежнему идет о покрытии, и видно, насколько оно важно для приложений.

Задачи

16. Предположим, в первой проблеме Турана речь идет о покрытии множествами из $\mathcal{K}$ не всей совокупности $\mathcal{L}$ (см. §5.1), но лишь некоторой ее части $\mathcal{M} \subset \mathcal{L}$, $|\mathcal{M}| = s$. Что тогда можно сказать о размере минимальной покрывающей системы?

17. Найдите точное значение величины A в §5.3.

18. Как должно оцениваться число $M(n, k, l)$ в конце §5.3, дабы при описанном там «турановском» подходе к лотерее вероятность отловить выигрышную тройку оказалась больше величины $\dfrac{A}{C_{36}^5}$ (см. задачу 17)?

Глава 6

Системы общих представителей в геометрии: ε-сети

Эту главу мы посвятим одной из красивейших дисциплин современной математики, лежащей на стыке геометрии, комбинаторики, математической статистики и теории сложности. Естественно, центральную роль сыграют здесь с. о. п.

§ 6.1. Постановка типичной задачи и формулировка частного результата

Рассмотрим обычную евклидову плоскость $\mathbb{R}^2$ и зафиксируем произвольное (конечное) множество точек S на ней. Положим $n = |S|$. В наших стандартных обозначениях S можно отождествить с $\mathcal{R}_n$. Пусть, далее, задано число $\varepsilon \in (0, 1)$. Рассмотрим множество $\mathfrak{T}$ всех (открытых) треугольников на плоскости. При этом на вид, размер и расположение треугольников мы абсолютно никаких ограничений не накладываем. Нас будет интересовать, как тот или иной треугольник $\Delta \in \mathfrak{T}$ пересекается с исходным множеством S. Понятно, что какие-то элементы множества $\mathfrak{T}$ с S вовсе не пересекаются, а какие-то, напротив, целиком содержат S. Мы изучим только те $\Delta \in \mathfrak{T}$, для которых

$$|\Delta \cap S| \geqslant \varepsilon |S| = \varepsilon n.$$

Иными словами, для нас будут важны лишь те треугольники, которые содержат значительную долю множества S. Смысл в том, что если мы начнем варьировать S и, в частности, устремим его мощность к бесконечности, то нас по-прежнему будут волновать ситуации, когда доля элементов из S, попадающих в Δ, постоянна; к случаям же, когда $|S \cap \Delta| = o(n)$, мы останемся безразличны. Обозначим множество всех упомянутых треугольников через $\mathfrak{T}_\varepsilon(S) \subset \mathfrak{T}$.

Определим совокупность множеств

$$\mathcal{M} = \mathcal{M}_\varepsilon(S, \mathfrak{T}) = \{M_1, \ldots, M_s\},$$

полагая

$$\mathcal{M} = \{S \cap \Delta\}_{\Delta \in \mathfrak{T}_\varepsilon(S)}.$$

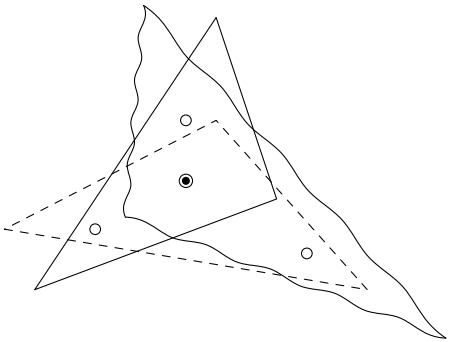

Рис. 5

Естественно, для разных Δ_1, Δ_2 вполне может получиться, что $\Delta_1 \cap S = \Delta_2 \cap S$. Такие пересечения образуют одно и то же множество в совокупности $\mathcal{M}$. Понятно, стало быть, что мы фактически вернулись к знакомой нам ситуации: $S = \mathcal{R}_n$, $\mathcal{M}$ — совокупность подмножеств множества $\mathcal{R}_n$. Более того, $k_j = |M_j| \geqslant \varepsilon n$, и только величина $s = |\mathcal{M}|$ нам неизвестна. Очевидно, $s \leqslant C_n^{[\varepsilon n]+1}$, коль скоро $\varepsilon < \frac{1}{2}$, и аналогичная оценка имеет место при $\varepsilon \geqslant \frac{1}{2}$. Однако в зависимости от структуры множества S подобная оценка, несомненно, может быть существенно уточнена (см. задачи).

Получение оценок величины минимальной с. о. п. для описанной совокупности $\mathcal{M}$ — это важная задача комбинаторной геометрии и статистики, являющаяся, очевидно, частным случаем задачи отыскания формул для $\zeta(n, s, k)$ и $Z(n, s, k_1, \ldots, k_s)$. Эта задача неожиданно сильно отличается от своего обобщения, уже изученного нами в гл. 4. Соответственно, и методы ее решения будут совершенно другими. Но об этом чуть позже. Пока заметим, что любую с. о. п. для $\mathcal{M}$ принято называть *ε-сетью*, и в этом нет ничего удивительного. На рис. 5 изображена типичная $3/4$ — сеть для множества S мощности 4. Эта сеть одноэлементна, хотя минимальная с. о. п. для совокупности всех трех- и четырехэлементных подмножеств в $\mathcal{R}_4$ имеет, конечно, размер 2.

У читателя может возникнуть резонный вопрос: а почему мы, собственно, рассматриваем множества именно на плоскости, и зачем мы пересекаем эти множества исключительно с треугольниками? Ответ здесь один: все это мы делаем для наглядности. Разумеется, можно работать не с плоскостью, а с пространством $\mathbb{R}^d$ произвольной размерности; можно пересекать множества с произвольными многоугольниками, многогранниками и пр. Более того, в следующем параграфе мы опишем все

многообразие подобных ситуаций. Сейчас же вернемся к совокупностям $\mathcal{M}_\varepsilon(S, \mathfrak{T})$ и их системам представителей (ε-сетям).

Теорема 6.1.1. *Существует такая константа $c > 0$, что, какова бы ни была множество $S \subset \mathbb{R}^2$, $|S| < \infty$, имеет место неравенство*

$$\tau\big(\mathcal{M}_\varepsilon(S, \mathfrak{T})\big) \leqslant \frac{c}{\varepsilon} \ln \frac{1}{\varepsilon}.$$

Теорема 6.1.1 является следствием значительно более общего результата, который был доказан В. Н. Вапником и А. Я. Червоненкисом в 1971 г. Этот результат мы сформулируем и докажем позднее, а заодно продемонстрируем, конечно, как утверждение теоремы 6.1.1 из него вытекает. Сейчас мы лучше прокомментируем это утверждение. А оно удивительно! В самом деле, стандартная техника не позволяет получить оценку точнее, чем $\tau(\mathcal{M}) \leqslant n - [\varepsilon n] + 1$ (ср. задачу 3). Зато теорема 6.1.1 утверждает, что оценка для $\tau(\mathcal{M})$ вовсе от n не зависит! Фактически, сколь бы велико ни было множество $S \subset \mathbb{R}^2$ и как бы хитро это множество на плоскости ни располагалось, все равно размер минимальной ε-сети зависит только от величины ε. Более того, зависимость эта практически обратно пропорциональная (мешает логарифм). Отметим, что несложно приводится пример множества S, для которого $\tau \geqslant \frac{c}{\varepsilon}$ при любом ε, но до сих пор остается нерешенной проблема устранения пресловутого логарифма в верхней оценке или доказательства его неустранимости (см. [46]).

В следующем параграфе мы начнем двигаться в направлении доказательства удивительной теоремы 6.1.1 и ее не менее удивительных обобщений. Для начала мы познакомимся с одним очень глубоким понятием — понятием размерности Вапника—Червоненкиса.

§ 6.2. Размерность Вапника—Червоненкиса, постановка общей задачи и формулировка общего результата

В этом параграфе мы дадим определение размерности Вапника—Червоненкиса. С помощью этого понятия мы сумеем добиться значительных продвижений в понимании проблематики текущей главы.

6.2.1. Размерность Вапника—Червоненкиса: определение, примеры и свойства

Пусть X — некоторое (возможно, даже бесконечное) множество, а R — произвольная совокупность подмножеств в X. Пару (X, R) назовем *пространством областей* (области суть элементы совокупности R). Если $|X| < \infty$, т. е. $|X| = n$, $n \in \mathbb{N}$, то в прежних обозначениях

$(X, R) = (\mathcal{R}_n, \mathcal{M})$ и пространство областей превращается в обычную пару «множество — совокупность подмножеств». Более того, если $|r| = 2$ для любого $r \in R$, то (X, R) — это *граф* (см. [23, 40] и § 9.1). В этой связи отметим, что пространство областей $(X, R) = (\mathcal{R}_n, \mathcal{M})$ зачастую называют *гиперграфом* (см. [27,28,44,46]). В случаях, когда $|X| = \infty$, можно говорить о бесконечных графах и гиперграфах, но в определенных ситуациях такая терминология не вполне разумна. Например, пусть $(X, R) = (\mathbb{R}^d, \mathcal{H})$, где $\mathcal{H}$ — совокупность всех (открытых) полупространств в $\mathbb{R}^d$. Такое пространство областей играет огромную роль в науке, и мы еще будем работать с ним. Однако довольно странно было бы отождествлять это пространство с гиперграфом, хотя бы даже и бесконечным. Ведь полбеды, что множество вершин у данного «гиперграфа» бесконечно, так еще и ребра его чересчур огромны: шутка в деле — полупространства.

Пусть дано пространство областей (X, R). Если $A \subset X$, то *проекцией совокупности R на A* называется совокупность

$$P_R(A) = \{r \cap A\}_{r \in R}.$$

Естественно, если для разных $r_1, r_2 \in R$ выполнено условие $r_1 \cap A = r_2 \cap A$, то два последних пересечения мы отождествляем. Мы говорим, что конечное множество $A \subset X$ *дробится*, если $P_R(A) = 2^A$, т. е. проекция R на A совпадает с множеством всех подмножеств множества A. *Размерность Вапника—Червоненкиса пространства областей* (X, R) — это мощность максимального множества $A \subset X$, которое дробится областями из R, если максимум достигается, и бесконечность, если для любого n найдется такое $A \subset X$, что $|A| = n$ и $P_R(A) = 2^A$. Иными словами, если обозначить через $VC(X, R)$ упомянутую размерность, то при условии, что

$$m = \max\{n\colon \exists\, A \subset X, \quad |A| = n, \quad P_R(A) = 2^A\} < \infty,$$

мы имеем $VC(X, R) = m$, а иначе $VC(X, R) = \infty$.

Разумеется, если $|X| < \infty$ (более привычная нам ситуация), то размерность $VC(X, R)$ заведомо конечна. Если же $|X| = \infty$, то возможны разные варианты. Тривиальные примеры пространств областей, имеющих бесконечную размерность Вапника—Червоненкиса, напрашиваются сами собой: достаточно взять любое бесконечное множество X и объявить областями в нем все возможные его подмножества. Другие подобные примеры мы обсудим в разделе задач. Также ничего, конечно, не стоит указать бесконечное пространство областей (X, R) с конечной величиной $VC(X, R)$: просто положим $R = \varnothing$, и вся недолгá. Вместо того чтобы обсуждать тривиальности, лучше заняться более любопытными вопросами. Скажем, чему равна размерность пространства $(\mathbb{R}^d, \mathcal{H})$?

Пусть для начала $A \subset \mathbb{R}^d$ таково, что $|A| \leqslant d + 1$ и элементы множества A суть вершины некоторого *симплекса* (треугольника, тетраэдра

и пр., см. [25]). Тогда практически очевидно, что A дробится посредством полупространств из $\mathcal{H}$. На рис. 6 изображено «дробление» трехточечного множества на плоскости соответствующими полуплоскостями. В то же время уже в $\mathbb{R}^2$ элементарно строится пример ситуации, когда дробление множества из четырех точек невозможно (см. рис. 7). На самом деле *никакие* четыре точки на плоскости дроблению не подлежат, и в этом читатель легко убедится сам. Более того, в произвольной размерности d любое множество A, у которого $|A| \geqslant d+2$, не дробится открытыми полупространствами. Этот факт есть прямое следствие знаменитой теоремы Радона в комбинаторной геометрии. Теорему Радона мы приводим ниже без доказательства, которое можно найти в книге [9].

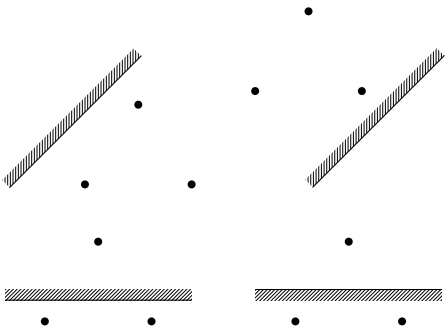

Рис. 6

Теорема 6.2.1.1. *Если конечное множество $A \subset \mathbb{R}^d$ таково, что $|A| \geqslant d+2$, то существуют множества A_1, A_2, удовлетворяющие условиям $A = A_1 \cup A_2$, $A_1 \cap A_2 = \varnothing$ и $\operatorname{conv} A_1 \cap \operatorname{conv} A_2 \neq \varnothing$.*

Здесь

$$\operatorname{conv} A = \left\{ \mathbf{x} \in \mathbb{R}^d : \mathbf{x} = \lambda_1 \mathbf{a}_1 + \ldots + \lambda_m \mathbf{a}_m,\ \forall i\ \lambda_i \geqslant 0,\ \sum_{i=1}^{m} \lambda_i = 1 \right\}$$

— *выпуклая оболочка* множества A, $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\} \subset \mathbb{R}^d$. Например, выпуклая оболочка двух точек — это отрезок, а выпуклая оболочка трех точек — треугольник; вообще, выпуклая оболочка конечного множества — всегда многоугольник или многогранник (см. [25, 59]). Отметим, что на рис. 7 как раз показано то разбиение множества $A \subset \mathbb{R}^2$ на части A_1, A_2, существование которого утверждается в теореме.

Итак, мы поняли, что каждое множество $A \subset \mathbb{R}^d$ дробится, если $|A| \leqslant d+1$ и A — симплекс, и что, напротив, никакое множество $A \subset \mathbb{R}^d$

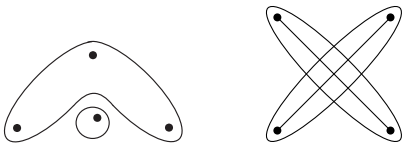

Рис. 7

дроблению не поддается, если $|A| \geqslant d+2$. Значит, $VC(\mathbb{R}^d,\ \mathcal{H}) = d+1$, и мы имеем нетривиальный пример бесконечного пространства областей с конечной размерностью Вапника—Червоненкиса.

Обсудим несколько важных свойств размерности Вапника—Червоненкиса. Прежде всего заметим, что если дано конечное пространство областей (X, R), т. е. $|X| = n < \infty$, и известно, что $|R| \leqslant m$ для некоторого $m \leqslant 2^n$, то и величина $VC(X, R)$ не может быть слишком большой. Выражение «не слишком большая», по идее, требует пояснений, но для наших дальнейших целей полезнее будет получить эффективную оценку числа областей в пространстве (X, R), коль скоро $|X| = n$ и $VC(X, R) = d \leqslant n$. И давать пояснения мы не станем.

Положим $g(n, d) = \sum\limits_{i=0}^{d} C_n^i$. В силу простого тождества $C_a^b = C_{a-1}^b + C_{a-1}^{b-1}$ ($a \geqslant 1,\ b \geqslant 1$, см. [3]) получаем $g(n, d) = g(n-1, d) + g(n-1, d-1)$ при $n \geqslant 1,\ d \geqslant 1$. На всякий случай поясним, что мы считаем C_a^b равным нулю при $a < b$ и равным единице при $a = b$ (даже если $a = b = 0$); вообще говоря, $0! = 1$. Таким образом, $g(0, d) = 1$ для всякого $d \geqslant 0$ и $g(n, 0) = 1$ при каждом $n \geqslant 0$. Имеем, по сути, рекуррентное соотношение с заданными наперед начальными условиями (см. [3, 7]).

Утверждение 6.2.1.1. *Если пространство областей* (X, R) *таково, что* $|X| = n$ *и* $VC(X, R) \leqslant d$ $(n \geqslant 0, d \geqslant 0)$, *то* $|R| \leqslant g(n, d)$.

Доказательство утверждения 6.2.1.1. Применим полную индукцию по n и d.

База индукции. Пусть $n = 0$. Тогда $X = \varnothing$. Стало быть, либо $R = \varnothing$, либо $R = \{\varnothing\}$, т. е. заведомо $|R| \leqslant 1$. В то же время, очевидно, $VC(X, R) \leqslant n = 0$, так что в любом случае $d = 0$. Таким образом, действительно, $|R| \leqslant 1 = g(0, 0)$. Пусть, наоборот, $d = 0$, а $n \geqslant 1$ — любое число. Предположим, что $|R| \geqslant 2$. Тогда возьмем произвольные $r_1,\ r_2 \in R$. Ясно, что $r_1 \neq r_2$. Следовательно, либо в $r_1 \setminus r_2$, либо в $r_2 \setminus r_1$ есть хотя бы один элемент x из X. Множество $A = \{x\}$ дробится областями $r_1,\ r_2$ по построению. Получим противоречие с условием $VC(X, R) = d = 0$. В конечном итоге $|R| \leqslant 1 = g(n, 0)$, и основание индукции у нас в кармане.

Шаг индукции. Пусть $n \geqslant 1$, $d \geqslant 1$. Зафиксируем пространство (X, R)с конкретными параметрами n, d. Поскольку $X \neq \varnothing$, мы вольны взять произвольный элемент $x \in X$. Рассмотрим $R_1 = \{r \setminus \{x\}\}_{r \in R}$. Если интерпретировать R_1 как мультимножество (т. е. разрешить некоторым элементам из R_1 совпадать между собою), то, разумеется, $|R_1| = |R|$. Тем не менее, мы посмотрим на R_1 именно как на обычное множество и, стало быть, отождествим те $r_1 \setminus \{x\}$ и $r_2 \setminus \{x\}$ $(r_1, r_2 \in R)$, для которых $r_1 \setminus \{x\} = r_2 \setminus \{x\}$. Это нужно для того, чтобы корректно определять пространство областей $(X \setminus \{x\}, R_1)$. Заметим, что равенство $r_1 \setminus \{x\} = r_2 \setminus \{x\}$ возможно лишь тогда, когда либо $r_2 = r_1 \setminus \{x\}$, либо $r_1 = r_2 \setminus \{x\}$. Следовательно, если мы желаем компенсировать потери, возникшие в результате отождествления элементов в *мультимножестве* R_1 в процессе превращения последнего в стандартное множество (с тем же именем R_1), то нам необходимо взять $R_2 = \{r \in R\colon x \notin r,\ r \cup \{x\} \in R\}$, и тогда окажется, что $|R| = |R_1| + |R_2|$ (см. рис. 8). При этом в дополнение к $S_1 = (X \setminus \{x\}, R_1)$ корректно определено пространство $S_2 = (X \setminus \{x\}, R_2)$.

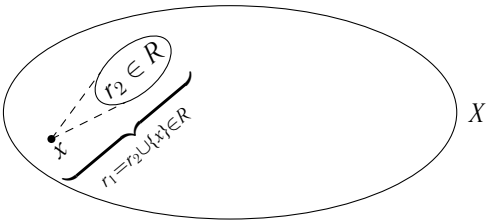

Рис. 8

Далее, $|X \setminus \{x\}| = n - 1$. Кроме того, очевидно, $VC(S_1) \leqslant d$, и нетрудно проверить, что $VC(S_2) \leqslant d - 1$. В самом деле, если $VC(S_2) = d$, то найдется такое множество $A \subset X \setminus \{x\}$, что $|A| = d$ и A дробится областями из R_2. Но тогда $A' = A \cup \{x\}$ таково, что $|A'| = d + 1$ и A' дробится областями из R. Получим противоречие с условием $VC(X, R) = d$. В итоге по предположению индукции $|R_1| \leqslant g(n-1, d)$, $|R_2| \leqslant g(n-1, d-1)$, и, стало быть,

$$|R| = |R_1| + |R_2| \leqslant g(n-1, d) + g(n-1, d-1) = g(n, d).$$

Шаг индукции завершен, и утверждение доказано.

Следствие 6.2.1.1. *Пусть (X, R) — пространство областей, у которого $VC(X, R) \leqslant d$. При этом на X и его мощность мы никаких ограничений не накладываем. Зафиксируем $n \in \mathbb{N}$ и рассмотрим произвольное множество $A \subseteq X$ мощности n (если таковое существует). Тогда $|P_R(A)| \leqslant g(n, d)$.*

Доказательство следствия 6.2.1.1. Возьмем пространство областей $S = (A, P_R(A))$. Очевидно, $VC(S) \leqslant d$, и мы знаем, что $|A| = n$. В силу утверждения 6.2.1.1 имеем $|P_R(A)| \leqslant g(n, d)$. Следствие доказано.

Пусть задано натуральное число $h \geqslant 2$. Назовем *h-измельчением* множества областей R в пространстве (X, R) множество

$$R_h = \{r_1 \cap \ldots \cap r_h \colon r_1, \ldots, r_h \in R\}.$$

Как обычно, совпадающие пересечения мы отождествляем, и в результате корректно определено пространство (X, R_h). Заметим, что если $(X, R) = (\mathbb{R}^d, \mathcal{H})$, то $C_h := R_h$ целиком содержит внутри себя совокупность всех выпуклых многогранников в $\mathbb{R}^d$, имеющих ровно h граней. В частности, при $d = 2$ и $h = 3$ приходим к объектам § 6.1 (скажем, $C_h \supset \mathfrak{T}$), и это отнюдь не случайно.

Утверждение 6.2.1.2. *Если пространство областей (X, R) имеет размерность $d \geqslant 2$ и задано число $h \geqslant 2$, то $VC(X, R_h) \leqslant 2dh \log_2 dh$.*

Доказательство утверждения 6.2.1.2. Зафиксируем произвольное натуральное $n > 2dh \log_2 dh$ и рассмотрим любое множество $A \subset X$, имеющее мощность n (если, конечно, такое множество вообще существует, т. е. если $|X| \geqslant n$). В силу следствия 6.2.1.1 имеем $|P_R(A)| \leqslant g(n, d)$. Очевидно,

$$|P_{R_h}(A)| \leqslant |P_R(A)|^h \leqslant g^h(n, d).$$

В то же время ясно, что $n \geqslant 2d$ (т. е. $d \leqslant \frac{n}{2}$), а значит, в сумме $g(n, d) = \sum\limits_{i=0}^{d} C_n^i$ максимально последнее слагаемое, и $g(n, d) \leqslant n^d$ (индукция). Таким образом,

$$|P_{R_h}(A)| \leqslant g^h(n, d) \leqslant n^{dh},$$

и если мы теперь покажем, что $n^{dh} < 2^n$, то получится, что никакое множество $A \subset X$ мощности $n > 2dh \log_2 dh$ дроблению не подлежит, т. е. в самом деле $VC(X, R_h) \leqslant 2dh \log_2 dh$. Установим, стало быть, нужное неравенство. Для начала заметим, что оно равносильно соотношению $\dfrac{n}{\log_2 n} > dh$. Функция $\dfrac{n}{\log_2 n}$ возрастает при $n > 2$, но у нас $n > 2 \cdot 2 \cdot 2 \log_2 (2 \cdot 2) = 16$, и в этом плане точно все в порядке. Значит,

$$\frac{n}{\log_2 n} > \frac{2dh \log_2 dh}{1 + \log_2 dh + \log_2 \log_2 dh}.$$

Далее функция $\log_2 dh - \log_2 \log_2 dh - 1$ при наших условиях опять-таки возрастает. Следовательно,

$$\log_2 dh - \log_2 \log_2 dh - 1 \geqslant \log_2 (2 \cdot 2) - \log_2 \log_2 (2 \cdot 2) - 1 = 0,$$

так что $1+\log_2\log_2 dh \leqslant \log_2 dh$ и

$$\frac{n}{\log_2 n} > \frac{2dh\log_2 dh}{1+\log_2 dh+\log_2\log_2 dh} \geqslant \frac{2dh\log_2 dh}{2\log_2 dh} = dh.$$

Утверждение доказано.

Следствие 6.2.1.2. *Пусть* $(X, R) = (\mathbb{R}^d, P_h)$ *— пространство, в котором множество областей состоит из всех возможных выпуклых многогранников (многоугольников) в* $\mathbb{R}^d$ $(d \geqslant 2)$, *имеющих ровно* h *граней. Тогда* $VC(X, R) \leqslant 2(d+1)h\log_2(d+1)h$. *В частности,* $(\mathbb{R}^2, P_3) = (\mathbb{R}^2, \mathfrak{T})$ *и* $VC(\mathbb{R}^2, \mathfrak{T}) \leqslant 18\log_2 9 \approx 60$.

Доказательство следствия 6.2.1.2. Мы знаем, что $VC(\mathbb{R}^d, \mathcal{H}) = d+1$. Значит, ввиду утверждения 6.2.1.2 получаем

$$VC(\mathbb{R}^d, C_h) \leqslant 2(d+1)h\log_2(d+1)h.$$

Но $P_h \subset C_h$, и, стало быть, тем более

$$VC(\mathbb{R}^d, P_h) \leqslant 2(d+1)h\log_2(d+1)h.$$

Следствие доказано. Следствие показывает, что, сколь бы много мы ни брали полиэдров с фиксированным числом граней и фиксированной размерностью, в пространстве той же размерности «слишком большое» множество точек нам раздробить не удастся. Например, на плоскости какое-нибудь множество из шестидесяти точек мы, быть может, посредством треугольников и раздробим, но уж точно мы не сумеем добиться подобного эффекта по отношению к какому-либо набору из семидесяти элементов $\mathbb{R}^2$. Это довольно любопытно, и именно этот факт окажется центральным при доказательстве теоремы 6.1.1 и ее более общих аналогов.

6.2.2. Постановка задачи об ε-сетях

Пусть (X, R) — произвольное пространство областей (конечное или бесконечное). Рассмотрим любое конечное множество $S \subset X$ и положим $n = |S|$. Зафиксируем какое угодно $\varepsilon \in (0, 1)$. Определим $R_\varepsilon(S)$ как совокупность всех элементов $r \in R$, которые обладают тем свойством, что $|r \cap S| \geqslant \varepsilon n$. Пусть, далее,

$$\mathcal{M} = \mathcal{M}_\varepsilon(S, R) = \{M_1, \ldots, M_s\} = \{S \cap r\}_{r \in R_\varepsilon(S)}.$$

Тогда *ε-сетью* для множества S называется любая с. о. п. для совокупности $\mathcal{M}$.

Если $(X, R) = (\mathbb{R}^2, \mathfrak{T})$, то мы возвращаемся к понятию ε-сети из § 6.1.

Предположим, что размерность Вапника—Червоненкиса изучаемого пространства (X, R) бесконечна. Тогда для любого $n \in \mathbb{N}$ существует

множество $S \subset X$ мощности n, которое дробится областями $r \in R$. В частности, для такого S совокупность $\mathcal{M}$ есть, очевидно,

$$\mathcal{M} = \{M \subseteq S\colon |M| \geqslant \varepsilon n\}.$$

Тогда понятно, что $\tau(\mathcal{M}) \geqslant n - \varepsilon n + 1$ (ср. задачу 3), т. е. любая ε-сеть для $\mathcal{M}$ содержит порядка n элементов. Ничего похожего на утверждение теоремы 6.1.1 не наблюдается. Что ж, это и не критично, ведь в теореме 6.1.1 речь идет о пространстве, размерность которого, напротив, конечна (см. п. 6.2.1). В следующем пункте мы сформулируем общий результат, справедливый для всякого конечномерного пространства областей.

6.2.3. Формулировки результатов

Справедлива следующая теорема.

Теорема 6.2.3.1. *Пусть (X, R) — пространство областей конечной размерности d, а ε — фиксированное число из интервала $(0, 1)$. Тогда, каково бы ни было множество $S \subset X$, $|S| < \infty$, имеет место неравенство*

$$\tau\bigl(\mathcal{M}_\varepsilon(S, R)\bigr) \leqslant \frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon}.$$

Теорема 6.2.3.1 была доказана Э. Вельцлем и Д. Хаусслером в 1987 г. На 16 лет раньше была опубликована замечательная работа Вапника—Червоненкиса, в которой доказан слегка другой, но, по сути, не менее сильный результат. Ниже мы сформулируем и его. Сейчас же заметим, что из теоремы 6.2.3.1 мгновенно следует теорема 6.1.1 с константой $c < 1000$ (здесь $d \approx 60$, $8d \approx 500$, ср. п. 6.2.1).

Пусть (X, R) — пространство областей, A — произвольное подмножество множества X, а ε — любое число из интервала $(0, 1)$. Назовем $B \subset X$ *ε-копией* множества A, если для всякого $r \in R$ выполнено неравенство

$$\left| \frac{|A \cap r|}{|A|} - \frac{|B \cap r|}{|B|} \right| \leqslant \varepsilon.$$

Нетрудно убедиться в том, что любая ε-копия является и ε-сетью для данного подмножества пространства областей. Обратное неверно. Следующая теорема принадлежит Вапнику и Червоненкису.

Теорема 6.2.3.2. *Существует такая положительная постоянная c, что, каковы бы ни были пространство областей (X, R) заданной размерности d, конечное множество $A \subset X$ и число $\varepsilon \in (0, 1)$, найдется множество $B \subset X$, являющееся ε-копией множества A и удовлетворяющее неравенству*

$$|B| \leqslant \frac{cd}{\varepsilon^2} \log_2 \frac{d}{\varepsilon}.$$

Теорему 6.2.3.1 мы докажем в § 6.3, а доказательство (очень похожее) теоремы 6.2.3.2 предоставим читателю. Отметим сразу, что уже из формулировок видно, насколько существенно различаются понятия ε-сети и ε-копии: в первом случае зависимость правой части оценки от величины ε (которая, собственно, и является единственной переменной при всем изобилии обозначений) с точностью до логарифмической поправки обратная линейной; во втором же случае она обратна квадратической. По поводу самой этой зависимости (хотя бы для ε-сетей, которые, впрочем, и теме нашей книги куда более соответствуют) мы скажем еще пару слов. Напомним, что в конце § 6.1, комментируя теорему 6.1.1, мы заметили, что принципиально уточнить неравенство $\tau \leqslant \frac{c}{\varepsilon}$ (т. е. более чем в константу раз) невозможно: существуют ситуации, когда τ растет заведомо не медленнее, нежели $\frac{c}{\varepsilon}$, при $\varepsilon \to 0$. Поскольку, как мы уже знаем, теорема 6.1.1 есть прямое следствие теоремы 6.2.3.1, это означает, что и последнее утверждение практически неулучшаемо: если на что и можно надеяться, то на устранение логарифма в оценке. Однако тут нас ожидает фиаско. Если в случае *геометрической* теоремы 6.1.1 такая надежда все еще сохраняется (см. § 6.1), то в случае *общей* теоремы 6.2.3.1 логарифмический сомножитель необходим: известны примеры пространств и их подмножеств, для которых нет ε-сетей с $s < \frac{c}{\varepsilon}\log_2\frac{1}{\varepsilon}$ элементами. Просто эти пространства более вычурны, нежели $(\mathbb{R}^2, \mathfrak{T})$.

§ 6.3. Доказательство теоремы 6.2.3.1 и небольшой комментарий к нему

В этом параграфе мы докажем теорему 6.2.3.1 и прокомментируем доказательство.

6.3.1. Начало доказательства и формулировки основных лемм

Зафиксируем некоторое пространство областей (X, R), имеющее размерность Вапника—Червоненкиса d. Зафиксируем также $\varepsilon \in (0, 1)$ и $S \subset X$; положим $n = |S|$. Фактически нам нужно найти теперь такое множество $N \subseteq S$, что для любого $r \in R$ из условия $|r \cap S| \geqslant \varepsilon n$ следует соотношение $(r \cap S) \cap N = r \cap N \neq \varnothing$.

Как и в § 4.5, воспользуемся замечательной вероятностной техникой. Положим сперва $m = \left\lceil \frac{8d}{\varepsilon}\log_2\frac{8d}{\varepsilon} \right\rceil$. Представим себе, что S — это такой ящик с n занумерованными и тщательно перемешанными карточками. Запустим в него руку и «наугад» извлечем одну карточку. Это будет какой-то элемент $x \in S$. Обозначим его x_1 и вернем карточку на ме-

сто, после чего снова тщательно перемешаем содержимое ящика. Опять запустим руку в ящик и возьмем случайную карточку. Назовем ее x_2. Действуя аналогично m раз, получим серию карточек $x_1, \ldots, x_m$. Разумеется, некоторые (и даже все) карточки в данной серии могут совпасть, но для нас это не страшно. Мы обозначим через N мультимножество $N = \{x_1, \ldots, x_m\}$. Это мультимножество мы нашли в процессе выполнения случайных действий. И действия эти были вполне определенными. Итак, чему же разумно положить равной вероятность $P(N)$ того, что случайное мультимножество N совпадет с некоторым наперед заданным мультимножеством из m элементов? По-видимому, ясно: $P(N) = \left(\frac{1}{n}\right)^m$. В самом деле, каждый элемент из N с одной и той же вероятностью (если говорить на языке интуиции) мог оказаться равным любому элементу $x \in S$; значит, вероятность того, что он равен очередному элементу x_i, $i = 1, \ldots, m$, естественно определять как $\frac{1}{n}$. Элементы («карточки») извлекались из множества S (из «коробки») независимо друг друга, вероятности перемножаются, и возникает формула $P(N) = \left(\frac{1}{n}\right)^m$.

Описанная схема построения случайного множества N называется *схемой выбора с возвращением* (см. [8, 35, 37]). В комбинаторике же говорят о случайном выборе размещения с повторениями.

Выражаясь более формально, мы рассматриваем вероятностное пространство $(\Omega_1, \mathcal{B}_1, P_1)$, в котором

$$\Omega_1 = \{\{x_1, \ldots, x_m\} \colon x_i \in S \ \forall i\}, \quad |\Omega_1| = n^m,$$

$$\mathcal{B}_1 = 2^{\Omega_1}, \quad P_1(N) = \frac{1}{n^m} \quad \forall N \in \Omega_1.$$

Соответственно, если $A \in \mathcal{B}_1$ — произвольное событие, то

$$P_1(A) = \sum_{N \in A} P_1(N).$$

Рассмотрим событие

$$E_1 = \{N \in \Omega_1 \colon \exists r \in R \quad |r \cap S| \geqslant \varepsilon n, \ r \cap N = \varnothing\}.$$

Это, так сказать, дурное событие. Если оно произойдет (т. е. если в результате всех процедур случайного выбора окажется, что $N \in E_1$), то мы успеха не добьемся: N тогда не есть искомое (мульти)множество. Иначе все в порядке, и превратить N в нормальную ε-сеть N', мощность которой не превосходит m, не составляет труда. Нам бы теперь показать, что $P_1(E_1) < 1$, и цель будет достигнута.

К сожалению, все не так просто. Взять и оценить $P_1(E_1)$ сразу не получается. Нужен дополнительный трюк. И вот что мы сделаем. Совершенно так же, как мы только что построили мультимножество N, построим m-размещение с повторениями T. Его выбор мы осуществим в рамках прежней схемы с возвращением, причем так, как если бы никакого N еще не было на свете. Ничто не препятствует, например, совпадению N и T. В результате появляется новое вероятностное пространство $(\Omega_2, \mathcal{B}_2, P_2)$, где

$$\Omega_2 = \{(N, T)\} = \big\{(\{x_1, \dots, x_m\}, \{y_1, \dots, y_m\})\colon x_i, y_i \in S\ \forall i\big\},$$
$$|\Omega_2| = n^{2m}, \quad \mathcal{B}_2 = 2^{\Omega_2}, \quad P_2((N, T)) = \frac{1}{n^{2m}} \quad \forall (N, T) \in \Omega_2.$$

В этом вероятностном пространстве присутствует аналог события E_1, и мы не станем его переименовывать:

$$E_1 = \{(N, T) \in \Omega_2\colon \exists r \in R\ |r \cap S| \geqslant \varepsilon n,\ r \cap N = \varnothing\}.$$

В нем T не играет, по сути, никакой роли, и читатель должен возмутиться: «Так зачем же весь огород городить? Какая разница — доказать, что $P_1(E_1) < 1$, или убедиться в том, что $P_2(E_1) < 1$?» Но разница все же есть. Дабы увидеть ее, введем событие E_2:

$$E_2 = \Big\{(N, T) \in \Omega_2\colon \exists r \in R\ |r \cap S| \geqslant \varepsilon n,\ r \cap N = \varnothing, |r \cap T| \geqslant \frac{\varepsilon m}{2}\Big\}.$$

Здесь

$$|r \cap T| = |r \cap \{y_1, \dots, y_m\}| = |\{i\colon 1 \leqslant i \leqslant m,\ y_i \in r\}|,$$

т. е. $r \cap T$ — это по-прежнему мультимножество. Аналогично мы в дальнейшем будем определять $|r \cap N|$, $|r \cap (N \cup T)|$ и пр. Имеет место следующий результат.

Лемма 6.3.1.1. *Выполнено неравенство* $P_2(E_2) \geqslant \frac{1}{2} P_2(E_1)$.

Что ж, чуть-чуть яснее стало. Видимо, технически удобнее доказывать оценку $P_2(E_2) < \frac{1}{2}$, ведь, если докажем мы ее, то в силу леммы 6.3.1.1 получится искомое неравенство $P_2(E_1) < 1$. И тут на помощь приходит следующее утверждение.

Лемма 6.3.1.2. *Выполнено неравенство* $P_2(E_2) \leqslant g(2m, d) 2^{-\frac{\varepsilon m}{2}}$.

Остается лишь удостовериться, что, в свою очередь, $g(2m, d) 2^{-\frac{\varepsilon m}{2}} < \frac{1}{2}$ при нашем выборе величины m. Последний факт мы установим в п. 6.3.4, лемму 6.3.1.1 мы докажем в п. 6.3.2, а лемму 6.3.1.2 — в п. 6.3.3.

6.3.2. Доказательство леммы 6.3.1.1

Удобно оперировать для начала *условными вероятностями*. Напомним, что если A и B суть некоторые события на данном вероятностном пространстве $(\Omega, \mathcal{B}, P)$, причем $P(B) \neq 0$, то *условной вероятностью события A при условии события B* называется величина $P(A|B) = \dfrac{P(A \cap B)}{P(B)}$. Нетрудно пояснить, почему именно так определяется указанное понятие. Один из лучших комментариев на сей счет приводится в книге [8], и мы не станем копировать его здесь. Смысл, как и должно быть, состоит в том, что все условия, описывающие событие B, мы предполагаем выполненными и в таком предположении стремимся вычислить вероятность выполнения условий, в терминах которых задается событие A.

В нашем случае речь пойдет о величине $P_2(E_2|E_1)$. Поскольку $E_2 \subset E_1$, имеем $E_2 \cap E_1 = E_2$, т. е. формально

$$P_2(E_2|E_1) = \frac{P_2(E_2 \cap E_1)}{P_2(E_1)} = \frac{P_2(E_2)}{P_2(E_1)}.$$

Таким образом, если мы желаем показать, что $P_2(E_2) \geqslant \dfrac{1}{2} P_2(E_1)$, то нам достаточно проверить неравенство $P_2(E_2|E_1) \geqslant \dfrac{1}{2}$.

Итак, пусть событие E_1 выполнено. Тогда, разумеется, существует конкретная область $r_1 \in R$, для которой $|r_1 \cap S| \geqslant \varepsilon n$ и $r_1 \cap N = \varnothing$. Очевидно, что интересующая нас условная вероятность заведомо не меньше вероятности того, что $|r_1 \cap T| \geqslant \dfrac{\varepsilon m}{2}$. Правда, не вполне понятно, быть может, о какой вероятности мы говорим в последнем случае. Формально стоило бы ввести пространство $(\Omega_3, \mathcal{B}_3, P_3)$, которое полностью аналогично пространству $(\Omega_1, \mathcal{B}_1, P_1)$ (совпадает с ним с точностью до замены обозначения N обозначением T), и рассуждать в терминах $P_3\left(\left\{T : |r_1 \cap T| \geqslant \dfrac{\varepsilon m}{2}\right\}\right)$. Так мы и поступим.

Заметим, что область r_1, конечно, не обязана целиком лежать внутри множества S; в то же время элементы размещения T мы извлекаем исключительно из S. Поэтому уместно рассмотреть $u = r_1 \cap S$ $(|u| \geqslant \varepsilon n)$ и оценить $P_3\left(\left\{T : |u \cap T| \geqslant \dfrac{\varepsilon m}{2}\right\}\right)$. Фактически мы имеем здесь дело со *схемой испытаний Бернулли* (см. [8, 37]): всего испытаний m (на каждом шаге мы извлекаем очередной элемент мультимножества T), и «успех» для нас состоит в попадании указанного элемента в u. Соответственно, искомая вероятность — это вероятность того, что в нашей схеме произошло не менее $\dfrac{\varepsilon m}{2}$ успехов. При этом вероятность отдельного успеха есть, безусловно, $\dfrac{|u|}{|S|} \geqslant \varepsilon$.

Пусть ξ — *биномиальная случайная величина* на каком-либо пространстве $(\Omega, \mathcal{B}, P)$ с *параметрами* m и ε (см. [8, 35, 37]). Иными словами, ξ — это любая функция из Ω в $\{0, 1, \ldots, m\}$, про которую известно, что

$$P(\{\omega\colon \xi(\omega) = k\}) = C_m^k \varepsilon^k (1-\varepsilon)^{n-k}, \quad k = 0, \ldots, m.$$

Или, еще по-другому, ξ — это число успехов в некоторой схеме с m испытаниями Бернулли и вероятностью успеха ε. Нетрудно, стало быть, видеть, что

$$P_3\left(\left\{T\colon |u \cap T| \geqslant \frac{\varepsilon m}{2}\right\}\right) \geqslant P\left(\left\{\omega\colon \xi(\omega) \geqslant \frac{\varepsilon m}{2}\right\}\right).$$

Воспользуемся следующим утверждением.

Неравенство Чебышёва. *Каковы бы ни были вероятностное пространство* $(\Omega, \mathcal{B}, P)$ *случайная величина* ξ *на нем, удовлетворяющая условию* $M\xi^2 < \infty$, *для любого* $\lambda > 0$ *выполнена оценка*

$$P(\{\omega \in \Omega\colon |\xi(\omega) - M\xi| \geqslant \lambda\}) \leqslant \frac{D\xi}{\lambda^2}.$$

Здесь $M\xi$ *— математическое ожидание случайной величины* ξ, *а* $D\xi = M\xi^2 - (M\xi)^2$ *— ее дисперсия.*

Доказательство этого (несложного) факта можно найти в книгах [8, 35, 37], и мы его тут не приводим.

В нашем случае $M\xi = m\varepsilon$, а $D\xi = m\varepsilon(1-\varepsilon) \leqslant m\varepsilon$. Значит,

$$\begin{aligned} P\left(\left\{\omega\colon \xi(\omega) \geqslant \frac{\varepsilon m}{2}\right\}\right) &= 1 - P\left(\left\{\omega\colon \xi(\omega) < \frac{\varepsilon m}{2}\right\}\right) = \\ = 1 - P\left(\left\{\omega\colon \xi(\omega) - M\xi < \frac{\varepsilon m}{2} - M\xi\right\}\right) &= 1 - P\left(\left\{\omega\colon \xi(\omega) - \varepsilon m < -\frac{\varepsilon m}{2}\right\}\right) = \\ = 1 - P\left(\left\{\omega\colon \varepsilon m - \xi(\omega) > \frac{\varepsilon m}{2}\right\}\right) &\geqslant 1 - \frac{\varepsilon m}{\left(\frac{\varepsilon m}{2}\right)^2} = 1 - \frac{4}{\varepsilon m}. \end{aligned}$$

Вспоминаем, что у нас

$$m \geqslant \frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon} \geqslant \frac{24}{\varepsilon}.$$

Следовательно,

$$1 - \frac{4}{\varepsilon m} \geqslant 1 - \frac{4}{24} > \frac{1}{2},$$

и доказательство леммы завершено.

6.3.3. Доказательство леммы 6.3.1.2

В предыдущих параграфах и пунктах книги мы достаточно долго работали с различного рода вероятностными объектами, стараясь вводить их максимально формально. Поэтому мы смеем надеяться, что читатель уже немного освоился с технологией и что, стало быть, мы можем слегка расслабиться и уменьшить вероятностную формалистику. В первую очередь нам бы хотелось избавить дальнейшее изложение от постоянной апелляции к «номеру» вероятностного пространства. Иначе говоря, если какое-то P_4 при очень строгом подходе необходимо, например, оценить тем или иным P_5, то мы явно это указывать не станем, заменяя и P_4, и P_5 единообразным P, символизирующим вероятность «вообще». При желании читатель сам разберется, что является случайным объектом и к какому пространству этот объект, тем самым, относится. Не стоит, однако, думать, что мы прекратим давать какие-либо пояснения. Просто порассуждаем на чуть более интуитивном уровне. Иначе, мы погрязнем в ненужных формальностях и только запутаемся.

Итак, у нас есть событие E_2, вероятность которого мы стремимся оценить. Напомним, что, по сути, E_2 состоит в существовании такого $r \in R$, $|r \cap S| \geqslant \varepsilon n$, что $r \cap N = \varnothing$ и $|r \cap T| \geqslant \frac{\varepsilon m}{2}$. При этом пару (N, T) мы строим, выбирая последовательно два m-размещения с повторениями (т. е., собственно, N и T) в рамках схемы случайного выбора с возвращением. То же самое «распределение вероятностей» можно получить, действуя по-другому. А именно, сперва выберем из S случайное $2m$-размещение с повторениями U (по прежней схеме), а затем извлечем из U случайное подмножество (вернее, «подмультимножество») N, имеющее m элементов. Последний акт предполагает, что если $U = \{z_1, \ldots, z_{2m}\}$, то $N = \{z_{i_1}, \ldots, z_{i_m}\}$ (индексы $i_1, \ldots, i_m$, конечно, все разные, но, безусловно, $\{i_1, \ldots, i_m\} \subset \{1, \ldots, 2m\}$) с вероятностью $\frac{1}{C_{2m}^m}$ независимо от вида конкретных $z_{i_1}, \ldots, z_{i_m}$. В результате у нас получится пара (N, T), в которой $T = U \setminus N$. Обязательно проверьте, что вероятность любого события, относящегося к такой паре, есть в точности вероятность аналогичного события в случае исходной процедуры построения (N, T)! Да и в чем, вообще-то, проблема? Если раньше мы фактически выбирали $U = \{z_1, \ldots, z_{2m}\}$ и, не мудрствуя лукаво, полагали

$$N = \{x_1, \ldots, x_m\} = \{z_1, \ldots, z_m\}, \quad T = \{y_1, \ldots, y_m\} = \{z_{m+1}, \ldots, z_{2m}\},$$

то отныне нам захотелось дополнительного произвола в разбиении U на два куска. Очевидно же, что это всего лишь трюк, а новым парам (N, T) и тут возникнуть неоткуда.

Разумеется, нас по-прежнему интересует $P(E_2)$ (индекс, как мы и обещали, исчез, да и само E_2 — это событие, относящееся, по-хорошему, к слегка обновленным объектам). По *формуле полной вероятности* (см. [8, 35, 37]) $P(E_2) = \sum\limits_U P(E_2|U)P(U)$, где суммирование распространяется на все $2m$-размещения с повторениями U из S, а $P(U) = \dfrac{1}{n^{2m}}$.

Событие E_2 можно представить в виде

$$E_2 = \bigcup_{r\in R,\ |r\cap S|\geqslant \varepsilon n} E_r,\ E_r = \left\{(N, T)\colon r\cap N = \varnothing,\ |r\cap T| \geqslant \frac{\varepsilon m}{2}\right\}.$$

Однако если U фиксировано (а так оно и будет, коль скоро мы рассмотрим $P(E_2|U)$ с тем или иным U), то для любых $r_1, r_2 \in R$, удовлетворяющих условию $r_1 \cap U = r_2 \cap U$, события E_{r_1}, E_{r_2} идентичны. Следовательно,

$$P(E_2|U) = P\left(\bigcup_{i=1}^{t} E_{r_i} \mid U\right) \leqslant \sum_{i=1}^{t} P(E_{r_i} \mid U),$$

где последнее объединение берется уже не по всем $r \in R$, а лишь по представителям классов эквивалентности ($r_1 \sim r_2$, если $r_1 \cap U = r_2 \cap U$). Так ведь t — это не что иное, как $|P_R(U)| \leqslant g(2m, d)$. Правда, небольшая тонкость состоит в том, что U — мультимножество, но эта тонкость легко преодолима.

Если, стало быть, мы докажем, что для любого i выполнено неравенство $P(E_{r_i} \mid U) \leqslant 2^{-\frac{\varepsilon m}{2}}$, то дело будет в шляпе. Тогда $P(E_2|U) \leqslant$ $\leqslant g(2m, d)2^{-\frac{\varepsilon m}{2}}$, и ввиду упомянутой выше формулы полной вероятности то же самое справедливо для $P(E_2)$. Что ж, давайте установим нужное неравенство.

Прежде всего все будет доказано

$$P(E_{r_i} \mid U) \leqslant P\left(r_i \cap N = \varnothing \,||\, r_i \cap U| \geqslant \frac{\varepsilon m}{2}\right).$$

Положим $p = |r_i \cap U|$. Тогда, очевидно, искомая условная вероятность имеет вид

$$\frac{C_{2m-p}^{m}}{C_{2m}^{m}} = \frac{(2m-p)(2m-p-1)\dots(m-p+1)}{2m(2m-1)\dots(m+1)} =$$

$$= \frac{m(m-1)\dots(m-p+1)}{2m(2m-1)\dots(2m-p+1)} \leqslant 2^{-p} \leqslant 2^{-\frac{\varepsilon m}{2}}.$$

Лемма доказана.

6.3.4. Завершение доказательства теоремы

Итак, леммы доказаны, и нам осталось убедиться в том, что при

$$m = \left\lceil \frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon} \right\rceil$$

выполнено неравенство

$$g(2m, d)2^{-\frac{\varepsilon m}{2}} < \frac{1}{2}.$$

Как и в доказательстве утверждения 6.2.1.2, имеет место оценка $g(2m, d) \leqslant (2m)^d$; тут важно лишь, что, очевидным образом, $d \leqslant m$. Значит, достаточно проверить, что

$$(2m)^d 2^{-\frac{\varepsilon m}{2}} < \frac{1}{2}.$$

Последнее неравенство эквивалентно (за счет взятия двоичного логарифма от обеих его частей) следующему:

$$d \log_2(2m) - \frac{\varepsilon m}{2} < -1,$$

т. е. нам нужно, чтобы получилось соотношение

$$f(d, \varepsilon, m) = d + 1 + d \log_2 m - \frac{\varepsilon m}{2} < 0.$$

Функция $f(d, \varepsilon, m)$ убывает по $m \geqslant \left\lceil \frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon} \right\rceil$ при фиксированных d и ε, поскольку

$$\frac{\partial f(d, \varepsilon, m)}{\partial m} = \frac{d}{m \ln 2} - \frac{\varepsilon}{2} \leqslant \frac{d}{\left(\frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon}\right) \ln 2} - \frac{\varepsilon}{2} = \frac{\varepsilon}{\left(8 \log_2 \frac{8d}{\varepsilon}\right) \ln 2} - \frac{\varepsilon}{2} < 0.$$

Здесь отрицательность величины

$$\frac{\varepsilon}{\left(8 \log_2 \frac{8d}{\varepsilon}\right) \ln 2} - \frac{\varepsilon}{2}$$

обусловлена тем фактом, что

$$\left(8 \log_2 \frac{8d}{\varepsilon}\right) \ln 2 \geqslant \left(8 \log_2 8\right) \ln 2 = 24 \ln 2 > 2.$$

У нас $m \geqslant \left\lceil \frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon} \right\rceil$, и только что установленная монотонность функции $f(d, \varepsilon, m)$ обеспечивает нам неравенство

$$f(d, \varepsilon, m) \leqslant d + 1 + d \log_2 \left(\frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon}\right) - 4d \log_2 \frac{8d}{\varepsilon}.$$

Мы по-прежнему хотим, чтобы выполнялась оценка $f(d, \varepsilon, m) < 0$. Ввиду последнего наблюдения такая оценка равносильна соотношению

$$d + 1 + d \log_2\Big(\frac{8d}{\varepsilon} \log_2 \frac{8d}{\varepsilon}\Big) - 4d \log_2 \frac{8d}{\varepsilon} = \\ = d + 1 - 3d \log_2 \frac{8d}{\varepsilon} + d \log_2 \log_2 \frac{8d}{\varepsilon} < 0.$$

Заметим, что

$$d \log_2 \frac{8d}{\varepsilon} \geqslant d \log_2 8 = 3d > d + 1,$$

т. е.

$$d + 1 - d \log_2 \frac{8d}{\varepsilon} < 0,$$

и все будет в порядке, коль скоро мы покажем, что

$$2d \log_2 \frac{8d}{\varepsilon} \geqslant d \log_2 \log_2 \frac{8d}{\varepsilon}.$$

Рассмотрим функцию $g(x) = 2 \log_2 x - \log_2 \log_2 x$. Ее производная имеет вид

$$g'(x) = \frac{2}{x \ln 2} - \frac{1}{(\log_2 x) \ln 2} \cdot \frac{1}{x \ln 2}.$$

Следовательно, при $x \geqslant 8$ выполняется неравенство

$$g'(x) = \frac{1}{x \ln 2}\Big(2 - \frac{1}{(\log_2 x) \ln 2}\Big) \geqslant \frac{1}{x \ln 2}\Big(2 - \frac{1}{3 \ln 2}\Big) > 0.$$

Таким образом, при $x \geqslant 8$ функция $g(x)$ заведомо возрастает. В нашем случае $\frac{8d}{\varepsilon} \geqslant 8$, значит,

$$g\Big(\frac{8d}{\varepsilon}\Big) \geqslant g(8) = 6 - \log_2 3 > 0,$$

т. е.

$$2 \log_2 \frac{8d}{\varepsilon} \geqslant \log_2 \log_2 \frac{8d}{\varepsilon},$$

а это неравенство равносильно интересующему нас неравенству

$$2d \log_2 \frac{8d}{\varepsilon} \geqslant d \log_2 \log_2 \frac{8d}{\varepsilon}.$$

Теорема доказана.

6.3.5. Замечания к доказательству

Доказательство теоремы мы осуществили с помощью вероятностного метода. При этом нам хватало того факта, что $P_2(E_1) < 1$, и мы не гнались за аккуратностью последней оценки. На самом деле можно сформулировать теорему так, чтобы в итоге получалось неравенство $P_2(E_1) < \delta$, если величина $\delta > 0$ с самого начала зафиксирована. Справедлива

Теорема 6.3.5.1. *Пусть* (X, R) *— пространство областей конечной размерности* d; ε, δ *— фиксированные числа из интервала* $(0, 1)$; S *— произвольное конечное подмножество* X. *Пусть, далее,*

$$m = \max\left\{\left\lceil \frac{8d}{\varepsilon}\log_2\frac{8d}{\varepsilon}\right\rceil, \left\lceil \frac{4}{\varepsilon}\log_2\frac{2}{\delta}\right\rceil\right\}$$

и N *— случайное* m*-размещение с повторениями, возникшее в результате схемы выбора с возвращением элементов множества* S. *Тогда с вероятностью больше* $1-\delta$ *множество, полученное удалением совпадающих элементов из* N, *является* ε*-сетью для* S, *т. е. с вероятностью больше* $1-\delta$ *выполнено неравенство*

$$\tau\bigl(\mathcal{M}_\varepsilon(S, R)\bigr) \leqslant m.$$

Очевидно, оценка с. о. п. в теореме 6.3.5.1 хуже своей предшественницы из теоремы 6.2.3.1. Да оно и не удивительно: должны же мы потерять что-нибудь, желая доказать, что не просто у множества S есть ε-сеть, размер которой не зависит от мощности самого S, но что к тому же таких «маленьких» ε-сетей — масса. В некотором смысле теорема 6.3.5.1 соотносится с теоремой 6.2.3.1 так же, как и результат теоремы 4.1.3 соотносится с результатом замечания, сделанного по завершении ее доказательства (см. § 4.5): с. о. п. не только есть; почти все есть с. о. п.!

Доказательство теоремы 6.3.5.1 практически дословно совпадает с доказательством теоремы 6.2.3.1, и мы его не проводим.

Интересно, что у теоремы 6.2.3.2 также есть «(ε, δ)-аналог». Правда, априори не вполне понятно, о каком δ вообще здесь может идти речь, ведь доказательства теоремы 6.2.3.2 мы не проводили. Мы лишь заметили в свое время, что оно очень похоже на доказательство теоремы 6.2.3.1, да и того достаточно, чтобы понять: без вероятностной технологии тут не обойтись. Однако небольшой нюанс все же имеется. Дело в том, что в теореме 6.2.3.1 (и, как следствие, в теореме 6.3.5.1) мы осуществляли случайный выбор искомого объекта (т. е. в тех ситуациях — ε-сети) в рамках схемы выбора с возвращением, разрешая извлекаемым элементам совпадать и, стало быть, образовывать размещения с повторениями; это нам не вредило, поскольку удаление совпадающих элементов только уменьшало потенциальную сеть, сохраняя неизменными ее свойства. На сей же раз нам необходимо извлечь из множества A (см. формулировку теоремы 6.2.3.2) его ε-копию, и по некоторым причинам это удобнее будет сделать посредством иной схемы выбора случайных элементов A. В сущности, данная схема в точности повторяет ту, которая была описана в § 4.5. Отныне мы вновь берем не случайное размещение с повторениями (известной мощности m), а случайное сочетание без повторений

(опять-таки известной мощности m), полагая вероятность возникновения конкретного множества $B \subset A$ равной $\frac{1}{C^m_{|A|}}$. При таком подходе имеет место следующий результат.

Теорема 6.3.5.2. *Пусть (X, R) — пространство областей конечной размерности d; ε, δ — фиксированные числа из интервала $(0, 1)$; A — произвольное конечное подмножество в X. Пусть, далее,*

$$m = \min\left\{\left\lceil \frac{c}{\varepsilon^2}\left(d \log_2 \frac{d}{\varepsilon} + \log_2 \frac{1}{\delta}\right)\right\rceil,\ |A|\right\},$$

где $c > 0$ — некая постоянная, величина которой не зависит ни от одного из прочих объектов и параметров, фигурирующих в формулировке. Пусть, наконец, B — это случайное m-сочетание без повторений, составленное из элементов множества A. Тогда с вероятностью больше $1 - \delta$ множество B является ε-копией для A.

Понятно, откуда возникло требование $m \leqslant |A|$. Формально без него просто нельзя было бы говорить о случайном m-сочетании в A. В теореме 6.3.5.1 такого требования не было, так как размещения с повторениями вполне могут иметь куда больший размер, чем то множество, из которого мы их «добываем».

§ 6.4. Несколько слов о математической статистике

Скажем пару слов о приложении идей Вапника и Червоненкиса к задачам статистики и теории вероятностей. Собственно, именно оттуда первоначально и возникла работа, благодаря которой впоследствии появилось понятие размерности. В самой этой работе слова «размерность» нет.

По большому счету, все крутится около одного из центральных законов теории вероятностей — закона больших чисел (ЗБЧ). В самой классической и понятной своей форме он восходит к Бернулли и касается именно той схемы вероятностных испытаний, которая носит имя этого замечательного математика. У нас такая схема встречалась в пункте 6.3.2, и смысл ее исключительно прост: мы n раз осуществляем "независимые испытания"(скажем, бросаем монетку); в каждом испытании происходит либо успех (событие A), либо неудача (событие $\overline{A}$); вероятность успеха p, неудачи — $q = 1 - p$. Пусть μ_n — число успехов в схеме из n испытаний. Это случайная величина. ЗБЧ гласит, что каково бы ни было $\varepsilon > 0$,

$$P\left(\left|\frac{\mu_n}{n} - p\right| > \varepsilon\right) \to 0, \quad n \to \infty.$$

Говоря словами, вероятность того, что среднее число успехов уклонится от вероятности отдельного успеха больше, нежели на сколь угодно малую

наперед заданную величину, с ростом числа испытаний пренебрежимо мала. Это своего рода основополагающий математический закон природы, который не составляет труда строго доказать (см. [8, 35, 37]).

Желая обобщить бернуллиевский вариант ЗБЧ, уточнить или усилить его, следует сперва записать μ_n в виде суммы более простых случайных величин — *индикаторных*. Действительно,

$$\mu_n = \xi_1 + \ldots + \xi_n,$$

где ξ_i — единица или ноль, смотря по тому, случилось в i-м испытании событие A или не случилось. Величину ξ_i называют *индикатором* события A. В новых обозначениях

$$P\left(\left|\frac{\xi_1 + \ldots + \xi_n}{n} - p\right| > \varepsilon\right) \to 0, \quad n \to \infty.$$

Если еще учесть, что $p = M\xi_i$ для любого i, то

$$P\left(\left|\frac{\xi_1 + \ldots + \xi_n}{n} - M\xi_1\right| > \varepsilon\right) =$$
$$= P\left(\left|\frac{\xi_1 + \ldots + \xi_n}{n} - M\left(\frac{\xi_1 + \ldots + \xi_n}{n}\right)\right| > \varepsilon\right) \to 0, \quad n \to \infty.$$

С одной стороны, естественны обобщения, когда вместо последовательности индикаторов берется последовательность произвольных случайных величин. Например, ЗБЧ справедлив, коль скоро $\xi_1, \ldots, \xi_n, \ldots$ — независимые одинаково распределенные случайные величины с конечным вторым моментом (см. [8, 35, 37]).

С другой стороны, усилению подлежит сам вид сходимости среднего к математическому ожиданию. Усиленный ЗБЧ (УЗБЧ) при определенных условиях говорит о том, что

$$P\left(\left|\frac{\xi_1 + \ldots + \xi_n}{n} - M\left(\frac{\xi_1 + \ldots + \xi_n}{n}\right)\right| \to 0\right) = 1.$$

Это гораздо более мощное увтверждение. Для схемы Бернулли оно справедливо, но верно оно и, скажем, при условии, что случайные величины независимы, одинаково распределены и имеют конечный первый момент (см. [8, 35, 37]).

Однако есть и еще одно направление исследований, крайне важное для статистических приложений. Давайте рассмотрим УЗБЧ в форме Бернулли. Его можно переписать следующим образом. Пусть $A_1, \ldots, A_n, \ldots$ — последовательность независимых событий, имеющих одну и ту же вероятность $P(A_1) = p$. Пусть I_{A_i} — индикатор события A_i. Тогда

$$P\left(\left|\frac{I_{A_1} + \ldots + I_{A_n}}{n} - p\right| \to 0\right) = 1, \quad n \to \infty.$$

Ну, это уже очевидно. Зачастую же необходимо, чтобы аналогичная сходимость имела место равномерно по целой совокупности последовательностей независимых равновероятных событий. А именно пусть даны последовательности $\{A_n^x\}$, где $x \in \mathcal{X} \subseteq \mathbb{R}$ и $P(A_n^x) = p^x$. Спрашивается, верно ли, что

$$P\left(\sup_{x\in\mathcal{X}}\left|\frac{I_{A_1^x}+\ldots+I_{A_n^x}}{n} - p^x\right| \to 0\right) = 1, \quad n \to \infty?$$

Ясно, что такого рода задача значительное труднее исходной. При этом смысл очень простой. Мы как бы наблюдаем одновременно за несколькими схемами испытаний Бернулли и хотим, чтобы средние количества успехов в них сходились к вероятности успеха не по отдельности, но равномерно.

Так вот оказывается, что размерность Вапника—Червоненкиса в аккурат отвечает за решение последней задачи. Пусть все события A_n^x «живут» на некотором пространстве Ω. Тогда, по Вапнику и Червоненкису: если $VC(\Omega, \{A_n^x\}_{x\in X}) < \infty$ для любого n, то равномерная сходимость в бернуллиевском варианте УЗБЧ есть. Иными словами, опять конечность размерности влечет искомый результат.

В чем состоит предмет статистики? Есть *выборка* — совокупность некоторых чисел $x_1, \ldots, x_n$. Например, мы в течение месяца каждый день в 15:00 записываем температуру воздуха за окном или курс доллара в ближайшем обменнике. Нам хочется понять закономерность, которая стоит за появлением чисел $x_1, \ldots, x_n$. Мы верим, что каждое из этих чисел есть реализация некоторой случайной величины, т.е. $x_i = \xi_i(\omega)$, где $\omega \in \Omega$. Для простоты обычно предполагают, что ξ_i одинаково распределены и независимы. В идеале, нам нужно по выборке воссоздать *функцию распределения* F_{ξ_i} каждой из наших величин (см. [8, 35, 37]). Наиболее разумный путь сделать это — рассмотреть *эмпирическую функцию распределения* (*э. ф. р.*)

$$\hat{F}_n(x_1, \ldots, x_n; x) = \frac{1}{n}\sum_{i=1}^{n} I_{\{x_i \leqslant x\}}.$$

Наглядно очевидно, почему э. ф. р. аппроксимирует неизвестную нам функцию F_{ξ_i}. Более того, есть ряд глубоких математических фактов, которые свидетельствуют об исключительных качествах э. ф. р. Подробности можно найти в любой хорошей книге по математической статистике (см., например, [2, 17, 32]). Для нас же актуален сейчас лишь один классический факт — теорема Гливенко—Кантелли. Эта теорема

утверждает, что

$$P\Big(\sup_{x\in\mathbb{R}}|F_{\xi_1}(x)-\hat{F}_n(\xi_1,\ldots,\xi_n;x)|\to 0\Big)=1.$$

Ничего не напоминает? А ведь крайне похоже на равномерную сходимость в УЗБЧ! Так и есть. Достаточно взять $\mathcal{X}=\mathbb{R}$, $A_n^x=\{\xi_n\leqslant x\}$. Тогда

$$F_{\xi_1}(x)=P(\xi_1\leqslant x)=P(A_n^x)=p^x,$$

а э. ф. р. и без перезаписей есть среднее от индикаторов. При этом конечность размерности Вапника—Червоненкиса для пространства $(\mathbb{R}, \{(-\infty, x]\})$ нам давно известна. Стало быть, теорема Гливенко—Кантелли есть тривиальный частный случай общего результата Вапника—Червоненкиса.

Задачи

19. Уточните оценку $s\leqslant C_n^{[\varepsilon n]+1}$ из §6.1.

20. Приведите пример счетной совокупности $\mathfrak{R}$ ограниченных множеств на плоскости, для которой $VC(\mathbb{R}^2,\mathfrak{R})=\infty$.

21. Найдите размерность Вапника—Червоненкиса совокупности множеств, изображенной на рис. 9.

22*. Что можно сказать о размерности Вапника—Червоненкиса пространства $(\mathbb{R}^d, B_h)$, где B_h — совокупность всех открытых шаров радиуса h в $\mathbb{R}^d$?

23. Принципиально ли требование открытости каждого треугольника в §6.1?

24. В утверждении 6.2.1.1 фигурирует функция $g(n, d)$. Нельзя ли заменить ее биномиальным коэффициентом C_n^d?

25. Докажите теорему 6.2.3.2.

26. Докажите теорему 6.3.5.1.

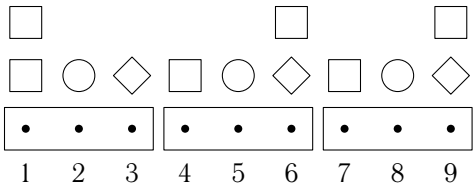

Рис. 9

Глава 7

Системы общих представителей в геометрии: раскраски пространств и разбиения множеств

В этой главе мы расскажем об одном из наиболее ярких применений технологии с. о. п. Речь пойдет о классических проблемах комбинаторной геометрии — о проблеме Борсука, проблеме Нелсона—Эрдёша—Хадвигера и проблеме Грюнбаума.

§ 7.1. Краткий экскурс в комбинаторную геометрию: проблемы Борсука и Нелсона—Эрдёша—Хадвигера

Ниже мы расскажем о двух классических проблемах комбинаторной геометрии, некоторые аспекты которых наиболее эффективно исследуются с помощью методов задачи о системах общих представителей.

Начнем с постановки проблемы Нелсона—Эрдёша—Хадвигера. Представим себе, что нам требуется так покрасить все точки обычной плоскости в несколько цветов, чтобы между точками одного цвета не было расстояния 1. Спрашивается, насколько экономно это можно сделать? Иными словами, много ли понадобится цветов для осуществления указанной раскраски? Как ни удивительно, но задача эта крайне трудна, и окончательный ответ в ней до сих пор не получен. Известно лишь, что трех цветов заведомо не хватит, а вот семицветной «палитры» будет уже вполне достаточно.

Описанная задача легко переносится на случай многомерного евклидова пространства $\mathbb{R}^n$. Строго говоря, всякий раз нас интересует минимальное количество цветов $\chi(\mathbb{R}^n)$, в которые можно так покрасить все точки пространства, чтобы точки, отстоящие друг от друга на расстояние 1, были непременно разноцветными. Если писать еще более формально, то

$$\chi(\mathbb{R}^n) = \\ = \min\bigl\{\chi\colon \mathbb{R}^n = V_1 \sqcup \ldots \sqcup V_\chi,\ \forall i \in \{1, \ldots, \chi\} \forall \mathbf{x}, \mathbf{y} \in V_i\ |\mathbf{x} - \mathbf{y}| \neq 1\bigr\}.$$

Таким образом, искомая раскраска — это, по сути, разбиение пространства на куски, в каждом из которых не реализуется расстояние 1. Заметим, что, вообще-то, «запрещенное расстояние» 1 (мы *запрещаем*

точкам одного цвета отстоять друг от друга на это расстояние) выбрано вполне произвольно, для красоты слога. Если бы мы с самого начала рассуждали не о нем, а, скажем, о расстоянии $e = 2{,}71\ldots$ или о расстоянии $\sqrt{2}^{\sqrt{3}}$, то ввиду гомотетичности пространства $\mathbb{R}^n$ самому себе мы пришли бы в точности к тому же определению: имея раскраску с запретом расстояния 1, «раздуем» ее или «сожмем» в надлежащее число раз, вот и будет раскраска с заданным наперед запретом типа e и пр. В дальнейшем это замечание нам пригодится.

Величина $\chi(\mathbb{R}^n)$ называется *хроматическим числом пространства*. И в недавних, и в более старых источниках — статьях, книгах — о ней говорится немало. Поэтому мы не станем вдаваться в детали ее — безусловно, интригующей — истории, отсылая читателя к соответствующим ресурсам: см., например, [22, 23, 27, 28, 33, 49, 53, 56]. Здесь мы обсудим лишь те аспекты проблематики, к которым впоследствии мы и станем применять технологию с. о. п., разработанную в предшествующих главах.

Собственно говоря, мы отметим следующие факты. Прежде всего, как мы уже говорили однажды,

$$4 \leqslant \chi(\mathbb{R}^2) \leqslant 7$$

(см. [23, 33]), и очевидно, что $\chi(\mathbb{R}^1) = 2$. А как ведет себя хроматическое число при $n \to \infty$? На данный момент самые лучшие оценки имеют вид

$$(1{,}239\ldots + o(1))^n \leqslant \chi(\mathbb{R}^n) \leqslant (3 + o(1))^n$$

(см. [22, 27, 28]). Принципиально, стало быть, понятно, что хроматическое число пространства растет экспоненциально; устранение же зазора между константами $1{,}239\ldots$ и 3 — задача не менее трудная, нежели задача отыскания величины $\chi(\mathbb{R}^2)$.

Довольно легко осознать общую идею доказательства нижних оценок хроматического числа. Берем в пространстве конечное множество точек V и фиксируем любое $a > 0$. Если уже V нельзя раскрасить в χ цветов с запретом расстояния a, то тем более нам не удастся осуществить аналогичную раскраску всего $\mathbb{R}^n$. Значит, $\chi(\mathbb{R}^n) > \chi$, и вся недолга. Искусство состоит в построении «хороших» конфигураций $V \subset \mathbb{R}^n$. Заметим, что на самом деле речь здесь идет о *хроматических числах графов* (см. [23, 40] и § 9.1), где в роли графа выступает либо граф $\mathfrak{G}_{n,a} = (\mathbb{R}^n, \mathrm{E}_{n,a})$, у которого

$$\mathrm{E}_{n,a} = \{(\mathbf{x}, \mathbf{y}) \colon |\mathbf{x} - \mathbf{y}| = a\},$$

либо граф $G = (V, E)$, у которого $V \subset \mathbb{R}^n$, $E \subset \mathrm{E}_{n,a}$. Ведь и впрямь

$$\chi(\mathbb{R}^n) = \chi(\mathfrak{G}_{n,a}) \geqslant \chi(G),$$

так что упомянутое выше искусство на «продвинутом» языке теории графов — это искусство вылавливания графов в пространстве, имеющих большое хроматическое число χ. Другое дело, что для наших целей хватит и интуитивного понимания сути происходящего; а знание основ теории графов вовсе не обязательно.

Главное же — это то, что одни из лучших (в описанном выше смысле) конфигураций устроены крайне просто: в качестве V берутся множества n-мерных векторов с координатами 0 и 1. Иными словами, рассмотрение совокупностей векторов $V \subseteq \{0, 1\}^n$ уже ведет к получению весьма сильных оценок хроматического числа пространства. Например, если взять

$$V = \left\{\mathbf{x} = (x_1, \ldots, x_n) \in \{0, 1\}^n : x_1 + \ldots + x_n = \frac{n}{2}\right\}, \quad n = 4k, \quad a = \sqrt{\frac{n}{2}},$$

то красивая алгебраическая технология позволит показать, что $\chi(\mathbb{R}^n) \geqslant \geqslant (1{,}139\ldots + o(1))^n$, и это близко к наилучшей известной оценке (см. [22, 27]).

Вывод такой. Помимо всего прочего, интересно поставить и решить аналог задачи Нелсона—Эрдёша—Хадвигера в частном случае совокупностей $(0, 1)$-векторов в $\mathbb{R}^n$. Эту задачу мы сформулируем в следующем параграфе, а пока перейдем к проблеме Борсука.

Упомянутая проблема была поставлена К. Борсуком в 1933 г. Вернее, Борсук задал вопрос, можно ли произвольное ограниченное множество Ω в пространстве $\mathbb{R}^n$ разбить на $n + 1$ часть меньшего диаметра? Напомним, что *диаметр* множества Ω — это величина

$$\operatorname{diam}\Omega = \sup_{\mathbf{x},\mathbf{y}\in\Omega} |\mathbf{x} - \mathbf{y}|.$$

Конечно, если диаметр самого Ω равен нулю (т. е. $|\Omega| = 1$), то ответ на вопрос Борсука отрицателен; поэтому для пущей аккуратности стоило бы с самого начала оговориться: множество Ω, которое мы будем пытаться разбивать на части, «неодноточечное»; просто, сделай мы это сразу, это бы странно прозвучало; теперь же все ясно.

Заметим, что разбивать множества или же раскрашивать их — разницы нет. В этом ключе задача Борсука очень похожа на задачу Нелсона—Эрдёша—Хадвигера. Если раньше мы красили (разбивали) целое пространство, то отныне нас интересуют раскраски (разбиения) всевозможных его подмножеств. И априори даже трудно понять, что сложнее: работать с одним, но бесконечным объектом или с массой объектов, каждый из которых, однако, ограничен.

В связи с проблемой Борсука разумно ввести величину, аналогичную хроматическому числу пространства. А именно, положим сперва

$$f(\Omega) = \min\left\{f : \Omega = \Omega_1 \sqcup \ldots \sqcup \Omega_f,\ \forall i \in \{1, \ldots, f\}\ \operatorname{diam}\Omega_i < \operatorname{diam}\Omega\right\}.$$

Например, если Ω — круг на плоскости, то $f(\Omega) = 3$, а если Ω — квадрат, то $f(\Omega) = 2$. Рассмотрим, далее,

$$f(n) = \max_{\Omega} f(\Omega).$$

Это и будет в некотором смысле «борсуковским» аналогом для $\chi(\mathbb{R}^n)$.

В новых терминах вопрос Борсука можно сформулировать так: верно ли, что $f(n) = n + 1$? История, связанная с этим вопросом, еще более интригующая, нежели история проблемы Нелсона—Эрдёша—Хадвигера. Тем более неудивителен тот факт, что о ней также очень много говорилось. Поэтому, как и в ситуации с хроматическим числом, мы отошлем читателя к разнообразным книгам и популярным обзорам по теме (см. [1, 22, 25–28, 45, 47, 57]), а здесь скажем лишь несколько слов, которые наиболее точно будут соответствовать сути нашего дальнейшего исследования с применением свойств с. о. п.

Переводя вопрос Борсука на язык величины $f(n)$, мы были, вообще-то, не вполне честны, ведь корректнее было бы спросить: правда ли, что $f(n) \leqslant n + 1$? В действительности обман невелик, ибо ясно, что $f(n) \geqslant n + 1$. Дабы убедиться в истинности последнего утверждения, достаточно рассмотреть правильный симплекс S в $\mathbb{R}^n$ (см. п. 6.2.1): из принципа Дирихле мгновенно следует соотношение $f(S) = n + 1$.

Долгое время большинство комбинаторных геометров свято верило в то, что ответ на вопрос Борсука должен быть положительным. Даже принялись говорить уже не о вопросе, а о гипотезе Борсука. Что называется, не помогла Борсуку его осторожность. Поначалу все складывалось в пользу гипотезы, и довольно быстро стало известно, что и впрямь $f(n) = n + 1$, коль скоро $n \leqslant 3$. Однако с ростом размерности все становилось куда менее радужно. Наконец, в 1993 г. случилось то, чего следовало ожидать: гипотезу опровергли (см. [25]). Сейчас мы знаем, что

$$(1{,}225\ldots + o(1))^{\sqrt{n}} \leqslant f(n) \leqslant (1{,}224\ldots + o(1))^n,$$

и да не смутит читателя наличие кажущегося противоречия между нижней и верхней оценками (странно же: $1{,}225 > 1{,}224$!): главное — сразу заметить, что в первой из них константа возводится в степень $\sqrt{n}$, а во второй — в степень n (см. [22, 27]). Это все, разумеется, шутки. Если по-серьезному, то видно, с каким треском провалилась гипотеза. Рассчитывали на линейный рост, а получили сверхполиномиальный. Отметим на всякий случай, что величины $o(1)$ в оценках разные; конкретизировать их можно, но большого смысла это не имеет. Однако если все же написать неравенства поаккуратнее, то окажется, что гипотеза Борсука неверна начиная с размерности 298. И любопытно, что пока никто так и не знает, что происходит при $n \in [4, 297]$.

В рамках данного повествования принципиально то, что практически все контрпримеры к гипотезе Борсука основаны на построении совокупностей все тех же векторов с координатами 0 и 1. Стало быть, как и в случае с хроматическим числом, задача о разбиении именно таких совокупностей на части меньшего диаметра крайне важна. В следующем параграфе мы поставим ее, а потом с помощью с. о. п. частично ее решим.

§ 7.2. Проблемы Борсука и Нелсона—Эрдёша—Хадвигера для совокупностей (0, 1)-векторов: постановки задач и обзор основных результатов

Рассмотрим в пространстве $\mathbb{R}^n$ множество векторов

$$\mathcal{V}_{n,k} = \{\mathbf{x} = (x_1, \ldots, x_n)\colon x_i \in \{0, 1\}\ \forall i \in \{1, \ldots, n\},\ x_1 + \ldots + x_n = k\}.$$

Здесь $1 \leqslant k \leqslant n-1$, так что $\mathcal{V}_{n,k}$ состоит из всех (0, 1)-векторов, у которых сумма координат равна данному числу k. Понятно, что $|\mathcal{V}_{n,k}| = C_n^k$. Пусть a — произвольное положительное число. Положим

$$\chi(n, k, a) =$$
$$= \min\{\chi\colon \mathcal{V}_{n,k} = V^1 \sqcup \ldots \sqcup V^\chi,\ \forall i \in \{1, \ldots, \chi\}\ \forall \mathbf{x}, \mathbf{y} \in V^i\ |\mathbf{x} - \mathbf{y}| \neq a\}.$$

Иначе говоря, мы от общей задачи Нелсона—Эрдёша—Хадвигера перешли к ее частному случаю, когда раскраске с некоторым запрещенным расстоянием подвергается не все пространство, но лишь его подмножество $\mathcal{V}_{n,k}$. Отметим, что при $n = 4t$, $k = 2t$, $a = \sqrt{k}$ мы попадаем в рамки ситуации, описанной в предыдущем параграфе. Там утверждалось фактически, что $\chi(n, k, a) \geqslant (1{,}139\ldots + o(1))^n$. А каковы верхние оценки? Этот вопрос (при произвольных n, k, a) мы и будем изучать в дальнейшем.

Теперь по аналогии с числом Борсука $f(n)$ введем величину

$$f(n, k, a) =$$
$$= \max_{\Omega} \min\{f\colon \Omega = \Omega_1 \sqcup \ldots \sqcup \Omega_f,\ \forall\, i \in \{1, \ldots, f\}\ \operatorname{diam}\Omega_i < a\}.$$

Здесь максимум берется по всем множествам $\Omega \subset \mathcal{V}_{n,k}$, имеющим диаметр a. Впоследствии мы опять обсудим верхние оценки функции $f(n, k, a)$ при различных значениях ее аргументов.

Прежде всего заметим, что всегда, с очевидностью,

$$f(n, k, a) \leqslant \chi(n, k, a).$$

Далее, нетрудно видеть, что есть значения параметров n, k, a, при которых задача отыскания соответствующих величин становится либо тривиальной, либо просто бессмысленной. Перечислим ряд подобных ситуаций.

1. Пусть a не имеет вид $a=\sqrt{b}$, где b — целое число. Тогда, поскольку $|\mathbf{x}-\mathbf{y}|^2\in\mathbb{Z}$ для любых $\mathbf{x},\mathbf{y}\in\mathcal{V}_{n,k}$, имеем $\chi(n,k,a)=1$: запрещенному расстоянию просто не на чем достигаться, и можно смело красить все элементы множества $\mathcal{V}_{n,k}$ в один и тот же цвет. Что же касается величины $f(n,k,a)$, то она и вовсе толком не определена, ведь максимум в ее определении берется фактически по пустому множеству.

2. Ясно, что $(\operatorname{diam}\mathcal{V}_{n,k})^2=2k$ при $k\leqslant\frac{n}{2}$ и $(\operatorname{diam}\mathcal{V}_{n,k})^2=2n-2k$ при $k\geqslant\frac{n}{2}$ (см. рис. 10). Таким образом, если a^2 не попадает в интервал от единицы до $2k$ или $2n-2k$ (в зависимости от соотношения между k и $\frac{n}{2}$), то говорить не о чем.

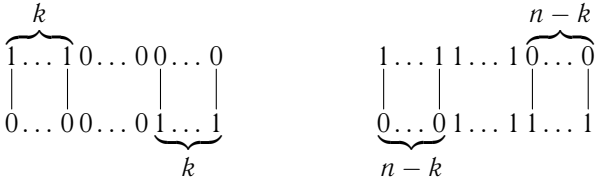

Рис. 10

3. Пусть $a=\sqrt{2b+1}$, $b\in\mathbb{Z}$. Тогда $\chi(n,k,a)=1$. Здесь ситуация такая же, как и в п. 1. Просто квадрат расстояния между любыми двумя векторами из $\mathcal{V}_{n,k}$, очевидно, четен.

Теперь поговорим о более продвинутых результатах. При $n\leqslant 9$ Г. М. Циглер, его ученики и несколько других замечательных математиков получили ряд точных значений для величин $\chi(n,k,a)$ и $f(n,k,a)$; кроме того, они установили весьма аккуратные оценки этих величин в ряде других ситуаций. В частности, из их результатов вытекает справедливость гипотезы Борсука для совокупностей n-мерных $(0,1)$-векторов при $n\leqslant 9$. Техника, которую применяли Циглер и др., далеко выходит за рамки этой книги. Она относится к теории кодирования и лишь отдаленно напоминает технику с. о. п. Поэтому, как ни любопытны методы Циглера и его окружения, здесь мы о них говорить не станем. Заинтересованный же читатель может обратиться к первоисточнику [60] и к книге [27].

Перейдем, наконец, к формулировкам теорем, утверждения которых доказываются за счет свойств с. о. п. Заметим сразу, что в большинстве ситуаций эти теоремы дают наилучшие известные результаты в задаче.

Теорема 7.2.1. *Пусть фиксированы нетривиальные n,k,a. Положим*

$$l=k-\frac{a^2}{2}+1,\quad \bar{n}=C_n^l,\quad \bar{s}=C_n^k,\quad \bar{k}=C_k^l.$$

Тогда

$$f(n, k, a) \leqslant \chi(n, k, a) \leqslant G(\bar{n}, \bar{s}, \bar{k}),$$

где $G(\cdot, \cdot, \cdot)$ *— функция из теоремы* 3.1.

Читателя не должно смущать то, что мы свободно делим a^2 на 2, ведь для нечетных a^2 все просто (см. «ситуацию» 3).

Теорема 7.2.2. *Пусть фиксированы нетривиальные* n, k, a. *Положим*

$$l = k - \frac{a^2}{2}, \quad m = k + \frac{a^2}{2}.$$

Тогда

$$f(n, k, a) \leqslant n \min\left\{C_k^l, C_{n-k}^{m-k}\right\}.$$

Если в теореме 7.2.1 наличие с. о. п. бросается в глаза, то в теореме 7.2.2 оно явно не наблюдается. Тем не менее, в обоих случаях, как и обещано, к помощи с. о. п. мы прибегнем. Отметим, кстати, что принципиальная разница между двумя теоремами состоит в том, что первая из них универсальна (применима и к проблеме Борсука, и к задаче о хроматическом числе), а вторая специфична (направлена исключительно на проблему Борсука). В этом есть некий глубокий смысл.

В § 7.3 мы докажем теоремы, сформулированные выше. Сперва для пущей ясности изложения мы на простом примере опишем общую идею подхода (п. 7.3.1); затем перейдем к обсуждению теоремы 7.2.1 (п. 7.3.2); и, наконец, обоснуем утверждения теоремы 7.2.2 (п. 7.3.3).

Еще раз подчеркнем, что во многих случаях теоремы 7.2.1, 7.2.2 самые сильные на данный момент. Однако иногда и на них есть «управа». Об этом мы поговорим в § 7.4.

§ 7.3. Доказательства теорем из § 7.2

Ниже мы приведем доказательства теорем 7.2.1, 7.2.2. Чтобы сделать наши рассуждения более прозрачными и мотивированными, обсудим сперва их основные идеи.

7.3.1. Идеи доказательств

Откуда же берутся системы общих представителей в задачах, которые мы только что сформулировали? Рассмотрим простой модельный пример.

Пусть в определении совокупности векторов $\mathcal{V}_{n,k}$ дано $n = 20$, $k = 5$. Положим $a = \sqrt{10}$. Спрашивается: как оценить сверху $f(\Omega)$ (см. § 7.1), если $\Omega \subset \mathcal{V}_{n,k}$, $|\Omega| = 20$ и $\operatorname{diam}\Omega = a$?

Поскольку в нашем случае $\operatorname{diam}\mathcal{V}_{n,k} = a$, последнее условие, наложенное нами на множество Ω, не слишком ограничительно. Достаточно взять любую совокупность векторов из $\mathcal{V}_{n,k}$, в которой *множества единичных координат* каких-либо двух элементов *не пересекаются*. С одной стороны, такая свобода играет против нас: ведь трудно, кажется, придумать единый подход к столь разнообразным ситуациям. А с другой стороны, мы не зря выделили курсивом выражение «множества единичных координат». Что-то подсказывает нам, что именно для таких множеств (вернее, для совокупностей таких множеств) нам придется строить с. о. п. или нечто вроде того.

Действительно, пусть $\Omega = \{\mathbf{x}_1, \ldots, \mathbf{x}_{20}\}$, причем в координатах

$$\mathbf{x}_i = (x_i^1, \ldots, x_i^n), \quad x_i^j \in \{0, 1\}, \quad \forall i \in \{1, \ldots, 20\}, \quad j \in \{1, \ldots, n\}.$$

Рассмотрим множество $\mathcal{R}_n$ (знакомое обозначение, см. гл. 2) и положим

$$M_i = \{\nu \in \mathcal{R}_n \colon x_i^\nu = 1\}, \quad i \in \{1, \ldots, 20\}.$$

Иными словами, каждому вектору $\mathbf{x}_i \in \Omega$ мы сопоставляем множество $M_i \subset \mathcal{R}_n$ его ненулевых координатных позиций. Получается совокупность множеств $\mathcal{M}$, в известном смысле однозначно отвечающая Ω.

Предположим, что $S = \{\nu_1, \ldots, \nu_\tau\}$ — любая минимальная с. о. п. для $\mathcal{M}$; $\tau = \tau(\mathcal{M})$. Тогда ясно, что

$$\mathcal{M} = \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_\tau,$$

где

$$\mathcal{M}_i = \{M \in \mathcal{M} \colon \nu_i \in M\}, \quad i \in \{1, \ldots, \tau\}.$$

Соответственно,

$$\Omega = \Omega_1 \cup \ldots \cup \Omega_\tau.$$

Здесь, очевидно,

$$\Omega_j = \{\mathbf{x}_i \in \Omega \colon M_i \in \mathcal{M}_j\}, \quad j \in \{1, \ldots, \tau\}.$$

Более того, понятно, что, каково бы ни было Ω_j и каковы бы ни были векторы $\mathbf{x}, \mathbf{y} \in \Omega_j$, расстояние между ними не превосходит $\sqrt{8}$ (см. рис. 11), т. е. $\operatorname{diam}\Omega_j < \operatorname{diam}\Omega$ для любого j. Перейти от покрытия $\Omega = \Omega_1 \cup \ldots \cup \Omega_\tau$ к разбиению $\Omega = \Omega_1' \sqcup \ldots \sqcup \Omega_\tau'$ труда не составляет, и, стало быть, $f(\Omega) \leqslant \tau$. Оценки же для τ у нас есть, и все в порядке. Например, можно утверждать, что

$$f(\Omega) \leqslant G(20, 20, 5) = 4\ln 5 + 5 \approx 11.$$

Не всегда, конечно, все так просто. Сейчас мы сделаем еще один шаг на пути к пониманию основных пружин будущих доказательств теорем 7.2.1, 7.2.2. А именно, предположим, что мы находимся в такой

$$\begin{array}{cccccccccccc} \overbrace{1\ 1}^{2} & \boxed{1\ 1\ 1} & 0 & 0 & 0 & \ldots & 0 \\ 0\ 0 & \boxed{1\ 1\ 1} & \underbrace{1\ 1} & 0 & \ldots & 0 \end{array}$$

Рис. 11

ситуации: $n = 10$, $k = 5$, $a = \sqrt{8}$, $\Omega \subset \mathcal{V}_{n,k}$, $\operatorname{diam}\Omega = a$. Что теперь делать, коль скоро наша цель по-прежнему состоит в отыскании верхней оценки величины $f(\Omega)$?

Очевидно, что векторы из Ω «диаметрально противоположны» (т. е. на них реализуется диаметр Ω) тогда и только тогда, когда соответствующие множества их ненулевых координатных позиций пересекаются ровно по одному элементу (см. рис. 12). Значит, нам достаточно покрыть Ω такими множествами $\Omega_1, \ldots, \Omega_r$ с некоторым (по возможности меньшим) r, чтобы каждая из отвечающих им совокупностей $\mathcal{M}_1, \ldots, \mathcal{M}_r$ подмножеств $\mathcal{R}_n$ не содержала пары множеств M, M', удовлетворяющих условию $|M \cap M'| = 1$. Поскольку в нашем случае заведомо $M \cap M' \neq \varnothing$ (иначе на векторах из Ω достигалось бы расстояние $\sqrt{10}$), последнее условие равносильно требованию $|M \cap M'| \geqslant 2$.

$$\begin{array}{cccccccccccc} \overbrace{1\ 1\ 1\ 1}^{4} & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \ldots & 0 \\ 0\ 0\ 0\ 0 & \boxed{1} & \underbrace{1\ 1\ 1\ 1}_{4} & 0 & \ldots & 0 \end{array}$$

Рис. 12

Рассмотрим задачу отыскания величины $m = m(10, 2, 5)$, являющуюся частным случаем одной из проблем Турана (см. гл. 5). Пусть $\mathcal{S} = \{K_1, \ldots, K_m\}$ есть произвольная система «двоек» (т. е. $|K_i| = 2$ для любого $i \in \{1, \ldots, m\}$), покрывающая совокупность $\mathcal{L} = \{L_1, \ldots, L_{C_{10}^5}\}$, которая состоит из всех пятиэлементных подмножеств десятиэлементного множества. Если $\mathcal{M}$ — это набор множеств, отвечающий нашему Ω, то, разумеется, он тем более покрыт системой $\mathcal{S}$. Значит, имеет место представление

$$\mathcal{M} = \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_m,$$

где

$$\mathcal{M}_i = \{M \in \mathcal{M} \colon K_i \subset M\}, \quad i \in \{1, \ldots, m\}.$$

Очевидно, любые два множества из какого бы то ни было $\mathcal{M}_i$ пересекаются не менее чем по двум общим элементам. Стало быть, искомое разложение $\mathcal{M}$ (а вместе с ним, конечно, и надлежащее разложение множества Ω) найдено, т. е. $f(\Omega) \leqslant m$. Остается воспользоваться хотя бы теоремой 5.2.5 и получить, тем самым, неравенство

$$f(\Omega) \leqslant G(45, 252, 10) \approx 24.$$

Последнее неравенство можно по-разному уточнять, но сейчас для нас важнее всего то, что технология с. о. п. и их обобщений естественным образом применима к проблеме Борсука. Можем приступать к доказательствам теорем 7.2.1, 7.2.2.

7.3.2. Доказательство теоремы 7.2.1

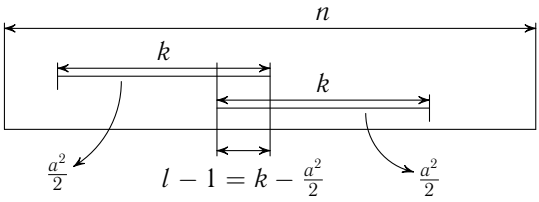

Рис. 13

С высоты наших теперешних знаний все представляется почти тривиальным. В самом деле, нам необходимо так раскрасить $\mathcal{V}_{n,k}$, чтобы точки, расстояние между которыми равно a, были разноцветными. Иными словами, если перейти от $\mathcal{V}_{n,k}$ к совокупности $\mathcal{M}$, состоящей из всех k-элементных подмножеств $\mathcal{R}_n$ (так же, как это делалось в п. 7.3.1), то задача сведется к представлению $\mathcal{M}$ в виде

$$\mathcal{M} = \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_m,$$

где никакое $\mathcal{M}_i$ не содержит пары множеств, пересекающихся ровно по $l - 1$ элементу (именно такое пересечение множеств отвечает расстоянию a между подходящими векторами из $\mathcal{V}_{n,k}$, см. рис. 13). Проще всего добиться выполнения последнего свойства, заменяя его более сильным требованием: $|M_1 \cap M_2| \geqslant l$ для любых $M_1, M_2 \in \mathcal{M}_i$ и для каждого $i \in \{1, \ldots, m\}$. А вот его-то аналог мы как раз и реализовали однажды. Только тогда у нас были конкретные значения

$$n = 10, \quad k = 5, \quad a = \sqrt{8}, \quad l = 2 = 5 - \frac{8}{2} + 1.$$

Все ясно! Возьмем $m = m(n, l, k)$ и произвольную систему

$$\mathcal{S} = \{L_1, \ldots, L_m\},$$

состоящую из l-элементных подмножеств $\mathcal{R}_n$ и покрывающую $\mathcal{M}$. Положим

$$\mathcal{M}_i = \{M \in \mathcal{M}\colon L_i \subset M\}, \quad i \in \{1, \ldots, m\},$$

и дело в шляпе: искомое разложение $\mathcal{M}$ построено, и в силу теоремы 5.2.5 мы получаем

$$\chi(n, k, a) \leqslant m \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Теорема доказана.

7.3.3. Доказательство теоремы 7.2.2

Тут все несколько тоньше, нежели в предыдущем параграфе, и по ходу дела нам реально придется использовать специфику проблемы Борсука. Ниже мы докажем оценку $f(n, k, a) \leqslant nC_k^l$; оценка $f(n, k, a) \leqslant nC_{n-k}^{m-k}$ доказывается аналогично и потому останется на совести читателя.

Сейчас мы займемся «покрытием», которое до крайности похоже на предъявленное в п. 7.3.2. Тем не менее, как мы уже говорили, здесь есть существенные нюансы. Итак, пусть Ω — произвольное подмножество множества $\mathcal{V}_{n,k}$, имеющее диаметр a. Наша цель — получить оценку $f(\Omega) \leqslant nC_k^l$. Сопоставим множеству Ω совокупность $\mathcal{M}$ по известному правилу. Тогда $\mathcal{M}$ состоит, разумеется, из k-элементых подмножеств множества $\mathcal{R}_n$. Более того, каковы бы ни были $M_1, M_2 \in \mathcal{M}$, выполнено неравенство $|M_1 \cap M_2| \geqslant l$ (иначе диаметр множества Ω был бы больше a). Попытаемся покрыть $\mathcal{M}$ некоторой системой $\mathcal{S}$, образованной l-элементными подмножествами множества $\mathcal{R}_n$ (покрытие мы понимаем в смысле п. 7.3.2). Безусловно, можно взять $\mathcal{S}$, у которого $|\mathcal{S}| = m(n, l, k) \leqslant G(C_n^l, C_n^k, C_k^l)$, но в таком случае мы вряд ли вправе рассчитывать на улучшение результата теоремы 7.2.1. В чем же тонкость? Дело в том, что $\mathcal{M}$ — не абы какая совокупность, а совокупность специфическая: в ней каждые два множества «зацепляются» по не менее чем l общим элементам. Возьмем, стало быть, любое множество $M \in \mathcal{M}$ и рассмотрим совокупность $\mathcal{S} = \{L_1, \ldots, L_{C_k^l}\}$, состоящую из всех возможных l-элементных подмножеств M. Ввиду упомянутой специфики такая совокупность $\mathcal{S}$ покрывает $\mathcal{M}$. Значит, имеет место разложение

$$\mathcal{M} = \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_{C_k^l},$$

где

$$\mathcal{M}_i = \{M \in \mathcal{M}\colon L_i \subset M\}, \quad i \in \{1, \ldots, C_k^l\}.$$

Ну, и чего хорошего? В рамках $\mathcal{M}_i$ ничто, по-видимому, не мешает множествам пересекаться по l элементам, т. е. на данном этапе мы не

сможем транслировать построенное покрытие в покрытие исходного Ω подмножествами меньшего диаметра. Остался маленький трюк.

Зафиксируем произвольную совокупность $\mathcal{M}_i$ и рассмотрим $\mathcal{R}_n \setminus L_i = \{\nu_1, \ldots, \nu_{n-l}\}$. Очевидно,

$$\mathcal{M}_i = \mathcal{M}_{i,1} \cup \ldots \cup \mathcal{M}_{i,n-l},$$

где

$$\mathcal{M}_{i,j} = \{M \in \mathcal{M}_i : \nu_j \in M\}, \quad j \in \{1, \ldots, n-l\}.$$

В каждом наборе $\mathcal{M}_{i,j}$ любые два множества пересекаются по не меньше чем $l+1$ общим элементам, так что, если Ω представлено в виде

$$\Omega = \bigcup_{i=1}^{C_k^l} \bigcup_{j=1}^{n-l} \Omega_{i,j}$$

($\Omega_{i,j}$ стандартным образом соответствует $\mathcal{M}_{i,j}$), то $\operatorname{diam} \Omega_{i,j} < a$, и нужное разбиение у нас в кармане. При этом в нем $(n-l)C_k^l < nC_k^l$ элементов, так что и впрямь $f(\Omega) \leqslant nC_k^l$. Теорема доказана.

§ 7.4. О способах уточнения результатов § 7.2; теорема Эрдёша—Ко—Радо

В этом параграфе мы подробно поговорим о том, как в ряде нетривиальных ситуаций можно уточнять результат теоремы 7.2.1.

Прежде всего условимся считать, что мы по-прежнему работаем в обозначениях п. 7.3.2. Иными словами, нам даны те или иные значения параметров n, k, a, и по ним мы определяем величину l, величины $\bar{n}$, $\bar{s}$, $\bar{k}$, множество векторов $\mathcal{V}_{n,k}$ и отвечающую ему совокупность множеств $\mathcal{M}$.

Давайте для начала поймем, что, по существу, представляет из себя оценка в теореме 7.2.1. Разумеется, эта оценка имеет вид

$$\chi(n, k, a) \leqslant G(\bar{n}, \bar{s}, \bar{k}) = \max\left\{\frac{\bar{n}}{\bar{k}}, \frac{\bar{n}}{\bar{k}} \ln \frac{\bar{s}\bar{k}}{\bar{n}}\right\} + \frac{\bar{n}}{\bar{k}} + 1.$$

Сейчас мы приведем модельный пример, который показывает, что величина $\ln \dfrac{\bar{s}\bar{k}}{\bar{n}}$ зачастую вносит незначительный вклад в асимптотику роста функции G. Действительно, сразу ясно, что при любых n, k, a выполняется неравенство

$$\ln \frac{\bar{s}\bar{k}}{\bar{n}} \leqslant \ln \bar{s} = \ln C_n^k \leqslant k \ln n.$$

Здесь последнее неравенство вытекает из тривиальной оценки $C_n^k \leqslant n^k$. В то же время, допустим, что n делится на 4, и положим $k = \dfrac{n}{2}$, $l = \dfrac{n}{4}$

(понятно, что́ при этом есть a). Тогда

$$\frac{\bar{n}}{\bar{k}} = \frac{C_n^l}{C_k^l} = \frac{n!\left(\frac{n}{4}\right)!}{\left(\frac{3n}{4}\right)!\left(\frac{n}{2}\right)!}.$$

При $t \to \infty$ имеет место классическая формула Стирлинга (см. [39]):

$$t! \sim \sqrt{2\pi t}\left(\frac{t}{e}\right)^t, \quad e = 2{,}71828\ldots$$

Пользуясь этой формулой, получаем

$$\frac{\bar{n}}{\bar{k}} \sim \frac{\sqrt{2\pi n} n^n e^{-n} \sqrt{2\pi\frac{n}{4}}\left(\frac{n}{4}\right)^{\frac{n}{4}} e^{-\frac{n}{4}}}{\sqrt{2\pi\frac{3n}{4}}\left(\frac{3n}{4}\right)^{\frac{3n}{4}} e^{-\frac{3n}{4}} \sqrt{2\pi\frac{n}{2}}\left(\frac{n}{2}\right)^{\frac{n}{2}} e^{-\frac{n}{2}}}.$$

Обозначим через $P(n)$ величину

$$P(n) = \frac{\sqrt{2\pi n}\sqrt{2\pi\frac{n}{4}}}{\sqrt{2\pi\frac{3n}{4}}\sqrt{2\pi\frac{n}{2}}}.$$

Нетрудно видеть, что

$$\frac{\bar{n}}{\bar{k}} \sim P(n)\left(\frac{2^{3/2}}{3^{3/4}}\right)^n = P(n)(1{,}24\ldots)^n.$$

Таким образом, с точностью до полиномиального сомножителя дробь $\frac{\bar{n}}{\bar{k}}$ растет как экспонента, и, стало быть, ее можно записать в виде $(1{,}24\ldots + o(1))^n$.

Вспоминаем, что выражение $\ln\frac{\bar{s}\bar{k}}{\bar{n}}$ оценивалось сверху функцией $k\ln n$, которая сама, очевидно, мажорируется полиномом. Суммируя накопленную информацию, заключаем, что $\frac{\bar{n}}{\bar{k}} = (1{,}24\ldots + o(1))^n$, $\ln\frac{\bar{s}\bar{k}}{\bar{n}} \leqslant Q(n)$, где $Q(n)$ — полином, так что $\frac{\bar{n}}{\bar{k}}\ln\frac{\bar{s}\bar{k}}{\bar{n}} = (1{,}24\ldots + o(1))^n$, и никакого принципиального влияния на вид последней функции логарифмический сомножитель не оказал (весь вклад остался на уровне бесконечно малых величин).

На самом деле пример, который мы только что рассмотрели, далеко не единичен. С таким же успехом мы могли положить $k = [c_1 n]$, $l = [c_2 n]$ с произвольными c_1, c_1 $0 < c_2 < c_1 < 1$. Читателю стоит самостоятельно убедиться в том, что при любых c_1, c_2 функция G асимптотически ведет себя, как $(\gamma(c_1, c_2) + o(1))^n$, где $\gamma(c_1, c_2) > 1$, а логарифм от известной дроби «тонет» в $o(1)$. Короче говоря, если не гнаться за мизерными

поправками, то вполне можно считать, что весьма часто оценка в теореме 7.2.1 определяется отношением $\frac{\bar{n}}{\bar{k}}$.

Теперь вспомним, как, собственно, доказывалась теорема 7.2.1. Очень просто. Мы раскладывали совокупность $\mathcal{M}$ в объединение некоторых совокупностей $\mathcal{M}_i$, $i = 1, \ldots, m$, причем структура каждой совокупности $\mathcal{M}_i$ была совершенно элементарна:

$$\mathcal{M}_i = \{M \in \mathcal{M} \colon M \supset L_i\},$$

где L_i — фиксированное (по определенному правилу) l-элементное подмножество множества $\mathcal{R}_n$. Ясно, что в любом случае $|\mathcal{M}_i| = C_{n-l}^{k-l}$. Поскольку совокупности $\mathcal{M}_i$, $\mathcal{M}_j$ вполне могут пересекаться,

$$C_n^k = |\mathcal{M}| \leqslant |\mathcal{M}_1| + \ldots + |\mathcal{M}_m| = mC_{n-l}^{k-l},$$

т. е. $m \geqslant \frac{C_n^k}{C_{n-l}^{k-l}}$. Иначе говоря, на указанном пути мы не добьемся лучшей оценки величины $\chi(n, k, a)$, нежели оценка вида $\chi(n, k, a) \leqslant \frac{C_n^k}{C_{n-l}^{k-l}}$. Замечательно то, что

$$\frac{C_n^k}{C_{n-l}^{k-l}} = \frac{n!(k-l)!}{(n-l)!k!} = \frac{\bar{n}}{\bar{k}}.$$

Получается, что во многих разумных ситуациях теорема 7.2.1 практически (с точностью до «мелочей») неуточнима, коль скоро мы совсем не меняем стратегии из п. 7.3.2.

Как же быть? Необходимо понять суть пресловутой стратегии. По счастью, эта суть лежит на поверхности. Мы всего лишь добивались того, чтобы в каждом $\mathcal{M}_i$ любые два множества пересекались не менее чем по l общим элементам. Именно с этой целью мы и брали то или иное множество $L_i \subset \mathcal{R}_n$, $|L_i| = l$, после чего «насаживали» на него все возможные $M \in \mathcal{M}$, $|M| = k$. Вот у нас и выходило, что $|\mathcal{M}_i| = C_{n-l}^{k-l}$. Однако чем черт не шутит: а вдруг можно строить гораздо более «жирные» совокупности $\mathcal{M}_i$ совсем по иной технологии, добиваясь, тем не менее, чтобы любые два множества в них надлежащим образом «зацеплялись»? Тогда бы мы вполне смогли рассчитывать на продвижение в задаче.

И правда: «жирные» совокупности встречаются. Вот типичный пример. Пусть n делится на 8, $k = \frac{n}{2}$, $l = \frac{n}{4}$. Ничего не напоминает? Да ведь это практически та же ситуации, что и в начале параграфа! Сейчас мы убедимся в ее показательности. Пока все, что мы умеем, — это строить совокупности $\mathcal{M}_i$ мощности $C_{\frac{3n}{4}}^{\frac{n}{4}}$. Если применить формулу Стирлинга к каждому из факториалов, фигурирующих в известном разложении биномиального коэффициента, то обнаружится, что данный коэффициент равен $(1{,}611\ldots + o(1))^n$.

Рассмотрим другую конструкцию. Пусть

$$\mathcal{M}_i = \Big\{M \subset \mathcal{R}_n\colon |M \cap \mathcal{R}_{\frac{n}{2}}| = \frac{3n}{8}\Big\}.$$

Тогда (формула Стирлинга)

$$|\mathcal{M}_i| = C_{\frac{3n}{8}}^{\frac{3n}{8}} C_{\frac{n}{2}}^{\frac{n}{8}} = \big(C_{\frac{n}{2}}^{\frac{n}{8}}\big)^2 = (1{,}754\ldots + o(1))^n.$$

При этом очевидно, что любые два множества из $\mathcal{M}_i$ зацепляются хотя бы по l элементам. И вся недолгá. Экспонента $(1{,}754\ldots + o(1))^n$ растет куда быстрее, нежели экспонента $(1{,}611\ldots + o(1))^n$.

Таким образом, как раз в классе тех ситуаций, для которых прежний подход заведомо нельзя было использовать в целях усиления теоремы 7.2.1, имеется лазейка, и мы с успехом в нее пролезем.

Для того чтобы сформулировать новый результат во всей полноте, необходимо, однако, понять, как же все-таки ведет себя функция

$$h(n, k, l) =$$
$$= \max\big\{|\mathcal{K}|\colon \forall K \in \mathcal{K}\ |K| = k,\ K \subset \mathcal{R}_n \text{ и } \forall K_1, K_2 \in \mathcal{K}\ |K_1 \cap K_2| \geqslant l\big\}.$$

Сейчас у нас есть лишь пара плохо сочетающихся друг с другом фактов типа «$h(n, k, l) \geqslant C_{n-l}^{k-l}$» и «$h(n, n/2, n/4)$ значительно превосходит $C_{3n/4}^{n/4}$».

Еще в 1938 г. П. Эрдёш, Ч. Ко и Р. Радо доказали (а в 1961 г. опубликовали) следующую теорему.

Теорема 7.4.1. *Если* $2k > n$, *то* $h(n, k, 1) = C_n^k$. *Иначе* $h(n, k, 1) = C_{n-1}^{k-1}$.

Первое утверждение теоремы тривиально, второе вполне по зубам школьнику. Мы не будем доказывать теорему, сославшись на книги [46] и [27]. Важный вывод из теоремы таков: бывают случаи, когда оценка $h(n, k, l) \geqslant C_{n-l}^{k-l}$ не улучшаема даже на единицу; например, это так при $l = 1$. Иными словами, при $l = 1$ мы и на новом пути вряд ли уточним теорему 7.2.1.

В действительности Эрдёш, Ко и Радо сформулировали более сильное утверждение. Справедлива (см. [27]) следующая теорема.

Теорема 7.4.2. *Рассмотрим произвольные* k *и* l. *Если* $2k - n \geqslant l$, *то* $h(n, k, l) = C_n^k$. *Иначе существует такое* $n_0 = n_0(k, l)$, *что при всех* $n \geqslant n_0$ *выполнено соотношение* $h(n, k, l) = C_{n-l}^{k-l}$.

Таким образом, если k и l в определенном смысле малы по сравнению с n, то конструкция из теоремы 7.2.1 вновь точна и ни о каком ее усилении речь не идет. Но в нашем-то примере k и l огромны: они лишь в постоянное число раз меньше n. Да и вообще: мы же не знаем, что представляет собой n_0 как функция от своих аргументов. Какова реальная зависимость n_0 от k и l?

Ответ на поставленный вопрос дает следующая теорема П. Франкла и Р. М. Уилсона (см. [27]).

Теорема 7.4.3. *Рассмотрим произвольные k и l. Если $2k-n \geqslant l$, то $h(n, k, l) = C_n^k$. Если $2k-n<l$ и $n \geqslant (k-l+1)(l+1)$, то $h(n, k, l) = C_{n-l}^{k-l}$. Если, наконец, $n<(k-l+1)(l+1)$, то $h(n, k, l) > C_{n-l}^{k-l}$.*

Теорема означает, что в качестве $n_0(k, l)$ в теореме 7.4.2 можно взять $(k-l+1)(l+1)$ и нельзя взять $(k-l+1)(l+1)-1$. Это удивительный по своей точности результат. Теперь картина становится почти ясной. Если $n \geqslant (k-l+1)(l+1)$, мы не вправе рассчитывать на улучшение теоремы 7.2.1; иначе — наоборот: все идет к тому, чтобы теорему 7.2.1 улучшить. Остается лишь понять, насколько величина $h(n, k, l)$ отличается от пресловутого числа сочетаний, коль скоро $n<(k-l+1)(l+1)$. Отметим, что, разумеется, параметры $k=\frac{n}{2}$, $l=\frac{n}{4}$ последнему неравенству удовлетворяют и что, более того, бывают даже значения $k=o(n)$, $l=o(n)$, для которых это неравенство справедливо; случаи же $k=[c_1 n]$, $l=[c_2 n]$ (ср. начало параграфа) все под него подпадают.

Если теорема Франкла—Уилсона была доказана на рубеже 70-х и 80-х годов XX века, то лишь в 1996 г. в проблеме Эрдёша—Ко—Радо была поставлена точка. Р. Алсведе и Л. Хачатрян дали абсолютно исчерпывающее описание величины $h(n, k, l)$. Ниже мы без доказательства приводим их замечательную теорему.

Теорема 7.4.4. *Рассмотрим произвольные k и l. Если $2k-n \geqslant l$, то $h(n, k, l) = C_n^k$. Пусть, напротив, $2k-n<l$. Тогда для каждого i, удовлетворяющего ограничениям $0 \leqslant i \leqslant \frac{n-l}{2}$ и $i \leqslant k-l$, положим*

$$\mathcal{F}_i(n, k, l) = \bigl\{F \subset \mathcal{R}_n \colon |F| = k,\ |F \cap \mathcal{R}_{l+2i}| \geqslant l+i\bigr\}.$$

Если при некотором $r \in \mathbb{N} \cup \{0\}$ выполнено соотношение

$$(k-l+1)\Bigl(2+\frac{l-1}{r+1}\Bigr) \leqslant n < (k-l+1)\Bigl(2+\frac{l-1}{r}\Bigr),$$

то $h(n, k, l) = |\mathcal{F}_r(n, k, l)|$ (мы считаем, что $\frac{l-1}{r} = \infty$, если $r=0$).

Теорема нуждается в комментариях. Прежде всего обсудим вопрос о корректности выбора параметров в ней. Ограничение $i \geqslant 0$ тривиально. Неравенство $i \leqslant \frac{n-l}{2}$ необходимо для того, чтобы выполнялась оценка $l+2i \leqslant n$, гарантирующая нам, что $\mathcal{R}_{l+2i} \subseteq \mathcal{R}_n$. Соотношение $i \leqslant k-l$ формально требуется для доказательства непустоты совокупности $\mathcal{F}_i(n, k, l)$. В самом деле, это соотношение влечет оценку $l+i \leqslant k$, без которой наличие k-элементных подмножеств F в $\mathcal{R}_n$, цепляющих

$\mathcal{R}_{l+2i}$ по не менее чем $l+i$ элементам, невозможно. Вместе с тем это же соотношение вкупе с неравенством $2k-n<l$ (каковым мы, безусловно, располагаем) означает, что $i\leqslant n-k$ и что, стало быть, $k-l-i\leqslant n-l-2i$. Последнее условие обеспечивает существование хотя бы одного такого $F\subset\mathcal{R}_n$, $|F|=k$, что $|F\cap\mathcal{R}_{l+2i}|\geqslant l+i$: на худой конец подойдет любое множество F, которое захватывает в точности $l+i\leqslant k$ элементов из $\mathcal{R}_{l+2i}$; оставшиеся $k-l-i$ элементов заведомо поместятся в множество $\mathcal{R}_n\setminus\mathcal{R}_{l+2i}$, ведь это множество как раз имеет мощность $n-l-2i$.

Далее, понятно, что, каковы бы ни были n, k, l, неотрицательная целая величина r, удовлетворяющая неравенствам из формулировки теоремы, существует и единственна. Если мы еще покажем, что $r\leqslant k-l$ и $r\leqslant\dfrac{n-l}{2}$, то станет окончательно ясна универсальность результата Алсведе—Хачатряна: берем любые n, k, l, однозначно по ним определяем r, которое корректно задает совокупность $\mathcal{F}_r(n,k,l)$, и получаем, что $h(n,k,l)=|\mathcal{F}_r(n,k,l)|$, где последняя величина без труда при желании записывается в виде суммы произведений биномиальных коэффициентов.

Проверим сперва, что $r\leqslant k-l$. Предположим противное. Тогда $r\geqslant k-l+1$. Значит, с учетом условия $2k-n\leqslant l-1$ имеем

$$(k-l+1)\Bigl(2+\frac{l-1}{r}\Bigr)\leqslant 2k-l+1\leqslant n.$$

Противоречие.

Убедимся в том, что $r\leqslant\dfrac{n-l}{2}$. Пусть сперва $2k-n=l-1$. Тогда $\dfrac{n-l}{2}=k-l+\dfrac{1}{2}$. Если $r>\dfrac{n-l}{2}$, то $r\geqslant k-l+1$, и мы возвращаемся к только что изученной ситуации. Пусть, стало быть, $2k-n\leqslant l-2$. Справедлива цепочка импликаций:

$$2k-n\leqslant l-2\ \Rightarrow\ 2k-2l+2\leqslant n-l\ \Rightarrow$$
$$\Rightarrow\ \frac{k-l+1}{n-l}\leqslant\frac{1}{2}\ \Rightarrow\ \frac{(2n-2)(k-l+1)}{n-l}\leqslant n.$$

Если еще предположить, что $r\geqslant\dfrac{n-l}{2}$, то окажется, что

$$(k-l+1)\Bigl(2+\frac{l-1}{r}\Bigr)\leqslant\frac{(2n-2)(k-l+1)}{n-l}\leqslant n,$$

т. е. мы опять получим противоречие, и все в порядке.

Для полного осознания существа теоремы 7.4.4 поглядим на ее частные случаи. Пусть $r=0$. Это означает, что в условиях теоремы $n\geqslant(k-l+1)(l+1)$. В то же время, теорема говорит нам, что

$h(n, k, l) = |\mathcal{F}_0(n, k, l)|$. Но ведь у нас сейчас $l + 2r = l + r = l$, т. е. мы имеем в точности

$$\mathcal{F}_0(n, k, l) = \{F \subset \mathcal{R}_n \colon |F| = k,\ F \supset \mathcal{R}_l\}, \quad |\mathcal{F}_0(n, k, l)| = C_{n-l}^{k-l}$$

и, стало быть, находимся в рамках теоремы Франкла—Уилсона.

Если же, например, n делится на 8, а $k = \frac{n}{2}$, $l = \frac{n}{4}$, то легко видеть, что $r = \frac{n}{8}$, а

$$\mathcal{F}_r(n, k, l) \supset \mathcal{M} = \left\{M \subset \mathcal{R}_n \colon |M| = k,\ |M \cap \mathcal{R}_{\frac{n}{2}}| = \frac{3n}{8}\right\},$$

и мы снова приходим к знакомой конструкции.

Наконец, мы готовы сформулировать и доказать теорему, которая в ряде нетривиальных ситуаций значительно усиливает теорему 7.2.1.

Теорема 7.4.5. *Пусть фиксированы нетривиальные n, k, a. Положим $l = k - \frac{a^2}{2} + 1$. По значениям n, k, l определим величину r так же, как она определяется в теореме* 7.4.4. *Введем*

$$x = l + 2r, \quad y = l + r, \quad \bar{n} = C_n^x, \quad \bar{s} = C_n^k, \quad \bar{k} = C_k^y C_{n-k}^{x-y}.$$

Тогда

$$f(n, k, a) \leqslant \chi(n, k, a) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Исходя из всего сказанного выше можно сразу же заключить, что утверждения теорем 7.2.1 и 7.4.5 идентичны, коль скоро n, k и a таковы, что $n \geqslant (k - l + 1)(l + 1)$. Однако при $n < (k - l + 1)(l + 1)$ новая теорема служит существенным уточнением старой. Доказательство ее будет вполне стандартным, но мы его аккуратно проведем ниже.

Доказательство теоремы 7.4.5. Пусть, как обычно, $\mathcal{M}$ — это совокупность множеств, отвечающих векторам из $\mathcal{V}_{n,k}$, $\mathcal{M} = \{M_1, \ldots, M_{\bar{s}}\}$. Рассмотрим совокупность $\mathcal{X} = \{X_1, \ldots, X_{\bar{n}}\}$, состоящую из всех возможных x-элементных подмножеств множества $\mathcal{R}_n$. Сопоставляя каждому множеству из $\mathcal{X}$ его номер, получаем взаимно однозначное соответствие между совокупностью $\mathcal{X}$ и множеством $\mathcal{R}_{\bar{n}}$. Положим

$$\Lambda_i = \{\nu \in \mathcal{R}_{\bar{n}} \colon |X_\nu \cap M_i| = y\} \subset \mathcal{R}_{\bar{n}}, \quad i = 1, \ldots, \bar{s}.$$

Имеем совокупность $\mathfrak{L} = \{\Lambda_1, \ldots, \Lambda_{\bar{s}}\}$. Это совокупность с параметрами $\bar{n}$, $\bar{s}$, $\bar{k}$, поскольку, очевидно, $\bar{k} = |\Lambda_i|$ для любого i. Возьмем произвольную минимальную с. о. п. для $\mathfrak{L}$ и обозначим ее элементы $\sigma_1, \ldots, \sigma_{\bar{\tau}}$, где

$$\bar{\tau} = \tau(\mathfrak{L}) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Рассмотрим совокупность $\mathcal{S} = \{X_{\sigma_1}, \ldots, X_{\sigma_{\bar{\tau}}}\}$. Понятно, что

$$\mathcal{M} = \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_{\bar{\tau}},$$

где

$$\mathcal{M}_i = \bigl\{M \in \mathcal{M} \colon |X_{\sigma_i} \cap M| = y\bigr\}, \quad i \in \{1, \ldots, \bar{\tau}\}.$$

Более того, как и требовалось, любые два множества из произвольной совокупности $\mathcal{M}_i$ зацепляются по хотя бы l общим элементам, по построению. Теорема доказана.

§ 7.5. Проблемы Борсука и Нелсона—Эрдёша—Хадвигера для совокупностей целочисленных векторов

Этот параграф мы посвятим важным обобщениям результатов, полученных нами на предыдущих этапах исследования.

7.5.1. Постановки задач

В § 7.1, мотивируя редукцию задач Нелсона—Эрдёша—Хадвигера и Борсука к случаям совокупностей $(0, 1)$-векторов, мы отмечали, что именно за счет таких совокупностей удается доказывать оценки вида $\chi(\mathbb{R}^n) \geqslant (1{,}139\ldots + o(1))^n$ и получать большинство контрпримеров к гипотезе Борсука. Тем не менее, самые лучшие результаты достигаются посредством небольшого усложнения «$(0, 1)$-технологии». А именно, к нулям и единицам добавляются еще и минус единицы в качестве потенциальных значений координат векторов. Иными словами, неравенства $\chi(\mathbb{R}^n) \geqslant (1{,}239\ldots + o(1))^n$ и $f(n) \geqslant (1{,}2255\ldots + o(1))^{\sqrt{n}}$ обосновываются в аккурат с помощью систем $(-1, 0, 1)$-векторов. Таким образом, очевиден смысл обобщения задач из § 7.2. Разумеется, в первую очередь, ввиду сказанного упомянутые задачи следует распространять на «$(-1, 0, 1)$-случай». Однако есть все основания рассмотреть и куда более обширное множество ситуаций (см. [27]).

Итак, самая общая постановка вопроса такова. Пусть даны натуральные числа n и $r \leqslant n$. Пусть, кроме того, фиксированы различные целые числа $b_1, \ldots, b_r$ и (возможно, совпадающие) целые положительные числа $k_{b_1}, \ldots, k_{b_r}$, удовлетворяющие условию $k_{b_1} + \ldots + k_{b_r} = n$. Положим

$$\mathcal{V} = \mathcal{V}_{n;b_1,\ldots,b_r;k_{b_1},\ldots,k_{b_r}} = \bigl\{\mathbf{x} = (x_1, \ldots, x_n) \colon$$
$$x_i \in \{b_1, \ldots, b_r\} \quad \forall i = 1, \ldots, n; \quad |\{i \colon x_i = b_j\}| = k_{b_j}\ \forall j = 1, \ldots, r\bigr\}.$$

Из определения совокупности векторов $\mathcal{V}$ сразу же видно, зачем нужно было условие $k_{b_1} + \ldots + k_{b_r} = n$. Просто каждый вектор из $\mathcal{V}$ — это

$(b_1, \ldots, b_r)$-вектор, у которого в точности k_{b_j} (тех или иных) координатных позиций занято величинами b_j. Понятно, что числа $b_1, \ldots, b_r$ совпадать не должны, в то время как совпадению каких-либо величин k_{b_i}, k_{b_j} ничто, по идее, не мешает. Отметим, что при данных конкретных параметрах выполняется соотношение

$$|\mathcal{V}_{n;\ b_1,\ldots,b_r;\ k_{b_1},\ldots,k_{b_r}}| = C_n^{k_{b_1}} \cdot C_{n-k_{b_1}}^{k_{b_2}} \cdot \ldots \cdot C_{n-k_{b_1}-\ldots-k_{b_{r-1}}}^{k_{b_r}} = \frac{n!}{k_{b_1}! \cdot \ldots \cdot k_{b_r}!}.$$

Если $r = 2$, $b_1 = 0$, $b_2 = 1$, $k_1 = k$, $k_0 = n - k$, то, очевидно,

$$\mathcal{V}_{n;b_1,\ldots,b_r;k_{b_1},\ldots,k_{b_r}} = \mathcal{V}_{n,k}.$$

Если, далее, $r=3$, $b_1=-1$, $b_2=0$, $b_3=1$, то мы имеем дело с $(-1, 0, 1)$-случаем. Интересно, наконец, что r вполне может изменяться с ростом n. Например, абсолютно осмысленна ситуация, когда

$$r = n, \quad b_1 = 1, \quad b_2 = 2, \quad \ldots, \quad b_r = n, \quad k_1 = k_2 = \ldots = k_n = 1.$$

Естественно, и прочие параметры, как видно, зависимости от n, вообще говоря, не избегают. Скажем, пусть даже $r = 3$ (как с минус единицами, нулями и единицами), но $b_1 = 3$, $b_2 = 5$, $b_3 = [\sqrt{n}]$. Этот случай тоже годится. Короче говоря, ситуаций море, и мы рискуем утомить читателя техническими деталями, если затеем тщательный разбор всего многообразия случаев. На сей предмет имеется весьма «навороченная» статья [24], с которой очень заинтересованный читатель, конечно, ознакомится. Здесь же мы лишь наметим план действий, постаравшись без спешки, спокойно обсудить хотя бы тот расклад, который возникает при $r = 3$, $b_1 = -1$, $b_2 = 0$, $b_3 = 1$.

Постойте, а о каком, собственно, раскладе речь? Ведь, кажется, мы пока лишь описали параметры и ввели совокупность векторов, отвечающую этим параметрам. Ну и что? А то, что надо задаться еще одним параметром $a = a(n) > 0$ и положить

$$\chi(n; b_1, \ldots, b_r; k_{b_1}, \ldots, k_{b_r}; a) = \\ = \min\bigl\{\chi\colon \mathcal{V}_{n;b_1,\ldots,b_r;k_{b_1},\ldots,k_{b_r}} = V^1 \sqcup \ldots \sqcup V^\chi, \\ \forall i \in \{1, \ldots, \chi\}\ \forall \mathbf{x}, \mathbf{y} \in V^i\ |\mathbf{x} - \mathbf{y}| \neq a\bigr\},$$

$$f(n; b_1, \ldots, b_r; k_{b_1}, \ldots, k_{b_r}; a) = \\ = \max_{\Omega} \min\bigl\{f\colon \Omega = \Omega_1 \sqcup \ldots \sqcup \Omega_f,\ \forall i \in \{1, \ldots, f\}\ \operatorname{diam}\Omega_i < a\bigr\},$$

где последний максимум берется по всем множествам $\Omega \subset \mathcal{V}_{n;\,b_1,\ldots,b_r;\,k_{b_1},\ldots,k_{b_r}}$, имеющим диаметр a. Нет уж, право слово, такая общность не для данной

книжки. Поговорим, как и хотели, только о

$$\chi(n; k_{-1}, k_0, k_1; a) = \chi(n; -1, 0, 1; k_{-1}, k_0, k_1; a),$$
$$f(n; k_{-1}, k_0, k_1; a) = f(n; -1, 0, 1; k_{-1}, k_0, k_1; a).$$

Связь же этих величин с проблемами Борсука и Нелсона—Эрдёша—Хадвигера в $(-1, 0, 1)$-случае очевидна.

В самом начале исследования заметим, что, как и в § 7.2, можно указать ряд ситуаций, в которых задача отыскания величин

$$\chi(n; k_{-1}, k_0, k_1; a), \quad f(n; k_{-1}, k_0, k_1; a)$$

вырождается. Так, ситуации 1 и 3 из § 7.2 повторяются просто дословно. Что же до ситуации 2, то и она, конечно, переносится на нынешнюю почву без особого труда. Вся сложность в написании явной формулы для величины диаметра совокупности векторов $\mathcal{V}_{n;-1,0,1;k_{-1},k_0,k_1}$ в зависимости от значений параметров. Последняя тонкость невелика, и читатель, без сомнения, сумеет сам ее превозмочь.

Нетривиальные ситуации мы обсудим в отдельных пунктах. В п. 7.5.2 мы приведем оценку хроматического числа $\chi(n; k_{-1}, k_0, k_1; a)$, в п. 7.5.3 речь пойдет уже об оценке числа Борсука $f(n; k_{-1}, k_0, k_1; a)$. В п. 7.5.4 и 7.5.5 мы докажем соответствующие результаты.

7.5.2. Оценка хроматического числа

Нам хочется получить как можно лучшую верхнюю оценку величины

$$\chi(n; k_{-1}, k_0, k_1; a)$$

при данных (нетривиальных) значениях параметров n, k_{-1}, k_0, k_1, a. Что для этого нужно сделать? В § 7.4, рассматривая аналогичную задачу для случая $(0, 1)$-векторов, мы пришли к выводу, что для реализации идентичных целей нужно уметь строить как можно бóльшие совокупности множеств, в которых любые два элемента надлежащим образом пересекаются, цепляют (говоря на нашем жаргоне) друг друга. Терминология множеств и зацепления была весьма уместна и крайне удобна. Мы еще применим ее в следующем параграфе. Однако сейчас полезнее вернуться к языку векторов и расстояний между ними. Что же, в переводе на этот язык, мы все-таки делали в § 7.4? Да мы попросту пытались конструировать максимально «жирные» совокупности $(0, 1)$-векторов, попарные расстояния между которыми строго меньше a. Условие же «расстояние между векторами меньше a» было тогда равносильно условию «мощность пересечения множеств больше или равна l». Понятно, стало быть, что и теперь нельзя ожидать хорошего результата, коль скоро с самого начала мы не ответим на вопрос, как устроена максимальная совокупность

векторов из $\mathcal{V}_{n;-1,0,1;k_{-1},k_0,k_1}$ в предположении, что любые два элемента этой совокупности удалены друг от друга на расстояние, меньше чем a? Если же, напротив, ответ на поставленный вопрос будет дан, то и формулировку подходящей теоремы написать будет, по-видимому, недолго.

К несчастью, здесь все далеко не так безоблачно, как в (0, 1)-ситуации. Если в рамках последней Алсведе и Хачатрян поставили точку, то относительно ситуации с минус единицами и пр. имеются лишь недоказанные по сей день гипотезы. Вернее, так. Известны очень «мощные» (по своему размеру) конструкции, которые, безусловно, обладают необходимыми свойствами. Неясно лишь, в самом ли дели эти конструкции максимальны. Иными словами, если одну из таких конструкций мы сейчас опишем, то с ее помощью мы получим, несомненно, сильный результат. Другой разговор, что отныне мы уже не сможем гарантировать неулучшаемость этого результата за счет нашей любимой техники с. о. п. Вдруг бывают конструкции еще мощнее? Кто знает...

Вообще, текущее состояние дел и пресловутые конструкции подробно обсуждаются (в ином контексте) в книге [27]. Там же приводится и мотивировка гипотезы, которая утверждает, что в известном смысле эти конструкции максимальны. Поэтому мы не станем давать здесь пространные комментарии, а просто построим нужную нам совокупность. Насколько она велика, видно будет сразу, а уж почему она именно такова и почему вряд ли существует бóльшая совокупность, читатель сможет узнать из книги [27].

Итак, пусть неотрицательные целые числа m_1, m_2, m_3 таковы, что

$$m_1 + m_2 + m_3 = n.$$

Зафиксируем, далее, произвольные неотрицательные целые числа

$$m_{-1,1},\ m_{0,1},\ m_{1,1},\ m_{-1,2},\ m_{0,2},\ m_{1,2},\ m_{-1,3},\ m_{0,3},\ m_{1,3},$$

удовлетворяющие условиям

$$\begin{aligned} m_{-1,1} + m_{0,1} + m_{1,1} &= m_1, \quad & m_{-1,1} + m_{-1,2} + m_{-1,3} &= k_{-1},\\ m_{-1,2} + m_{0,2} + m_{1,2} &= m_2, & m_{0,1} + m_{0,2} + m_{0,3} &= k_0,\\ m_{-1,3} + m_{0,3} + m_{1,3} &= m_3, & m_{1,1} + m_{1,2} + m_{1,3} &= k_1. \end{aligned}$$

Но и это еще не все. Положим

$$t_i = \operatorname{diam}\bigl\{\mathbf{x}\colon \mathbf{x} = (x_1, \dots, x_{m_i}), \quad \forall j \quad x_j \in \{-1, 0, 1\},$$
$$\forall \nu \in \{-1, 0, 1\} \quad |\{j\colon x_j = \nu\}| = m_{\nu,i}\bigr\}, \quad i = 1, 2, 3.$$

Корректность данного определения вытекает из указанных выше свойств величин

$$m_1,\ m_2,\ m_3,\ m_{-1,1},\ m_{0,1},\ m_{1,1},\ m_{-1,2},\ m_{0,2},\ m_{1,2},\ m_{-1,3},\ m_{0,3},\ m_{1,3}.$$

Страшно? Отнюдь нет: t_i — это всего-навсего максимум расстояний между m_i-мерными $(-1, 0, 1)$-векторами, у каждого из которых в точности $m_{-1,i}$ координат величины -1, $m_{0,i}$ координат величины 0 и $m_{1,i}$ координат величины 1. Понятно, что t_i явным образом зависят от параметров

$$m_1,\ m_2,\ m_3,\ m_{-1,1},\ m_{0,1},\ m_{1,1},\ m_{-1,2},\ m_{0,2},\ m_{1,2},\ m_{-1,3},\ m_{0,3},\ m_{1,3}.$$

Мы потребуем, чтобы выполнялось неравенство

$$t_1 + t_2 + t_3 < a,$$

и это будет последним ограничением на значения наших параметров.

Положим

$$\mathcal{F} = \mathcal{F}(m_1, m_2, m_3, m_{-1,1}, m_{0,1}, m_{1,1}, m_{-1,2}, m_{0,2}, m_{1,2}, m_{-1,3}, m_{0,3}, m_{1,3}) =$$
$$= \{\mathbf{x} = (x_1, \ldots, x_n) \colon \forall i \quad x_i \in \{-1, 0, 1\}, \quad \forall \nu \in \{-1, 0, 1\},$$
$$|\{i = 1, \ldots, m_1 \colon x_i = \nu\}| = m_{\nu,1},\ |\{i = m_1{+}1, \ldots, m_1{+}m_2 \colon x_i = \nu\}| = m_{\nu,2},$$
$$|\{i = m_1{+}m_2{+}1, \ldots, n \colon x_i = \nu\}| = m_{\nu,3}\}.$$

Модельный пример вектора из совокупности $\mathcal{F}$ изображен на рис. 14. Корректность определения обусловлена свойствами параметров. При этом свойство $t_1 + t_2 + t_3 < a$ означает, что $\operatorname{diam} \mathcal{F} < a$, а нам это и надо. Ясно также, что

$$|\mathcal{F}(m_1, m_2, m_3, m_{-1,1}, m_{0,1}, m_{1,1}, m_{-1,2}, m_{0,2}, m_{1,2}, m_{-1,3}, m_{0,3}, m_{1,3})| =$$
$$= \frac{m_1!}{m_{-1,1}!m_{0,1}!m_{1,1}!} \cdot \frac{m_2!}{m_{-1,2}!m_{0,2}!m_{1,2}!} \cdot \frac{m_3!}{m_{-1,3}!m_{0,3}!m_{1,3}!}.$$

Иначе говоря, искомая совокупность — та, у которой параметры реализуют максимум величины

$$M = \frac{m_1!}{m_{-1,1}!m_{0,1}!m_{1,1}!} \cdot \frac{m_2!}{m_{-1,2}!m_{0,2}!m_{1,2}!} \cdot \frac{m_3!}{m_{-1,3}!m_{0,3}!m_{1,3}!}.$$

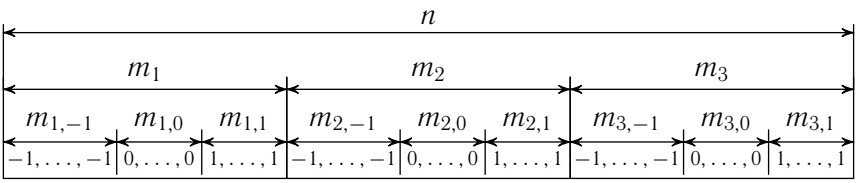

Рис. 14

Теперь мы готовы сформулировать основную теорему.

Теорема 7.5.2.1. *Пусть параметры*

$$m_1,\ m_2,\ m_3,\ m_{-1,1},\ m_{0,1},\ m_{1,1},\ m_{-1,2},\ m_{0,2},\ m_{1,2},\ m_{-1,3},\ m_{0,3},\ m_{1,3}$$

максимизируют величину M при известных ограничениях. Положим

$$\bar{n} = \frac{n!}{m_1!m_2!m_3!}, \quad \bar{s} = \frac{n!}{k_{-1}!k_0!k_1!},$$

$$\bar{k} = \frac{k_{-1}!}{m_{-1,1}!m_{-1,2}!m_{-1,3}!} \cdot \frac{k_0!}{m_{0,1}!m_{0,2}!m_{0,3}!} \cdot \frac{k_1!}{m_{1,1}!m_{1,2}!m_{1,3}!}.$$

Тогда

$$\chi(n; k_{-1}, k_0, k_1; a) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Доказательство теоремы мы приведем в п. 7.5.4.

7.5.3. Оценка числа Борсука

Вспомним, какова была основная идея, приведшая нас к доказательству теоремы 7.2.2, в которой давалась специфическая оценка числа Борсука для совокупностей (0, 1)-векторов. Действительно, ключевое соображение состояло в том, что если у нас любые два вектора в некоторой совокупности Ω отстоят друг от друга на расстояние, не превосходящее данного a (т. е. если, проще говоря, $\operatorname{diam}\Omega \leqslant a$), то множества единичных координат произвольных двух таких векторов сильно зацепляются (пересекаются по не менее чем $l = l(a)$ общим элементам). Хочется думать, что аналогичное соображение сработает и в случае $(-1, 0, 1)$-векторов. Только теперь нам будет полезно следить как за зацеплением множеств единичных координат этих векторов, так и за зацеплением множеств их минус единичных компонент.

Рассмотрим пример. Пусть n делится на 4, $k_{-1} = k_1 = \frac{n}{4}$, $k_0 = \frac{n}{2}$, $a = \sqrt{n}$. И что в этом хорошего? Ничего не стоит взять векторы

$$\mathbf{x} = (1, \ldots, 1, -1, \ldots, -1, \quad 0, \ldots, \quad 0),$$
$$\mathbf{y} = (0, \ldots, 0, \quad 1, \ldots, \quad 1, -1, \ldots, -1),$$

у которых, очевидно, всяческое интересующее нас зацепление отсутствует напрочь, хотя $|\mathbf{x} - \mathbf{y}| = a$. Однако если в описанной ситуации заменить a величиной $\sqrt{\frac{n}{4}}$, то зацепление все-таки появится. Сказанное означает, что нам не всегда удастся сколь-нибудь существенно использовать идею зацепления, но зачастую эта идея играет значительную роль.

Пусть фиксированы все необходимые параметры $(n, k_{-1}, \ldots)$. Отнесем пару неотрицательных целых чисел u_{-1}, u_1 к множеству пар

$$\mathcal{U} = \{(u_{-1}, u_1)\},$$

если $u_{-1} \leqslant k_{-1}$, $u_1 \leqslant k_1$ и существуют два таких $(-1, 0, 1)$-вектора

$$\mathbf{x} = (x_1, \ldots, x_{n-u_{-1}-u_1}) \in \mathcal{V}_{n-u_{-1}-u_1;\ -1,0,1;\ k_{-1}-u_{-1},\ k_0,k_1-u_1},$$
$$\mathbf{y} = (y_1, \ldots, y_{n-u_{-1}-u_1}) \in \mathcal{V}_{n-u_{-1}-u_1;\ -1,0,1;\ k_{-1}-u_{-1},\ k_0,k_1-u_1},$$

что $|\mathbf{x}-\mathbf{y}| \leqslant a$ и

$$\{i\colon x_i = -1\} \cap \{i\colon y_i = -1\} = \varnothing, \quad \{i\colon x_i = 1\} \cap \{i\colon y_i = 1\} = \varnothing.$$

Положим

$$p_{-1} = \min\{u_{-1}\colon (u_{-1}, u_1) \in \mathcal{U}\}, \quad p_1 = \min\{u_1\colon (u_{-1}, u_1) \in \mathcal{U}\}.$$

Может статься, $p_{-1} = p_1 = 0$ (скажем, это так в первом из рассмотренных выше примеров), но вполне возможно и противное. Справедлива следующая теорема.

Теорема 7.5.3.1. *Имеет место неравенство*

$$f(n; k_{-1}, k_0, k_1; a) \leqslant C_{k_{-1}}^{p_{-1}} C_{k_1}^{p_1} f(n - p_{-1} - p_1; k_{-1} - p_{-1}, k_0, k_1 - p_1; a).$$

Утверждение теоремы представляет из себя что-то вроде рекурсии. Однако не стоит думать, что величину

$$f(n - p_{-1} - p_1; k_{-1} - p_{-1}, k_0, k_1 - p_1; a)$$

мы станем оценивать снова за счет той же теоремы. Легко понять, что это и невозможно (соответствующие p_ν равны нулю, и возникает тавтология). Как же быть? Да мы просто применим теперь неравенство

$$f(n - p_{-1} - p_1; k_{-1} - p_{-1}, k_0, k_1 - p_1; a) \leqslant$$
$$\leqslant \chi(n - p_{-1} - p_1; k_{-1} - p_{-1}, k_0, k_1 - p_1; a).$$

Последняя величина оценивается уже за счет теоремы 7.5.2.1. Иными словами, если с самого начала обе величины p_ν окажутся нулевыми, то теорема 7.5.3.1 совпадет с теоремой 7.5.2.1; если же хотя бы одна из величин p_ν нетривиальна, то мы сможем рассчитывать на продвижение в задаче. Сколь велико это продвижение, см. в статье [24]. Теорему же мы докажем в п. 7.5.5.

7.5.4. Доказательство теоремы 7.5.2.1

Чтобы доказательство стало совсем прозрачным, отметим следующее обстоятельство. При построении совокупности

$$\mathcal{F} = \mathcal{F}(m_1, m_2, m_3, m_{-1,1}, m_{0,1}, m_{1,1}, m_{-1,2}, m_{0,2}, m_{1,2}, m_{-1,3}, m_{0,3}, m_{1,3})$$

в п. 7.5.2 мы прежде всего разбивали множество $\mathcal{R}_n$ координатных позиций на части $\mathcal{R}_{1,m_1}$, $\mathcal{R}_{m_1+1,m_1+m_2}$, $\mathcal{R}_{m_1+m_2+1,n}$ (ср. обозначения в §4.3).

Ничто не мешало нам, однако, строить абсолютно произвольное разбиение $\mathcal{R}_n = R_1 \sqcup R_2 \sqcup R_3$ на куски мощности m_1, m_2, m_3, соответственно. По стандартному принципу мы бы все равно потом сконструировали полный аналог совокупности $\mathcal{F}$.

Рассмотрим совокупность $\mathcal{D} = \{D_1, \ldots, D_{\bar{n}}\}$, состоящую из всех возможных (упорядоченных) разбиений $D_i = (R_{1,i}, R_{2,i}, R_{3,i})$ множества $\mathcal{R}_n$ на части мощности m_1, m_2, m_3. Сопоставляя каждому разбиению из $\mathcal{D}$ его номер, получаем взаимно однозначное соответствие между совокупностью $\mathcal{D}$ и множеством $\mathcal{R}_{\bar{n}}$. Для всякого вектора

$$\mathbf{x}_i = (x_{1,i}, \ldots, x_{n,i}) \in \mathcal{V} = \mathcal{V}_{n;-1,0,1;k_{-1},k_0,k_1}, \quad i = 1, \ldots, \bar{s},$$

определим

$$\begin{aligned}
\Lambda_i = \{\nu \in \mathcal{R}_{\bar{n}}\colon\ & |R_{1,\nu} \cap \{j\colon x_{j,i} = -1\}| = m_{-1,1}, \quad |R_{2,\nu} \cap \{j\colon x_{j,i} = -1\}| = m_{-1,2},\\
& |R_{3,\nu} \cap \{j\colon x_{j,i} = -1\}| = m_{-1,3}, \quad |R_{1,\nu} \cap \{j\colon x_{j,i} = 0\}| = m_{0,1},\\
& |R_{2,\nu} \cap \{j\colon x_{j,i} = 0\}| = m_{0,2}, \quad |R_{3,\nu} \cap \{j\colon x_{j,i} = 0\}| = m_{0,3},\\
& |R_{1,\nu} \cap \{j\colon x_{j,i} = 1\}| = m_{1,1}, \quad |R_{2,\nu} \cap \{j\colon x_{j,i} = 1\}| = m_{1,2},\\
& |R_{3,\nu} \cap \{j\colon x_{j,i} = 1\}| = m_{1,3}\} \qquad \subset \mathcal{R}_{\bar{n}}.
\end{aligned}$$

Имеем совокупность $\mathfrak{L} = \{\Lambda_1, \ldots, \Lambda_{\bar{s}}\}$. Это совокупность с параметрами $\bar{n}, \bar{s}, \bar{k}$, ибо нетрудно проверить, что $\bar{k} = |\Lambda_i|$ для любого i. Возьмем произвольную минимальную с. о. п. для $\mathfrak{L}$ и обозначим ее элементы $\sigma_1, \ldots, \sigma_{\bar{\tau}}$, где

$$\bar{\tau} = \tau(\mathfrak{L}) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Рассмотрим совокупность $\mathcal{S} = \{D_{\sigma_1}, \ldots, D_{\sigma_{\bar{\tau}}}\}$. Понятно, что

$$\mathcal{V} = \mathcal{V}_1 \cup \ldots \cup \mathcal{V}_{\bar{\tau}},$$

где

$$\begin{aligned}
\mathcal{V}_i = \big\{\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{V}\colon\ & |R_{1,\sigma_i} \cap \{j\colon x_j = -1\}| = m_{-1,1}, \quad |R_{2,\sigma_i} \cap \{j\colon x_j = -1\}| = m_{-1,2},\\
& |R_{3,\sigma_i} \cap \{j\colon x_j = -1\}| = m_{-1,3}, \quad |R_{1,\sigma_i} \cap \{j\colon x_j = 0\}| = m_{0,1},\\
& |R_{2,\sigma_i} \cap \{j\colon x_j = 0\}| = m_{0,2}, \quad |R_{3,\sigma_i} \cap \{j\colon x_j = 0\}| = m_{0,3},\\
& |R_{1,\sigma_i} \cap \{j\colon x_j = 1\}| = m_{1,1}, \quad |R_{2,\sigma_i} \cap \{j\colon x_j = 1\}| = m_{1,2},\\
& |R_{3,\sigma_i} \cap \{j\colon x_j = 1\}| = m_{1,3}\big\}, \qquad i \in \{1, \ldots, \bar{\tau}\}.
\end{aligned}$$

Остается осознать, что каждая совокупность векторов $\mathcal{V}_i$ и есть обещанный аналог совокупности $\mathcal{F}$. Следовательно, для любого i и для всех $\mathbf{x}, \mathbf{y} \in \mathcal{V}_i$ имеем $|\mathbf{x} - \mathbf{y}| < a$, и теорема доказана.

7.5.5. Доказательство теоремы 7.5.3.1

Пусть фиксированы все параметры $(n, k_{-1}, \ldots, a)$, а также множество $\Omega \subset \mathcal{V}_{n;-1,0,1;k_{-1},k_0,k_1}$, $\operatorname{diam}\Omega = a$.

Сперва мы сформулируем и докажем некое вспомогательное утверждение, появление которого, впрочем, давно ожидаемо.

Утверждение 7.5.5.1. *Для любых двух векторов*

$$\mathbf{x} = (x_1, \ldots, x_n), \quad \mathbf{y} = (y_1, \ldots, y_n) \in \Omega$$

выполнены неравенства

$$|\{i\colon x_i = -1\} \cap \{i\colon y_i = -1\}| \geqslant p_{-1}, \quad |\{i\colon x_i = 1\} \cap \{i\colon y_i = 1\}| \geqslant p_1.$$

Доказательство утверждения 7.5.5.1. Предположим противное. Пусть, например,

$$|\{i\colon x_i = -1\} \cap \{i\colon y_i = -1\}| = q_{-1} < p_{-1}, \quad |\{i\colon x_i = 1\} \cap \{i\colon y_i = 1\}| = q_1.$$

При этом нам даже не важно, как соотносятся величины q_1 и p_1.

Удаляя из векторов $\mathbf{x}$ и $\mathbf{y}$ координатные позиции, принадлежащие множеству

$$\{i\colon x_i = -1 \text{ и } y_i = -1\} \cup \{i\colon x_i = 1 \text{ и } y_i = 1\},$$

получаем два новых вектора

$$\mathbf{x}' = (x'_1, \ldots, x'_{n-q_{-1}-q_1}) \in \mathcal{V}_{n-q_{-1}-q_1;\ -1,0,1;\ k_{-1}-q_{-1},k_0,k_1-q_1},$$
$$\mathbf{y}' = (y'_1, \ldots, y'_{n-q_{-1}-q_1}) \in \mathcal{V}_{n-q_{-1}-q_1;\ -1,0,1;\ k_{-1}-q_{-1},k_0,k_1-q_1}.$$

Эти векторы таковы, что $|\mathbf{x}' - \mathbf{y}'| \leqslant a$ и

$$\{i\colon x'_i = -1\} \cap \{i\colon y'_i = -1\} = \varnothing, \quad \{i\colon x'_i = 1\} \cap \{i\colon y'_i = 1\} = \varnothing.$$

Значит, $(q_{-1}, q_1) \in \mathcal{U}$. Однако $q_{-1} < p_{-1}$, что невозможно ввиду минимальности последней величины. Получим противоречие, и в случае $q_{-1} < p_{-1}$ утверждение доказано. Ясно, что случай $q_1 < p_1$ полностью аналогичен рассмотренному, и доказательство завершено.

Зафиксируем произвольный вектор $\mathbf{x} = (x_1, \ldots, x_n) \in \Omega$ и рассмотрим совокупность

$$\mathcal{P} = \{(P_{-1}, P_1)\colon$$
$$P_{-1} \subset \{i\colon x_i = -1\},\ |P_{-1}| = p_{-1}, \quad P_1 \subset \{i\colon x_i = 1\},\ |P_1| = p_1\},$$

которая состоит из всех возможных пар множеств $P_{-1}, P_1 \subset \mathcal{R}_n$, обладающих перечисленными выше свойствами. Очевидно, $|\mathcal{P}| = C_{k_{-1}}^{p_{-1}} C_{k_1}^{p_1}$. В то же время утверждение 7.5.5.1 фактически говорит нам, что, каков бы ни был вектор $\mathbf{y} = (y_1, \ldots, y_n) \in \Omega$, найдется пара $(P_{-1}, P_1) \in \mathcal{P}$, для которой

$$P_{-1} \subset \{i\colon y_i = -1\}, \quad P_1 \subset \{i\colon y_i = 1\}.$$

Это означает, что

$$\Omega = \Omega_1 \cup \ldots \cup \Omega_c,$$

где $c = C_{k_{-1}}^{p_{-1}} C_{k_1}^{p_1}$,

$$\Omega_i = \{\mathbf{y} = (y_1, \ldots, y_n) \in \Omega\colon \{i\colon y_i = -1\} \supset P_{-1}^i,\ \{i\colon y_i = 1\} \supset P_1^i\},$$
$$\mathcal{P} = \{(P_{-1}^1, P_1^1), \ldots, (P_{-1}^c, P_1^c)\}.$$

Доказательство будет завершено, коль скоро мы научимся разбивать $\Omega_1, \ldots, \Omega_c$ на части, диаметр каждой из которых строго меньше a, ведь пока нет никакой гарантии, что $\operatorname{diam}\Omega_i < a$ хотя бы для какого-то i.

Удалим из каждого вектора, принадлежащего произвольной совокупности Ω_i, $i = 1, \ldots, c$, все координатные позиции, номера которых попадают в множество $P_{-1}^i \cup P_1^i$. Возникнут новые совокупности

$$\Omega_1', \ldots, \Omega_c' \subset \mathcal{V}_{n-p_{-1}-p_1;-1,0,1;k_{-1}-p_{-1},k_0,k_1-p_1},$$
$$\operatorname{diam}\Omega_i' \leqslant a, \quad i = 1, \ldots, c.$$

Их мы разобьем оптимально (как именно — сейчас не имеет значения). Пусть, например, в результате мы получим

$$\Omega_i' = \Omega_{i,1}' \cup \ldots \cup \Omega_{i,f_i}', \quad i = 1, \ldots, c,$$
$$f_i \leqslant f(n - p_{-1} - p_1; k_{-1} - p_{-1}, k_0, k_1 - p_1; a), \quad i = 1, \ldots, c.$$

Если $\mathbf{x}, \mathbf{y} \in \Omega_i$ с тем или иным i, а $\mathbf{x}', \mathbf{y}'$ — отвечающие им «урезанные» векторы из Ω_i', то, разумеется, $|\mathbf{x} - \mathbf{y}| = |\mathbf{x}' - \mathbf{y}'|$. Таким образом, «восстанавливая» векторы $\mathbf{x} \in \Omega_i$ по соответствующим $\mathbf{x}' \in \Omega_i'$, $i = 1, \ldots, c$, получаем покрытия

$$\Omega_i = \Omega_{i,1} \cup \ldots \cup \Omega_{i,f_i}, \quad i = 1, \ldots, c,$$

в которых $\operatorname{diam}\Omega_{i,j} < a$ для всех $i \in \{1, \ldots, c\}$ и всех $j \in \{1, \ldots, f_i\}$. В итоге получаем

$$\Omega = \bigcup_{i=1}^{c} \bigcup_{j=1}^{f_i} \Omega_{i,j},$$

и, стало быть,

$$f(\Omega) \leqslant \sum_{i=1}^{c} f_i \leqslant c f(n - p_{-1} - p_1; k_{-1} - p_{-1}, k_0, k_1 - p_1; a).$$

Теорема доказана.

§ 7.6. Проблема Грюнбаума

Здесь мы, наконец, отступим от проблематики Борсука и Нелсона—Эрдёша—Хадвигера и обсудим проблему Грюнбаума — практически столь же классическую, как и две ее «предшественницы».

7.6.1. Постановка задачи и несколько слов об ее истории

В комбинаторной геометрии есть еще одна очень важная и красивая задача, которая тесно связана с проблемами Борсука и Нелсона—Эрдёша—Хадвигера. Эта задача была поставлена Б. Грюнбаумом в 50-е годы XX в. Цель состоит в оптимальном покрытии ограниченных множеств в $\mathbb{R}^n$ шарами данного диаметра. Говоря более аккуратно и формально, речь идет об отыскании величины

$$g(n, a) = \max_{\Omega} \min\{g\colon \Omega \subset B_1 \cup \ldots \cup B_g,\ \forall i\ B_i \text{— шар},\ \operatorname{diam} B_i = a\}.$$

Здесь максимум берется по всем множествам $\Omega \subset \mathbb{R}^n$, имеющим единичный диаметр, a — произвольное вещественное число.

Классическая теорема Юнга утверждает, что любое n-мерное множество диаметра 1 покрывается шаром радиуса $\sqrt{\frac{n}{2n+2}}$ (см. [9]). Более того, оценка Юнга неулучшаема, поскольку шар, описанный около правильного n-мерного симплекса (см. п. 6.2.1), имеет радиус, в точности равный величине $\sqrt{\frac{n}{2n+2}}$ ($\frac{1}{\sqrt{3}}$ для треугольника на плоскости и $\sqrt{\frac{3}{8}}$ для тетраэдра в пространстве). Таким образом, при $a \geqslant 2\sqrt{\frac{n}{2n+2}}$ заведомо выполняется условие $g(n, a) = 1$, и проблема теряет смысл; однако если $a < 2\sqrt{\frac{n}{2n+2}}$, то $g(n, a) > 1$, и задача приобретает нетривиальный характер.

Вероятно, наиболее интересна ситуация, когда $a = 1$, ведь $f(n) \leqslant (n+1)\, g(n, 1)$, где $f(n)$ — число Борсука (см. [25]). Впрочем, обратного неравенства, которое бы связывало величины $f(n)$ и $g(n, 1)$, не существует, и в дальнейшем мы увидим, насколько, по сути, разнятся задачи Борсука и Грюнбаума.

Сам Грюнбаум, как и большинство специалистов в этой области, верил, по-видимому, в справедливость гипотезы Борсука. Говорят иногда даже о гипотезе Грюнбаума: $g(n, 1) = n + 1$. Любопытно, что при $n \leqslant 3$ эта гипотеза верна, подобно гипотезе Борсука. Двумерный случай довольно прост, а с трехмерным разобралась в 1967 г. П. Кацарова-Каранова, которой удалось доказать чуть более тонкий результат: $g(3;\ 0{,}99983) = 4$.

В отличие от гипотезы Борсука, гипотеза Грюнбаума провалилась быстро и без особого треска. Еще в 1965 г. Л. Данцер установил оценку

$g(n, 1) \geqslant 1{,}003^n$, а в 1991 г. Ж. Бургейном и Й. Линденштраусом был получен самый сильный на данный момент результат: $g(n, 1) \geqslant 1{,}067^n$. Правда, как и в случае задачи Борсука, вопрос о минимальной размерности, в которой возникает контрпример, остается пока открытым.

Что касается верхних оценок для $g(n, 1)$, то самые точные из них опять-таки принадлежат Бургейну и Линденштраусу, которые в 1991 году (в той же статье) показали, что $g(n, 1) \leqslant (1{,}224\ldots + o(1))^n$ (ср. оценку величины $f(n)$ из §7.1).

В целом, как видно, положение не столь уж скверное: здесь, как и в случае хроматического числа, неизвестна лишь правильная константа в основании экспоненты, которой следовало бы оценить сверху и снизу величину $g(n, 1)$. Тем не менее, до окончательного результата еще весьма далеко, и потому интересно рассматривать специальные частные случаи.

Прежде чем переходить к постановке той конкретной задачи, которая может быть исследована за счет свойств с. о. п., заметим, что относительно $g(n, a)$ в общем случае также имеется масса сведений, но не в наших интересах перегружать эту книгу излишней информацией.

Разумеется, мы вновь возвращаемся (см. п. 7.5.1) к совокупности векторов

$$\mathcal{V} = \mathcal{V}_{n;\ b_1,\ldots,b_r;\ k_{b_1},\ldots,k_{b_r}}$$

и полагаем

$$g(n;\ b_1, \ldots, b_r;\ k_{b_1}, \ldots, k_{b_r};\ a) = \\ = \max_{\Omega} \min\bigl\{ g\colon \Omega \subset B_1 \cup \ldots \cup B_g,\ \forall i\ \operatorname{diam} B_i = a\bigr\},$$

где последний максимум берется по всем множествам $\Omega \subset \mathcal{V}_{n;b_1,\ldots,b_r;k_{b_1},\ldots,k_{b_r}}$, имеющим диаметр a, тогда как $B_1, \ldots, B_g$ — это, естественно, шары. Стоит отметить, что, хотя величина a и вернулась к нам в качестве аргумента новой функции g, эта функция напрямую связана именно с $g(n, 1)$. В самом деле, ведь мы сейчас множества диаметра a покрываем шарами *того же*, а не какого-нибудь другого диаметра.

В указанной общности задача получения верхних оценок функции g детально исследована в статье [24]. Мы же скажем ниже лишь несколько слов о простейшей ситуации, когда

$$\mathcal{V} = \mathcal{V}_{n;\ 0,1;\ k_0,\ k_1} = \mathcal{V}_{n,k}, \quad k = k_1, \quad g(n, k, a) = g(n;\ 0, 1;\ k_0,\ k_1;\ a).$$

7.6.2. Наводящие соображения для формулировки основного результата

Не останавливаясь на рассмотрении «тривиальных» ситуаций (ср. §7.2 и п. 7.5.1), перейдем непосредственно к существу дела. Пусть фиксированы параметры n, k, a, а также множество $\Omega \subset \mathcal{V}_{n,k}$, $\operatorname{diam}\Omega = a$.

Нам хочется найти наиболее экономное покрытие множества Ω шарами диаметра a. Естественно, каждый шар, который мог бы войти в подобное покрытие, однозначно задается своим центром. Стало быть, нужно искать оптимальный набор центров, удаленных на «не слишком большое» расстояние от векторов множества Ω. Не правда ли, вряд ли есть смысл в том, например, чтобы взять в качестве одного из таких центров вектор с координатами $1000, 11, \sqrt{17}$ и пр.? Представляется наиболее разумным обращаться лишь к тем векторам, координаты которых суть $0, 1, \frac{1}{2}$. Именно такие векторы «равномерно» недалеки от $(0, 1)$-векторов из Ω, и потому они являются, по-видимому, наилучшими кандидатами на роль центров будущих шаров в покрытии Ω.

Более или менее ясно, как мы будем теперь осуществлять само покрытие. Действительно, мы в некотором роде «представим» произвольный вектор из Ω любым $\left(0, 1, \frac{1}{2}\right)$-вектором, который удален от него на расстояние, не превосходящее $\frac{a}{2}$ (радиус будущего шара). С точки зрения нашей стандартной технологии полезным окажется зафиксировать прежде всего какие-либо неотрицательные целые числа $m_0, m_1, m_{1/2}$, отвечающие за количества координат соответствующей величины в каждом из $\left(0, 1, \frac{1}{2}\right)$-векторов, с помощью которых будет в конечном итоге произведено надлежащее «представление». Таким образом, $m_0 + m_1 + m_{1/2} = n$.

$$\bar{x} = \overbrace{1\ldots\ldots\ldots\ldots\ldots\ldots 1}^{k}\,\overbrace{0\ldots\ldots\ldots\ldots\ldots\ldots 0}^{n-k}$$

$$\bar{y} = \underbrace{0\ldots0}_{m_{1,0}}\,\underbrace{1\ldots1}_{m_{1,1}}\,\underbrace{\tfrac{1}{2}\ldots\tfrac{1}{2}}_{m_{1,\frac{1}{2}}}\,\underbrace{0\ldots0}_{m_{0,0}}\,\underbrace{1\ldots1}_{m_{0,1}}\,\underbrace{\tfrac{1}{2}\ldots\tfrac{1}{2}}_{m_{0,\frac{1}{2}}}$$

Рис. 15

Мы слегка погорячились, пообещав фактически, что будем представлять тот или иной вектор $\mathbf{x} \in \Omega$ произвольным $\left(0, 1, \frac{1}{2}\right)$-вектором $\mathbf{y}$, пусть даже количества нулей, единиц и половинок в векторе $\mathbf{y}$ фиксированы заранее. На самом деле удобнее потребовать, чтобы у данного вектора $\mathbf{x}$ и отвечающего ему центра $\mathbf{y}$ были определенные количества общих нулей и определенные количества общих единиц, определенные количества координатных позиций, на которых у $\mathbf{x}$ стоят, скажем, нули, а у $\mathbf{y}$ — половинки и т. д. (см. рис. 15). В принципе, можно показать, что такое

требование практически не ограничивает общности. Но да Бог с ним: нам бы результат получить. Главное сейчас, что возникает еще ряд параметров

$$m_{0,0},\, m_{0,1},\, m_{0,1/2},\, m_{1,0},\, m_{1,1},\, m_{1,1/2},$$

смысл которых хорошо иллюстрируется рисунком. Понятно, в частности, что

$$m_{1,0}+m_{1,1}+m_{1,1/2}=k,\quad m_{0,0}+m_{0,1}+m_{0,1/2}=n-k,$$
$$m_{0,0}+m_{1,0}=m_0,\quad m_{0,1}+m_{1,1}=m_1,\quad m_{0,1/2}+m_{1,1/2}=m_{1/2}.$$

Ясно, кроме того, что с необходимостью

$$m_{0,1}+m_{1,0}+\frac{1}{4}(m_{0,1/2}+m_{1,1/2})\leqslant\frac{a^2}{4}.$$

Иначе мы получим $|\mathbf{x}-\mathbf{y}|>\dfrac{a}{2}$, и ни о каком покрытии вектора $\mathbf{x}$ шаром диаметра a с центром в $\mathbf{y}$ речь не пойдет.

В следующем пункте мы аккуратно сформулируем теорему, но изобилие параметров в формулировке нас уже пугать не будет.

7.6.3. Формулировка основного результата

Пусть фиксированы параметры n, k, a, а также произвольные величины

$$m_0,\ m_1,\ m_{1/2},\ m_{0,0},\ m_{0,1},\ m_{0,1/2},\ m_{1,0},\ m_{1,1},\ m_{1,1/2},$$

удовлетворяющие всем ограничениям из предыдущего пункта. Тогда справедлива следующая теорема.

Теорема 7.6.3.1. *Положим*

$$\bar n=\frac{n!}{m_0!m_1!m_{1/2}!},\quad \bar s=C_n^k,\quad \bar k=\frac{k!}{m_{1,0}!m_{1,1}!m_{1,1/2}!}\cdot\frac{(n-k)!}{m_{0,0}!m_{0,1}!m_{0,1/2}!}.$$

Тогда выполнено неравенство

$$g(n,k,a)\leqslant G(\bar n,\bar s,\bar k).$$

Теорему мы докажем в следующем пункте. Самое (технически) нетривиальное в ней — это минимизация выражения $G(\bar n,\bar s,\bar k)$ по всем

$$m_0,\ m_1,\ m_{1/2},\ m_{0,0},\ m_{0,1},\ m_{0,1/2},\ m_{1,0},\ m_{1,1},\ m_{1,1/2}$$

с известными свойствами. На ней мы, однако, останавливаться не будем.

Здесь есть еще прямой аналог теорем 7.2.2 и 7.5.3.1. Мы его приведем, а несложное доказательство оставим читателю.

Теорема 7.6.3.2. *Положим* $l=k-\dfrac{a^2}{2}$. *Тогда*

$$g(n,k,a)\leqslant C_k^l\,g(n-l,k-l,a).$$

7.6.4. Доказательство теоремы 7.6.3.1

Фиксируем все параметры, а также множество $\Omega \subset \mathcal{V}_{n,k}$, $\operatorname{diam}\Omega = a$.

Рассмотрим совокупность $\mathcal{Y} = \{\mathbf{y}^1, \dots, \mathbf{y}^{\bar{n}}\}$, состоящую из всех возможных n-мерных векторов $\mathbf{y}^i = (y_1^i, \dots, y_n^i)$, у которых

$$|\{j\colon y_j^i = 0\}| = m_0, \quad |\{j\colon y_j^i = 1\}| = m_1, \quad \left|\left\{j\colon y_j^i = \frac{1}{2}\right\}\right| = m_{1/2}.$$

Сопоставляя каждому вектору из $\mathcal{Y}$ его номер, получаем взаимно однозначное соответствие между $\mathcal{Y}$ и $\mathcal{R}_{\bar{n}}$.

Для всякого $\mathbf{x}^i = (x_1^i, \dots, x_n^i) \in \Omega$, $i = 1, \dots, |\Omega| \leqslant \bar{s}$, определим

$$\Lambda_i = \Big\{\nu \in \mathcal{R}_{\bar{n}}\colon$$

$$|\{j\colon y_j^\nu = 0\} \cap \{j\colon x_j^i = 0\}| = m_{0,0}, \qquad |\{j\colon y_j^\nu = 0\} \cap \{j\colon x_j^i = 1\}| = m_{1,0},$$

$$|\{j\colon y_j^\nu = 1\} \cap \{j\colon x_j^i = 0\}| = m_{0,1}, \qquad |\{j\colon y_j^\nu = 1\} \cap \{j\colon x_j^i = 1\}| = m_{1,1},$$

$$\left|\left\{j\colon y_j^\nu = \frac{1}{2}\right\} \cap \{j\colon x_j^i = 0\}\right| = m_{0,\frac{1}{2}}, \quad \left|\left\{j\colon y_j^\nu = \frac{1}{2}\right\} \cap \{j\colon x_j^i = 1\}\right| = m_{1,\frac{1}{2}}\Big\}$$

$$\subset \mathcal{R}_{\bar{n}}.$$

Нетрудно видеть, что $|\Lambda_i| = \bar{k}$ для любого i, и мы имеем совокупность $\mathfrak{L} = \{\Lambda_1, \dots, \Lambda_{|\Omega|}\}$ с параметрами $\bar{n}$, $|\Omega|$, $\bar{k}$. Пусть $\sigma_1, \dots, \sigma_{\bar{\tau}}$ — произвольная минимальная с. о. п. для $\mathfrak{L}$, где

$$\bar{\tau} = \tau(\mathfrak{L}) \leqslant G(\bar{n}, |\Omega|, \bar{k}) \leqslant G(\bar{n}, \bar{s}, \bar{k}).$$

Возьмем векторы $\mathbf{y}^{\sigma_1}, \dots, \mathbf{y}^{\sigma_{\bar{\tau}}}$. Ввиду определения с. о. п. и свойств наших параметров для любого $\mathbf{x} \in \Omega$ найдется такое $i \in \{1, \dots, \bar{\tau}\}$, что $|\mathbf{x} - \mathbf{y}^i| \leqslant \dfrac{a}{2}$. Значит, обещанная программа реализована, и покрытие найдено. Теорема доказана.

Задачи

27. Пусть $\mathcal{V}_n$ — множество всех n-мерных $(0, 1)$-векторов. Положим

$$\chi(n, a) =$$

$$= \min\{\chi\colon \mathcal{V}_n = V^1 \sqcup \dots \sqcup V^\chi, \ \forall i \in \{1, \dots, \chi\}\ \forall \mathbf{x}, \mathbf{y} \in V^i\ |\mathbf{x} - \mathbf{y}| \neq a\}.$$

Докажите, что $\chi(n, a) \leqslant 2$, коль скоро a^2 — нечетное число, и $\chi(n, a) \leqslant 2^{n - a^2 + 1}$, коль скоро a^2 — четное число.

28.** Найдите максимальное n, при котором удается доказать гипотезу Грюнбаума для совокупностей $(0, 1)$-векторов. Иными словами, как можно точнее оцените величину $g(n, k, a)$ при малых n.

29. а) Дано множество $S \subset \mathbb{R}^2$, $|S| = n$. Докажите, что не более n пар точек в S реализуют диаметр множества S.

б*) В условиях предыдущего пункта задачи докажите, что в S есть не более $O(n^{4/3})$ пар точек, отстоящих друг от друга на расстояние 1.

30.** Скажем, что множество $S \subset \mathbb{R}^2$ *имеет большое хроматическое число*, если элементы этого множества нельзя так покрасить в три цвета, чтобы между одноцветными точками не было расстояния 1. В произвольном множестве $T \subset \mathbb{R}^2$, $|T| = n$, выделим все подмножества S с большим хроматическим числом. Возникнет совокупность $\mathcal{M}(T)$. Оцените величину $\zeta(n) = \max\limits_{T \subset \mathbb{R}^2,\ |T|=n} \tau(\mathcal{M}(T))$.

Глава 8

Системы общих представителей в геометрии чисел

В этой главе мы довольно резко сменим курс и поговорим о приложениях с. о. п. к геометрическим задачам теории чисел.

§ 8.1. Несколько слов о науке и ее базовых объектах

Геометрия чисел — это красивый и важный раздел теории чисел, в рамках которого (говоря совсем общо) различные свойства чисел изучаются с помощью геометрических методов.

Первые результаты, которые естественно было бы отнести к геометрии чисел, возникли еще в XIX в.; однако в самостоятельную дисциплину геометрия чисел оформилась лишь на рубеже позапрошлого и прошлого веков. Ее основателем следует считать Г. Минковского, который фактически заложил фундамент этой науки (см. [54]). Также «классиками» геометрии чисел являются Г. Ф. Вороной (см. [5]), А. Н. Коркин, Е. И. Золотарёв и др.

Основным объектом классической геометрии чисел является *решетка* в пространстве $\mathbb{R}^n$. Говорят, что множество точек $\Lambda \subset \mathbb{R}^n$ образует решетку, если существует такой набор линейно независимых векторов $\mathbf{e}_1, \ldots, \mathbf{e}_k \in \mathbb{R}^n$, что каждая точка $\mathbf{x} \in \Lambda$ представляется в виде

$$\mathbf{x} = a_1\mathbf{e}_1 + \ldots + a_k\mathbf{e}_k, \quad a_1, \ldots, a_k \in \mathbb{Z},$$

т. е. в виде линейной комбинации векторов $\mathbf{e}_1, \ldots, \mathbf{e}_k$ с целыми коэффициентами («целочисленной комбинации»). При этом множество векторов $\mathbf{e}_1, \ldots, \mathbf{e}_k$ называется *базисом* решетки Λ. Очевидно, что $k \leqslant n$. Решетку называют *полной*, если $k = n$. Иногда говорят также об «n-мерных» и «k-мерных» решетках, указывая, тем самым, на размер (размерность) базиса. Такое словоупотребление удобно, хотя и не вполне корректно, ведь любая решетка, будучи счетным набором точек в пространстве, в разумном смысле имеет «размерность» 0.

Стандартные соображения из линейной алгебры показывают, что различных базисов в одной и той же решетке много. Например, простейшая решетка $\mathbb{Z}^2$ на плоскости, состоящая из всех двумерных векторов с целыми координатами, порождается как «стандартным» базисом $\mathbf{e}_1 = (1, 0)$,

$\mathbf{e}_2 = (0, 1)$, так и базисом $\mathbf{e}_1 = (1, 0)$, $\mathbf{e}_2 = (1, 1)$. Мы не станем вдаваться здесь в более детальный анализ алгебраических свойств базисов и связей между ними, отсылая заинтересованного читателя к наиболее значимым источникам [12, 13, 16, 52].

Можно дать альтернативное определение решетки, сказав, что решетка — это произвольная дискретная абелева подгруппа (по сложению) пространства $\mathbb{R}^n$. Такая терминология подчас весьма удобна, а тот факт, что она равносильна первоначальной, практически очевиден (см., впрочем, [12] и пр.).

Подрешетка Γ в решетке Λ — это любое подмножество Λ, которое само является решеткой. Иначе говоря, Γ — это подгруппа в группе Λ. Зачастую «надрешетку» Λ называют *центрировкой* решетки Γ.

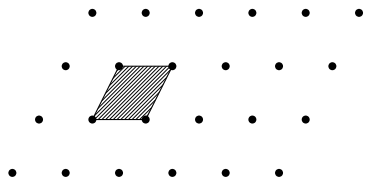

Рис. 16

Один из основных «инвариантов» решетки — это ее *определитель*, т. е. объем ее минимальной («фундаментальной») ячейки (см. рис. 16). Если в некоторой системе координат векторы какого-то базиса (полной) n-мерной решетки Λ имеют вид

$$\mathbf{e}_1 = (e_1^1, \ldots, e_1^n), \quad \ldots, \quad \mathbf{e}_n = (e_n^1, \ldots, e_n^n),$$

то определитель можно вычислить по формуле

$$\det \Lambda = \left| \det \begin{pmatrix} e_1^1 & \ldots & e_n^1 \\ \vdots & \ddots & \vdots \\ e_1^n & \ldots & e_n^n \end{pmatrix} \right|.$$

Определитель действительно не зависит от выбора базиса, поскольку детерминант линейного преобразования, которое переводит один базис в другой, очевидно, равен ± 1.

Заметим, что, тривиальным образом, определитель любой подрешетки всегда не меньше определителя самой решетки. Более того, даже из картинок видно, что меньший детерминант является делителем большего.

Индексом подрешетки Γ в решетке Λ называется порядок факторгруппы Λ/Γ. Нетрудно понять, что на самом деле индекс — это отношение определителей решетки и ее центрировки.

Вот, пожалуй, и все азы. Наука про решетки огромна, но нам и этого хватит. Вернемся к геометрии чисел. С точки зрения последней, интересны даже не сами решетки, а их «взаимодействие» с различными телами в $\mathbb{R}^n$. Основной вопрос: попадают точки решетки в тело, на его границу и пр., или нет?

В § 8.2 мы расскажем о наиболее важных для нас и в то же время наиболее классических результатах геометрии чисел. Там же мы упомянем и ряд приложений этой науки, которые станут к тому моменту более очевидными. Вот только при чем здесь с. о. п.? Пока рано об этом говорить, но постепенно мы поставим и решим соответствующую задачу.

§ 8.2. Теорема Минковского и ее окрестности

Следующий результат можно назвать «основной теоремой геометрии чисел». Принадлежит он Минковскому.

Теорема 8.2.1. *Пусть $\Omega \subset \mathbb{R}^n$ — выпуклое тело, симметричное относительно начала координат O, причем $\operatorname{Vol}\Omega > 2^n$. Тогда*

$$\Omega \cap \mathbb{Z}^n \setminus \{O\} \neq \varnothing,$$

т. е. в Ω есть нетривиальные точки целочисленной решетки.

Напомним, что *тело* в $\mathbb{R}^n$ — это множество с непустой внутренностью; оно *выпукло*, если вместе с любыми двумя своими внутренними точками оно содержит и весь отрезок, которым эти точки соединены; симметрия относительно начала координат означает, что точки $\mathbf{x}$ и $-\mathbf{x}$ принадлежат или не принадлежат данному телу одновременно. Условие выпуклости, в частности, обеспечивает корректность определения объема тела Ω — величины $\operatorname{Vol}\Omega$: выпуклое тело всегда имеет объем.

Теорема Минковского фактически утверждает, что если тело достаточно «регулярное» и притом «жирное», то в нем есть нетривиальные точки $\mathbb{Z}^n$. В кружках обычно доказывают упрощенный вариант теоремы: *если на плоскости взять любой симметричный прямоугольник площади больше четырех, то он непременно поймает точку с целыми координатами, хотя бы одна из которых не равна нулю.*

Теорема Минковского допускает небольшое уточнение. А именно, ее утверждение сохраняется, коль скоро мы предполагаем, что Ω замкнуто и $\operatorname{Vol}\Omega = 2^n$. Более важным для нас является следующее обобщение теоремы Минковского.

Теорема 8.2.2. *Пусть Λ — произвольная n-мерная решетка, а $\Omega \subset \mathbb{R}^n$ — выпуклое тело, симметричное относительно начала ко-*

ординат O, *причем* $\operatorname{Vol}\Omega > 2^n \det\Lambda$. *Тогда*

$$\Omega \cap \Lambda \setminus \{O\} \neq \varnothing,$$

т. е. в Ω *есть нетривиальные точки решетки* Λ.

Ни один из вариантов теоремы мы доказывать не станем. При желании читатель сделает это самостоятельно, а при отсутствии такового он может обратиться, например, к книге [12].

Очень важной для геометрии чисел является проблема «обращения» теоремы Минковского, которая до сих пор отнюдь не решена. Грубо говоря, вопрос состоит в том, насколько большим можно сделать объем данного тела (линейно преобразовывая его), чтобы в новом теле не было нетривиальных целых точек. Или, наоборот: насколько маленьким может быть определитель решетки, которая не пересекается с данным Ω? Удобно формализовать поставленный вопрос в терминах *критического определителя* тела Ω:

$$\Delta(\Omega) = \inf\{\det\Lambda\colon \Lambda \cap \Omega \setminus \{O\} = \varnothing\}.$$

Теорема 8.2.2 говорит, по сути, что $\dfrac{\operatorname{Vol}\Omega}{\Delta(\Omega)} \leqslant 2^n$, коль скоро множество Ω в известном смысле регулярно. Так вот «обращение» — это оценка величины $\dfrac{\operatorname{Vol}\Omega}{\Delta(\Omega)}$ снизу.

Знаменитая теорема Минковского—Главки, доказанная Э. Главкой в 40-е годы XX в., гласит (см. [12, 52]): *каково бы ни было множество* Ω, *обладающее объемом*, *справедливо неравенство* $\dfrac{\operatorname{Vol}\Omega}{\Delta(\Omega)} \geqslant 1$. С одной стороны, утверждение очень сильное, ведь мы не требуем от Ω ничего, кроме наличия у него объема (никакой выпуклости и пр.). С другой стороны, единица и 2^n как-то слишком уж несоизмеримы. Зазор постепенно устраняли (см. [12, 52]), но и по сей день наилучшим остается результат В. Шмидта и К. А. Роджерса (см. [52]): $\dfrac{\operatorname{Vol}\Omega}{\Delta(\Omega)} \geqslant cn$, $c > 0$. Не правда ли, есть чем заняться?

Отметим, что для специальных тел (шаров, октаэдров и пр.) имеются гораздо более точные утверждения, нежели те, о которых шла речь только что, но мы об этом говорить не станем (см. [13, 52]).

Еще один любопытный факт, который мы не можем не упомянуть здесь (при всей отрывочности нашего изложения), принадлежит сэру П. Суиннертону-Дайеру. Для того чтобы сформулировать соответствующую теорему, заметим, что *критическая решетка* тела — это любая решетка Λ, для которой

$$\Omega \cap \Lambda \setminus \{O\} = \varnothing, \quad \det\Lambda = \Delta(\Omega).$$

Критическая решетка есть, конечно, не у всякого тела (точная нижняя грань не обязана достигаться), но в ситуации, о которой пойдет речь, критические решетки существуют (см. [12]).

Теорема 8.2.3. *Пусть $\Omega \subset \mathbb{R}^n$ — выпуклое открытое тело, симметричное относительно начала координат O, и пусть Λ — критическая решетка тела Ω. Тогда Λ имеет не менее $\dfrac{n(n+1)}{2}$ пар точек на границе тела Ω.*

Это очень изящный результат с не менее изящным доказательством (см. [12])!

Чаще всего результаты геометрии чисел применяют в рамках теории диофантовых приближений (см. [11, 36]). Напомним, что эта теория связана с приближением вещественных чисел рациональными и ее отправной точкой служит классическая теорема Дирихле: *для любого иррационального числа α существует бесконечно много различных рациональных чисел $\dfrac{p}{q}$, удовлетворяющих условию $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{q^2}$.* Теорема Дирихле без труда выводится из теоремы Минковского. Грубо говоря, достаточно рассмотреть параллелограмм $|\alpha x - y| \leqslant a$, оценить его площадь при данном a и найти в нем нетривиальную целую точку (p, q).

Короче говоря, наука многогранна и имеет множество приложений. Одну из ее граней мы и изучим в дальнейшем. Удивительным образом, там понадобятся наши любимые с. о. п.

§ 8.3. Постановка задачи о дефектах и формулировки результатов

Назовем множество $\mathcal{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$,

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \quad \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \quad \ldots, \quad \mathbf{e}_n = (0, 0, \ldots, 0, 1),$$

стандартным репером в $\mathbb{R}^n$. Оно образует естественный базис в решетке $\mathbb{Z}^n$. Рассмотрим произвольную центрировку Λ решетки $\mathbb{Z}^n$. Разумеется, репер $\mathcal{E}$ уже не обязан быть базисом в Λ. Спрашивается, насколько сильно отличается $\mathcal{E}$ от какого-либо базиса в Λ? Формализуем поставленный вопрос.

Пусть f — это максимальное число, при котором найдутся такие подмножества $\{\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_f}\} \subset \mathcal{E}$ и $\{\mathbf{b}_1, \ldots, \mathbf{b}_{n-f}\} \subset \Lambda$, что набор

$$\{\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_f}, \mathbf{b}_1, \ldots, \mathbf{b}_{n-f}\}$$

образует базис в Λ. Положим $d(\mathcal{E}; \Lambda) = n - f$ и назовем эту величину *дефектом репера $\mathcal{E}$ относительно центрировки Λ*. По существу, де-

фект — это минимальное количество векторов, которые необходимо удалить из репера, с тем чтобы оставшаяся система векторов все еще была «дополнима» до базиса решетки.

Сейчас мы поймем, что величина $d(\mathcal{E};\Lambda)$ устроена весьма несложно. Скажем, что центрировка Λ *циклическая*, если циклической является факторгруппа $\Lambda/\mathbb{Z}^n$. Иначе говоря, найдется такой вектор $\mathbf{a}=\left(\frac{a_1}{q},\ldots,\frac{a_n}{q}\right)$, что любой вектор $\mathbf{x}\in\Lambda$ записывается в виде $\mathbf{x}=k\mathbf{a}+\mathbf{b}$, где $k\in\mathbb{Z}$, $\mathbf{b}\in\mathbb{Z}^n$, т. е. $\Lambda/\mathbb{Z}^n=<\mathbf{a}>$. Обозначим циклическую центрировку $\Lambda_{\mathbf{a}}$. В этом случае, кстати, даже термин «центрировка» становится яснее: мы к векторам исходной решетки добавляем еще один, как бы сажаем его в «центр» той или иной ячейки нашей решетки, тем самым измельчая, «центрируя» ее. Понятно, впрочем, что далеко не всякая центрировка циклическая.

Покажем, что за счет выбора вектора $\mathbf{a}$ величину $d(\mathcal{E};\Lambda_{\mathbf{a}})$ можно сделать равной любому наперед заданному числу, которое лежит, конечно, в пределах от 0 до n. Для пущей простоты рассмотрим сперва плоскость.

Пусть $\mathbf{a}\in\mathbb{Z}^2$. Тогда, без сомнения, $d(\mathcal{E};\Lambda_{\mathbf{a}})=0$. Пусть, далее, $\mathbf{a}=\left(\frac{1}{2},\frac{1}{2}\right)$. Тогда, очевидно, $\mathcal{E}$ базиса в $\Lambda_{\mathbf{a}}$ не образует, т. е. $d(\mathcal{E};\Lambda_{\mathbf{a}})\geqslant 1$; однако любой из векторов $\mathbf{e}_1$, $\mathbf{e}_2$ без труда дополняется вектором $\mathbf{a}$ до базиса в $\Lambda_{\mathbf{a}}$, и, стало быть, $d(\mathcal{E};\Lambda_{\mathbf{a}})=1$. Пусть, наконец, $\mathbf{a}=\left(\frac{1}{2},\frac{1}{3}\right)$. Тогда имеются векторы

$$2\mathbf{a}-\mathbf{e}_1=\left(0,\frac{2}{3}\right)\in\Lambda_{\mathbf{a}}\quad\text{и}\quad 3\mathbf{a}-\mathbf{e}_2-\mathbf{e}_1=\left(\frac{1}{2},0\right)\in\Lambda_{\mathbf{a}},$$

из которых первый заставляет нас пожертвовать вектором $\mathbf{e}_2$, а второй — вектором $\mathbf{e}_1$, в результате чего мы получаем $d(\mathcal{E};\Lambda_{\mathbf{a}})=2$.

Аналогично можно действовать и в произвольной размерности. Там на роль величин $\frac{1}{2},\frac{1}{3}$ вполне можно взять величины $\frac{1}{p_1},\ldots,\frac{1}{p_n}$, где $p_1,\ldots,p_n$ — какие угодно простые числа. Если все они различны, то дефект равен n, если все они совпадают, то дефект обращается в единицу (с нулем и так все понятно), и т. д.

В чем же суть? Суть в том, что при данном $\mathbf{a}$ правильный подбор $k\in\mathbb{Z}$ и $\mathbf{b}\in\mathbb{Z}^n$ в выражении $k\mathbf{a}+\mathbf{b}$ позволяет «запортить» все координатные подпространства определенной размерности l, т. е. добиться того, чтобы в каждом из этих подпространств нашлась нецелая точка решетки $\Lambda_{\mathbf{a}}$, которую, тем самым, нельзя выразить в виде целочисленной комбинации векторов, порождающих данное подпространство. Как следствие, никакие l векторов из репера не оказываются дополнимыми до базиса в $\Lambda_{\mathbf{a}}$, так что $f<l$, а $d(\mathcal{E};\Lambda_{\mathbf{a}})>n-l$. Эта идея сработает и позже, когда мы усложним задачу. Сейчас же ясно, что при нынешней постановке вопроса заниматься абсолютно нечем.

Еще в § 8.2 мы продемонстрировали смысл деятельности в геометрии чисел, и он сводился к исследованию соотношений между решетками и телами в пространстве. Рассмотренные безотносительно связи с каким-либо телом, решетки куда менее интересны. Пусть Ω — произвольное тело в $\mathbb{R}^n$. Скажем, что Ω *допустимо относительно решетки* Λ, если

$$\Omega \cap \Lambda \setminus (\mathcal{E} \cup -\mathcal{E} \cup \{O\}) = \varnothing.$$

Положим $d(\Omega; \Lambda) = d(\mathcal{E}; \Lambda)$, коль скоро Ω допустимо относительно Λ, и будем считать величину $d(\Omega; \Lambda)$ неопределенной в противном случае.

Довольно тяжело уловить суть науки, если сразу же изучить ее во всей мыслимой общности. Поэтому мы не станем заниматься здесь произвольным множеством $\Omega \subset \mathbb{R}^n$, но лишь рассмотрим один конкретный (хотя и важнейший) пример. Общая же ситуация может быть найдена в статье [21].

Итак, пусть

$$\Omega = \mathcal{O} = \{\mathbf{x} = (x_1, \ldots, x_n) \colon |x_1| + \ldots + |x_n| \leqslant 1\}.$$

Это так называемый n-мерный *единичный октаэдр* (ср. § 8.2). Его еще иногда называют «ортаэдром» и «кроссполитопом». Рассмотрим $d(\mathcal{O}; \Lambda)$ и положим

$$d_n = \max_{\Lambda \supset \mathbb{Z}^n} d(\mathcal{O}; \Lambda), \quad d_n^* = \max_{\Lambda_{\mathbf{a}} \supset \mathbb{Z}^n} d(\mathcal{O}; \Lambda_{\mathbf{a}}).$$

Следующая теорема была доказана Н. Г. Мощевитиным в 1994 г.

Теорема 8.3.1. *Имеет место неравенство*

$$d_n^* \leqslant \frac{cn}{\ln n} (\ln \ln n)^2,$$

где $c > 0$ *— абсолютная постоянная.*

Ничего не напоминает? А ведь ужасно похоже на с. о. п. (ср. гл. 3)! Так оно и окажется.

В 1996 г. автор этой книги показал, что теорема 8.3.1 по существу не улучшаема. Справедлива следующая теорема.

Теорема 8.3.2. *Имеет место неравенство*

$$d_n^* \geqslant \frac{cn}{\ln n} (\ln \ln n)^2,$$

где $c > 0$ *— абсолютная постоянная.*

Теорему 8.3.1 мы аккуратно докажем в § 8.4, теореме 8.3.2 мы посвятим § 8.5. Что же до d_n, то сейчас самые лучшие оценки таковы:

$$n - c \log_2 n \leqslant d_n \leqslant n, \quad c > 0.$$

Нижняя оценка очень проста и может рассматриваться как упражнение (см., впрочем, [58]), верхняя оценка постыдно тривиальна. И хотя мы знаем асимптотику величины d_n ($d_n \sim n$) и даже имеем неплохую оценку остаточного члена в ней (тогда как для d_n^* нам известен лишь порядок роста), ситуация с d_n, пожалуй, хуже, нежели с d_n^*: для $n - d_n$ никакой оценки «по порядку» у нас заведомо нет.

Для полноты картины стоит привести серию точных результатов в малых размерностях: $d_2 = d_2^* = 0$; $d_3 = d_3^* = 1$; $d_4 = d_4^* = 1$.

§ 8.4. Доказательство теоремы 8.3.1

Как и во многих подобных ситуациях, мы разобьем доказательство на несколько этапов.

8.4.1. Основная конструкция и формулировки лемм

Пусть фиксирован вектор $\mathbf{a}$, и пусть октаэдр $\mathcal{O}$ допустим относительно решетки $\Lambda_{\mathbf{a}}$. Запишем $\mathbf{a}$ в виде

$$\mathbf{a} = \left(\frac{a_1}{q}, \ldots, \frac{a_n}{q}\right), \quad \text{где НОД}\,(a_1, \ldots, a_n, q) = 1.$$

По основной теореме арифметики существует единственное «каноническое разложение» числа q в произведение степеней простых чисел: $q = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Рассмотрим $\mathcal{R}_n$ и положим

$$M_i = \{\nu \in \mathcal{R}_n \colon \text{НОД}(a_\nu, p_i) = 1\}, \quad i = 1, \ldots, s.$$

Возникают совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$ и серия лемм.

Лемма 8.4.1.1. *Имеет место равенство*

$$d(\mathcal{O}; \Lambda_{\mathbf{a}}) = d(\mathcal{E}; \Lambda_{\mathbf{a}}) = \tau(\mathcal{M}).$$

Лемма 8.4.1.2. *Имеет место неравенство* $s \leqslant n$.

Лемма 8.4.1.3. *Имеют место неравенства*

$$|M_i| = k_i \geqslant c\frac{\ln p_i}{\ln \ln p_i}, \quad c > 0, \quad i = 1, \ldots, s.$$

Доказательства лемм мы дадим в п. 8.4.2—8.4.4. В п. 8.4.5 мы суммируем накопленную информацию и завершим доказательство теоремы.

8.4.2. Доказательство леммы 8.4.1.1

Пусть $\nu_1, \ldots, \nu_\tau$ — произвольная минимальная с. о. п. для $\mathcal{M}$, $\tau = \tau(\mathcal{M})$. Тогда практически очевидно, что НОД$(a_{\nu_1}, \ldots, a_{\nu_\tau}, q) = 1$ (для

каждого p_j, входящего в разложение q, найдется a_{ν_i}, которое с ним несократимо). Положим

$$\{\mu_1, \ldots, \mu_{n-\tau}\} = \mathcal{R}_n \setminus \{\nu_1, \ldots, \nu_\tau\}.$$

Рассмотрим пересечение решетки $\Lambda_{\mathbf{a}}$ с координатным подпространством, порожденным направлениями с номерами $\mu_1, \ldots, \mu_{n-\tau}$. Любая точка из этого пересечения обязана иметь нулевые координаты на позициях $\nu_1, \ldots, \nu_\tau$. В то же время каждая точка из $\Lambda_{\mathbf{a}}$ имеет вид $k\mathbf{a} + \mathbf{b}$, где $k \in \mathbb{Z}$, $\mathbf{b} \in \mathbb{Z}^n$. Поскольку НОД$(a_{\nu_1}, \ldots, a_{\nu_\tau}, q) = 1$, желая получить нули на позициях $\nu_1, \ldots, \nu_\tau$ за счет выбора k и $\mathbf{b}$, мы вынуждены брать k кратным q. А это означает, что в указанном пересечении все векторы решетки $\Lambda_{\mathbf{a}}$ целые, т. е. систему $\mathbf{e}_{\mu_1}, \ldots, \mathbf{e}_{\mu_{n-\tau}}$ можно дополнить до базиса в нашей центрировке. Иными словами, $f \geqslant n - \tau$, а $d(\mathcal{E}; \Lambda_{\mathbf{a}}) \leqslant \tau$.

Обратное неравенство доказывается практически так же. Берем любые $\nu_1, \ldots, \nu_{\tau-1}$. Они не образуют с. о. п. для $\mathcal{M}$ ввиду минимальности τ. Значит, НОД$(a_{\nu_1}, \ldots, a_{\nu_{\tau-1}}, q) = p > 1$. Полагаем $k = \dfrac{q}{p} \in \mathbb{Z}$ и без труда находим вектор $\mathbf{b} \in \mathbb{Z}^n$, при котором у точки $k\mathbf{a} + \mathbf{b}$ на позициях с номерами $\nu_1, \ldots, \nu_{\tau-1}$ стоят нули. При этом, поскольку НОД$(a_1, \ldots, a_n, q) = 1$, мы имеем $k\mathbf{a} + \mathbf{b} \notin \mathbb{Z}^n$. Мы *испортили* (ср. § 8.3) каждое координатное подпространство размерности $n - \tau + 1$, т. е. $f \leqslant n - \tau$ и $d(\mathcal{E}; \Lambda_{\mathbf{a}}) \geqslant \tau$. Лемма доказана.

8.4.3. Доказательство леммы 8.4.1.2

Нетрудно видеть, что $\det \Lambda_{\mathbf{a}} = \dfrac{1}{q}$. Поскольку октаэдр $\mathcal{O}$ допустим относительно решетки $\Lambda_{\mathbf{a}}$, теорема Минковского дает нам оценку

$$\operatorname{Vol} \mathcal{O} \leqslant 2^n \det \Lambda_{\mathbf{a}} = \frac{2^n}{q}.$$

Хорошо известно, что $\operatorname{Vol} \mathcal{O} = \dfrac{2^n}{n!}$. Значит, $\dfrac{2^n}{n!} \leqslant \dfrac{2^n}{q}$, т. е. $q \leqslant n!$. В то же время,

$$q = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s} \geqslant p_1 \cdot p_2 \cdot \ldots \cdot p_s \geqslant 1 \cdot 2 \cdot \ldots \cdot s = s!.$$

Иными словами, $s! \leqslant n!$, а стало быть, и $s \leqslant n$. Лемма доказана.

8.4.4. Доказательство леммы 8.4.1.3

Зафиксируем i. Положим $M = M_i$, $k = k_i$, $p = p_i$. Пусть $M = \{\nu_1, \ldots, \nu_k\}$. Рассмотрим проекцию октаэдра $\mathcal{O}$ на координатное подпространство, порожденное направлениями с номерами $\nu_1, \ldots, \nu_k$. Получится k-мерный октаэдр $\mathcal{O}'$. Решетку $\Lambda_{\mathbf{a}}$ мы также пересечем с подпространством, в котором уже живет $\mathcal{O}'$. Понятно, что возникнет решетка Λ', у которой

$\det \Lambda' \leqslant \frac{1}{p}$. При этом октаэдр $\mathcal{O}'$, разумеется, допустим относительно Λ'. Рассуждая так же, как и в п. 8.4.3, получаем неравенство $p \leqslant k!$. Предположим, что $k \leqslant \frac{\ln p}{\ln \ln p}$. Тогда

$$k! \leqslant k^k = e^{k \ln k} \leqslant e^{\frac{\ln p}{\ln \ln p} \ln\left(\frac{\ln p}{\ln \ln p}\right)} < e^{\ln p} = p,$$

и мы получим противоречие. Значит, $k \geqslant \frac{\ln p}{\ln \ln p}$, и лемма доказана.

8.4.5. Завершение доказательства теоремы

Итак, мы знаем, что дефект — это размер минимальной с. о. п. для $\mathcal{M}$. При этом в совокупности $s \leqslant n$ множеств, мощность каждого из которых как-то оценивается снизу. Мы не станем применять результаты § 4.8, а поступим проще. Представим совокупность $\mathcal{M}$ в виде $\mathcal{M} = \mathcal{M}_1 \sqcup \mathcal{M}_2$, где

$$\mathcal{M}_1 = \{M_i \in \mathcal{M} \colon p_i \leqslant n\}, \quad \mathcal{M}_2 = \{M_i \in \mathcal{M} \colon p_i > n\}.$$

Очевидно, $\tau(\mathcal{M}) \leqslant \tau(\mathcal{M}_1) + \tau(\mathcal{M}_2)$. Более того, $|\mathcal{M}_1| \leqslant \frac{cn}{\ln n}$, $c > 0$, поскольку имеет место так называемый асимптотический закон распределения простых чисел (см. [6, 10, 18]):

$$\pi(n) = |\{p \leqslant n \colon p \text{ — простое}\}| \sim \frac{n}{\ln n}.$$

Ввиду задачи 3 а выполнено неравенство $\tau(\mathcal{M}_1) \leqslant \frac{cn}{\ln n}$.

Функция $\frac{\ln x}{\ln \ln x}$ возрастает при $x \geqslant n$. Следовательно, раз у нас в рамках совокупности $\mathcal{M}_2$ все простые числа больше n, мы тоже получаем, что все k_i больше $c' \frac{\ln n}{\ln \ln n}$. Тогда $\tau(\mathcal{M}_2) \leqslant \tau(\mathcal{M}')$, где $\mathcal{M}'$ — это совокупность с параметрами

$$n, \quad k = \left[\frac{c' \ln n}{\ln \ln n}\right], \quad s,$$

получаемая из $\mathcal{M}_2$ произвольным «обрезанием» каждого множества в этой совокупности. Ввиду теоремы 3.1 имеем

$$\tau(\mathcal{M}') \leqslant G(n, s, k) \leqslant c'' \frac{n}{\ln n} (\ln \ln n)^2, \quad c'' > 0.$$

Таким образом,

$$d(\mathcal{O}; \Lambda_{\mathbf{a}}) = \tau(\mathcal{M}) \leqslant \tau(\mathcal{M}_1) + \tau(\mathcal{M}_2) \leqslant \tau(\mathcal{M}_1) + \tau(\mathcal{M}') \leqslant$$
$$\leqslant \frac{cn}{\ln n} + c'' \frac{n}{\ln n} (\ln \ln n)^2 \leqslant c''' \frac{n}{\ln n} (\ln \ln n)^2, \quad c''' > 0,$$

и теорема доказана.

§ 8.5. Доказательство теоремы 8.3.2

Здесь мы также будем действовать поэтапно.

8.5.1. Основная конструкция и формулировки лемм

Идея, которую мы постепенно реализуем, состоит в том, чтобы перевернуть доказательство теоремы 8.3.1 «с ног на голову». Смысл в том, что в теореме 8.3.1 мы по вектору, задающему центрировку, относительно которой октаэдр допустим, строим совокупность множеств, у которой на поверку оказывается небольшая минимальная с. о. п.; здесь мы, наоборот, попробуем организовать совокупность с достаточно большой минимальной с. о. п. и по ней сформировать вектор, порождающий центрировку с допустимым октаэдром.

Пусть для начала дана совершенно произвольная совокупность множеств $\mathcal{M} = \{M_1, \ldots, M_s\}$, расположенная в $\mathcal{R}_n$. Никаких ограничений ни на s, ни на $|M_i|$, $i = 1, \ldots, s$, ни тем более на $\tau(\mathcal{M})$ мы пока не накладываем. Хочется найти какой-нибудь вектор $\mathbf{a} = \left(\frac{a_1}{q}, \ldots, \frac{a_n}{q}\right)$, по которому совокупность $\mathcal{M}$ строится так же, как и ее «тезка» из п. 8.4.1. Ничего сложного! Каждому $M_i \in \mathcal{M}$ сопоставим некоторое простое число p_i (числа $p_1, \ldots, p_s$ обязаны быть различными) и положим $q = p_1 \cdot \ldots \cdot p_s$. Рассмотрим произвольный элемент $\nu \in \mathcal{R}_n$. Если в совокупности $\mathcal{M}$ нет множеств, которые бы не содержали ν, то запишем $q_\nu = 1$ (правда, тогда $\tau(\mathcal{M}) = 1\ldots$). Иначе положим q_ν равным произведению всех тех p_i, которые отвечают множествам $M_i \in \mathcal{M}$, не содержащим ν. Пусть $\mathbf{a}$ — любой вектор вида

$$\mathbf{a} = \left(\frac{a_1 q_1}{q}, \ldots, \frac{a_n q_n}{q}\right), \quad \text{НОД}(a_\nu, q) = 1, \quad \nu = 1, \ldots, n.$$

Очевидно ведь, что такому $\mathbf{a}$ соответствует именно совокупность $\mathcal{M}$. Отметим, что с точки зрения центрировки $\Lambda_{\mathbf{a}}$ мы не ограничим общности, если будем считать заранее, что $1 \leqslant a_\nu \leqslant q$, $\nu = 1, \ldots, n$. В таких предположениях возникает множество векторов

$$\mathcal{V} = \mathcal{V}(\mathcal{M};\, p_1, \ldots, p_s),$$

мощность которого есть $\varphi^n(q)$, где φ — это функция Эйлера, выражающая количество натуральных чисел, взаимно простых с данным и не превосходящих его.

Отлично. Значит, отныне остается два открытых вопроса: как правильно построить $\mathcal{M}$ и как выбрать $\mathbf{a} \in \mathcal{V}$? Понятно, что вопросы тесно сплетаются: ведь вполне может оказаться и так, что для данной совокупности $\mathcal{M}$ ни один вектор из $\mathcal{V}$ не задает центрировку с допустимым октаэдром.

Глядя на выкладки из §8.4 кажется естественным потребовать, чтобы искомая совокупность $\mathcal{M}$ обладала следующими свойствами:

$$s = |\mathcal{M}| \approx n, \quad |M_i| \approx \frac{\ln n}{\ln\ln n}, \quad i = 1, \dots, s, \quad \tau(\mathcal{M}) \geqslant c\frac{n}{\ln n}(\ln\ln n)^2.$$

Здесь первые два условия, как мы помним, суть прямые следствия допустимости (см. п. 8.4.3, 8.4.4), и нам не удастся достичь успеха, если мы пренебрежем ими. Последнее же условие гарантирует нам, что если при некотором $\mathbf{a} \in \mathcal{V}$ с допустимостью все в порядке, то (см. лемму 8.4.1.1)

$$d(\mathcal{O}; \Lambda_{\mathbf{a}}) = d(\mathcal{E}; \Lambda_{\mathbf{a}}) \geqslant c\frac{n}{\ln n}(\ln\ln n)^2.$$

С существованием совокупностей указанного вида проблем нет: достаточно применить любую из теорем 4.1.1—4.1.3. Таким образом, с точностью до чисто технической конкретизации значков «$\approx$» в перечисленных выше условиях есть лишь одна проблема: для всякой ли совокупности $\mathcal{M}$, удовлетворяющей этим условиям, найдется такой вектор $\mathbf{a} \in \mathcal{V}$, что октаэдр $\mathcal{O}$ допустим относительно решетки $\Lambda_{\mathbf{a}}$?

Отметим, что даже при фиксированной совокупности $\mathcal{M}$ имеется явный произвол в определении $\mathcal{V}$. В самом деле, простые числа $p_1, \dots, p_s$ априори вольны принимать какие угодно значения. Более или менее ясно, однако, что правильнее всего выбирать числа $p_1, \dots, p_s$ так, чтобы все они были не слишком большими и чтобы в то же время величина $\dfrac{\ln p_i}{\ln\ln p_i}$ была не меньше, чем $c\dfrac{\ln n}{\ln\ln n}$ (ср. п. 8.4.5). Возьмем, стало быть, в качестве p_1 минимальное простое число, большее n, в качестве p_2 — следующее за ним по величине, и т. д. Асимптотический закон распределения простых чисел (см. п. 8.4.5) с учетом условия $s \approx n$ обеспечивает тогда неравенство $p_s \leqslant cn\ln n$.

Оказывается, не все так радужно. Как ни наполняй смыслом значки «$\approx$», как ни переиначивай выбор простых чисел, а без дополнительных ухищрений не обойтись: допустимость оборачивается довольно крепким орешком. Выясняется, впрочем, что и p_i мы подобрали верно, и с совокупностью $\mathcal{M}$ все в порядке, только необходимость выполнения еще одного свойства мы пока не учли — так называемого свойства *равномерной расположенности* в $\mathcal{R}_n$ с константой $c > 0$.

Назовем совокупность $\mathcal{M}$ равномерно расположенной в $\mathcal{R}_n$ с константой $c > 0$, если для любого $t \in \{1, \dots, n\}$ и для всякого множества $R \subseteq \mathcal{R}_n$, имеющего мощность t, выполнено неравенство

$$|\{M \in \mathcal{M} \colon M \subseteq R\}| \leqslant \frac{t\ln t}{c\ln n}.$$

Это загадочное свойство. Конечно, название легко объяснимо: мы равномерно «размазываем» множества из совокупности по всему $\mathcal{R}_n$, так, чтобы любое подмножество $\mathcal{R}_n$ содержало не слишком много элементов совокупности. Но вот откуда такая странная функция $\frac{t \ln t}{c \ln n}$ и почему она столь важна, совсем не ясно. Что ж, всему свое время. Сейчас мы, наконец, готовы сформулировать основную лемму.

Лемма 8.5.1.1. *Для любого достаточно большого n существует совокупность подмножеств $\mathcal{M} = \{M_1, \ldots, M_s\}$ множества $\mathcal{R}_n$, для которой выполняются следующие условия*:

1) $s = |\mathcal{M}| \leqslant n$;

2) $c_1 \frac{\ln n}{\ln \ln n} \leqslant k = |M_i| \leqslant c_2 \frac{\ln n}{\ln \ln n}$, $c_1 > 0$, $c_2 > 0$, $i = 1, \ldots, s$;

3) $\tau(\mathcal{M}) \geqslant \frac{cn}{\ln n} (\ln \ln n)^2$, $c > 0$;

4) *имеет место равномерная расположенность с константой* 11.

Подчеркнем еще раз, что существование совокупностей со свойствами 1—3 мы уже доказали в теоремах 4.1.1—4.1.3, и вся тонкость леммы в том, что мы хотим дополнительно потребовать от таких совокупностей обладания свойством 4. К сожалению, ни одна из перечисленных теорем выполнения этого свойства не гарантирует (проверьте это).

Мы не станем доказывать лемму во всех подробностях, ибо это технически весьма тяжело. В п. 8.5.2 мы изложим схему вероятностного обоснования нашего утверждения, однако выкладок проводить не будем. При этом обидно будет даже не то, что выкладки отсутствуют (их читатель при желании воспроизведет), а то, что найденную совокупность не удастся «пощупать»: как всегда, вероятность лишь даст нам гарантию существования нужного объекта, не снабжая нас при этом ни малейшей информацией о том, как именно такой объект устроен. Дабы ослабить чувство разочарования, мы в п. 8.5.3 опишем явную конструкцию целого класса равномерно расположенных совокупностей с известными значениями параметров n, s, k. Правда, на сей раз мы не станем рассказывать, как из этого класса выбрать совокупность с большой минимальной с. о. п. Взамен мы отошлем читателя к первоисточнику [19], но и это уже кое-что.

Завершение доказательства теоремы 8.3.2 мы оформим в виде следующей леммы.

Лемма 8.5.1.2. *Пусть n достаточно велико, совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$ такая же, как в лемме* 8.5.1.1, *а $p_1, \ldots, p_s$ — последовательные простые числа*,

$$n \leqslant p_1 < \ldots < p_s \leqslant cn \ln n, \quad c > 0.$$

Тогда в множестве $\mathcal{V} = \mathcal{V}(\mathcal{M}; p_1, \ldots, p_s)$*найдется вектор* $\mathbf{a}$*, для которого октаэдр* $\mathcal{O}$ *допустим относительно центрировки* $\Lambda_{\mathbf{a}}$.

В п. 8.5.4 мы эту лемму докажем. Очевидно, что из нее вытекает утверждение теоремы 8.3.2 при $n \geqslant n_0$. При $n < n_0$ это утверждение тривиально, коль скоро мы не гонимся за значениями констант.

8.5.2. Схема доказательства леммы 8.5.1.1

Идея совершенно стандартная. Рассмотрим вероятностное пространство $(\Omega, \mathcal{B}, P)$, описанное в §4.5 (пока параметры n, s, k любые). Пусть $\mathfrak{A} \in \mathcal{B}$ — это событие, состоящее в том, что (случайная) совокупность $\mathcal{M}$ не является равномерно расположенной в $\mathcal{R}_n$ с константой 11. Тогда

$$\mathfrak{A} = \bigcup_{t=1}^{n} \bigcup_{R \subseteq \mathcal{R}_n,\ |R|=t} \mathfrak{A}_{t,R},$$

где $\mathfrak{A}_{t,R}$ — событие, образованное теми совокупностями, у которых на данном t-элементном подмножестве $R \subseteq \mathcal{R}_n$ нарушается свойство равномерной расположенности, т. е.

$$|\{M \in \mathcal{M} \colon M \subseteq R\}| > \frac{t \ln t}{11 \ln n}.$$

Теперь требуется нехитрая комбинаторика, позволяющая оценить (сверху) количество совокупностей с параметрами n, s, k, которые попадают в $\mathfrak{A}_{t,R}$. Допустим, полученная (достаточно аккуратная) оценка имеет величину $w(n, s, k, t)$ (явной зависимости от R нет). Тогда, очевидно,

$$P(\mathfrak{A}_{t,r}) \leqslant \frac{w(n, s, k, t)}{|\Omega|} = \frac{w(n, s, k, t)}{C^s_{C^k_n}},$$

и, стало быть,

$$P(\mathfrak{A}) \leqslant \sum_{t=1}^{n} \sum_{R \subseteq \mathcal{R}_n,\ |R|=t} P(\mathfrak{A}_{t,R}) \leqslant \sum_{t=1}^{n} C^t_n \frac{w(n, s, k, t)}{C^s_{C^k_n}}.$$

Далее, можно, например, показать, что при надлежащем выборе величин s и k, удовлетворяющих ограничениям $c_3 n \leqslant s \leqslant n$, $c_3 \in (0, 1)$, и $c_1 \dfrac{\ln n}{\ln \ln n} \leqslant k \leqslant c_2 \dfrac{\ln n}{\ln \ln n}$, $c_1 > 0$, $c_2 > 0$, выполнено неравенство

$$\sum_{t=1}^{n} C^t_n \frac{w(n, s, k, t)}{C^s_{C^k_n}} < \frac{1}{2}.$$

Это будет означать, что с вероятностью больше чем $\dfrac{1}{2}$ случайная совокупность равномерно расположена (ср. §4.5).

С другой стороны, как видно из § 4.5, при тех же значениях n, s, k имеет место неравенство

$$C_n^l \frac{C^s_{C_n^k - C_{n-l}^k}}{C^s_{C_n^k}} < \frac{1}{2},$$

коль скоро $l \leqslant \frac{c_4 n}{\ln n}(\ln\ln n)^2$, $c_4 > 0$. Отсюда, в свою очередь, следует, что с вероятностью больше чем $\frac{1}{2}$ для случайной совокупности $\mathcal{M}$ имеем $\tau(\mathcal{M}) \geqslant \frac{c_4 n}{\ln n}(\ln\ln n)^2$.

Суммируя накопленную информацию, замечаем, что при нужных нам n, s, k и равномерная расположенность, и большая минимальная с. о. п. «случаются» у наугад выбранной совокупности с вероятностью больше чем $\frac{1}{2}$. Ясно, стало быть, что оба свойства одновременно возникают с положительной вероятностью, т. е. искомая совокупность и впрямь существует.

Схематичное доказательство леммы завершено.

8.5.3. Явные конструкции в лемме 8.5.1.1

Положим $n = k^k$. Тогда (ср. п. 8.4.4) $c_1 \frac{\ln n}{\ln\ln n} \leqslant k \leqslant c_2 \frac{\ln n}{\ln\ln n}$, $c_1 > 0$, $c_2 > 0$. Параметры выбраны, как надо. Остается описать построение совокупности, в которой будет, скажем, n штук k-элементных множеств и которая будет, по-видимому, равномерно расположенной.

Представим $\mathcal{R}_n$ в виде

$$\mathcal{R}_n = \mathcal{R}_{1,k} \sqcup \mathcal{R}_{k+1,2k} \sqcup \ldots \sqcup \mathcal{R}_{n-k+1,k}$$

Всего в указанном разбиении $\frac{n}{k} = k^{k-1}$ множеств (см. рис. 17). Соберем их в некую совокупность.

Теперь разложим $\mathcal{R}_n$ на части по-другому:

$$\mathcal{R}_n = \mathcal{R}_{1,k^2} \sqcup \mathcal{R}_{k^2+1,2k^2} \sqcup \ldots \sqcup \mathcal{R}_{n-k^2+1,n}.$$

Здесь уже $\frac{n}{k^2} = k^{k-2}$ элементов разбиения. Возьмем первый из них, т. е. $\mathcal{R}_{1,k^2}$, и подразобьем его:

$$\mathcal{R}_{1,k^2} = \mathcal{R}_{1,k} \sqcup \mathcal{R}_{k+1,2k} \sqcup \ldots \sqcup \mathcal{R}_{k^2-k+1,k^2}.$$

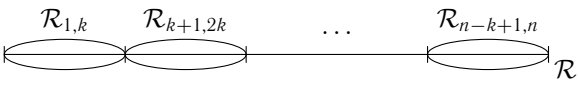

Рис. 17

Рассмотрим любое k-элементное подмножество в $\mathcal{R}_{1,k^2}$, которое пересекает ровно по одному элементу каждое из множеств (см. рис. 18)

$$\mathcal{R}_{1,k}, \quad \mathcal{R}_{k+1,2k}, \quad \ldots, \quad \mathcal{R}_{k^2-k+1,k^2}.$$

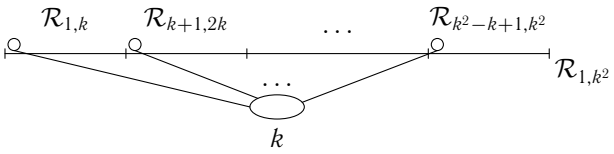

Рис. 18

Добавим к нему еще одно такое же множество, которое с ним не пересекается. Потом еще одно и т. д. В общей сложности образуется k попарно не пересекающихся множеств, каждое из которых захватывает ровно по одному элементу из (см. рис. 19)

$$\mathcal{R}_{1,k}, \quad \mathcal{R}_{k+1,2k}, \quad \ldots, \quad \mathcal{R}_{k^2-k+1,k^2}.$$

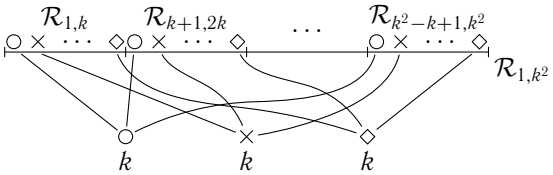

Рис. 19

Точно такую же конструкцию осуществим в рамках

$$\mathcal{R}_{k^2+1,2k^2} = \mathcal{R}_{k^2+1,k^2+k} \sqcup \mathcal{R}_{k^2+k+1,k^2+2k} \sqcup \ldots \sqcup \mathcal{R}_{2k^2-k+1,2k^2}.$$

Появится еще k попарно не пересекающихся множеств и т. д. (см. рис. 20). В итоге мы проделаем описанную операцию $\frac{n}{k^2}$ раз и получим в целом $\frac{n}{k}$ множеств.

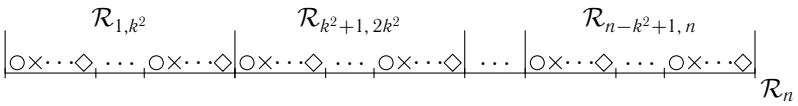

Рис. 20

Наверное, уже ясно, что делать дальше. Верно:

$$\mathcal{R}_n = \mathcal{R}_{1,k^3} \sqcup \mathcal{R}_{k^3+1,2k^3} \sqcup \ldots \sqcup \mathcal{R}_{n-k^3+1,n}.$$

При этом, скажем,

$$\mathcal{R}_{1,k^3} = \mathcal{R}_{1,k^2} \sqcup \mathcal{R}_{k^2+1,2k^2} \sqcup \ldots \sqcup \mathcal{R}_{k^3-k^2+1,k^3}.$$

Вытаскиваем произвольное k-элементное множество из $\mathcal{R}_{1,k^3}$, которое цепляет каждое из множеств

$$\mathcal{R}_{1,k^2}, \quad \mathcal{R}_{k^2+1,2k^2}, \quad \ldots, \quad \mathcal{R}_{k^3-k^2+1,k^3}$$

в точности по одному элементу (см. рис. 21). Потом вытягиваем еще одно аналогичное множество, не пересекающееся с первым и т. д. (см. рис. 22). На сей раз на выходе будет k^2 множеств.

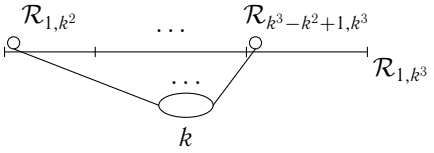

Рис. 21

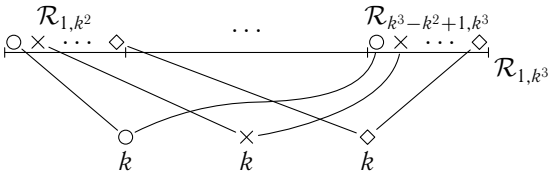

Рис. 22

Столько же (k^2) множеств будет и при схожей обработке куска

$$\mathcal{R}_{k^3+1,2k^3} = \mathcal{R}_{k^3+1,k^3+k^2} \sqcup \mathcal{R}_{k^3+k^2+1,k^3+2k^2} \sqcup \ldots \sqcup \mathcal{R}_{2k^3-k^2+1,2k^3}$$

и т. д. (см. рис. 23). Кусков $\frac{n}{k^3}$, и каждый из них порождает совокупность из k^2 множеств. Значит, опять общий баланс составляет $\frac{n}{k}$ множеств.

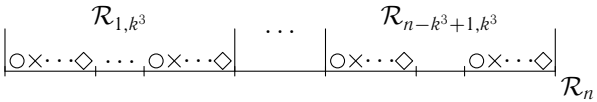

Рис. 23

Продолжая этот процесс, мы всякий раз разбиваем $\mathcal{R}_n$ на куски мощности k^i, $i = 1, \ldots, k$, и, подразделяя каждый кусок на части размера k^{i-1}, организуем $\frac{n}{k} = k^{i-1}\frac{n}{k^i}$ очередных множеств. В самом конце процесса

будет в точности

$$\frac{n}{k}+\frac{n}{k}+\ldots+\frac{n}{k}=n$$

множеств.

Видно, что процесс не был однозначным. На каждом шаге мы допускали значительный произвол в выборе множеств. Тем не менее, можно показать, что любая совокупность $\mathcal{M}$, полученная на выходе, равномерно расположена (см. [19]). Вот несколько намеков, проясняющих суть дела и, в частности, вид функции $\frac{t\ln t}{\ln n}$.

Действительно, пусть $t<k$. Тогда очевидно, что, каково бы ни было $R\subset\mathcal{R}_n$, $|R|=t$, мы получаем

$$|\{M\in\mathcal{M}\colon M\subseteq R\}|=0\leqslant\frac{t\ln t}{\ln n},$$

и все в порядке. Пусть, далее, $t=k$. Тогда, поскольку $k\ln k=\ln n$, имеем

$$|\{M\in\mathcal{M}\colon M\subseteq R\}|\leqslant 1=\frac{t\ln t}{\ln n},$$

и снова все чудесно. Пусть теперь $t=k^2$, $R=\mathcal{R}_{1,k^2}$. В этом случае

$$|\{M\in\mathcal{M}\colon M\subseteq R\}|=2k=\frac{2k^2\ln k}{k\ln k}=\frac{t\ln t}{\ln n},$$

и по-прежнему никаких противоречий. Кроме того, вид конструкции подсказывает нам, что $\mathcal{R}_{1,k^2}$ и ему подобные «куски» наиболее «насыщены» множествами из $\mathcal{M}$, т. е. вполне следует ожидать выполнения неравенства

$$|\{M\in\mathcal{M}\colon M\subseteq R\}|\leqslant 2k,$$

коль скоро $R\subset\mathcal{R}_n$ и $|R|=k^2$.

В общем, интуиция есть, а доказательства см. в [19].

8.5.4. Доказательство леммы 8.5.1.2

Итак, мы считаем, что n достаточно велико, совокупность $\mathcal{M}$ фиксирована, простые числа $p_1,\ldots,p_s$ заданы, а стало быть, полностью описано и множество векторов $\mathcal{V}$, из которого мы стремимся выбрать (хотя бы один) такой вектор $\mathbf{a}$, что октаэдр $\mathcal{O}$ допустим относительно $\Lambda_{\mathbf{a}}$.

Напомним, что у нас всякий вектор $\mathbf{a}\in\mathcal{V}$ имеет вид (см. п. 8.5.1)

$$\mathbf{a}=\left(\frac{a_1q_1}{q},\ldots,\frac{a_nq_n}{q}\right),\quad \text{НОД}\,(a_\nu,q)=1,$$
$$a_\nu\in\{1,\ldots,q\},\quad \nu=1,\ldots,n.$$

Положим для удобства

$$r_\nu=\frac{q}{q_\nu},\quad \nu=1,\ldots,n.$$

Иными словами, r_ν — это произведение всех тех простых чисел из множества $\{p_1, \dots, p_s\}$, которым отвечают множества из совокупности $\mathcal{M}$, содержащие данный элемент $\nu \in \mathcal{R}_n$. По идее, если таких множеств нет (т. е. ν не принадлежит никакому $M \in \mathcal{M}$), то $q_\nu = q$, а $r_\nu = 1$. Однако мы можем отбросить эту ситуацию, потребовав заранее, чтобы каждый элемент множества $\mathcal{R}_n$ был реально использован при построении совокупности $\mathcal{M}$: например, достаточно взять в качестве $\mathcal{M}$ любую подходящую совокупность из п. 8.5.3. В ней, очевидно, и $q_\nu \neq 1$, и $r_\nu \neq 1$ для любого ν.

В новых обозначениях

$$\mathbf{a} = \left(\frac{a_1}{r_1}, \dots, \frac{a_n}{r_n}\right), \quad \text{НОД}(a_\nu, q) = 1, \quad a_\nu \in \{1, \dots, q\}, \quad \nu = 1, \dots, n.$$

Рассмотрим решетку Γ с базисом

$$\left(\frac{1}{r_1}, 0, \dots, 0\right), \ \dots, \ \left(0, \dots, 0, \frac{1}{r_n}\right),$$

т. е. решетку, которая включает в себя и $\mathbb{Z}^n$, и даже любую решетку $\Lambda_{\mathbf{a}}$, $\mathbf{a} \in \mathcal{V}$. Положим

$$\mathcal{X} = \mathcal{O} \cap \Gamma \setminus (\mathcal{E} \cup -\mathcal{E} \cup \{O\})$$

и введем индикатор $\delta = \delta(\mathbf{x})$, $\mathbf{x} \in \mathbb{R}^n$, полагая $\delta(\mathbf{x}) = 1$, если $\mathbf{x} \in \mathbb{Z}^n$, и $\delta(\mathbf{x}) = 0$, если $\mathbf{x} \notin \mathbb{Z}^n$.

Справедливо следующее утверждение.

Утверждение 8.5.4.1. *Для каждого вектора* $\mathbf{a} \in \mathcal{V}$ *октаэдр* $\mathcal{O}$ *допустим относительно* $\Lambda_{\mathbf{a}}$ *тогда и только тогда, когда*

$$S_{\mathbf{a}} = \sum_{l=1}^{q} \sum_{\mathbf{x} \in \mathcal{X}} \delta(\mathbf{a}l - \mathbf{x}) = 0.$$

Доказательство утверждения 8.5.4.1. Пусть сперва вектор $\mathbf{a} \in \mathcal{V}$ таков, что $S_{\mathbf{a}} \neq 0$. Тогда, разумеется, $S_{\mathbf{a}} > 0$, т. е. найдутся такие $l \in \{1, \dots, q\}$ и $\mathbf{x} \in \mathcal{X}$, что $\delta(\mathbf{a}l - \mathbf{x}) = 1$. Значит, $\mathbf{a}l - \mathbf{x} = \mathbf{b} \in \mathbb{Z}^n$. Записывая по-другому, получаем $\mathbf{x} = \mathbf{a}l - \mathbf{b} \in \Lambda_{\mathbf{a}}$. Таким образом, в $\Lambda_{\mathbf{a}}$ нашелся вектор, который, будучи элементом множества $\mathcal{X}$, принадлежит одновременно и октаэдру (без вершин и центра). Следовательно, октаэдр не является допустимым относительно $\Lambda_{\mathbf{a}}$, и в одну сторону утверждение доказано.

Пусть, напротив, вектор $\mathbf{a} \in \mathcal{V}$ таков, что $S_{\mathbf{a}} = 0$. Предположим, что октаэдр, тем не менее, не допустим в $\Lambda_{\mathbf{a}}$. Тогда имеется вектор $\mathbf{x} = \mathbf{a}l + \mathbf{b} \in \Lambda_{\mathbf{a}}$, попадающий в нетривиальную часть октаэдра. При этом, конечно, $l \in \{1, \dots, q\}$, $\mathbf{b} \in \mathbb{Z}^n$. Ввиду сделанного выше замечания $\mathbf{x} \in \Gamma$, а стало быть, и $\mathbf{x} \in \mathcal{X}$. Таким образом, мы нашли $l \in \{1, \dots, q\}$ и $\mathbf{x} \in \mathcal{X}$, для которых $\mathbf{a}l - \mathbf{x} = -\mathbf{b} \in \mathbb{Z}^n$, или, что то же самое, $\delta(\mathbf{a}l - \mathbf{x}) = 1$. Поскольку в сумме $S_{\mathbf{a}}$ все слагаемые неотрицательны, имеем $S_{\mathbf{a}} > 0$. Получим противоречие, и утверждение полностью доказано.

Из утверждения 8.5.4.1 мгновенно следует возможность «усреднения».

Утверждение 8.5.4.2. *Если*

$$\frac{1}{|\mathcal{V}|}\sum_{\mathbf{a}\in\mathcal{V}} S_{\mathbf{a}} = \frac{1}{\varphi^n(q)}\sum_{\mathbf{a}\in\mathcal{V}} S_{\mathbf{a}} < 1,$$

то найдется такой вектор $\mathbf{a}\in\mathcal{V}$, *что октаэдр* $\mathcal{O}$ *допустим относительно* $\Lambda_{\mathbf{a}}$.

Доказательство утверждения 8.5.4.2. Если выполнено условие утверждения, то ввиду неотрицательности каждого $S_{\mathbf{a}}$ найдется вектор $\mathbf{a}\in\mathcal{V}$, для которого $S_{\mathbf{a}} = 0$. В силу утверждения 8.5.4.1 такой вектор и есть тот, что нам нужен. Утверждение доказано.

Итак, для завершения доказательства леммы 8.5.1.2 нам достаточно установить неравенство

$$\frac{1}{\varphi^n(q)}\sum_{\mathbf{a}\in\mathcal{V}} S_{\mathbf{a}} < 1.$$

Что ж, будем действовать.

Начнем с элементарной перестановки порядков суммирования. В самом деле,

$$\frac{1}{\varphi^n(q)}\sum_{\mathbf{a}\in\mathcal{V}} S_{\mathbf{a}} = \frac{1}{\varphi^n(q)}\sum_{\mathbf{a}\in\mathcal{V}}\sum_{l=1}^{q}\sum_{\mathbf{x}\in\mathcal{X}} \delta(\mathbf{a}l-\mathbf{x}) = \frac{1}{\varphi^n(q)}\sum_{l=1}^{q}\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{a}\in\mathcal{V}} \delta(\mathbf{a}l-\mathbf{x}).$$

Нетрудно видеть, что $l = q$ дает нулевой вклад в сумму, ведь $\mathbf{a}q - \mathbf{x}\in\mathbb{Z}^n$ тогда и только тогда, когда $\mathbf{x}\in\mathbb{Z}^n$, но $\mathbf{x}\in\mathcal{X}$, причем $\mathcal{X}\cap\mathbb{Z}^n = \varnothing$. Следовательно, оценивать будем величину

$$\frac{1}{\varphi^n(q)}\sum_{l=1}^{q-1}\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{a}\in\mathcal{V}} \delta(\mathbf{a}l-\mathbf{x}).$$

Пусть $l\in\{1,\ldots,q-1\}$ фиксировано. Посмотрим внимательно на вектор $\mathbf{a}l-\mathbf{x}$. Когда этот вектор является целым? То бишь когда возникает очередное ненулевое слагаемое в сумме? Разумеется, тогда, когда каждая координата указанного вектора есть целое число. Вспоминая, что $\mathbf{x}\in\Gamma$ и, стало быть,

$$\mathbf{x} = \left(\frac{x_1}{r_1},\ldots,\frac{x_n}{r_n}\right),$$

получаем

$$\mathbf{a}l-\mathbf{x} = \left(\frac{a_1l-x_1}{r_1},\ldots,\frac{a_nl-x_n}{r_n}\right).$$

Иными словами, нас волнует выполнение свойств

$$\frac{a_\nu l - x_\nu}{r_\nu}\in\mathbb{Z},\quad \nu = 1,\ldots,n.$$

Положим $l_\nu = \text{НОД}\,(l, r_\nu)$, $\nu = 1,\ldots,n$. Условие $\dfrac{a_\nu l - x_\nu}{r_\nu}\in\mathbb{Z}$ равносильно условию $a_\nu l - x_\nu = br_\nu$, $b\in\mathbb{Z}$. Таким образом, если $\delta(\mathbf{a}l-\mathbf{x}) = 1$,

то каждое x_ν обязано делиться на l_ν. Это означает, что

$$\frac{1}{\varphi^n(q)}\sum_{l=1}^{q-1}\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{a}\in\mathcal{V}}\delta(\mathbf{a}l-\mathbf{x})=\frac{1}{\varphi^n(q)}\sum_{l=1}^{q-1}\sum_{\mathbf{x}\in\mathcal{X}_l}\sum_{\mathbf{a}\in\mathcal{V}}\delta(\mathbf{a}l-\mathbf{x}),$$

где

$$\mathcal{X}_l=\mathcal{O}\cap\Gamma_l\setminus(\mathcal{E}\cup-\mathcal{E}\cup\{O\}),$$

а Γ_l — решетка с базисом

$$\Big(\frac{l_1}{r_1},0,\ldots,0\Big),\ \ldots,\ \Big(0,\ldots,0,\frac{l_n}{r_n}\Big).$$

Сейчас внешнее суммирование по l мы разобьем на некоторые части в соответствии с определенными свойствами делимости числа l. Зафиксируем натуральное $\rho\in\{1,\ldots,s\}$ (здесь $s=|\mathcal{M}|$). Зададимся также произвольными натуральными $i_1,\ldots,i_\rho$, удовлетворяющими условию

$$1\leqslant i_1<i_2<\ldots<i_{\rho-1}<i_\rho\leqslant s.$$

Возьмем $p_{i_1},\ldots,p_{i_\rho}\in\{p_1,\ldots,p_s\}$ и рассмотрим множество

$$\mathcal{L}_{i_1,\ldots,i_\rho}=\{l,\ 1\leqslant l\leqslant q-1\colon l \text{ не делится на } p_{i_1},\ldots,p_{i_\rho} \text{ и делится на все остальные числа из множества } \{p_1,\ldots,p_s\}.$$

Понятно, что и впрямь возникло разбиение

$$\{1,\ldots,q-1\}=\sqcup_{\rho=1}^{s}\sqcup_{i_1,\ldots,i_\rho}\mathcal{L}_{i_1,\ldots,i_\rho}.$$

Здесь лишь полезно заметить, что ρ действительно не должно принимать значение 0, так как $l<q$: хотя бы на одно простое число l заведомо не делится.

В итоге мы имеем дело с «ужасной» суммой

$$\frac{1}{\varphi^n(q)}\sum_{\rho=1}^{s}\sum_{i_1,\ldots,i_\rho}\sum_{l\in\mathcal{L}_{i_1,\ldots,i_\rho}}\sum_{\mathbf{x}\in\mathcal{X}_l}\sum_{\mathbf{a}\in\mathcal{V}}\delta(\mathbf{a}l-\mathbf{x}),$$

которую отныне нам предстоит сворачивать.

Хорошо. Пусть числа $\rho, i_1,\ldots,i_\rho$ и $l\in\mathcal{L}_{i_1,\ldots,i_\rho}$ по-прежнему фиксированы. Обозначим через $t(l)$ величину $t(l)=|\{\nu\colon l_\nu\neq r_\nu\}|$. Можно сказать, что $t(l)$ — это количество нецелых векторов в базисе решетки Γ_l. Для дальнейших целей нам понадобится следующее утверждение.

Утверждение 8.5.4.3. *Имеет место неравенство*

$$\frac{t(l)\ln t(l)}{11\ln n}\geqslant\rho.$$

Не правда ли, до боли напоминает условие равномерной расположенности? Так оно и окажется: в некотором смысле утверждение 8.5.4.3 является ключевым, и именно оно проясняет суть столь, на первый взгляд, загадочного комбинаторного ограничения, которое мы наложили на совокупность $\mathcal{M}$. Если прочесть неравенство из формулировки утверждения задом наперед, то напрашивается комментарий: равномерная расположенность не позволяет величине ρ быть слишком большой, коль скоро мы ее оцениваем в терминах $t(l)$. Это-то, по-видимому, и даст нам шанс добиться в конечном счете успеха.

Доказательство утверждения 8.5.4.3. Пусть $p_{i_1}, \ldots, p_{i_\rho}$ — простые числа из определения множества $\mathcal{L}_{i_1,\ldots,i_\rho}$, которому принадлежит наше l. Возьмем $M_{i_1}, \ldots, M_{i_\rho} \in \mathcal{M}$ — множества из совокупности $\mathcal{M}$, которые «помечены» этими простыми числами. Положим $R = M_{i_1} \cup \ldots \cup M_{i_\rho} \subseteq \mathcal{R}_n$.

Если $\nu \in \mathcal{R}_n$ таково, что $\nu \in R$, то найдется множество M_{i_γ}, $\gamma \in \{1, \ldots, \rho\}$, которое содержит ν. Значит, ввиду своего определения r_ν делится на p_{i_γ}. В то же время l на p_{i_γ} делиться не может, ибо оно не делится ни на одно из чисел $p_{i_1}, \ldots, p_{i_\rho}$. Таким образом, l на r_ν при $\nu \in R$ нацело не делится, т. е. $l_\nu \neq r_\nu$ и $R \subseteq \{\nu\colon l_\nu \neq r_\nu\}$.

С другой стороны, если $\nu \notin R$, то, опять-таки ввиду своего определения, r_ν не делится ни на одно из чисел $p_{i_1}, \ldots, p_{i_\rho}$. Возможно, r_ν не делится и на некоторые из чисел в множестве $\{p_1, \ldots, p_s\} \setminus \{p_{i_1}, \ldots, p_{i_\rho}\}$ (это так, если в R содержатся еще какие-то элементы совокупности $\mathcal{M}$, помимо множеств $M_{i_1}, \ldots, M_{i_\rho}$); однако l на них делится безусловно. Таким образом, r_ν является делителем l, т. е. $\nu \notin \{\nu\colon l_\nu \neq r_\nu\}$ и $R \supseteq \{\nu\colon l_\nu \neq r_\nu\}$.

Окончательно получаем $R = \{\nu\colon l_\nu \neq r_\nu\}$, так что $|R| = t(l)$. Следовательно, с учетом равномерной расположенности

$$\rho \leqslant |\{M \in \mathcal{M}\colon M \subseteq R\}| \leqslant \frac{t(l)\ln t(l)}{11 \ln n}.$$

Утверждение доказано.

Вернемся к изучению «ужасной» суммы. Зафиксируем в ней все, кроме вектора $\mathbf{a} \in \mathcal{V}$. Положим

$$\mathcal{V}_{l,\mathbf{x}} = \{\mathbf{a} \in \mathcal{V}\colon \delta(\mathbf{a}l - \mathbf{x}) = 1\}.$$

Здесь $l \in \mathcal{L}_{i_1,\ldots,i_\rho}$ и $\mathbf{x} \in \mathcal{X}_l$, и мы для краткости просто не указываем явно зависимость множества $\mathcal{V}_{l,\mathbf{x}}$ от ρ и от $i_1, \ldots, i_\rho$. В результате получаем

$$\sum_{\mathbf{a}\in\mathcal{V}} \delta(\mathbf{a}l - \mathbf{x}) = \sum_{\mathbf{a}\in\mathcal{V}_{l,\mathbf{x}}} \delta(\mathbf{a}l - \mathbf{x}) = |\mathcal{V}_{l,\mathbf{x}}|.$$

Поскольку в координатах

$$\mathbf{a}l - \mathbf{x} = \left(\frac{a_1 l - x_1}{r_1}, \ldots, \frac{a_n l - x_n}{r_n}\right),$$

разумеется, выполняется равенство

$$|\mathcal{V}_{l,\mathbf{x}}| = \prod_{\nu=1}^{n} |\mathcal{V}^{\nu}_{l,\mathbf{x}}|,$$

где

$$\mathcal{V}^{\nu}_{l,\mathbf{x}} = \left\{a_\nu \colon a_\nu \in \{1,\dots,q\},\ \text{НОД}\,(a_\nu, q) = 1,\ \frac{a_\nu l - x_\nu}{r_\nu} \in \mathbb{Z}\right\},$$
$$\nu = 1,\dots,n.$$

Если $\nu \notin \{\nu \colon l_\nu \neq r_\nu\}$, т. е. если $l_\nu = r_\nu$, то дробь $\dfrac{a_\nu l - x_\nu}{r_\nu}$ всегда целая, и, значит, $|\mathcal{V}^{\nu}_{l,\mathbf{x}}| = \varphi(q)$. Таких ситуаций, ясное дело, ровно $n - t(l)$.

В противном случае слегка огрубим оценку: $|\mathcal{V}^{\nu}_{l,\mathbf{x}}| \leqslant |\tilde{\mathcal{V}}^{\nu}_{l,\mathbf{x}}|$, где

$$\tilde{\mathcal{V}}^{\nu}_{l,\mathbf{x}} = \left\{a_\nu \colon a_\nu \in \{1,\dots,q\},\ \frac{a_\nu l - x_\nu}{r_\nu} \in \mathbb{Z}\right\}.$$

Найдем $|\tilde{\mathcal{V}}^{\nu}_{l,\mathbf{x}}|$. Для этого заметим, что

$$\frac{a_\nu l - x_\nu}{r_\nu} = \frac{l_\nu(a_\nu l' - x'_\nu)}{l_\nu r'_\nu} = \frac{a_\nu l' - x'_\nu}{r'_\nu}.$$

При этом $\text{НОД}\,(l', r'_\nu) = 1$. Простое арифметическое наблюдение состоит в том, что тогда отыщутся такие целые a_ν и b_ν, что $a_\nu l' + b_\nu r'_\nu = x'_\nu$ (см. [4, 6]). Более того, на каждом из промежутков

$$\{1,\dots,r'_\nu\},\quad \{r'_\nu + 1,\quad \dots,\quad 2r'_\nu\},\dots,\{q - r'_\nu + 1,\dots,q\}$$

указанное a_ν не только существует, но еще и единственно. Значит, имеется в точности

$$\frac{q}{r'_\nu} = \frac{q}{r_\nu/l_\nu} = \frac{ql_\nu}{r_\nu}$$

способов выбрать $a_\nu \in \{1,\dots,q\}$, так, чтобы при подходящем $b_\nu \in \mathbb{Z}$ выполнялось равенство $a_\nu l' + b_\nu r'_\nu = x'_\nu$. Но последнее равенство эквивалентно условию

$$\frac{a_\nu l - x_\nu}{r_\nu} = \frac{a_\nu l' - x'_\nu}{r'_\nu} = -b_\nu \in \mathbb{Z}.$$

Иначе говоря, мы показали, что $|\tilde{\mathcal{V}}^{\nu}_{l,\mathbf{x}}| = \dfrac{ql_\nu}{r_\nu}$.

Из всего сказанного следует, что

$$|\mathcal{V}_{l,\mathbf{x}}| \leqslant (\varphi(q))^{n-t(l)} \prod_{\nu \in \{\nu \colon l_\nu \neq r_\nu\}} \frac{ql_\nu}{r_\nu} = q^{t(l)}(\varphi(q))^{n-t(l)} \det \Gamma_l$$

с учетом

$$\det\Gamma_l = \left|\det\begin{pmatrix} \frac{l_1}{r_1} & 0 & \dots & 0 & 0 \\ 0 & \frac{l_2}{r_2} & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \frac{l_{n-1}}{r_{n-1}} & 0 \\ 0 & 0 & \dots & 0 & \frac{l_n}{r_n} \end{pmatrix}\right| = \prod_{\nu=1}^{n}\frac{l_\nu}{r_\nu} = \prod_{\nu\in\{\nu\colon\, l_\nu\neq r_\nu\}}\frac{l_\nu}{r_\nu}.$$

Таким образом,

$$\sum_{\mathbf{x}\in\mathcal{X}_l}\sum_{\mathbf{a}\in\mathcal{V}}\delta(\mathbf{a}l-\mathbf{x}) \leqslant \sum_{\mathbf{x}\in\mathcal{X}_l} q^{t(l)}(\varphi(q))^{n-t(l)}\det\Gamma_l = |\mathcal{X}_l|q^{t(l)}(\varphi(q))^{n-t(l)}\det\Gamma_l.$$

Надо, стало быть, оценить $|\mathcal{X}_l|$.

Рассмотрим проекцию $\mathcal{O}'$ октаэдра $\mathcal{O}$ на $t(l)$-мерное координатное подпространство, порожденное направлениями с номерами $\nu\in\{\nu\colon\, l_\nu\neq r_\nu\}$. Пусть Γ_l' — это решетка, которая образуется при пересечении описанного подпространства с решеткой Γ_l. Положим, наконец,

$$\mathcal{X}_l' = \mathcal{O}'\cap\Gamma_l'\setminus\mathcal{A},$$

где $\mathcal{A}$ состоит из множества вершин $t(l)$-мерного октаэдра $\mathcal{O}'$ и его центра O. Практически очевидно, что $|\mathcal{X}_l| = |\mathcal{X}_l'|$. При этом $\det\Gamma_l = \det\Gamma_l'$.

Каждой точке решетки Γ_l', которая попала в $\mathcal{O}'$, сопоставим по определенному правилу ячейку этой решетки (см. рис. 24). Объединение таких

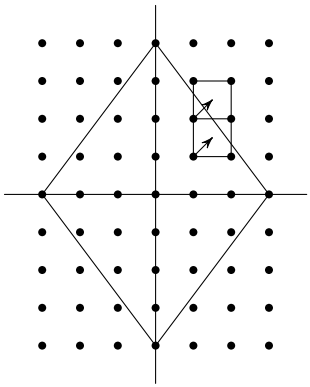

Рис. 24

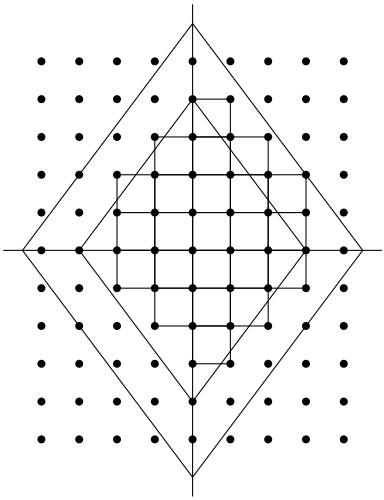

Рис. 25

ячеек содержится в слегка «раздутом» октаэдре $\mathcal{O}'' \supset \mathcal{O}'$, у которого в ν-м направлении ($\nu \in \{\nu\colon l_\nu \neq r_\nu\}$) координата соответствующей вершины равна не 1, как это было у $\mathcal{O}'$, а, скажем, $1 + \sum\limits_{\nu\in\{\nu\colon l_\nu\neq r_\nu\}} \dfrac{l_\nu}{r_\nu}$ (см. рис. 25). Следовательно,

$$|\mathcal{X}_l'| \det \Gamma_l' \leqslant \operatorname{Vol} \mathcal{O}'' = \operatorname{Vol} \mathcal{O}' \Big(1 + \sum_{\nu\in\{\nu\colon l_\nu\neq r_\nu\}} \frac{l_\nu}{r_\nu}\Big)^{t(l)} =$$

$$= \frac{2^{t(l)}}{t(l)!}\Big(1 + \sum_{\nu\in\{\nu\colon l_\nu\neq r_\nu\}} \frac{l_\nu}{r_\nu}\Big)^{t(l)} \leqslant \frac{e^{t(l)}}{t(l)^{t(l)}e^{-t(l)}}\Big(1 + \frac{t(l)}{n}\Big)^{t(l)}.$$

Последнее неравенство обусловлено, во-первых, тем, что $m! \geqslant m^m e^{-m}$ для любого m, и, во-вторых, тем, что $\dfrac{l_\nu}{r_\nu} \leqslant \dfrac{1}{p}$ с некоторым $p \in \{p_1, \ldots, p_s\}$ и, стало быть, $\dfrac{l_\nu}{r_\nu} \leqslant \dfrac{1}{n}$ ввиду условия $p \geqslant n$.

В результате имеем оценку

$$|\mathcal{X}_l| = |\mathcal{X}_l'| \leqslant \frac{e^{2t(l)}}{t(l)^{t(l)}}\Big(1 + \frac{t(l)}{n}\Big)^{t(l)} (\det \Gamma_l)^{-1} \leqslant$$

$$\leqslant \frac{e^{2t(l)}}{t(l)^{t(l)}} e^{\frac{t^2(l)}{n}} (\det \Gamma_l)^{-1} \leqslant e^{3t(l) - t(l)\ln t(l)} (\det \Gamma_l)^{-1}.$$

С помощью этой оценки приходим к выводу, что

$$\frac{1}{\varphi^n(q)}\sum_{\mathbf{x}\in\mathcal{X}_l}\sum_{\mathbf{a}\in\mathcal{V}}\delta(\mathbf{a}l-\mathbf{x})\leqslant(\varphi(q))^{-n}|\mathcal{X}_l|q^{t(l)}(\varphi(q))^{n-t(l)}\det\Gamma_l\leqslant$$
$$\leqslant e^{3t(l)-t(l)\ln t(l)}(\det\Gamma_l)^{-1}q^{t(l)}(\varphi(q))^{-t(l)}\det\Gamma_l=$$
$$=e^{3t(l)-t(l)\ln t(l)}q^{t(l)}(\varphi(q))^{-t(l)}.$$

Хорошо известно (см. [42]), что

$$\varphi(q)=q\Big(1-\frac{1}{p_1}\Big)\cdot\ldots\cdot\Big(1-\frac{1}{p_s}\Big).$$

В нашем случае $p_i\geqslant n$ для всех i, так что

$$\varphi(q)\geqslant q\Big(1-\frac{1}{n}\Big)^s\geqslant qe^{-1},$$

и, значит, $q^{t(l)}(\varphi(q))^{-t(l)}\leqslant e^{t(l)}$, т. е.

$$\frac{1}{\varphi^n(q)}\sum_{\rho=1}^{s}\sum_{i_1,\ldots,i_\rho}\sum_{l\in\mathcal{L}_{i_1,\ldots,i_\rho}}\sum_{\mathbf{x}\in\mathcal{X}_l}\sum_{\mathbf{a}\in\mathcal{V}}\delta(\mathbf{a}l-\mathbf{x})\leqslant\sum_{\rho=1}^{s}\sum_{i_1,\ldots,i_\rho}\sum_{l\in\mathcal{L}_{i_1,\ldots,i_\rho}}e^{4t(l)-t(l)\ln t(l)}.$$

Поскольку

$$t(l)=|R|\geqslant|M|\geqslant c_1\frac{\ln n}{\ln\ln n},\quad M\in\mathcal{M},$$

имеем $t(l)\to\infty$ при $n\to\infty$. Это означает, что при достаточно большом n выполнено неравенство

$$e^{4t(l)-t(l)\ln t(l)}\leqslant e^{-\frac{1}{2}t(l)\ln t(l)}.$$

Из утверждения 8.5.4.3, в свою очередь, следует оценка $t(l)\ln t(l)\geqslant$ $\geqslant 11\rho\ln n$. Стало быть,

$$e^{-\frac{1}{2}t(l)\ln t(l)}\leqslant e^{-5\rho\ln n}=\frac{1}{n^{5\rho}}.$$

Получаем

$$\sum_{\rho=1}^{s}\sum_{i_1,\ldots,i_\rho}\sum_{l\in\mathcal{L}_{i_1,\ldots,i_\rho}}e^{4t(l)-t(l)\ln t(l)}\leqslant$$
$$\leqslant\sum_{\rho=1}^{s}\sum_{i_1,\ldots,i_\rho}\sum_{l\in\mathcal{L}_{i_1,\ldots,i_\rho}}\frac{1}{n^{5\rho}}=\sum_{\rho=1}^{s}\sum_{i_1,\ldots,i_\rho}\frac{|\mathcal{L}_{i_1,\ldots,i_\rho}|}{n^{5\rho}}.$$

Здесь, очевидно,

$$|\mathcal{L}_{i_1,\ldots,i_\rho}|\leqslant p_{i_1}\cdot\ldots\cdot p_{i_\rho}\leqslant n^{2\rho}.$$

Последнее неравенство имеет место при достаточно большом n, так как $p_i \leqslant cn \ln n \leqslant n^2$ при всех i.

Таким образом,

$$\sum_{\rho=1}^{s} \sum_{i_1,\ldots,i_\rho} \frac{|\mathcal{L}_{i_1,\ldots,i_\rho}|}{n^{5\rho}} \leqslant \sum_{\rho=1}^{s} \sum_{i_1,\ldots,i_\rho} \frac{1}{n^{3\rho}} = \sum_{\rho=1}^{s} \frac{C_n^\rho}{n^{3\rho}} \leqslant \sum_{\rho=1}^{s} \frac{1}{n^{2\rho}} \leqslant \sum_{\rho=1}^{s} \frac{1}{n^2} \leqslant \frac{1}{n} < 1.$$

Лемма доказана.

Отметим, что среднее значение, рассмотренное при доказательстве леммы, оказалось не только меньшим единицы, но и бесконечно малым при $n \to \infty$. Это означает (в нашем стандартном смысле), что почти всякий вектор $\mathbf{a} \in \mathcal{V}$ задает центрировку, относительно которой октаэдр допустим. И как же трудно такой вектор найти...

Задачи

31. С помощью теоремы Минковского аккуратно докажите теорему Дирихле (см. § 8.2).

32. С помощью теоремы Минковского докажите обобщение теоремы Дирихле — так называемую теорему Кронекера: *для любых иррациональных чисел* $\alpha_1, \ldots, \alpha_s$ *существует бесконечно много различных дробей* $\frac{p_1}{q}, \ldots, \frac{p_s}{q}$, *с которыми выполнено* $\max\limits_{i=1,\ldots,s} \left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+1/s}}$.

33. а) Докажите, что $d_n \geqslant n - c \log_2 n$, $c > 0$.

б*) Докажите, что $d_n \geqslant n - c\dfrac{\log_2 n}{\log_2 \log_2 n}$, $c > 0$.

в*) Докажите, что $d_n \leqslant n - c$, $c > 0$.

г**) Найдите порядок роста величины $n - d_n$.

34**. Пусть $\mathbf{a}_1, \ldots, \mathbf{a}_t$ — векторы с рациональными координатами, лежащие в $\mathbb{R}^n$. Рассмотрим решетку $\Lambda_{\mathbf{a}_1,\ldots,\mathbf{a}_t}$, которая состоит из всевозможных векторов вида $\mathbf{x} = c_1\mathbf{a}_1 + \ldots + c_t\mathbf{a}_t + \mathbf{b}$, где $c_1, \ldots, c_t \in \mathbb{Z}$, а $\mathbf{b} \in \mathbb{Z}^n$. Положим $d_{n,t} = \max\limits_{\Lambda_{\mathbf{a}_1,\ldots,\mathbf{a}_t}} d(\mathcal{O}; \Lambda_{\mathbf{a}_1,\ldots,\mathbf{a}_t})$. Найдите точные оценки для величины $d_{n,t}$.

35**. Верно ли, что если рациональный вектор $\mathbf{a}$ таков, что октаэдр $\mathcal{O}$ допустим относительно центрировки $\Lambda_{\mathbf{a}}$, а совокупность $\mathcal{M}$ из п. 8.4.1 такова, что $\tau(\mathcal{M}) \geqslant c_1 \dfrac{n}{\ln n}(\ln \ln n)^2$, $c_1 > 0$, то эта совокупность равномерно расположена в $\mathcal{R}_n$ с какой-либо константой $c_2 > 0$? Иными словами, принципиально ли условие равномерной расположенности в доказательстве теоремы 8.3.2, или же оно носит лишь технический характер «помощника» при проведении усреднения?

Глава 9

Дополнение: системы различных представителей и их приложения в комбинаторной геометрии

В этой главе мы обсудим весьма важный специальный тип с. о. п. — системы различных представителей. Кроме того, мы поговорим об одном из многих применений таких систем, а именно об их применении к известной проблеме Эрдёша—Секереша в комбинаторной геометрии.

§ 9.1. Формулировки основной теоремы

Пусть, как обычно, дана совокупность подмножеств $\mathcal{M} = \{M_1, \ldots, M_s\}$ множества $\mathcal{R}_n$, $|M_i| = k_i$ при любом i. Назовем произвольную с. о. п. S для $\mathcal{M}$ ее *системой различных представителей* (*с. р. п.*), если $S = \{\nu_1, \ldots, \nu_s\}$ и $\nu_1 \in M_1, \ldots, \nu_s \in M_s$. Иными словами, мы более не стремимся выбрать *наименьшую* «команду для олимпиады»; нам хочется теперь, чтобы, напротив, каждый игрок отвечал за какую-то одну специальность, за ним и только за ним закрепленную. Таким образом, результаты задач 3 а и 4 мы как бы «детривиализуем»: тот факт, что для совокупности $\mathcal{M}$ имеется с. о. п. мощности не больше s, в сущности, тривиален; а вот пойди разберись, есть ли у $\mathcal{M}$ с. о. п. размера в точности s!

В 1935 г. с последней задачей разобрался-таки Ф. Холл. Он доказал следующий критерий существования с. р. п.

Теорема 9.1.1. *Данная совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$ обладает с. р. п. тогда и только тогда, когда для каждого $t \in \{1, \ldots, s\}$ объединение любых t множеств $M_{i_1}, \ldots, M_{i_t} \in \mathcal{M}$ имеет мощность не меньше t.*

Более или менее очевидно, что если данная совокупность обладает с. р. п., то выполнено свойство из формулировки теоремы. Обратное утверждение требует для своего обоснования некоторых усилий. Поскольку в замечательной книге [41] эти усилия уже предприняты, мы не станем повторять «подвига» ее автора и отошлем читателя к указанному источнику. Нам будут более интересны приложения теоремы 9.1.1.

Одним из самых известных приложений является теорема Д. Кёнига, которая, по сути, равносильна теореме Ф. Холла. В этом смысле речь идет

даже не о приложении как таковом, а о переформулировке результата, о «вариации» на его тему. Теорема Кёнига относится к теории графов (см. [40]), и потому мы напомним несколько определений из этой теории.

Графом называется пара $G = (V, E)$ (ср. § 7.1), где V — некоторое (как правило, конечное) множество, а E — любая совокупность его двухэлементных подмножеств. При этом порядок элементов в «парах» из E значения не имеет, совпадающих пар в E нет и пары вида (v, v) мы к рассмотрению не допускаем. Элементы множества V называются *вершинами* графа, элементы E — его *ребрами*. Определим *паросочетание* в графе G как произвольный набор ребер этого графа, никакие два из которых не имеют общей вершины (см. рис. 26). Скажем, что граф *двудолен*, если множество его вершин можно так разделить на две части («доли») V_1, V_2, чтобы каждое его ребро имело вид (v_1, v_2), где $v_1 \in V_1$, $v_2 \in V_2$. Иначе говоря, граф двудолен, если его вершины можно так покрасить в два цвета, чтобы все его ребра оказались неодноцветными (см. рис. 27).

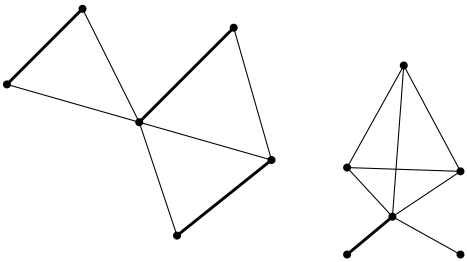

Рис. 26

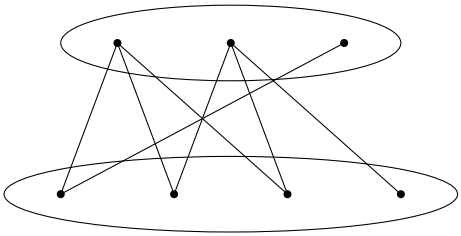

Рис. 27

Пусть $\alpha(G) = \tau(E)$ — размер минимальной с. о. п. для совокупности ребер E. Пусть, кроме того, $\beta(G)$ — размер (любого) самого «мощного» паросочетания в G. Вот результат, полученный Кёнигом.

Теорема 9.1.2. *Для двудольного графа справедливо тождество* $\alpha(G) = \beta(G)$.

Не правда ли, удивительные сплетения сюжетов? Минимальная с. о. п. для совокупности ребер графа ищется, так сказать, за счет неких с. р. п. Мы не станем доказывать и теорему 9.1.2, по-прежнему отсылая читателя к книге [41], а также к книге [40].

В следующих двух параграфах мы обсудим куда менее известные приложения теоремы 9.1.1, и речь пойдет о двух классических задачах комбинаторной геометрии, предложенных П. Эрдёшом и Д. Секерешом.

§ 9.2. О двух проблемах Эрдёша—Секереша

Скажем, что множество точек на плоскости *находится в общем положении*, если никакие три его элемента не лежат на одной прямой. В 1935 г. Эрдёш и Секереш вслед за Э. Кляйн задались вопросом: при всяком ли $n \in \mathbb{N}$, $n \geqslant 3$, существует такое N, что из любых $M \geqslant N$ точек на плоскости, находящихся в общем положении, можно выбрать n точек, являющихся вершинами выпуклого n-угольника? Тогда же Эрдёш и Секереш показали, что ответ на поставленный вопрос положительный. Доказательство этого замечательного факта можно найти в книге [41].

В соответствии со сказанным выше разумно ввести величину $g(n)$, равную минимуму из всех N, для которых выполнено условие Эрдёша—Секереша. Первая проблема Эрдёша—Секереша состоит в отыскании $g(n)$. Сейчас известно лишь, что

$$2^{n-2} + 1 \leqslant g(n) \leqslant C_{2n-5}^{n-2} = (4 + o(1))^n.$$

Авторы проблемы сразу же высказали гипотезу о том, что правильной является нижняя оценка. Эта гипотеза доказана лишь при $n \leqslant 6$.

Вторая проблема Эрдёша—Секереша очень близка к первой. Вопрос почти дословно повторяется: при всяком ли $n \in \mathbb{N}$, $n \geqslant 3$, существует такое N, что из любых $M \geqslant N$ точек на плоскости, находящихся в общем положении, можно выбрать n точек, являющихся вершинами выпуклого и *пустого* n-угольника? Минимальная (казалось бы) оговорка состоит в предвнесении дополнительного свойства «пустоты» искомого многоугольника. Подразумевается, что этот многоугольник не должен содержать внутри себя ни одной точки исходного множества (на границе точек этого множества, отличных от вершин, заведомо не будет ввиду условия общности положения). Обозначим через $h(n)$ аналог величины $g(n)$ применительно ко второй проблеме Эрдёша—Секереша.

Любопытно, что величина $h(n)$ устроена принципиально не так, как ее предшественница. А именно, уже при $n \geqslant 7$ она бесконечна. Правда, верно

и то, что

$$h(3) = g(3) = 3, \quad h(4) = g(4) = 5.$$

Первое небольшое отличие возникает лишь при $n = 5$:

$$h(5) = 10 \neq 9 = g(5).$$

А вот про $n = 6$ долгое время вообще ничего известно не было. Разве что оценку $h(6) \geqslant 30$ доказали. И только в 2006 г. Т. Геркен показал, что $h(6) \leqslant g(9) \leqslant 1717$. Год спустя результат Геркена значительно усилил В. А. Кошелев, которому удалось получить неравенство

$$h(6) \leqslant \min\{g(8), 400\} \leqslant 463.$$

Рассуждение Кошелева занимает больше пятидесяти страниц, и один из его маленьких, но важных кусочков опирается на теорему 9.1.1. Мы обсудим это в следующем параграфе.

Заметим, что с более подробной и красочной историей проблем и их окрестностей можно ознакомиться по недавнему обзору [55]. Стоит подчеркнуть, однако, что даже там еще нет информации о работах Геркена (см. [51]) и Кошелева (см. [14]). Зато она есть популярных статьях [30, 31].

§ 9.3. Применение с. р. п. к частному случаю второй проблемы Эрдёша—Секереша

Итак, наше цель — отыскание выпуклых и пустых шестиугольников в множествах точек на плоскости, находящихся в общем положении. Пусть $\mathcal{X}$ — одно из таких множеств и $|\mathcal{X}| \geqslant g(8)$. Тогда в $\mathcal{X}$ есть выпуклые восьмиугольники (т. е. восьмерки точек, являющихся вершинами выпуклых восьмиугольников). Рассмотрим любой такой восьмиугольник, который к тому же минимален в том смысле, что внутри него нет других аналогичных восьмиугольников. Обозначим сам этот восьмиугольник через $\mathcal{H}'$, а множество его вершин через $\mathcal{H}$. Внутри $\mathcal{H}'$ есть (возможно) еще какие-то точки множества $\mathcal{X}$. Пусть многоугольник $\mathcal{I}'$ представляет собой их выпуклую оболочку (см. п. 6.2.1); соответственно, $\mathcal{I}$ — множество его вершин. Конечно, $|\mathcal{I}|$ вполне может оказаться равной одному или двум, и тогда $\mathcal{I}'$ — не совсем, скажем так, многоугольник, но для нас это неважно.

Внутри $\mathcal{I}'$ найдем (быть может) еще один «слой» (для этого необходимо выполнение неравенства $|\mathcal{I}| \geqslant 3$). Назовем его $\mathcal{J}'$ (с множеством вершин $\mathcal{J}$). Продолжим этот процесс. Образуется последовательность вложенных многоугольников, пример которой изображен на рис. 28.

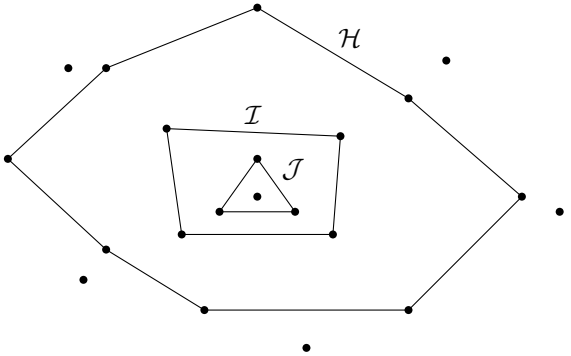

Рис. 28

Мы рассмотрим частный случай, когда $|\mathcal{I}| = 5$, $|\mathcal{J}| = 3$, а больше ничего и нет (см. рис. 29). Назовем полученную конструкцию *конфигурацией вида*$(8, 5, 3)$, а внутренние пятиугольник с треугольником — *подконфигурацией вида*$(5, 3)$.

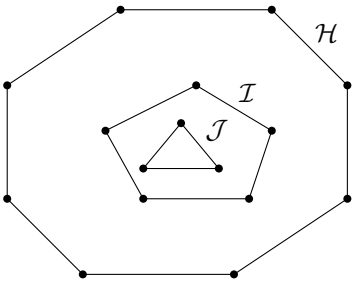

Рис. 29

Покажем, что если $\mathcal{X}$ содержит упомянутую конфигурацию, то в $\mathcal{X}$ есть выпуклый и пустой шестиугольник.

В своей работе [51] Геркен доказал некое утверждение, частный случай которого мы, не обосновывая его, приводим ниже.

Утверждение 9.3.1. *Предположим, что в данной конфигурации вида* $(8, 5, 3)$ *подконфигурация вида* $(5, 3)$ *выпуклых и пустых шестиугольников не содержит. Тогда в той полуплоскости относительно прямой* AB, *которая не включает в себя треугольник* ABC, *обязательно найдется хотя бы одна сторона пятиугольника*

$PQRST$; то же самое верно и для прямых BC и CD: они как бы «отделяют» от треугольника, через стороны которого проходят, по крайней мере две последовательные точки из множества $\{P, Q, R, S, T\}$ (см. рис. 30). Более того, если посмотреть на множества $\mathcal{T}_{AB}$, $\mathcal{T}_{BC}$, состоящие из сторон пятиугольника $PQRST$, которые отделены от треугольника ABC прямыми AB и BC соответственно (мы уже знаем, что $|\mathcal{T}_{AB}| \geqslant 1$ и $|\mathcal{T}_{BC}| \geqslant 1$), то окажется, что в их объединении находится не менее двух сторон пятиугольника; та же картина имеет место и для множеств $\mathcal{T}_{BC}$, $\mathcal{T}_{CA}$, и для множеств $\mathcal{T}_{CA}$, $\mathcal{T}_{AB}$, определение которых очевидно.

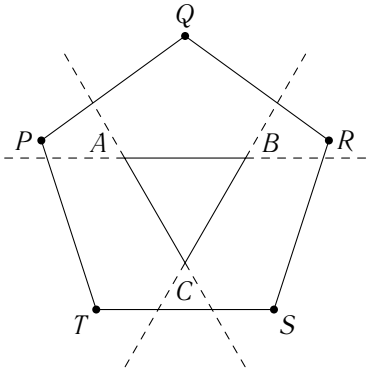

Рис. 30

Что же означает утверждение? А вот что: либо в подконфигурации вида (5, 3) данной конфигурации вида (8, 5, 3), найденной нами в исходном множестве $\mathcal{X}$, есть выпуклый и пустой шестиугольник, и тогда сразу все в порядке, либо, коль скоро такого шестиугольника нет, у нас возникает дополнительная информация о взаимном расположении сторон пятиугольника и сторон треугольника. Отметим, что эта информация не появилась бы, не предположи мы с самого начала, что восьмиугольник в известной конфигурации минимален.

Итак, что же будет, если удача нам тотчас же не улыбнулась и в подконфигурации вида (5, 3) пустых шестиугольников не оказалось? Рассмотрим множества $\mathcal{T}_{AB}$, $\mathcal{T}_{BC}$, $\mathcal{T}_{CA}$. В силу утверждения получаем

$$|\mathcal{T}_{AB}| \geqslant 1, \quad |\mathcal{T}_{BC}| \geqslant 1, \quad |\mathcal{T}_{CA}| \geqslant 1,$$
$$|\mathcal{T}_{AB} \cup \mathcal{T}_{BC}| \geqslant 2, \quad |\mathcal{T}_{BC} \cup \mathcal{T}_{CA}| \geqslant 2, \quad |\mathcal{T}_{CA} \cup \mathcal{T}_{AB}| \geqslant 2.$$

Нетрудно также проверить, что

$$|\mathcal{T}_{AB} \cup \mathcal{T}_{BC} \cup \mathcal{T}_{CA}| \geqslant 3.$$

Ничего не напоминает? Да ведь это в точности условия теоремы 9.1.1, примененной к совокупности, которая состоит из множеств $\mathcal{T}_{AB}$, $\mathcal{T}_{BC}$, $\mathcal{T}_{CA}$. Значит, имеется с. р. п., образованная сторонами $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{L}_3$ пятиугольника $PQRST$. Сопоставим стороне AB треугольника ABC сторону $\mathcal{L}_1$, стороне BC — сторону $\mathcal{L}_2$ и стороне CA — сторону $\mathcal{L}_3$. Всякий раз сторона $\mathcal{L}_i$ «отделяется» в стандартном смысле от треугольника прямой, проходящей через его соответствующую сторону (см. рис. 31).

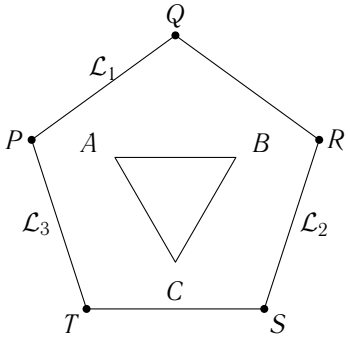

Рис. 31

Рассмотрим выпуклые четырехугольники, которые ввиду описанного выше соответствия корректно «натягиваются» на пары отрезков $(AB, \mathcal{L}_1)$, $(BC, \mathcal{L}_2)$ и $(CA, \mathcal{L}_3)$; «продолжим» эти четырехугольники до бесконечности так, как это изображено на рис. 32. Возникнут области, которые Геркен и Кошелев называют «4-секторами». Эти области покроют часть плоскости вне пятиугольника. Оставшуюся часть плоскости мы покроем двумя «3-секторами» (см. рис. 33). Существование такого покрытия

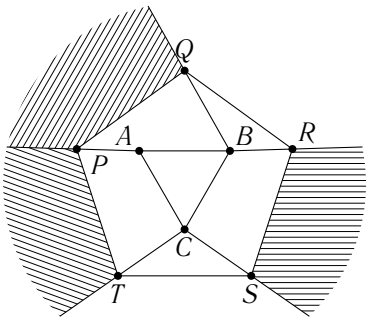

Рис. 32

отныне очевидно, и главную роль в его обосновании сыграла, конечно, теорема Холла.

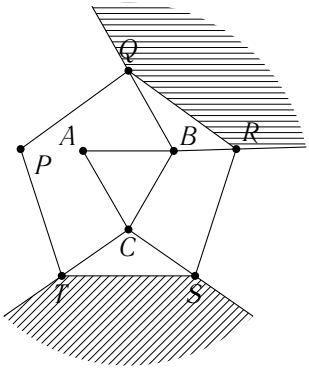

Рис. 33

Вспоминаем, что вершины восьмиугольника в исходной конфигурации вида (8, 5, 3) обязаны располагаться «снаружи» пятиугольника, т. е. какие-то из них должны попасть в 4-секторы, а какие-то — в 3-секторы.

Допустим, в тот или иной 4-сектор попали две вершины восьмиугольника. Отлично: выпуклый и пустой шестиугольник нам обеспечен (см. рис. 34). Предположим, что в одном из двух 3-секторов лежат три вершины восьмиугольника. Тогда опять все в порядке (см. рис. 35). Пусть, наконец, в каждом 3-секторе находится не более двух вершин, а в каждом 4-секторе — не более одной вершины восьмиугольника. Но это нонсенс, ведь $3 \cdot 1 + 2 \cdot 2 = 7 < 8$. Таким образом, в конфигурации вида (8, 5, 3) (а стало быть, и в первоначальном множестве $\mathcal{X}$) выпуклый и пустой шестиугольник непременно отыщется, и наша цель достигнута.

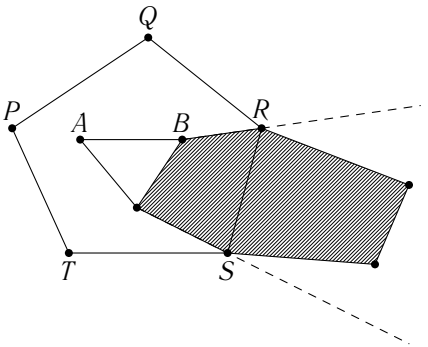

Рис. 34

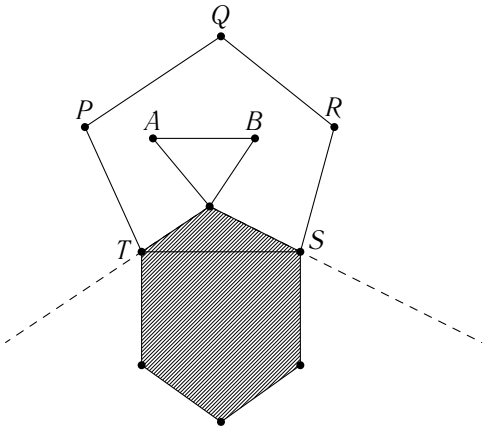

Рис. 35

Подчеркнем еще раз, что центральным моментом в доказательстве было построение покрытия «подозрительной» части плоскости 3- и 4-секторами. Это построение оказалось возможным лишь благодаря теореме об с. р. п.

Задачи

36. По аналогии с понятиями конфигурации вида (8, 5, 3) и подконфигурации вида (5, 3) введите понятия конфигурации вида (8, 6, 5) и подконфигурации вида (6, 5). Попробуйте сформулировать аналог утверждения 9.3.1 в новой ситуации. С помощью этого аналога и теоремы Холла постройте покрытие плоскости 3- и 4-секторами и докажите, как следствие, что в любом множестве $\mathcal{X} \subset \mathbb{R}^2$, которое находится в общем положении и содержит в себе конфигурацию вида (8, 6, 5), обязательно есть выпуклый и пустой шестиугольник.

Литература

1. *Болтянский В. Г.*, *Гохберг И. Ц.* Теоремы и задачи комбинаторной геометрии. М.: Наука, 1965.
2. *Боровков А. А.* Математическая статистика. Оценка параметров. Проверка гипотез. М.: Наука, 1984.
3. *Виленкин Н. Я.* Комбинаторика. М.: Наука, 1969.
4. *Виноградов И. М.* Основы теории чисел. М.; Ижевск: РХЛ, 2003.
5. *Вороной Г. Ф.* Собрание сочинений: В 3 т. Киев, 1952—1953.
6. *Галочкин А. И.*, *Нестеренко Ю. В.*, *Шидловский А. Б.* Введение в теорию чисел. М.: Изд-во МГУ, 1995.
7. *Гельфонд А. О.* Исчисление конечных разностей. М.: Наука, 1967.
8. *Гнеденко Б. В.* Курс теории вероятностей. М.: Физматлит, 1961.
9. *Данцер Л.*, *Грюнбаум Б.*, *Кли В.* Теорема Хелли. М.: Мир, 1968.
10. *Карацуба А. А.* Основы аналитической теории чисел. М.: УРСС, 2004.
11. *Касселс Дж.* Введение в теорию диофантовых приближений. М.: ИЛ, 1961.
12. *Касселс Дж.* Введение в геометрию чисел. М.: Мир, 1965.
13. *Конвей Дж.*, *Слоэн Н.* Упаковки шаров, решетки и группы. М.: Мир, 1990.
14. *Кошелев В. А.* О проблеме Эрдёша—Секереша // Доклады РАН. 2007. Т. 415, №6. Р. 734—736.
15. *Кузюрин Н. Н.* Асимптотическое исследование задачи о покрытии // Проблемы кибернетики. 1980. № 37. С. 19—56.
16. *Ленг С.* $SL_2(\mathbb{R})$. М.: Мир, 1977.
17. *Леман Э.* Теория точечного оценивания. М.: Наука, 1991.
18. *Прахар К.* Распределение простых чисел. М.: Мир, 1967.
19. *Райгородский А. М.* Дефект допустимых шаров и октаэдров в решетке и системы общих представителей // Матем. сборник. 1998. Т. 189, № 6. С. 117—141.
20. *Райгородский А. М.* Системы общих представителей // Фунд. и прикл. мат. 1999. Т. 5, № 3. С. 851—860.
21. *Райгородский А. М.* Вероятностный подход к задаче о дефектах допустимых множеств в решетке // Матем. заметки. 2000. Т. 68, № 6. Р. 910—916.
22. *Райгородский А. М.* Проблема Борсука и хроматические числа некоторых метрических пространств // Успехи матем. наук. 2001. Т. 56, № 1. Р. 107—146.
23. *Райгородский А. М.* Хроматические числа. М.: МЦНМО, 2003.
24. *Райгородский А. М.* Проблемы Борсука и Грюнбаума для решетчатых многогранников // Известия РАН. 2005. Т. 69, № 3. Р. 96—121.
25. *Райгородский А. М.* Проблема Борсука. М.: МЦНМО, 2006.

26. *Райгородский А. М.* Вокруг гипотезы Борсука // Итоги науки и техники. 2007. (Серия «Современные проблемы математики и ее приложения»; Т. 23). С. 147—164.
27. *Райгородский А. М.* Линейно-алгебраический метод в комбинаторике. М.: МЦНМО, 2007.
28. *Райгородский А. М.* Вероятность и алгебра в комбинаторике. М.: МЦНМО, 2008.
29. *Райгородский А. М.* Остроугольные треугольники Данцера—Грюнбаума. М.: МЦНМО, 2009.
30. *Райгородский А. М.*, *Кошелев В. А.* Задача Эрдёша—Секереша о выпуклых многоугольниках — I // Квант. 2009. № 2. С. 6—13.
31. *Райгородский А. М.*, *Кошелев В. А.* Задача Эрдёша—Секереша о выпуклых многоугольниках — II // Квант. 2009. № 4.
32. *Севастьянов Б. А.* Курс теории вероятностей и математической статистики. Ижевск: Ин-т компьютерных исследований, 2004.
33. *Сойфер А.* Хроматическое число плоскости: его прошлое, настоящее и будущее // Мат. просвещение. 2004. Вып. 8.
34. *Тараканов В. Е.* Комбинаторные задачи и (0, 1)-матрицы. М.: Наука, 1985.
35. *Ширяев А. Н.* Вероятность. М.: Наука, 1989.
36. *Шмидт В.* Диофантовы приближения. М.: УРСС, 1983.
37. *Феллер В.* Введение в теорию вероятностей и ее приложения. М.: Мир, 1967.
38. *Фельдман Н. И.* Седьмая проблема Гильберта. М.: Изд-во МГУ, 1982.
39. *Фихтенгольц Г. М.* Курс дифференциального и интегрального исчисления. М.; Ижевск: Физматлит, 2003.
40. *Харари Ф.* Теория графов. М.: Мир, 1973.
41. *Холл М.* Комбинаторика. М.: Мир, 1970.
42. *Чандрасекхаран К.* Арифметические функции. М.: Наука; Физматлит, 1975.
43. *Шидловский А. Б.* Трансцендентные числа. М.: Наука, 1987.
44. *Эрдёш П.*, *Спенсер Дж.* Вероятностные методы в комбинаторике. М.: Мир, 1976.
45. *Aigner M.*, *Ziegler G. M.* Proofs from THE BOOK. Berlin: Springer-Verlag, 1998.
46. *Alon N.*, *Spencer J.* The probabilistic method, Wiley — Interscience Series in Discrete Math. and Optimization, Second Edition, 2000. (Имеется русский перевод: *Алон Н.*, *Спенсер Дж.* Вероятностный метод. М.: Бином. Лаборатория знаний, 2007.)
47. *Boltyanski V. G.* H. Martini and *Soltan P. S.* Excursions into combinatorial geometry. Berlin: Universitext, Springer, 1997.
48. *Boros E.*, *Caro Y.* *Füredi Z.*, *Yuster R.* Covering non-uniform hypergraphs // J. of Combinatorial Theory. Ser. B. 2001. V. 82. № 2. С. 270—284.
49. *Brass P.*, *Moser W.*, *Pach J.* Research problems in discrete geometry. Springer, 2005.

50. *Füredi Z.* Turán's type problems, Surveys in Combinatorics, Proc. of the 13th British Combin. Conference / Ed. A. D. Keedwell, Cambridge Univ. Press, London Math. Soc. Lecture Note Series. 1991. V. 166. P. 253—300.
51. *Gerken T.* On empty convex hexagons in planar point set // Discrete Comput. Geom. в печати; on-line: `http://www.springerlink.com/content/h04hr51082j7u4k8/fulltext.pdf`.
52. *Gruber P. M.*, *Lekkerkerker C. G.* Geometry of numbers. Amsterdam: North-Holland, 1987. (Имеется русский перевод: *Грубер П. М. Леккеркеркер К. Г.* Геометрия чисел. М.: Наука, 2008.)
53. *Klee V.*, *Wagon S.* Old and new unsolved problems in plane geometry and number theory // Math. Association of America. 1991.
54. *Minkowski H.* Geometrie der Zahlen // Lfg. 1—2. Lpz, 1896—1910.
55. *Morris W.*, *Soltan V.* The Erdős—Szekeres problem on points in convex position // Bulletin (new series) of the Amer. Math. Soc. 2000. V. 37. № 4. P. 437—458.
56. *Pach J.*, *Agarwal P. K.* Combinatorial geometry. New York: John Wiley and Sons Inc., 1995.
57. *Raigorodskii A. M.* The Borsuk partition problem: the seventieth anniversary // Mathematical Intelligencer. 2004. V. 26, № 4. P. 4—12.
58. *Raigorodskii A. M.* On a problem of the geometry of numbers // Труды Института Математики НАН Беларуси. 2007. Т. 15, № 1. С. 111—117.
59. *Ziegler G. M.* Lectures on 0/1 — polytopes // Polytopes — Combinatorics and Computation / Eds. G. Kalai and G. M. Ziegler. DMV — seminar. V. 29. Birkhäuser: Verlag Basel, 2000. P. 1—44.
60. *Ziegler G. M.* Coloring Hamming graphs, optimal binary codes, and the0/1 — Borsuk problem in low dimensions // Lect. Notes Comput. Sci. 2001. V. 2122. P. 159—171.

Андрей Михайлович Райгородский

СИСТЕМЫ ОБЩИХ ПРЕДСТАВИТЕЛЕЙ В КОМБИНАТОРИКЕ
И ИХ ПРИЛОЖЕНИЯ В ГЕОМЕТРИИ

Подписано в печать 3.07.2009 г. Формат $60 \times 90\ 1/16$. Бумага офсетная.
Печать офсетная. Печ. л. 8,5. Тираж 800 экз. Заказ № .

Издательство Московского центра
непрерывного математического образования.
119002, Москва, Большой Власьевский пер., д. 11. Тел. (499) 241–74–83

Отпечатано с готовых диапозитивов в ООО «Типография „САРМА“»

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. (499) 241–72–85. E-mail: biblio@mccme.ru