

А. М. Райгородский

Линейно-алгебраический метод в комбинаторике

Москва
Издательство МЦМНО
2007

УДК 519.1
ББК 22.15
P18

Райгородский А. М.

P18 Линейно-алгебраический метод в комбинаторике. — М.: МЦНМО, 2007. — 136 с.

ISBN 987-5-94057-313-5

Современная комбинаторика — это весьма многогранная и активно развивающаяся область математики. В XX веке был разработан ряд мощных методов, позволяющих решать многие трудные задачи комбинаторики. Среди этих методов особое место занимает линейно-алгебраический метод. С его помощью удалось добиться прорыва в таких классических проблемах, как, например, проблема Борсука о разбиении множеств на части меньшего диаметра. В книге излагаются основы метода и описываются наиболее яркие примеры его применения. Для понимания материала достаточно знания элементарных понятий линейной алгебры и математического анализа. Книга будет полезна студентам и аспирантам, интересующимся комбинаторным анализом, а также специалистам в области дискретной математики.

ББК 22.15

Райгородский Андрей Михайлович

ЛИНЕЙНО-АЛГЕБРАИЧЕСКИЙ МЕТОД В КОМБИНАТОРИКЕ

ISBN 987-5-94057-313-5

© Райгородский А. М., 2007,
© МЦНМО, 2007.

Оглавление

1. Введение	5
2. Задачи о пересечениях конечных множеств	8
2.1. Немного истории и формулировка теоремы Франкла—Уилсона	8
2.2. Доказательство теоремы Франкла—Уилсона	10
2.3. Точность теоремы Франкла—Уилсона и ее неожиданность	15
2.4. Вокруг теоремы Франкла—Уилсона	18
3. Задачи о скалярных произведениях векторов	26
3.1. Постановка одной из задач и формулировка одного из результатов	26
3.2. Доказательство теоремы 9	29
3.3. Смысл оценки из теоремы 9	32
3.4. Точна ли теорема 9?	37
3.5. Вокруг теоремы 9	48
4. Применение полученных результатов в комбинаторной геометрии	56
4.1. Постановки основных задач	56
4.2. Задача Нельсона—Эрдёша—Хадвигера	60
4.3. Задача Борсука	69
4.4. О числах Борсука и Нельсона—Эрдёша—Хадвигера	76
4.5. О хроматических числах с несколькими запретами	80
4.6. Вокруг задачи Нельсона—Эрдёша—Хадвигера	86
5. Теория Рамсея	94
5.1. Круг задач и формулировка результата	94
5.2. Доказательство теоремы 17	101
6. Задача об отклонении	105
6.1. Постановка задачи и краткий исторический экскурс	105
6.2. Доказательство теоремы 20	108
6.3. Доказательство теоремы 21	111

6.4. Дополнение 1. «Свойство В» Эрдёша	115
6.5. Дополнение 2. Матрицы Адамара и проблема Борсука . .	116
7. Теорема Эрдёша—Гинзбурга—Зива и ее окрестности	125
7.1. Классический результат	125
7.2. Вспомогательные факты	127
7.3. Доказательство оценки Роньяи $f(n, 2) \leq 4n - 2$	129
7.4. Доказательство оценки Райхера $f(n, 2) \leq 4n - 3$	131
Литература	135

1 || Введение

Комбинаторика — один из наиболее увлекательных, многогранных и нетривиальных разделов современной математики. Имея множество приложений, она развивается настолько бурно, что даже простая попытка перечислить ее основные направления, по-видимому, обречена на провал. Десятки специализированных журналов ежемесячно публикуют сотни новых статей, каждый год выходят в свет монографии и учебники, и уследить за всем этим колоссальным потоком информации весьма нелегко. Вряд ли найдется человек, имеющий право заявить, что знает все последние достижения в комбинаторике.

В то же время многие из тех, кто не совсем хорошо ориентируется в области «дискретных» (т.е. в сущности комбинаторных) задач, полагают, что комбинаторика, так сказать, «не вполне научна». Считается, что если формулировки задач доступны школьнику, а объекты, с которыми приходится иметь дело, не требуют знания того, что такое интеграл Лебега или когомология, то и развивать соответствующую теорию незачем. При этом бытует мнение, что задачи в комбинаторике разрозненны и для их решения не существует единых содержательных подходов. Правда, иной раз вспоминают о методе производящих функций, который активно используется при перечислении различных объектов, — но и только. Такой взгляд, с одной стороны, способствует чрезмерной мифологизации комбинаторики — дескать, только гениям под силу решать «штучные» задачи-головоломки, — а с другой стороны, он ведет к возникновению пренебрежительного отношения к комбинаторным проблемам, которые якобы «олимпиадные» и в контекст «серьезных» исследований включены быть не могут. Действительно, постановка многих комбинаторных вопросов носит весьма олимпиадный характер, и известного рода изобретательность (если не изощренность) очень важна для успешной работы с ними.

И тем не менее, методология этой работы отнюдь не исчерпывается одним лишь методом производящих функций. В XX веке — веке наиболее активного развития комбинаторики и внедрения ее идей во всевозможные области знания (компьютерные технологии, биоинженерия и пр.) — был построен мощный аппарат, позволяющий эффективно бороться с комбинаторными трудностями.

Одновременно с быстрым ростом числа направлений и специальных проблем комбинаторики шло становление целых «наук в науке», группировавшихся вокруг общих методов, приводивших, в частности, к решению классических дискретных задач. Среди таких методов и вероятностный метод в комбинаторике, который сам заслуживает долгого и тщательного обсуждения, и *линейно-алгебраический* метод, вынесенный в название этой брошюры.

Казалось бы, какая может быть связь между комбинаторикой и весьма геометричной линейной алгеброй? Однако связь есть, и она удивительно глубока и красива. Мысль о том, что линейно-алгебраические факты можно увязать с фактами дискретной математики, как раз «олимпиадна». Нужно было обладать большим остроумием, чтобы породить ее. Некоторые наиболее яркие результаты, полученные с помощью линейно-алгебраического метода, кажутся на первый взгляд и вовсе невероятными.

Знаменитый венгерский математик Поль Эрдёш, благодаря которому современная комбинаторика в значительной степени выглядит такой, какой мы ее знаем, заявлял даже, что подобные результаты хранятся в некоей особой божественной Книге. Эрдёш, разумеется, шутил, но результаты эти настолько изящны, что «Книгу» (или часть ее) недавно издали, и она уже переведена на несколько различных языков (см. [1]). Впрочем, для нас главное — это наличие метода и тонких фактов, установленных за счет него.

В этой брошюре рассматривается несколько наиболее популярных и интересных задач комбинаторики, решаемых с помощью линейной алгебры. Среди решений рассмотрены и те, что удостоились упоминания в «Книге», и другие. Наша цель — через призму этих удивительных задач и решений увидеть суть общего метода, его многоплановость и перспективность. Мы должны понять, что комбинаторика — это в первую очередь красивая *наука* и что задачи ее можно и стоит решать. Например, посредством линейно-алгебраического метода.

Завершая введение, скажем несколько слов о структуре книги. В книге семь глав, каждая из которых посвящена какой-нибудь известной задаче комбинаторики, решаемой с помощью того или иного варианта линейно-алгебраического метода. Основные результаты формулируются в виде теорем; однако приводятся и менее значимые утверждения, называемые в тексте предложениями, а также доказывается ряд вспомогательных фактов (лемм).

Всего в книге 26 теорем. Теоремы 1–8, 17, 19, 21–26 именные, и их авторство указано в заголовках теорем. Теоремы 18 и 20 безымянные. Будучи глубокими, но не слишком трудными, они давно вошли в ма-

тематический фольклор, и установить, кому они принадлежат, мы не можем. Теоремы 9—15 доказаны автором этой книги; в их заголовках мы также информацию об авторстве опускаем. Чуть сложнее ситуация с теоремой 16. В ней содержится серия результатов. Некоторые из них совсем простые, некоторые, напротив, именные, некоторые опять-таки принадлежат автору этой книги. В последнем случае мы снова ничего не указываем в заголовках соответствующего пункта теоремы. В конце каждой главы есть задачи. Иногда они сводятся к доказательству известного утверждения. В этом случае мы пишем в скобках имя его автора.

2

Задачи о пересечениях конечных множеств

2.1. Немного истории и формулировка теоремы Франкла—Уилсона

Ответ на следующий вопрос многие знают еще со школы — как раз из олимпиадной деятельности. Пусть \mathcal{R}_n — некоторое конечное множество, состоящее из n различных элементов. Например, мы можем считать, что $\mathcal{R}_n = \{1, \dots, n\}$. Рассмотрим в \mathcal{R}_n произвольную совокупность трехэлементных подмножеств (сочетаний) $\mathcal{M} = \{M_1, \dots, M_s\}$, обладающую таким свойством: $|M_i \cap M_j| \neq 1$ для любых несовпадающих индексов $i, j \in \{1, \dots, s\}$. Здесь «модуль» множества — это его мощность, и, в частности, $|M_i| = 3$ для каждого $i \in \{1, \dots, s\}$, в то время как $|\mathcal{M}| = s$ (совокупность — это ведь тоже множество, элементы которого суть M_i). Понятно, что заведомо $s \leq C_n^3$. Однако на элементы совокупности \mathcal{M} (3-сочетания в \mathcal{R}_n) наложено дополнительное ограничение, состоящее в том, что никакие два из них не могут иметь в пересечении ровно один общий элемент. Разумеется, далеко не всякая совокупность \mathcal{M} подчиняется указанному ограничению, и, стало быть, возникает обещанный вопрос: *а насколько большой может оказаться величина $s = |\mathcal{M}|$ в сделанных предположениях?* Вопрос этот совершенно типичен для так называемой *экстремальной комбинаторики* (ищутся экстремальные значения тех или иных комбинаторных характеристик), и в естественности его усомниться трудно. Впрочем, любые сомнения отпадут позже, когда мы не только изучим общую проблематику подобного рода, но и приведем красивые приложения соответствующих результатов в геометрии.

Итак, как мы уже говорили, ответ на поставленный вопрос многим известен. Те же, кто с ним еще не знаком, вполне способны обосновать его самостоятельно. Посему мы лишь приведем его формулировку, а доказательство оставим за читателем. Заметим только, что проще всего воспользоваться стандартным методом математической индукции. Кстати, именно так действовал венгерский математик Жигмунд Надь, который и был, по-видимому, автором следующего утверждения, полученного им в 60-е годы прошлого века.

Теорема 1 (Ж. Надь). *Если в совокупности \mathcal{M} , состоящей из трехэлементных подмножеств множества \mathcal{R}_n , никакие два множества не пересекаются в точности по одному общему элементу, то $s = |\mathcal{M}| \leq n'$, где*

$$\begin{aligned} n' &= n && \text{при } n = 4k, \\ n' &= n - 1 && \text{при } n = 4k + 1, \\ n' &= n - 2 && \text{при } n = 4k + 2 \text{ и } n = 4k + 3. \end{aligned}$$

Конечно, k принимает в теореме любые натуральные значения. Имеется в виду попросту, что остаток от деления числа n на 4 может оказаться нулем, единицей, двойкой или тройкой. В зависимости от этого остатка и находится величина оценки в теореме. В дальнейшем же мы будем использовать обозначения, принятые в теории чисел: $n \equiv i \pmod{p}$ (читается « n сравнимо с i по модулю p ») означает, что $n - i$ делится на p или, в терминах теоремы 1, $n = pk + i$ (i — остаток от деления n на p).

С одной стороны, замечательно то, что теорема неулучшаема. Иными словами, для каждого n ничего не стоит построить совокупность \mathcal{M} , обладающую всеми нужными свойствами и, тем не менее, содержащую в аккурат n' элементов (проделайте это!). С другой стороны, разочаровывает то, что мы как бы сами себе противоречим: вроде бы, во введении мы заявляли, что комбинаторика не есть чисто олимпиадная дисциплина и что задачи в ней не решаются одними «изысканными», олимпиадными методами; однако налицо обратная ситуация, ведь мы сами признаем, что теорема 1 как раз относится к олимпиадной вотчине. Впрочем, довольно-таки очевиден тот факт, что постановка вопроса, исчерпывающий ответ на который мы только что привели, весьма специальна. Действительно, настоящая проблема, на которую лишь намекает теорема 1, куда как более общая, и сейчас мы к ней обратимся.

Опять-таки, пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ — это произвольная совокупность подмножеств (сочетаний) в \mathcal{R}_n . Однако теперь мы будем считать, что $|M_i| = k$, $i = 1, \dots, s$, где k — некоторое наперед заданное число. Более того, мы предположим, что при каком-нибудь фиксированном t , $0 \leq t \leq k$, выполнено условие $|M_i \cap M_j| \neq t$, $i \neq j \in \{1, \dots, s\}$. Обозначим через $m(n, k, t)$ величину $\max |\mathcal{M}|$, где максимум берется по всем совокупностям \mathcal{M} с указанными ограничениями. Ясно, что $m(n, 3, 1)$ — это число, изученное в теореме 1 Ж. Надем, и что работать с $m(n, k, t)$ в общем случае намного увлекательнее и труднее.

По-видимому первым, кто стал активно исследовать $m(n, k, t)$, был Поль Эрде́ш, которого мы упоминали во введении. Мы не станем вдаваться здесь в подробности «кустарного», так сказать, периода в истории проблемы отыскания величины $m(n, k, t)$ или хотя бы ее оценок. Заметим только, что проблема очень быстро сделалась крайне популярной. Ею занимались многие выдающиеся «дискретчики», но даже, скажем, при $k = 5$, $t = 2$ полного решения ее найти не удавалось. Что уж говорить о ситуациях, когда $k = k(n)$ и $t = t(n)$, например, $k = \lfloor n/2 \rfloor$, $t = \lfloor n/4 \rfloor$! И вот тут линейная алгебра пришла на помощь: в конце семидесятых — начале восьмидесятых годов XX века два великодушных «комбинатора» П. Франкл и Р. М. Уилсон разработали целый линейно-алгебраический метод, позволивший отыскать $m(n, k, t)$ при очень многих значениях параметров n, k, t .

Мы поступим следующим образом. Сперва сформулируем частный случай теоремы Франкла—Уилсона. Уже он будет исключительно нетривиален, и все изящество, всю глубину линейно-алгебраического подхода можно будет наблюдать в процессе его доказательства, которое мы проведем в п. 2.2. Затем в п. 2.3 мы еще раз убедимся в силе метода, установив, что результат, полученный с его помощью, не улучшаем. В то же время мы увидим там, насколько неожиданным и почти невероятным является этот результат. Наконец, в п. 2.4 мы дадим общую формулировку теоремы Франкла—Уилсона и постараемся развернуть панораму многочисленных результатов, которые возникли в связи с ней и около нее — в том числе (и в первую очередь) за счет линейно-алгебраического метода.

Итак, имеет место

Теорема 2 (П. Франкл и Р. М. Уилсон). Пусть p — некоторое простое число, $n = 4p$, $k = 2p$, $t = p$. Тогда

$$m(n, k, t) \leq 2C_{n-1}^{p-1}.$$

Повторим еще раз, что пока сформулирован лишь весьма специальный случай теоремы. Тем не менее уже он не может не производить впечатление (ср. п. 2.3). Правда, немного странным выглядит появление простого числа в формулировке, но оно там существенно, и в этом мы тоже потом убедимся.

2.2. Доказательство теоремы Франкла—Уилсона

Доказательство. Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ — это совокупность k -элементных подмножеств множества \mathcal{R}_n , где $k = 2p$, $n = 4p$, причем никакие два множества $M_i, M_j \in \mathcal{M}$ не пересекаются ровно по p

элементам из \mathcal{R}_n . Сперва мы применим простой технический трюк. Рассмотрим отдельно те множества из \mathcal{M} , которые содержат элемент $1 \in \mathcal{R}_n$, и отдельно — те множества, которые этот элемент не содержат. Таким образом, совокупность \mathcal{M} распадется на две непересекающиеся подсовокупности — скажем,

$$\mathcal{M}_1 = \{M \in \mathcal{M} : 1 \in M\}$$

и

$$\mathcal{M}_2 = \{M \in \mathcal{M} : 1 \notin M\}.$$

Если нам удастся показать, что $|\mathcal{M}_\nu| \leq C_{n-1}^{p-1}$, $\nu = 1, 2$, то утверждение теоремы 2 будет обосновано. На самом деле все равно, с какой из двух совокупностей работать в дальнейшем. Дабы не загромождать текст одинаковыми рассуждениями, мы проведем их во всех подробностях лишь для \mathcal{M}_2 . А уж разобраться с аналогичными выкладками для \mathcal{M}_1 заинтересованный читатель сможет без труда. К тому же так и метод будет понятнее. К нему мы теперь и перейдем.

Итак, мы можем считать отныне, что наша новая совокупность

$$\mathcal{N} = \mathcal{M}_2 = \{N_1, \dots, N_s\}$$

состоит из k -элементных подмножеств множества $\mathcal{R}_n \setminus \{1\}$, которое ничто не мешает нам отождествить с $\mathcal{R}_{n-1} = \{1, \dots, n-1\}$. При этом

$$|N_i \cap N_j| \neq p \quad \text{для любых } i, j \in \{1, \dots, s\}.$$

Нетривиальная идея, которую мы будем реализовывать, сводится к тому, чтобы k -элементным подмножествам \mathcal{R}_{n-1} сопоставить некоторую матрицу и векторное пространство размерности не более C_{n-1}^{p-1} , порожденное ее строками. Если нам удастся сделать это достаточно хитро, то затем мы сумеем так преобразовать нашу матрицу, что мощность совокупности \mathcal{N} окажется не превосходящей ранга новой матрицы, а он, в свою очередь, будет не выше размерности нашего векторного пространства, т. е. как раз ожидаемой нами величины C_{n-1}^{p-1} . В этом суть линейно-алгебраического метода, но как ее воплотить в жизнь? Ниже мы ответим на поставленный вопрос.

Пусть $A_1, \dots, A_{C_{n-1}^j}$ — это все возможные j -элементные подмножества, а $B_1, \dots, B_{C_{n-1}^i}$ — это все возможные i -элементные подмножества в \mathcal{R}_{n-1} . Будем считать, что $0 \leq i \leq j \leq n-1$, и потенциальное равенство нулю величин i и j никого не должно смущать: «ноль-элементные подмножества» какого-либо множества — это ровно одно его пустое подмножество, и мы просто доопределим значения биномиальных коэффициентов, полагая (стандартно) $C_m^0 = \frac{m!}{m!0!} = 1$ и, более

того, $C_m^l = 0$, коль скоро $l > m$, $m \geq 0$ (в частности, даже $C_0^0 = 1$, а, например, $C_3^5 = 0$).

Рассмотрим прямоугольную матрицу $\Lambda(i, j)$ размера C_{n-1}^i (число строк) на C_{n-1}^j (число столбцов), у которой (u, v) -й элемент $\lambda_{u,v}(i, j)$ равен единице, если $B_u \subseteq A_v$, и нулю в противном случае. Здесь индексы u и v меняются в естественных пределах:

$$1 \leq u \leq C_{n-1}^i, \quad 1 \leq v \leq C_{n-1}^j.$$

Понятно, что матрица $\Lambda(i, j)$ будет квадратной только при $i = j$: она тогда единичная, т. е.

$$\Lambda(i, j) = E(i, j) = E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

но это не страшно. Кроме того, $i \leq j$, так что из одних нулей матрица состоять не будет. Заметим, что в науке матрицы, состоящие из нулей и единиц, принято называть $(0, 1)$ -матрицами.

Пусть $i = p - 1$, а $j = k$. Возьмем векторы $\mathbf{x}_1, \dots, \mathbf{x}_{C_{n-1}^{p-1}}$, образованные строками матрицы $\Lambda(p - 1, k)$. Эти векторы суть вершины C_{n-1}^k -мерного «единичного куба», и они уж заведомо лежат в $\mathbb{R}^{C_{n-1}^k}$. Мы можем «натянуть» на векторы $\mathbf{x}_1, \dots, \mathbf{x}_{C_{n-1}^{p-1}}$ подпространство пространства $\mathbb{R}^{C_{n-1}^k}$. Получится «плоскость» Π , размерность которой, очевидно, не превосходит числа ее образующих, т. е. величины C_{n-1}^{p-1} . Вот они — матрица и векторное пространство. Остается немного «пожонглировать» ими.

Лемма 1. При любом $i \in \{0, \dots, p - 1\}$ выполнено соотношение

$$\Lambda(i, p - 1)\Lambda(p - 1, k) = C_{k-i}^{p-1-i}\Lambda(i, k).$$

Доказательство леммы 1. Во-первых, заметим, что умножение матриц, стоящих в левой части соотношения, заявленного в лемме, определено корректно: число столбцов в $\Lambda(i, p - 1)$ совпадает с числом строк в $\Lambda(p - 1, k)$. Разумеется, размер результирующей матрицы должен и впрямь совпадать с размером матрицы $\Lambda(i, k)$, т. е. с величиной $C_{n-1}^i \times C_{n-1}^k$. Надо бы еще с элементами наших матриц определиться. Если u -е i -элементное подмножество B_u не содержится в v -м k -элементном подмноестве A_v множества \mathcal{R}_{n-1} , то (u, v) -й элемент $\lambda_{u,v}(i, k)$ матрицы $\Lambda(i, k)$ равен нулю. Однако при тех же условиях

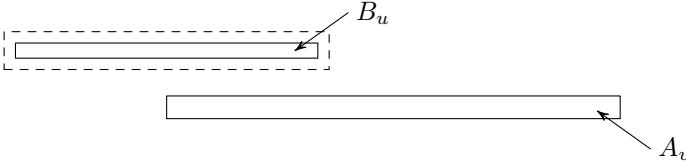


Рис. 1

никакое $(p - 1)$ -элементное подмножество \mathcal{R}_{n-1} , содержащее B_u , тем более не может быть вложенным в A_v (см. рис. 1). Значит, в этом случае и при перемножении матриц на позиции с номером (u, v) возникнет ноль. В противном случае (u -е i -элементное подмножество B_u вложено в v -е k -элементное подмножество A_v множества \mathcal{R}_{n-1}) единиц при перемножении матриц возникнет столько же, сколько есть различных $(p - 1)$ -элементных подмножеств \mathcal{R}_{n-1} , лежащих, так сказать, «между» B_u и A_v (см. рис. 2). Ясно, что таковых подмножеств в точности C_{k-i}^{p-1-i} штук, и лемма 1 доказана. \square

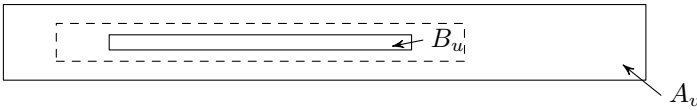


Рис. 2

Из леммы 1 мгновенно следует принадлежность вектор-строк матрицы $\Lambda(i, k)$, $i = 0, \dots, p - 1$, пространству Π . Справедлива

Лемма 2. При любом $i \in \{0, \dots, p - 1\}$ имеет место соотношение

$$\Lambda(i, k)^T \Lambda(i, k) = \Gamma(i, k).$$

Здесь верхний индекс T означает операцию транспонирования, а $\Gamma(i, k)$ — это матрица размера $C_{n-1}^k \times C_{n-1}^k$, элементы которой имеют вид

$$\gamma_{u,v}(i, k) = C_{|A_u \cap A_v|}^i, \quad 1 \leq u, v \leq C_{n-1}^k \quad (|A_u| = |A_v| = k).$$

Доказательство леммы 2 мало отличается от доказательства леммы 1, и мы оставляем его читателю. Заметим только, что биномиальный коэффициент ввиду сделанных нами выше оговорок корректно определен даже в ситуациях, когда мощность пересечения k -элементных множеств A_u, A_v меньше i . Для нас главное, что вектор-строки матрицы $\Gamma(i, k)$ при каждом $i \in \{0, \dots, p - 1\}$ суть линейные

комбинации вектор-строк матрицы $\Lambda(i, k)$, которые, как мы знаем благодаря лемме 1, лежат в плоскости Π . Таким образом, и строки $\Gamma(i, k)$, $i = 0, \dots, p-1$, являются элементами нашего векторного пространства.

Лемма 3. *При любом целом неотрицательном x выполнено соотношение*

$$\prod_{i=1}^{p-1} (i-x) \equiv \sum_{j=0}^{p-1} (-1)^{j+1} C_x^j \pmod{p}.$$

Доказательство леммы 3. При $x = 0$ имеем в левой части искомого соотношения величину $(p-1)!$. По известной теореме Вильсона (см. [2], хотя это почти очевидно) $(p-1)! \equiv -1 \pmod{p}$. В то же время в правой части соотношения есть только $-C_0^0 = -1$, так что пока все в порядке. Если $x \in \{1, \dots, p-1\}$, то слева стоит просто ноль. Вместе с тем справа возникает сумма вида

$$\sum_{j=0}^x (-1)^{j+1} C_x^j = -(1-1)^x = 0,$$

и значит, вновь проблем нет. Наше соотношение оказалось верным при всех возможных остатках от деления x на p (как говорят, при всех *вычетах по модулю p*). Нетрудно убедиться в том (см. [2]), что оно, таким образом, справедливо всегда. Лемма 3 доказана. \square

Рассмотрим $\Gamma = \sum_{i=0}^{p-1} (-1)^{i+1} \Gamma(i, k)$ (матрицы складываются покомпонентно). Тогда (u, v) -й элемент $\gamma_{u,v}$ матрицы Γ выглядит так:

$$\gamma_{u,v} = \sum_{i=0}^{p-1} (-1)^{i+1} C_{|A_u \cap A_v|}^i.$$

Матрица Γ — квадратная, и определена она так, что ее вектор-строки принадлежат пространству Π . Значит,

$$\text{rank } \Gamma \leq \dim \Pi \leq C_{n-1}^{p-1}.$$

Пусть теперь $\Gamma(\mathcal{N})$ — это минор, порожденный элементами $\gamma_{u,v}$, в которых $A_u, A_v \in \mathcal{N}$ (такие у нас, безусловно, имеются, ведь и мощности A_u, A_v , и мощности множеств из совокупности \mathcal{N} равны k). По лемме 3 в этом миноре

$$\gamma_{u,v} = \sum_{i=0}^{p-1} (-1)^{i+1} C_{|A_u \cap A_v|}^i \equiv \prod_{j=1}^{p-1} (j - |A_u \cap A_v|).$$

Коль скоро множества A_u, A_v лежат в \mathcal{N} , мощность их пересечения заведомо находится в пределах от единицы до $k = 2p$ (не пересекаются

они не могут, так как мы их с самого начала именно ради этого загнали в \mathcal{R}_{n-1}). Однако она и p по условию теоремы не равняется. Следовательно, $|A_u \cap A_v| \equiv 0 \pmod{p}$ тогда и только тогда, когда $A_u = A_v$ (т. е. $u = v$). Таким образом, как нетрудно видеть (и здесь важна простота p), $\gamma_{u,u} \not\equiv 0 \pmod{p}$, в то время как $\gamma_{u,v} \equiv 0 \pmod{p}$ при $u \neq v$ (разумеется, мы не выходим за пределы минора). Отсюда, опять-таки за счет простоты p , вытекает неравенство $\det \Gamma(\mathcal{N}) \not\equiv 0 \pmod{p}$, влекущее за собой неравенство $\det \Gamma(\mathcal{N}) \neq 0$. Получается, что

$$|\mathcal{N}| = \text{rank} \Gamma(\mathcal{N}) \leq \text{rank} \Gamma \leq C_{n-1}^{p-1},$$

и теорема доказана. □

2.3. Точность теоремы Франкла—Уилсона и ее неожиданность

Если предыдущий раздел был насыщен идеями, то нынешний носит скорее технический характер. В этом плане он довольно скучен, но зато мы увидим, насколько глубокий результат был получен Франклом и Уилсоном даже в той специальной формулировке, которую мы пока что знаем. Основным нашим инструментом будет известная формула Стирлинга для факториала, утверждающая, что

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

Здесь $\pi = 3,1415\dots$, $e = 2,7182\dots$, а значок « \sim » говорит о том, что формула асимптотическая, т. е.

$$\frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} \rightarrow 1 \quad \text{при } n \rightarrow \infty.$$

Покажем сначала, насколько удивительна оценка в теореме, а именно, попытаемся понять, как устроена величина $2C_{n-1}^{p-1}$. Напомним, что $p = n/4$. Итак,

$$\begin{aligned} 2C_{n-1}^{p-1} &= 2 \frac{(n-1)!}{\left(\frac{n}{4}-1\right)! \left(\frac{3n}{4}\right)!} = 2 \frac{n/4}{n} \frac{n!}{\left(\frac{n}{4}\right)! \left(\frac{3n}{4}\right)!} \sim \\ &\sim \frac{1}{2} \frac{\sqrt{2\pi n} n^n e^{-n}}{\sqrt{2\pi \frac{n}{4}} \left(\frac{n}{4}\right)^{n/4} e^{-n/4} \sqrt{2\pi \frac{3n}{4}} \left(\frac{3n}{4}\right)^{3n/4} e^{-3n/4}}. \end{aligned}$$

Очевидно, все экспоненты (степени числа e) уничтожаются, сокращаются также и величины вида $n^{\gamma n}$. Остается выражение

$$\frac{\sqrt{2}}{\sqrt{3\pi n}} \left(\frac{4}{3^{3/4}} \right)^n = \left(\frac{4}{3^{3/4}} + o(1) \right)^n = (1,754\dots + o(1))^n.$$

Получается, что мощность любой совокупности $2p$ -элементных подмножеств $4p$ -элементного множества, удовлетворяющей всего одному запрету на мощность пересечения своих элементов (эта мощность не может совпадать с p), не превосходит $(1,754\dots + o(1))^n$. Однако едва мы снимаем запрет, и количеству множеств уже ничто не мешает достичь величины

$$C_n^{n/2} = \frac{n!}{\left(\left(\frac{n}{2} \right)! \right)^2} \sim \frac{\sqrt{2\pi n} n^n e^{-n}}{\left(\sqrt{2\pi \frac{n}{2}} \left(\frac{n}{2} \right)^{n/2} e^{-\frac{n}{2}} \right)^2} = (2 + o(1))^n.$$

Поразительно: один-единственный запрет — и такие последствия. Если спросить любого неспециалиста в области комбинаторики, какого бы он ожидал результата, то очень маловероятно, что он предположил бы подобное. Более того, автору попадались математики, до последнего не верившие в столь необычное явление, и только доказательство разубеждало их.

Теперь обсудим точность теоремы. Для ясности изложения мы докажем, что теорема «практически» точна. Вернее, мы предъявим совокупность \mathcal{M} , имеющую все надлежащие свойства и такую, вместе с тем, что $|\mathcal{M}| = (1,754\dots + o(1))^n$. Иными словами, если в чем и будет различие между оценкой Франкла—Уилсона и значением $|\mathcal{M}|$, так это в величине бесконечно малого. Разобьем множество \mathcal{R}_n на две равные части $\mathcal{R}_n = \mathcal{R}^1 \sqcup \mathcal{R}^2$, где

$$\mathcal{R}^1 = \left\{ 1, \dots, \frac{n}{2} \right\}, \quad \mathcal{R}^2 = \left\{ \frac{n}{2} + 1, \dots, n \right\},$$

а значок « \sqcup » подчеркивает, что мы имеем дело с *дизъюнктивным объединением*, то есть с объединением непересекающихся множеств. Пусть $N = C_{n/2}^{\lfloor 3n/8 \rfloor + 1}$,

$$\mathcal{M}^1 = \{M_1^1, \dots, M_N^1\}$$

— совокупность всех возможных $(\lfloor 3n/8 \rfloor + 1)$ -элементных подмножеств в \mathcal{R}^1 , а

$$\mathcal{M}^2 = \{M_1^2, \dots, M_N^2\}$$

— совокупность всех возможных $(n/2 - \lfloor 3n/8 \rfloor - 1)$ -элементных подмножеств в \mathcal{R}^2 . Понятно, что и впрямь

$$|\mathcal{M}^1| = |\mathcal{M}^2| = N.$$

Целая же часть берется от дроби $3n/8$ неспроста: ведь n не обязано делиться на 8. Впрочем, у нас $n/4 = p$, где p простое, так что делимости на 8 заведомо нет, и тут уместно заметить, что простота величины $n/4$ нам нигде в дальнейшем не понадобится: конструкция совокупности, предъявить которую мы стремимся, более обща, нежели теорема Франкла—Уилсона.

Возьмем каждое множество вида

$$M_i^1 \sqcup M_j^2, \quad i, j = 1, \dots, N.$$

Получится $s = N^2$ множеств M_1, \dots, M_s , имеющих мощности $n/2$. Более того,

$$|M_i \cap M_j| > \frac{n}{4}$$

для любых $i, j \in \{1, \dots, s\}$, что отраднo. Остается лишь осознать, почему $s = (1,754\dots + o(1))^n$. Воспользуемся опять-таки формулой Стирлинга и заметим, что

$$\left[\frac{3n}{8} \right] = \frac{3n}{8} - \varepsilon, \quad \text{где } \varepsilon \in [0, 1).$$

Положим $\kappa = 1 - \varepsilon$.

$$|\mathcal{M}| = N^2 = (C_{n/2}^{\lceil 3n/8 \rceil + 1})^2 \sim \left(\frac{\sqrt{2\pi} \frac{n}{2} \left(\frac{n}{2}\right)^{n/2} e^{-n/2}}{\sqrt{2\pi} \left(\frac{3n}{8} + \kappa\right) \left(\frac{3n}{8} + \kappa\right)^{\frac{3n}{8} + \kappa} e^{-\frac{3n}{8} - \kappa} \sqrt{2\pi} \left(\frac{n}{8} - \kappa\right) \left(\frac{n}{8} - \kappa\right)^{\frac{n}{8} - \kappa} e^{-\frac{n}{8} + \kappa}} \right)^2.$$

Рассмотрим отдельно величину $\left(\frac{3n}{8} + \kappa\right)^{\frac{3n}{8} + \kappa}$. Она равна

$$\left(\frac{3n}{8}\right)^{\frac{3n}{8} + \kappa} \left(1 + \frac{\kappa}{3n/8}\right)^{\frac{3n}{8} + \kappa}.$$

Понятно, что с точностью до сомножителей «полиномиального» порядка роста или убывания (таких, которые можно оценить сверху многочленом от n и снизу единицей, деленной на многочлен от n) мы имеем дело с величиной $(3n/8)^{3n/8}$. Аналогичное наблюдение имеет место в других похожих случаях. Посему, обозначая через $P(n)$ функцию, составленную из сомножителей полиномиального порядка, получаем

$$|\mathcal{M}| \sim P(n) \left(\frac{\left(\frac{n}{2}\right)^{n/2}}{\left(\frac{3n}{8}\right)^{3n/8} \left(\frac{n}{8}\right)^{n/8}} \right)^2 = (1,754\dots + o(1))^n.$$

Совокупность \mathcal{M} доставляет нам искомый пример. Стоит заметить, однако, что в ней множества удовлетворяют даже более сильному ограничению, чем требовалось: их пересечение не только не совпадает с $n/4$, но также не может быть и меньше этой величины. Выходит, запретить множествам пересекаться ровно по $n/4$ общим элементам и не более чем по $n/4$ общим элементам — это, по сути, одно и то же? Один запрет дает тот же результат, что и $n/4$ запретов? Не следует, конечно, забывать, что для верхней оценки величины $m(n, k, t)$ мы использовали нетривиальное условие простоты числа t , и все же результат поразителен.

На самом деле задачи о запрете одного и нескольких пересечений — разные, и мы расскажем, в частности, об этом в следующем параграфе.

2.4. Вокруг теоремы Франкла—Уилсона

Начнем с общей формулировки теоремы Франкла—Уилсона.

Теорема 3 (П. Франкл и Р. М. Уилсон). Пусть $k - t$ — степень некоторого простого числа. Если $k \geq 2t + 1$, то $m(n, k, t) \leq C_n^{k-t-1}$. Иначе, полагая $d = 2t - k + 1$, имеем

$$m(n, k, t) \leq \frac{C_n^d C_n^{t-d}}{C_k^d}.$$

Давайте поймем, насколько широка область применения теоремы 3. Во-первых, убедимся в том, что теорема 2 есть весьма специальный ее случай. В самом деле, если $n = 4p$, $k = 2p$, $t = p$, то, безусловно, $k - t = p$ — это (первая) степень простого числа, и мы сразу видим, что теорема 3 шире теоремы 2: в ней, вообще говоря, степень может не быть первой. Далее, $k = 2p < 2t + 1 = 2p + 1$, и, стало быть, нам следует обратиться ко второй части утверждения теоремы 3. Поскольку $d = 1$, из нее вытекает неравенство

$$m(n, k, t) \leq \frac{n}{k} C_{n-1}^{t-1} = 2C_{n-1}^{p-1},$$

и все в порядке. В то же время ясно, что использовать теорему 3 можно гораздо чаще. Мало того, что, как мы уже отмечали, простота «запрета» не является принципиальным ограничением, так еще и k , t вовсе не обязаны принимать столь конкретные значения, какие они имели в теореме 2. Лишь бы разность мощности множества и величины запрещенного пересечения была степенью простого. И все — это линейно-алгебраический метод, аналогичный тому, что мы подробно изложили в п. 2.2.

Между прочим, и теорема Ж.Надя мгновенно следует из теоремы 3 — правда, в чуть-чуть ослабленной формулировке. Действительно, там $k = 3$, $t = 1$, и, значит, $k - t = 2$ — степень простого. К тому же $k = 3 \leq 2t + 1 = 3$, в результате чего $m(n, 3, 1) \leq C_n^1 = n$. Индукция давала слегка более точную формулировку, повязанную на остатки от деления числа n на 4, но зато здесь совершенно общий метод. Помните, мы говорили, что уже отыскание величины $m(n, 5, 2)$ было большой проблемой? Теперь и думать не о чем: метод моментально свидетельствует о том, что $m(n, 5, 2) \leq C_n^2$, а это при «кустарных» подходах казалось запредельным. Тем более, что оценка почти точна. Если, например, взять совокупность пятиэлементных подмножеств множества \mathcal{R}_n , у которых первые три элемента из \mathcal{R}_n (элементы 1, 2, 3) общие, то в этой совокупности будет как раз $C_{n-3}^2 \sim C_n^2$ элементов: разница, как и в п. 2.3, лишь на уровне бесконечно малых величин. Заметим, кстати, что и в совершенно произвольной ситуации теорема Франкла—Уилсона практически точна. Единственная неприятность состоит в необходимости работать со степенями простых чисел. Это большая проблема, и до сих пор с ней бороться не научились. Впрочем, с точки зрения многих приложений наличие подобного ограничения не критично. Дело в том, что простых чисел (и тем более их степеней) «очень много», — а именно, они достаточно плотно встречаются в натуральном ряде. Строго говоря, как многие знают, между x и $2x$ обязательно есть простое число. Это старый постулат Бертрана, и к настоящему времени имеются куда более точные результаты.

Одна из тяжелейших проблем *аналитической теории чисел*, в область интересов которой входит, в частности, и вопрос о распределении простых чисел внутри натурального ряда, состоит в отыскании как можно более точных оценок на такую функцию $f(x)$, что при $x \geq x_0$ между x и $x + f(x)$ заведомо найдется простое число. Гипотеза состоит в том, что в качестве $f(x)$ можно взять $O(\sqrt{x}(\log x)^\gamma)$ с некоторым $\gamma > 0$. Однако даже самые мощные современные методы анализа дают лишь результаты типа

$$f(x) = O(x^\delta), \quad \text{где } \delta > \frac{1}{2}.$$

К примеру, $\delta = 38/61$ вполне подходит, а дотянуть δ до половины пока не удастся. Оценка $f(x) = O(x^{38/61})$ неоправданно сложна, да нам, по сути, она нигде и не понадобится. Нам достаточно понимать, что $f(x) = o(x)$, а это может быть получено из классического *асимптотического закона распределения простых чисел*, доказанного еще в 1896 году Ж. Адамаром и Ш. Ж. Валле Пуссенном (см. [3]): *количество $\pi(x)$ простых чисел, не превосходящих x , есть выражение вида*

$$\pi(x) = (1 + o(1)) \frac{x}{\ln x}.$$

Мы не станем утверждать, что теорема Адамара—Валле Пуссена легкая, но в ней при желании разобраться можно за разумное время. Для нас главное, что в сколь угодно малой «окрестности» любого числа есть простое (не говоря уж о его степени), а значит, теорема Франкла—Уилсона в некотором естественном смысле применима «почти всегда». Это не устраняет необходимости борьбы с «непростыми» запретами на мощности пересечения множеств, но демонстрирует силу линейно-алгебраического метода. К тому же упомянутые теоремы аналитической теории чисел нам пригодятся в будущем.

Вот еще пара красивых теорем, доказанных Франклом и Уилсоном с помощью линейной независимости.

Теорема 4 (П. Франкл и Р. М. Уилсон). Пусть $q = p^\alpha$ — это степень некоторого простого числа. Рассмотрим произвольную совокупность $\mathcal{M} = \{M_1, \dots, M_s\}$, состоящую из k -элементных подмножеств множества \mathcal{R}_n и обладающую свойством:

$$|M_i \cap M_j| \not\equiv k \pmod{q}$$

для любых $i \neq j \in \{1, \dots, s\}$. Тогда $s = |\mathcal{M}| \leq C_n^{q-1}$.

Теорема 5 (П. Франкл и Р. М. Уилсон). Пусть $0 \leq l_1 < l_2 < \dots < l_r \leq n$ — некоторые целые числа. Рассмотрим совокупность $\mathcal{M} = \{M_1, \dots, M_s\}$, состоящую из подмножеств произвольной мощности в \mathcal{R}_n и обладающую свойством:

$$|M_i \cap M_j| \in \{l_1, \dots, l_r\}$$

для любых $i, j \in \{1, \dots, s\}$. Тогда

$$s = |\mathcal{M}| \leq \sum_{i=0}^r C_n^i.$$

Последняя теорема говорит уже не о запрещенных, а наоборот, о разрешенных пересечениях. Попробуйте доказать теоремы 4 и 5 самостоятельно.

В п. 2.3, рассуждая о точности теоремы 2, мы пришли к удивительному выводу: в случае выполнения всех необходимых условий (типа простоты запрета) более или менее все равно, что запрещать — величину $n/4$ или все величины, не превосходящие $n/4$. Однако там же мы заметили, что некоторая разница все-таки есть. Дабы разъяснить ее, надо определить функцию $f(n, k, t)$, аналогичную $m(n, k, t)$ и равную $\max |\mathcal{M}|$, где максимум берется по всем совокупностям k -элементных

подмножеств множества \mathcal{R}_n , в которых любые два множества пересекаются не менее чем по t общим элементам. Сразу же ясно, что $f(n, k, t) = C_n^k$, коль скоро $2k - n \geq t$, т. е. k -элементные подмножества \mathcal{R}_n заведомо пересекаются по t элементам. С другими возникает проблема. Ее изучение было инициировано в работе П. Эрдёша, Ч. Ко и Р. Радо, опубликованной в начале шестидесятых годов прошлого века, и, хотя ни один из полученных в этой связи результатов не опирается на линейно-алгебраический метод, мы не можем удержаться от того, чтобы не рассказать о фактах, установленных к настоящему времени. Поразительно, но, несмотря на всю уже подмеченную нами близость между двумя задачами, проблема отыскания величины $f(n, k, t)$ несколько проще, и сейчас мы имеем исчерпывающее и по существу неуллучшаемое ее решение. В отыскании этого решения поучаствовали, кстати, и Франкл с Уилсоном, но последнюю точку поставили в 1996 году Р. Альсведе и Л. Хачатрян. Вот их замечательная теорема.

Теорема 6 (П. Франкл, Р. М. Уилсон, Р. Альсведе, Л. Хачатрян).

Пусть

$$2k - n < t, \quad 1 \leq t \leq k \leq n.$$

Пусть, кроме того, при $0 \leq i \leq (n - t)/2$ и $i \leq k - t$ определена совокупность

$$\mathcal{F}_i(n, k, t) = \{F \subseteq \mathcal{R}_n : |F| = k, |F \cap \{1, \dots, t + 2i\}| \geq t + i\},$$

т. е. $\mathcal{F}_i(n, k, t)$ — это совокупность всех возможных k -элементных подмножеств множества \mathcal{R}_n , у которых не менее $t + i$ элементов заведомо взято из

$$\{1, \dots, t + 2i\} \subseteq \mathcal{R}_n = \{1, \dots, n\}.$$

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

$$(k - t + 1) \left(2 + \frac{t - 1}{r + 1} \right) \leq n < (k - t + 1) \left(2 + \frac{t - 1}{r} \right),$$

то $f(n, k, t) = |\mathcal{F}_r(n, k, t)|$ (мы считаем, что $(t - 1)/r = \infty$, коль скоро $r = 0$).

Теорему нельзя не прокомментировать. Прежде всего, конечно, мы заметим, что параметры в ней выбраны очень аккуратно. Например, корректность определения совокупности множеств $\mathcal{F}_i(n, k, t)$ сразу же вытекает из того факта, что, во-первых, $i \leq (n - t)/2$ (а стало быть, $t + 2i \leq n$, так что и впрямь $\{1, \dots, t + 2i\} \subseteq \mathcal{R}_n = \{1, \dots, n\}$), и во-вторых, $i \leq k - t$ (и значит, $t + i \leq k$, ввиду чего наша совокупность непууста: k -элементные множества F , обладающие свойством

$|F \cap \{1, \dots, t + 2i\}| \geq t + i$, в \mathcal{R}_n действительно существуют). В то же время, из своего соотношения и неотрицательная целая величина $r \leq k - t$ находится однозначно. (Если допустить, что $r > k - t$, т. е. $r \geq k - t + 1$, то тогда

$$(k - t + 1) \left(2 + \frac{t - 1}{r} \right) \leq 2k - t + 1 \leq n,$$

так как $2k - n < t$, а это невозможно.) Но это все пока, так сказать, техника. Куда интереснее сам результат.

Пусть в теореме 6 $r = 0$. В таком случае

$$n \geq (k - t + 1)(t + 1).$$

Между прочим, параметры типа $t = n/4$, $k = n/2$, с которыми мы имели дело в теоремах 2 и 3, к этому случаю не относятся: если $k \asymp n$ (т. е. $k = O(n)$ и $n = O(k)$), то $t \asymp 1$, а иначе условия нарушаются. Тут, скорее, речь идет о величинах вроде $k \asymp t \asymp \sqrt{n}$ и пр. И тогда теорема 6 утверждает, что $f(n, k, t) = |\mathcal{F}_0(n, k, t)|$. Но $\mathcal{F}_0(n, k, t)$ — это ведь попросту совокупность всех k -элементных подмножеств в \mathcal{R}_n , которые непременно содержат «начальный отрезок» \mathcal{R}_n , имеющий как раз мощность t . Очевидно, что элементы $\mathcal{F}_0(n, k, t)$ пересекаются так, как надо, и следовательно, $\mathcal{F}_0(n, k, t)$ представляет собою пример той самой совокупности, на которой достигается максимум из определения величины $f(n, k, t)$. В сущности, довольно естественно было бы с самого начала предположить, что «экстремальную» совокупность множеств, каждые два из которых «цепляют» друг друга по не менее чем t элементам, строится в точности ровно так, как построена $\mathcal{F}_0(n, k, t)$. И Эрдёш еще в семидесятые годы прошлого века высказывал соответствующую гипотезу, добавляя, впрочем, что для ее справедливости n должно быть достаточно большим: $n \geq n_0(k, t)$. Как видно, так оно и вышло: $n \geq (k - t + 1)(t + 1)$. Кстати, указанное ограничение было найдено в 1978 году Франклом при $t \geq 15$, а последнее (явно искусственное) неравенство устранил в 1984 году Уилсон. Именно в этом состоял вклад Франкла и Уилсона в теорему 6, и долгое время сохранялась проблема «перейти Рубикон» — осознать, что же получается при $n < (k - t + 1)(t + 1)$. Альсведе и Хачатрян преодолели рубеж.

Теперь с высоты наших знаний становится, наоборот, странным, почему не при любых n, k, t максимум из определения величины $f(n, k, t)$ достигается на совокупности $\mathcal{F}_0(n, k, t)$. Казалось бы, как все здорово: фиксировал t элементов в \mathcal{R}_n (скажем, первые — как в теореме), зацепил по ним все множества попарно, и порядок. В том-то, однако, и пафос теоремы, что максимум вовсе не обязательно

так очевидно устроен. Правда, понять это не очень трудно. Помните, в предыдущем разделе мы предъявили совокупность множеств, свидетельствующую о точности оценки из теоремы 2? После этого мы неоднократно замечали, что та конструкция обладает более сильным свойством, чем требовалось с точки зрения изучения величины $m(n, k, t)$. Она показывала, что

$$m(n, k, t) \geq (C_{n/2}^{\lfloor 3n/8 \rfloor + 1})^2 \quad \text{при } n = 4t, k = 2t,$$

но ясно, что вместе с тем она при аналогичных условиях влечет неравенство

$$f(n, k, t) \geq (C_{n/2}^{\lfloor 3n/8 \rfloor + 1})^2 = (1,754 \dots + o(1))^n.$$

Однако $|\mathcal{F}_0(n, k, t)| = C_{n-t}^{k-t}$, то есть, обратись мы к оценке, получаемой за счет совокупности $\mathcal{F}_0(n, k, t)$, мы бы не продвинулись дальше неравенства

$$f(4t, 2t, t) \geq C_{3n/4}^{n/4} = (1,611 \dots + o(1))^n.$$

И Эрдёш, и все вообще, кто занимался обсуждаемой нами проблематикой, прекрасно понимали эту сложность. Но только в 1996 году усилиями Альсведе и Хачатряна была сформулирована и доказана окончательная теорема 6. Отныне общая конструкция совокупности, на которой достигается значение величины $f(n, k, t)$ при любых данных n, k, t , известна, и представляет она собою в аккурат $\mathcal{F}_r(n, k, t)$. В частности, легко понять, что она очень похожа на конструкцию из предыдущего раздела, коль скоро мы положим в ней $n = 4t, k = 2t$ (убедитесь в этом!). Догадаться до нее несколько тяжелее, чем до ее специального случая при $r = 0$, но мы еще раз подчеркнем, что значение теоремы в первую очередь в том, что угаданные конструкции оказались ни на йоту не улучшаемыми. И доказательство там крайне нетривиальное.

Заметим еще, что теорема 6 допускает даже более удивительную формулировку, нежели та, которую мы привели и прокомментировали. А именно, верно поразительное уточнение. В самом деле, понятно вроде бы, что совокупностью $\mathcal{F}_r(n, t, k)$ не исчерпывается многообразие тех совокупностей, на которых достигается максимум в определении $f(n, k, t)$. Можем же мы фиксировать не первые $t + 2r$ элементов в \mathcal{R}_n , а, допустим, последние. Вообще, если мы возьмем любую из $n!$ перестановок σ в \mathcal{R}_n , то под ее действием появится новая совокупность $\mathcal{F}_r^\sigma(n, t, k)$, с прежним успехом реализующая искомый максимум. Однако различия между совокупностями $\mathcal{F}_r^\sigma(n, t, k)$ ничтожны: не все ли равно, в каком порядке мы нумеруем элементы конечного

множества? Но вот вопрос: а можно ли придумать еще какие-нибудь совокупности, отличные от $\mathcal{F}_r^\sigma(n, t, k)$ при каждом σ и реализующие вместе с тем $f(n, k, t)$? И обещанное поразительное уточнение теоремы 6 состоит в том, что ответ на поставленный вопрос отрицателен. Вернее, так. Если

$$(k - t + 1) \left(2 + \frac{t-1}{r+1} \right) < n < (k - t + 1) \left(2 + \frac{t-1}{r} \right),$$

то $\mathcal{F}_r(n, k, t)$ единственна с точностью до перестановок, а если

$$n = (k - t + 1) \left(2 + \frac{t-1}{r+1} \right),$$

то $|\mathcal{F}_r(n, k, t)| = |\mathcal{F}_{r+1}(n, k, t)|$, и ничего иного с точностью до перестановок придумать нельзя.

В заключение приведем еще две любопытные и важные теоремы по рассмотренной тематике.

Теорема 7 (А. Хилтон и Е. Милнер). Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ — совокупность попарно пересекающихся k -элементных подмножеств множества \mathcal{R}_n . Предположим, однако, что

$$\bigcap_{i=1}^s M_i = \emptyset.$$

Тогда при $k \leq n/2$ выполнено неравенство

$$s \leq 1 + C_{n-1}^{k-1} - C_{n-k-1}^{k-1}.$$

Теорема 8 (Д. Клейтман). Пусть

$$\mathcal{M} = \{M_1, \dots, M_s\} \quad \text{и} \quad \mathcal{N} = \{N_1, \dots, N_t\}$$

— это совокупности k -элементных подмножеств множества \mathcal{R}_n . Предположим, что $M_i \cap N_j \neq \emptyset$ для любых i и j . Тогда при $k \leq n/2$ выполнено неравенство

$$\min\{s, t\} \leq C_{n-1}^{k-1}.$$

Задачи

1. Докажите простейший вариант теоремы 6 — теорему Эрдёша—Ко—Радо: если $k \leq n/2$ и в совокупности \mathcal{M} любые два множества пересекаются, то мощность \mathcal{M} не превосходит C_{n-1}^{k-1} . Докажите теорему Хилтона—Милнера, уточняющую результат Эрдёша—Ко—Радо.

2. Докажите теорему 2 при $t = p^\alpha$, $k = 2t$, $n = 4t$.
3. Как много может быть четырехэлементных подмножеств в \mathcal{R}_n , никакие два из которых не пересекаются по двум общим элементам? любые два из которых пересекаются не менее чем по двум общим элементам?
4. (*Теорема Франкла—Уилсона.*) Пусть $\mathcal{M} = \{M_1, \dots, M_s\}$ — произвольная совокупность семиэлементных подмножеств множества \mathcal{R}_n , обладающая свойством:

$$|M_i \cap M_j| \in \{0, 2, 3, 5, 6\}$$

для любых $i \neq j \in \{1, \dots, s\}$. Докажите, что $|\mathcal{M}| < C_n^2$.

3

Задачи о скалярных произведениях векторов

3.1. Постановка одной из задач и формулировка одного из результатов

Для начала напомним стандартное обозначение

$$(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \dots + x_n y_n$$

скалярного произведения векторов

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

в (евклидовом) пространстве \mathbb{R}^n . Слово «евклидово» взято в скобки не случайно: в принципе под \mathbb{R}^n можно понимать простую совокупность упорядоченных последовательностей, состоящих из n произвольных вещественных чисел (тогда \mathbb{R}^n принято называть *вещественным арифметическим пространством*). Но, коль скоро наше скалярное произведение определено, и притом ровно так, как это было только что сделано, \mathbb{R}^n становится евклидовым, и расстояние между его элементами (векторами) задается обычным путем:

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

Это, как всегда, равносильно записи

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}),$$

которая нам пригодится.

Пусть фиксированы величины $n, k_{-1}, k_0, k_1 \in \mathbb{N}$, удовлетворяющие условию $k_{-1} + k_0 + k_1 = n$. Рассмотрим совокупность векторов

$$\Sigma = \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{-1, 0, 1\}, \\ |\{i : x_i = -1\}| = k_{-1}, |\{i : x_i = 0\}| = k_0, |\{i : x_i = 1\}| = k_1\}.$$

Понятно, что совокупность Σ определена корректно, и, в частности, очевидно, что

$$|\Sigma| = C_n^{k_{-1}} C_{n-k_{-1}}^{k_0} = P(k_{-1}, k_0, k_1) = \frac{n!}{k_{-1}! k_0! k_1!},$$

где $P(u_1, \dots, u_m) = \frac{(u_1 + \dots + u_m)!}{u_1! \dots u_m!}$ — это «полиномиальный коэффициент», возникающий, например, по аналогии с коэффициентом биномиальным при раскрытии скобок в выражении типа $(a_1 + \dots + a_m)^l$.

Обозначим через

$$\underline{s} = \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)$$

минимальное скалярное произведение векторов из Σ :

$$\underline{s} = \min_{\mathbf{x}, \mathbf{y} \in \Sigma} (\mathbf{x}, \mathbf{y}).$$

Точно так же введем величину

$$\bar{s} = \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = \max_{\mathbf{x}, \mathbf{y} \in \Sigma} (\mathbf{x}, \mathbf{y}).$$

Последняя величина считается очень легко, и равна она, конечно же, «скалярному квадрату» любого вектора из Σ , каковой у нас постоянен:

$$\bar{s} = (\mathbf{x}, \mathbf{x}) = k_{-1} + k_1.$$

Величина \underline{s} может быть без особого труда найдена алгоритмически, но, как правило, ее значение нас волновать не будет, и мы предоставим читателю самостоятельно разобраться с различными ситуациями, которые могут возникнуть при решении несложной задачи вычисления \underline{s} как функции от параметров k_{-1}, k_0, k_1 .

Фиксируем произвольное $t \in \{\underline{s}, \dots, \bar{s}\}$ и рассмотрим любую совокупность $\mathcal{F} \subset \Sigma$, в которой нет пар векторов, имеющих скалярное произведение t . Возникает задача, очень похожая на ту, что мы в подробностях изучили в главе 2. Опять-таки, мы берем некоторую совершенно произвольную совокупность каких-то объектов и накладываем на нее всего один запрет; только если раньше мы запрещали множествам данной мощности пересекаться по тому или иному количеству общих элементов, то теперь мы берем векторы (« $(-1, 0, 1)$ -векторы»), у которых числа координат определенного вида заданы наперед, и запрещаем им иметь то или иное скалярное произведение. Естественно, величина запрета лежит в тех самых пределах, в которых меняется скалярное произведение элементов из Σ , ведь иначе и никакого запрета, по сути, не было бы. Спрашивается, как и в главе 2, *а сколь велика может быть мощность совокупности \mathcal{F} ?*

Прежде чем давать какой-либо ответ на поставленный вопрос, заметим, что задачи из прошлой и нынешней глав не просто близки: в некотором роде первая есть частный случай второй. Конечно, мы считали, что k_{-1}, k_0, k_1 — натуральные числа, но, во-первых, многие

математики давно относят к натуральным и ноль, а во-вторых, даже если чисто формально положить $k_{-1} = 0$ в определении совокупности векторов Σ , то это заведомо ничему не повредит. Но тогда

$$\Sigma(\{-1, 0, 1\}^n; 0, k_0, k_1)$$

есть не что иное, как совокупность n -мерных « $(0, 1)$ -векторов», имеющих ровно k_1 единичных и k_0 нулевых координат, и эти векторы мгновенно отождествляются с k_1 -элементными подмножествами \mathcal{R}_n . Действительно, множеству M отвечает $(0, 1)$ -вектор $\mathbf{x} = (x_1, \dots, x_n)$, у которого $x_i = 1$, если $i \in M$, и $x_i = 0$, если $i \notin M$; обратная операция очевидна. В то же время скалярное произведение $(0, 1)$ -векторов попросту совпадает с мощностью пересечения отвечающих им множеств, и наше утверждение обосновано. Таким образом, если мы научимся решать задачу, поставленную в конце предыдущего абзаца, то, по идее, мы как «бонус» получим и альтернативное решение задачи о пересечениях конечных множеств.

Интересно то, что в определенном смысле решение и впрямь будет носить альтернативный характер. Оно опять будет апеллировать к линейно-алгебраическому методу; однако теперь объекты, с которыми нам придется иметь дело, сменят свою природу: вместо матриц и векторных пространств мы обратимся к многочленам над конечными полями. В принципе, будет видно, что новый подход является лишь перевоплощением старого, и тем не менее язык, на котором он позволит нам разговаривать, окажется куда более удобным. Мало того, что соответствующие доказательства станут значительно более компактными, изящными и прозрачными, так еще и к нетривиальным обобщениям полученных результатов перейти не составит труда. Этот язык был в значительной мере разработан в 80–90-е годы XX века Н. Алоном, Л. Бабаи, Х. Судзуки, П. Франклом и автором настоящей брошюры, которому, в частности, удалось в 1999 году доказать следующую теорему, аналогичную теореме 2 Франкла–Уилсона.

Теорема 9. Пусть p — нечетное простое число,

$$n = 2p, \quad k_{-1} + k_1 = p, \quad k_{-1} = \left\lfloor \frac{p}{2} \right\rfloor < k_1, \quad t = 0.$$

Тогда мощность произвольной совокупности векторов

$$\mathcal{F} = \{\mathbf{x}_1, \dots, \mathbf{x}_s\} \subset \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

в которой скалярное произведение любых двух элементов не равняется t (векторы из \mathcal{F} попарно неортогональны), не превосходит величины

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_n^{m_2},$$

где

$$\mathcal{A} = \{(m_1, m_2) : m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq p - 1\}.$$

Далее мы поступим примерно так же, как и во второй главе. Сперва в п. 3.2 мы докажем теорему 9 с помощью линейно-алгебраического метода. Затем в п. 3.3 мы поймем, в чем сила полученного результата, т. е. убедимся в том, что разница между асимптотикой для мощности $\Sigma = \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)$ с параметрами из формулировки теоремы и асимптотикой для величины доказанной оценки (оценки мощности совокупности \mathcal{F} попарно неортогональных векторов из Σ) огромна (сейчас это, кстати, гораздо менее понятно, чем в случае с теоремой 2; однако, как мы увидим позже, результат еще более глубок). В п. 3.4 мы обсудим вопрос о точности теоремы 9, и, наконец, в п. 3.5 мы расскажем о многочисленных важных обобщениях этой теоремы.

3.2. Доказательство теоремы 9

Доказательство. Пусть, как и в формулировке теоремы, $n = 2p$, $k_1 + k_{-1} = p$, $k_{-1} = \lfloor p/2 \rfloor$ с простым нечетным p . Понятно, что тогда

$$\bar{s} = \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = p,$$

а

$$\underline{s} = \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = -2 \left\lfloor \frac{p}{2} \right\rfloor > -p,$$

поскольку p нечетно. Отсюда вытекает тривиальная

Лемма 4. *Скалярное произведение любых двух векторов из*

$$\Sigma = \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)$$

сравнимо с нулем по модулю p тогда и только тогда, когда оно равняется либо нулю, либо p (т. е. когда векторы либо ортогональны, либо совпадают).

Отметим, что аналогичное замечание мы делали относительно мощности пересечения k -элементных множеств при доказательстве теоремы Франкла—Уилсона. Только тогда мы не называли его леммой.

Зафиксируем $\mathbf{x} \in \Sigma$ и рассмотрим полином $\mathcal{P}_{\mathbf{x}}$ от n переменных y_1, \dots, y_n следующего вида:

$$\mathcal{P}_{\mathbf{x}}(\mathbf{y}) = \mathcal{P}_{\mathbf{x}}(y_1, \dots, y_n) = \prod_{i=1}^{p-1} (i - (\mathbf{x}, \mathbf{y})).$$

Подчеркнем, что последнее выражение очень похоже на выражение из леммы 3, и это неслучайно.

Полином отвечает вектору $\mathbf{x} = (x_1, \dots, x_n)$, а переменные его суть координаты другого вектора $\mathbf{y} = (y_1, \dots, y_n)$. Важно еще сказать, какому полю принадлежат коэффициенты полинома, возникающие в результате раскрытия скобок в произведении. Мы будем считать, что это поле — \mathbb{Z}/p , т. е. конечное поле, состоящее из простого числа элементов. Иногда удобно это поле интерпретировать как фактор-группу $\mathbb{Z}/p\mathbb{Z}$, в которой целые числа отождествляются, коль скоро они сравнимы между собой по модулю p . Ясно, что смежные классы — это множества одинаковых вычетов по модулю p (см. п. 2.2), и потому $\mathbb{Z}/p\mathbb{Z}$ часто называют *полем классов вычетов по модулю p* . Итак, $\mathcal{P}_{\mathbf{x}} \in \mathbb{Z}/p\mathbb{Z}[y_1, \dots, y_n]$ (стандартное обозначение) для каждого $\mathbf{x} \in \Sigma$. Справедлива

Лемма 5. Пусть $\mathbf{x}, \mathbf{y} \in \Sigma$. Тогда условие

$$\mathcal{P}_{\mathbf{x}}(\mathbf{y}) \equiv 0 \pmod{p}$$

равносильно условию

$$(\mathbf{x}, \mathbf{y}) \not\equiv 0 \pmod{p}.$$

Лемма очевидна, и мы ее не доказываем. Правда, именно в ней существенна простота p . Теперь раскроем скобки в каждом из полиномов $\mathcal{P}_{\mathbf{x}}$, $\mathbf{x} \in \Sigma$. Получится запись вроде

$$\mathcal{P}_{\mathbf{x}}(\mathbf{y}) = \sum_{q=0}^{p-1} \sum_{i_1, \dots, i_q} c_{i_1, \dots, i_q} y_{i_1}^{\alpha_{i_1}} \cdots y_{i_q}^{\alpha_{i_q}}.$$

Здесь q — количество различных переменных в мономе — меняется в пределах от нуля до $p-1$, так как степень нашего полинома, очевидно, равна $p-1$. Сами переменные в каждом из мономов суть какие-то y_{i_1}, \dots, y_{i_q} , где $1 \leq i_1 < \dots < i_q \leq n$. Степени этих переменных — величины $\alpha_{i_1}, \dots, \alpha_{i_q}$ — заведомо не превосходят $p-1$, а впрочем, и их сумма не может быть больше того же числа. Наконец, $c_{i_1, \dots, i_q} \in \mathbb{Z}/p\mathbb{Z}$ — просто некоторая константа.

Проделаем такую процедуру: если α_{i_ν} , $\nu \in \{1, \dots, q\}$, — четное число, то заменяем его на двойку, а если оно нечетно, то — на единицу. Получатся новые полиномы вида

$$\mathcal{P}'_{\mathbf{x}}(\mathbf{y}) = \sum_{q=0}^{p-1} \sum_{i_1, \dots, i_q} c_{i_1, \dots, i_q} y_{i_1}^{\beta_{i_1}} \cdots y_{i_q}^{\beta_{i_q}},$$

где каждое $\beta_{i_\nu} \in \{1, 2\}$. Разумеется,

$$\mathcal{P}'_{\mathbf{x}} \in \mathbb{Z}/p\mathbb{Z}[y_1, \dots, y_n], \quad \mathbf{x} \in \Sigma.$$

Любопытно, что лемма 5 верна и для полиномов $\mathcal{P}'_{\mathbf{x}}$. В самом деле, если $\mathbf{y} = (y_1, \dots, y_n) \in \Sigma$ (а в лемме оно так), то $y_i \in \{-1, 0, 1\}$. Однако для таких y_i выполнено соотношение $y_i^3 = y_i$, которым мы фактически и пользовались при переходе от нештрихованных полиномов к штрихованным.

Лемма 6. *Если совокупность*

$$\mathcal{F} = \{\mathbf{x}_1, \dots, \mathbf{x}_s\} \subset \Sigma$$

обладает свойством из формулировки теоремы 9, т. е. ее элементы попарно неортогональны, то полиномы $\mathcal{P}'_{\mathbf{x}_1}, \dots, \mathcal{P}'_{\mathbf{x}_s}$ линейно независимы над полем $\mathbb{Z}/p\mathbb{Z}$.

Доказательство леммы 6. Предположим противное. Тогда, в частности, найдутся такие константы $c_1, \dots, c_s \in \mathbb{Z}/p\mathbb{Z}$, что не все они равны нулю в $\mathbb{Z}/p\mathbb{Z}$ (делятся на p) и имеет место тождество

$$c_1 \mathcal{P}'_{\mathbf{x}_1}(\mathbf{y}) + \dots + c_s \mathcal{P}'_{\mathbf{x}_s}(\mathbf{y}) \equiv 0 \pmod{p},$$

верное для всех $\mathbf{y} \in \Sigma$. Зафиксируем произвольный индекс $i \in \{1, \dots, s\}$ и рассмотрим $\mathbf{y} = \mathbf{x}_i \in \Sigma$. Ввиду нашего предположения

$$c_1 \mathcal{P}'_{\mathbf{x}_1}(\mathbf{x}_i) + \dots + c_s \mathcal{P}'_{\mathbf{x}_s}(\mathbf{x}_i) \equiv 0 \pmod{p}.$$

С одной стороны,

$$(\mathbf{x}_i, \mathbf{x}_i) = p \equiv 0 \pmod{p},$$

и, стало быть, по лемме 5

$$\mathcal{P}'_{\mathbf{x}_i}(\mathbf{x}_i) \not\equiv 0 \pmod{p}.$$

С другой стороны, скалярное произведение $(\mathbf{x}_j, \mathbf{x}_i)$ при разных i и j не равно, конечно же, p . Более того, оно не равно нулю по условию леммы (и теоремы), а значит благодаря лемме 4 оно и не сравнимо с нулем по модулю p . В силу леммы 5 имеем

$$\mathcal{P}'_{\mathbf{x}_j}(\mathbf{x}_i) \equiv 0 \pmod{p}.$$

Все это вместе показывает нам, что $c_i \equiv 0 \pmod{p}$ (важна простота p), но i любое, и мы приходим к противоречию. \square

Из леммы 6 сразу следует тот факт, что мощность совокупности \mathcal{F} из формулировки теоремы не превосходит размерности пространства полиномов $\mathcal{P}'_{\mathbf{x}}$. Но базис в этом пространстве образуют мономы вида

$$y_{i_1}^{\beta_{i_1}} \cdots y_{i_q}^{\beta_{i_q}},$$

где, как мы помним, $q \leq p - 1$, $\beta_{i_\nu} \in \{1, 2\}$. Понятно, что, желая отыскать число различных таких мономов, мы должны сперва выбрать из n переменных произвольные $m_1 \in \mathbb{N} \cup \{0\}$ штук, которые

будут входить в строящийся моном в первой степени, а потом из оставшихся $n - m_1$ переменных — любые $m_2 \in \mathbb{N} \cup \{0\}$, которые, в свою очередь, будут иметь в мономе степень 2. Естественно, $m_1 + m_2 \leq n$ и $m_1 + 2m_2 \leq p - 1$, так что все в порядке:

$$|\mathcal{F}| \leq \dim\{\mathcal{P}'_{\mathbf{x}}\}_{\mathbf{x} \in \Sigma} \leq \sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2},$$

где, как мы и ожидали,

$$\mathcal{A} = \{(m_1, m_2): m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq p - 1\}.$$

Теорема доказана. \square

Из доказательства видно, насколько близко оно к рассуждению с матрицами. В частности, не составит труда перевести доказательство теоремы Франкла—Уилсона на полиномиальный язык, и мы советуем читателю заняться этим. Но, пожалуй, новое обличье линейно-алгебраического метода еще более выигрышно. К тому же более подробнейшее доказательство теоремы 9, которое мы только что провели, заняло почти на целую страницу меньше места, чем столь же развернутое обоснование *более простой* теоремы 2. Это не может не производить впечатление.

3.3. Смысл оценки из теоремы 9

Сейчас, как и в п. 2.3, мы убедимся в том, что всего один запрет, наложенный нами на величины допустимых скалярных произведений векторов из произвольной совокупности $\mathcal{F} \subset \Sigma$, заставляет эту совокупность катастрофически «сжаться». Иными словами, мы покажем, что при наших параметрах

$$n = 2p, \quad k_{-1} + k_1 = p, \quad k_{-1} = \left\lfloor \frac{p}{2} \right\rfloor$$

мощность Σ есть $(c_1 + o(1))^n$, $c_1 > 1$ — константа, в то время как оценка на мощность \mathcal{F} , данная в теореме 9, асимптотически равна $(c_2 + o(1))^n$, где $1 < c_2 < c_1$ и c_2 — абсолютная постоянная. Точнее, мы докажем

Предложение 1. *В условиях теоремы 9 имеют место асимптотические формулы*

$$|\Sigma| = (2\sqrt{2} + o(1))^n = (2,8284 \dots + o(1))^n, \quad (1)$$

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2} = (2,4628 \dots + o(1))^n. \quad (2)$$

Доказательство предложения 1. Сперва установим асимптотику (1). Для этого, как и в п. 2.3, нам хватит формулы Стирлинга и несложных аналитических преобразований. В самом деле,

$$|\Sigma| = P(k_{-1}, k_0, k_1) = \frac{n!}{k_{-1}!k_0!k_1!} = \frac{n!}{\left[\frac{p}{2}\right]!(n-p)!\left(p - \left[\frac{p}{2}\right]\right)!}.$$

Последнее выражение легко переписывается в терминах одного n :

$$\frac{n!}{\left[\frac{p}{2}\right]!(n-p)!\left(p - \left[\frac{p}{2}\right]\right)!} = \frac{n!}{\left[\frac{n}{4}\right]!\left(\frac{n}{2}\right)!\left(\frac{n}{2} - \left[\frac{n}{4}\right]\right)!}.$$

Рассмотрим величину $\left[\frac{n}{4}\right]!$. По формуле Стирлинга получаем

$$\left[\frac{n}{4}\right]! \sim \sqrt{2\pi\left[\frac{n}{4}\right]} \left(\left[\frac{n}{4}\right]\right)^{\left[\frac{n}{4}\right]} e^{-\left[\frac{n}{4}\right]}. \quad (3)$$

Мы знаем, что при $m \rightarrow \infty$ и $\varepsilon \asymp 1$ (ε может быть и отрицательным)

$$(m + \varepsilon)^{m+\varepsilon} = m^m P(m),$$

где порядок роста (или убывания) функции $P(m)$ полиномиальный (ср. п. 2.3). Если принять во внимание это соображение, учесть, что

$$\left[\frac{n}{4}\right] = \frac{n}{4} + \varepsilon, \quad \varepsilon \in [-1, 1],$$

и собрать воедино все сомножители полиномиального порядка в асимптотике (3), то получится выражение

$$\left[\frac{n}{4}\right]! \sim P_1(n) \left(\frac{n}{4}\right)^{n/4} e^{-\frac{n}{4}}.$$

Аналогичным путем приходим к записи

$$\left(\frac{n}{2} - \left[\frac{n}{4}\right]\right)! \sim P_2(n) \left(\frac{n}{4}\right)^{n/4} e^{-\frac{n}{4}}.$$

Наконец, с величиной $(n/2)!$ вообще все ясно:

$$\left(\frac{n}{2}\right)! \sim P_3(n) \left(\frac{n}{2}\right)^{n/2} e^{-n/2}.$$

Таким образом,

$$|\Sigma| = \frac{n!}{\left[\frac{n}{4}\right]!\left(\frac{n}{2}\right)!\left(\frac{n}{2} - \left[\frac{n}{4}\right]\right)!} \sim P_4(n) \frac{n^n e^{-n}}{\left(\left(\frac{n}{4}\right)^{n/4} e^{-n/4}\right)^2 \left(\frac{n}{2}\right)^{n/2} e^{-n/2}}.$$

Экспоненты чудесно уничтожаются, величины типа $n^{\gamma n}$ — тоже. Остается как раз то, что нужно:

$$|\Sigma| \sim P_4(n) (2\sqrt{2})^n = (2\sqrt{2} + o(1))^n.$$

Формула (1) доказана.

Теперь нам необходимо разобраться с формулой (2). Прежде всего сделаем из кратной суммы

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2}$$

повторную: очевидно, что

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2} = \sum_{q=0}^{p-1} \sum_{i=0}^{\lfloor q/2 \rfloor} C_n^i C_{n-i}^{q-2i}.$$

Докажем, что выражение $\sum_{i=0}^{\lfloor q/2 \rfloor} C_n^i C_{n-i}^{q-2i}$ максимально при $q = p - 1$. Для этого воспользуемся тривиальным фактом, состоящим в том, что $C_m^{l_1} \leq C_m^{l_2}$, коль скоро $l_1 \leq l_2 \leq m/2$. У нас

$$q - 2i \leq p - 1 - 2i < \frac{n}{2} - 2i = \frac{n - 4i}{2} \leq \frac{n - i}{2},$$

и, стало быть, ввиду упомянутого факта

$$C_n^i C_{n-i}^{q-2i} \leq C_n^i C_{n-i}^{p-1-2i} \quad \text{для всех } q \in \{0, \dots, p-1\}, \quad i \in \left\{0, \dots, \left\lfloor \frac{q}{2} \right\rfloor\right\},$$

т. е., действительно,

$$\sum_{i=0}^{\lfloor q/2 \rfloor} C_n^i C_{n-i}^{q-2i} \leq \sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i} \quad \text{для всех } q \in \{0, \dots, p-1\}.$$

Последнее неравенство означает, что

$$\sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i} \leq \sum_{q=0}^{p-1} \sum_{i=0}^{\lfloor q/2 \rfloor} C_n^i C_{n-i}^{q-2i} \leq p \sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i}.$$

Следовательно,

$$\sum_{q=0}^{p-1} \sum_{i=0}^{\lfloor q/2 \rfloor} C_n^i C_{n-i}^{q-2i} = Q_1(n) \sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i},$$

где порядок роста функции $Q_1(n)$ полиномиален.

Если мы докажем, что асимптотика максимального слагаемого в сумме $\sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i}$ имеет вид $(2,4628\dots + o(1))^n$, то получится, что

$$(2,4628\dots + o(1))^n \leq \sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i} \leq \frac{p+1}{2} (2,4628\dots + o(1))^n,$$

т. е.

$$\sum_{q=0}^{p-1} \sum_{i=0}^{[q/2]} C_n^i C_{n-i}^{q-2i} = Q_1(n) \sum_{i=0}^{(p-1)/2} C_n^i C_{n-i}^{p-1-2i} = (2,4628 \dots + o(1))^n,$$

и все в порядке. Что ж, будем действовать.

План действий нехитрый: возьмем функцию

$$f(x) = C_n^x C_{n-x}^{p-1-2x}$$

и найдем ее максимум в промежутке $x \in [0, (p-1)/2]$. Однако, во-первых, $f(x)$ определена лишь для целых x из указанного промежутка, а во-вторых, не совсем понятно, как с ней работать. Хотелось бы, как обычно, расписать биномиальные коэффициенты через факториалы и применить формулу Стирлинга. Тогда возникнет более или менее разумное выражение, у которого максимум ищется стандартно (если пренебречь — хотя бы на время — целочисленностью икса): вычисляется производная, и максимум находится либо там, где она равна нулю, либо на границах области, в которой «живет» x . Беда в том, что формула Стирлинга для $x!$ верна лишь при условии, что x стремится к бесконечности. А у нас есть и $x = 0$, и $x = 1$, и пр. Придется, стало быть, немного попотеть.

Рассмотрим три случая:

$$x < [\log n], \quad x > \frac{p-1}{2} - [\log n] \quad \text{и} \quad [\log n] \leq x \leq \frac{p-1}{2} - [\log n].$$

Ясно, что ими все исчерпывается. Предположим для верности, что n достаточно велико.

Случай 1. Итак, пусть $x < [\log n]$ и x целое. Тогда за счет тривиального неравенства $C_n^x \leq n^x$ получаем $C_n^x < n^{[\log n]} = e^{o(n)}$. В то же время

$$C_{n-x}^{p-1-2x} \leq C_n^{p-1-2x} \leq C_n^p.$$

Последняя оценка верна ввиду того, что

$$p-1-2x \leq p \leq \frac{n}{2}.$$

Однако

$$C_n^p = C_n^{n/2} = (2 + o(1))^n$$

благодаря стандартным выкладкам, вытекающим из формулы Стирлинга (ср. п. 2.3). Таким образом, в нашем случае

$$f(x) = C_n^x C_{n-x}^{p-1-2x} \leq e^{o(n)} (2 + o(1))^n = (2 + o(1))^n.$$

Это куда меньше, чем $(2,4628 \dots + o(1))^n$, и что-то подсказывает нам, что максимум не здесь.

Случай 2. Этот случай очень похож на предыдущий. В самом деле, пусть $x > \frac{p-1}{2} - [\log n]$ и x целое. Тогда

$$C_{n-x}^{p-1-2x} \leq C_n^{p-1-2x} \leq C_n^{2[\log n]} \leq n^{2[\log n]} = e^{o(n)}.$$

Одновременно

$$C_n^x \leq C_n^{(p-1)/2} = (1,754 \dots + o(1))^n.$$

Последняя асимптотика вытекает из уже привычных нам рутинных выкладок с формулой Стирлинга (ср. п. 2.3). Значит,

$$f(x) = C_n^x C_{n-x}^{p-1-2x} \leq e^{o(n)} (1,754 \dots + o(1))^n = (1,754 \dots + o(1))^n,$$

и это еще меньше, чем оценка из случая 1.

Случай 3. Пусть, наконец, целое число x лежит на отрезке

$$\left[[\log n], \frac{p-1}{2} - [\log n] \right].$$

Случаи 1 и 2 свидетельствуют о том, что если где на этом отрезке функция $f(x)$ и имеет вид $f(x) = (2,4628 \dots + o(1))^n$, то уж заведомо не на его концах. Так или иначе, но теперь мы вольны применять формулу Стирлинга и к величине $x!$, и к величине $(p-1-2x)!$. В результате несложных преобразований мы приходим к выражению

$$f(x) = Q_2(n) \frac{n^n}{x^x \left(\frac{n}{2} - 2x\right)^{n/2-2x} \left(\frac{n}{2} + x\right)^{n/2+x}},$$

где, как всегда, $Q_2(n)$ либо убывает, либо растет полиномиально. При этом мы по-прежнему апеллируем лишь к фактам типа

$$(m + \varepsilon)^{m+\varepsilon} = m^m P(m)$$

и не забываем, что $p = \frac{n}{2}$.

Удобно перейти к экспоненциальной форме записи

$$f(x) = Q_2(n) \exp \left\{ n \ln n - x \ln x - \left(\frac{n}{2} - 2x\right) \ln \left(\frac{n}{2} - 2x\right) - \left(\frac{n}{2} + x\right) \ln \left(\frac{n}{2} + x\right) \right\}.$$

Понятно, что если максимум последней экспоненты окажется равным $(2,4628 \dots + o(1))^n$, то $Q_2(n)$ уйдет в $o(1)$, и про него можно будет не вспоминать. Нужно, стало быть, манипулировать величиной

$$g(x) = n \ln n - x \ln x - \left(\frac{n}{2} - 2x\right) \ln \left(\frac{n}{2} - 2x\right) - \left(\frac{n}{2} + x\right) \ln \left(\frac{n}{2} + x\right),$$

стоящей как раз в показателе нашей экспоненты.

Допустим на время, что x — вещественная переменная. Тогда максимум функции $g(x)$ можно найти, дифференцируя ее по x . Производная $g'(x)$ имеет вид

$$g'(x) = -\ln x + 2 \ln\left(\frac{n}{2} - 2x\right) - \ln\left(\frac{n}{2} + x\right) = \ln \frac{\left(\frac{n}{2} - 2x\right)^2}{x\left(\frac{n}{2} + x\right)}.$$

Обозначая $\kappa = x/n$, с легкостью убеждаемся в том, что уравнение $g'(x) = 0$ совпадает с уравнением

$$12\kappa^2 - 10\kappa + 1 = 0,$$

корни которого суть

$$\kappa_{1,2} = \frac{5 \pm \sqrt{13}}{12}.$$

Корень

$$\kappa_2 = \frac{5 + \sqrt{13}}{12} = 0,717\dots > \frac{1}{2}$$

нам не подходит, так как иначе $x > n/2 = p$, что в рамках текущего случая невозможно. Корень же

$$\kappa_1 = \frac{5 - \sqrt{13}}{12} = 0,116\dots$$

воплне осмыслен: $x = \kappa_1 n$ лежит в интервале

$$\left([\log n], \frac{p-1}{2} - [\log n]\right),$$

коль скоро n велико (а у нас это так).

Подставляя $x = \kappa_1 n$ в функцию $e^{g(x)}$, в результате получаем в аккурат $(2,4628\dots + o(1))^n$. Уже и сейчас ясно, что

$$f(x) \leq (2,4628\dots + o(1))^n.$$

Однако и точное равенство достигается. Взять, например, $x = [\kappa_1 n]$ вполне достаточно.

Предложение 1 доказано. \square

3.4. Точна ли теорема 9?

В п. 2.3 мы показали, что линейно-алгебраический метод, примененный к задаче о совокупностях конечных множеств, обладает сразу двумя прекрасными свойствами: он дает очень сильную оценку, и эта оценка оказывается к тому же точна, коль скоро мы пренебрегаем

значениями бесконечно малых величин, стоящих в основании экспоненты вида $(1,754 \dots + o(1))^n$. Мы знаем, что задачи о совокупностях множеств и о $(0, 1)$ -векторах совпадают. Стало быть, там и говорить не о чем. А вот с задачей о $(-1, 0, 1)$ -векторах, которой мы сейчас занимаемся, пока не все ясно. Безусловно, мы только что убедились в том, что нетривиальная модификация линейно-алгебраического метода приводит к весьма глубокому результату: один запрет, и экспонента $(2,828 \dots + o(1))^n$ заменяется экспонентой $(2,4628 \dots + o(1))^n$, так что отношение этих двух функций само растет экспоненциально. Тем не менее, впадать в эйфорию рано. Каким бы мощным ни был наш метод, ничто не мешает ему быть несовершенным. К сожалению, так оно, по-видимому, и есть. Метод мощный, но существуют соображения, показывающие, что и его следует улучшать. В частности, как ни удивительна оценка $(2,4628 \dots + o(1))^n$, она вряд ли точна. Как говорится, не все коту масленица, и ниже мы постараемся продемонстрировать возможность фиаско. В сущности, это ведь не просто интересно: это еще и стимул для получения новых самостоятельных результатов.

Заметим, что в теореме 9, точность которой мы ставим теперь под сомнение, все параметры, описывающие совокупность векторов, жестко фиксированы, и потому нам бы стоило работать именно с ними. Однако гораздо проще осознать слабые места метода, рассматривая несколько иные конструкции. Мы поступим так: сперва обсудим задачи, похожие на изученную в рамках теоремы 9, а затем вернемся, собственно, к самой теореме и в свете новых знаний предметно поговорим о ней.

Итак, ниже мы приведем три примера, свидетельствующих о том, что линейно-алгебраический метод в том виде, в каком мы его знаем, не всегда оптимален, коль скоро речь идет о задачах про $(-1, 0, 1)$ -векторы. Первые два примера будут иметь «малую» размерность, последний — растущую.

Рассмотрим совокупность векторов

$$\Sigma = \{ \mathbf{x} = (x_1, \dots, x_8) : x_i \in \{-1, 0, 1\}, |\{i : x_i = 0\}| = 4 \}.$$

Таким образом, $|\Sigma| = C_8^4 2^4 = 1120$. В некотором роде Σ очень близка к совокупности из теоремы 9: конечно, n отныне фиксировано, но зато, как и прежде, число ненулевых координат в каждом векторе из совокупности равно половине размерности. Правда, есть и две тонкости. Во-первых, количество минус единиц мы никак не регламентируем, а во-вторых, $n = 8 = 2 \cdot 4$, и 4 не является простым числом. Ну, все это более для удобства.

Возьмем в Σ подсовокупность векторов Σ_1 , в которой первая ненулевая координата каждого элемента равна 1. Понятно, что

$$|\Sigma_1| = C_8^4 2^3 = 560.$$

Линейно-алгебраический метод позволяет доказать

Предложение 2. *Если совокупность*

$$\mathcal{F} = \{\mathbf{x}_1, \dots, \mathbf{x}_s\} \subset \Sigma_1$$

состоит из попарно неортогональных векторов, то элементов в ней не больше чем 157.

Заметим, что запрет в предложении 2 тоже нам привычен: мы лишь не хотим, чтобы скалярные произведения векторов из \mathcal{F} обнулялись.

Доказательство предложения 2. Мы не станем излагать практически никаких подробностей, поскольку схема доказательства повторяет ту, которая имела место при обосновании теоремы 9. Даже леммы по большому счету будут теми же. Мы их, таким образом, сформулируем заново, добавляя штрих к соответствующему номеру, и кратко прокомментируем.

Лемма 4'. *Скалярное произведение любых двух векторов из Σ_1 сравнимо с нулем по модулю 4 тогда и только тогда, когда оно равняется либо нулю, либо 4 (т. е. когда векторы либо ортогональны, либо совпадают).*

Именно для этой леммы мы и взяли, вместо всей исходной Σ , ее подсовокупность Σ_1 , в которой минимальное скалярное произведение элементов не меньше -3 .

Перед леммой 5' надо определить полиномы $\mathcal{P}_{\mathbf{x}}$ от 8 переменных y_1, \dots, y_8 , отвечающие векторам $\mathbf{x} \in \Sigma_1$. В данном случае мы полагаем

$$\mathcal{P}_{\mathbf{x}}(\mathbf{y}) = \mathcal{P}_{\mathbf{x}}(y_1, \dots, y_8) = \frac{1}{2} \prod_{i=1}^3 (i - (\mathbf{x}, \mathbf{y})).$$

Нетривиальное отличие нынешних полиномов от их аналогов из раздела 3.2 состоит в том, что их коэффициенты нельзя считать элементами конечного поля. Посему мы скажем, что $\mathcal{P}_{\mathbf{x}} \in \mathbb{Q}[y_1, \dots, y_8]$, где \mathbb{Q} — поле рациональных чисел. От $\mathcal{P}_{\mathbf{x}}$ мы перейдем к $\mathcal{P}'_{\mathbf{x}}$ в точности так же, как мы это делали в разделе 3.2. Справедлива

Лемма 5'. *Пусть $\mathbf{x}, \mathbf{y} \in \Sigma_1$. Тогда $\mathcal{P}'_{\mathbf{x}}(\mathbf{y}) \in \mathbb{Z}$, и условие*

$$\mathcal{P}'_{\mathbf{x}}(\mathbf{y}) \equiv 0 \pmod{2}$$

равносильно условию

$$(\mathbf{x}, \mathbf{y}) \not\equiv 0 \pmod{4}.$$

Имеет место

Лемма 6'. *Если совокупность \mathcal{F} устроена так же, как и в формулировке предложения 2, то полиномы $\mathcal{P}'_{\mathbf{x}_1}, \dots, \mathcal{P}'_{\mathbf{x}_s}$ линейно независимы над полем \mathbb{Q} .*

Для доказательства нужно повторить рассуждения, изложенные в отношении леммы 6. Однако сперва следует воспользоваться новой леммой 5' и считать на время, что полиномы суть функции из Σ_1 в \mathbb{Z} . Уже эти функции, благодаря стандартным соображениям, окажутся линейно независимыми над полем $\mathbb{Z}/2\mathbb{Z}$, а значит, и они, и тем более исходные полиномы как чисто алгебраические объекты будут независимы также над полем \mathbb{Q} . \square

Ясно в конечном итоге, что мощность произвольной совокупности $\mathcal{F} \subset \Sigma_1$, удовлетворяющей нашему ограничению, не превосходит числа мономов от восьми переменных, имеющих степень 3 (суммарную) и степень не выше 2 по каждой из переменных. Соответственно,

$$|\mathcal{F}| \leq C_8^3 + 56 + C_8^2 + 8 + 8 + 1 = 157.$$

Здесь первое слагаемое — это число мономов вида $x_i x_j x_k$, второе — число мономов $x_i^2 x_j$, третье — число мономов $x_i x_j$ и так далее. Предложение 2 доказано.

Заметим, что заодно мы намекнули на то, как можно работать с модулями, являющимися степенями простых (ср. главу 2).

Разумеется, метод опять проявил свою силу. Чего бы, казалось, еще желать? 157 куда как меньше, чем 560. Да в том-то и беда, что совсем легко доказывается

Предложение 3. *Если совокупность*

$$\mathcal{F} = \{\mathbf{x}_1, \dots, \mathbf{x}_s\} \subset \Sigma_1$$

состоит из попарно неортогональных векторов, то элементов в ней не больше чем 70.

Доказательство предложения 3. Разобьем совокупность Σ_1 на 70 частей, каждая из которых имеет мощность 8 и состоит из попарно ортогональных векторов. Скажем, первая часть может содержать векторы

$$\begin{aligned} (1, 1, 1, 1, 0, 0, 0, 0), & \quad (1, 1, -1, -1, 0, 0, 0, 0), \\ (1, -1, -1, 1, 0, 0, 0, 0), & \quad (1, -1, 1, -1, 0, 0, 0, 0), \\ (0, 0, 0, 0, 1, 1, 1, 1), & \quad (0, 0, 0, 0, 1, 1, -1, -1), \\ (0, 0, 0, 0, 1, -1, -1, 1), & \quad (0, 0, 0, 0, 1, -1, 1, -1). \end{aligned}$$

И так далее. Из каждой части в \mathcal{F} может попасть только один вектор, и предложение доказано. \square

Не правда ли, поразительный эффект? Конечно, тут $n = 8$, и подобные соображения вряд ли будут столь же значимыми при $n \rightarrow \infty$. Тем не менее, не задуматься нельзя.

Возникает, как следствие из сказанного, второй пример, подтверждающий подозрение, что метод подлежит усилению. Пусть

$$\Sigma = \{\mathbf{x} = (x_1, \dots, x_{16}) : x_i \in \{-1, 0, 1\}, |\{i : x_i = 0\}| = 8\},$$

а Σ_1 состоит из тех и только тех векторов в Σ , у которых первая ненулевая координата равна единице. Понятно, что $|\Sigma| = C_{16}^8 2^8 = 3\,294\,720$, в то время как $|\Sigma_1| = C_{16}^8 2^7 = 1\,647\,360$. Спрашивается снова: *а как велика может быть мощность совокупности $\mathcal{F} \subset \Sigma_1$, состоящей из попарно неортогональных векторов?* Линейно-алгебраический метод дает оценку $|\mathcal{F}| \leq 169\,677$ (попробуйте доказать это). Однако В. Дрёмов осуществил нетривиальное развитие идеи из предложения 3 и показал, что $|\mathcal{F}| \leq 156\,213$. Разница уже ничтожна, но и на нее хорошо бы обратить внимание. Впрочем, еще интереснее, что с большой вероятностью верна

Гипотеза 1. *В сделанных выше предположениях $|\mathcal{F}| < 12\,000$.*

Иными словами, правдоподобна возможность понижения и линейно-алгебраической, и дрёмовской оценок эдак в 12–13 раз! Было бы исключительно здорово, если бы кто-нибудь доказал гипотезу. Тем более, что позже мы еще обратимся к ней.

Во всем изложенном неубедительно то, что всякий раз $n \asymp 1$. Вдруг при $n \rightarrow \infty$ все слабости метода уйдут в какое-нибудь $o(1)$ под знаком очередной экспоненты? Что тогда? Ан нет, и сейчас мы в последнем примере увидим, как все тонко.

Итак, пусть p — нечетное простое число и $n = 4p - 8$. Рассмотрим совокупность

$$\Sigma = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{-1, 0, 1\}, \\ |\{i : x_i = 0\}| = 2p - 4, |\{i : x_i = -1\}| = 1\}.$$

Понятно, что Σ снова отдаленно напоминает аналогичное множество из теоремы 9. Однако и разница не может не броситься в глаза: отрицательная-то координата в каждом векторе из Σ всегда одна. В этом различии есть некоторый смысл, который мы проясним в конце раздела.

Запретим векторам из Σ иметь скалярное произведение $p - 4$, т. е. будем искать максимум мощности совокупности $\mathcal{F} \subset \Sigma$, свободной от пар векторов, дающих в скалярном произведении упомянутую величину. С помощью линейно-алгебраического метода доказывается

Предложение 4. Если совокупность

$$\mathcal{F} = \{\mathbf{x}_1, \dots, \mathbf{x}_s\} \subset \Sigma$$

состоит из векторов, скалярные произведения которых не равняются $p-4$, то

$$|\mathcal{F}| \leq \sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2},$$

где

$$\mathcal{A} = \{(m_1, m_2) : m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq p-1\}.$$

Доказательство предложения 4. Все стандартно, и мы лишь перечислим необходимые леммы.

Лемма 4''. Скалярное произведение любых двух векторов из Σ сравнимо с минус четверкой по модулю p тогда и только тогда, когда оно равняется либо $p-4$, либо $2p-4$.

Лемма 5''. Пусть $\mathbf{x}, \mathbf{y} \in \Sigma$. Тогда условие

$$\mathcal{P}'_{\mathbf{x}}(\mathbf{y}) \equiv 0 \pmod{p}$$

равносильно условию

$$(\mathbf{x}, \mathbf{y}) \not\equiv -4 \pmod{p}.$$

Здесь полиномы

$$\mathcal{P}'_{\mathbf{x}} \in \mathbb{Z}/p\mathbb{Z}[y_1, \dots, y_n]$$

получаются, как обычно, кратным применением соотношения $y_i^3 = y_i$, $i = 1, \dots, n$, к мономам, возникающим при раскрытии скобок в полиномах

$$\mathcal{P}_{\mathbf{x}}(\mathbf{y}) = \frac{\prod_{i=0}^{p-1} (i - (\mathbf{x}, \mathbf{y}))}{p-4 - (\mathbf{x}, \mathbf{y})}.$$

Лемма 6''. Если совокупность \mathcal{F} устроена так же, как и в формулировке предложения 4, то полиномы $\mathcal{P}'_{\mathbf{x}_1}, \dots, \mathcal{P}'_{\mathbf{x}_s}$ линейно независимы над полем $\mathbb{Z}/p\mathbb{Z}$.

В конечном счете $|\mathcal{F}|$ не превосходит размерности пространства штрихованных полиномов, а она, очевидно, не больше величины

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2}.$$

Предложение доказано. \square

Посредством выкладок, почти дословно повторяющих те, что мы произвели в п. 3.3, можно установить асимптотику

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2} = (1,852\dots + o(1))^n.$$

И это плохо, так как сейчас мы с легкостью докажем

Предложение 5. *Если совокупность*

$$\mathcal{F} = \{\mathbf{x}_1, \dots, \mathbf{x}_s\} \subset \Sigma$$

состоит из векторов, скалярные произведения которых не равняются $p - 4$, то

$$|\mathcal{F}| \leq nC_{n-1}^{p-1} = (1,754\dots + o(1))^n.$$

Доказательство предложения 5. По существу, мы опять воспользуемся идеей из предложения 3: разобьем сперва \mathcal{F} на части $\mathcal{F}_1, \dots, \mathcal{F}_n$, где

$$\mathcal{F}_i = \{\mathbf{x} = (x_1, \dots, x_n) : x_i = -1\}, \quad i = 1, \dots, n.$$

Рассмотрим, например, \mathcal{F}_1 . У векторов из этой совокупности первая координата равна -1 . Удалим эту общую координату, так что в результате возникнут $(n - 1)$ -мерные $(0, 1)$ -векторы, образующие совокупность

$$\mathcal{F}'_1 = \{\mathbf{x}' = (x_2, \dots, x_n) : \mathbf{x} = (-1, x_2, \dots, x_n) \in \mathcal{F}_1\}.$$

Отождествим по стандартному принципу совокупность векторов \mathcal{F}'_1 с совокупностью \mathcal{M}'_1 подмножеств множества \mathcal{R}_{n-1} . Ясно, что мощность k каждого множества в \mathcal{M}'_1 равна $2p - 5$, причем ввиду исходного запрета на скалярные произведения векторов из $\mathcal{F}_1 \subset \mathcal{F}$ этим множествам запрещено пересекаться по $t = p - 5$ элементам. Применяя теорему 3 Франкля—Уилсона с $k - t = p$ и $k > 2t + 1$, получаем, что

$$|\mathcal{F}_1| = |\mathcal{F}'_1| = |\mathcal{M}'_1| \leq C_{n-1}^{p-1}.$$

Разумеется, та же оценка верна и для других \mathcal{F}_i . Значит,

$$|\mathcal{F}| \leq |\mathcal{F}_1| + \dots + |\mathcal{F}_n| \leq nC_{n-1}^{p-1}.$$

Наконец, $p \sim n/4$, и давно привычное нам аналитическое искусство (формула Стирлинга и пр.) влечет асимптотику

$$C_{n-1}^{p-1} = (1,754\dots + o(1))^n.$$

Предложение доказано. \square

Обсудим, как и обещали, суть последнего примера. Представим себе на минуту, что в векторах из этого примера отрицательных координат вовсе нет. Тогда координаты y_i этих векторов суть нули и единицы, а они удовлетворяют соотношению $y_i^2 = y_i$. Если бы в рамках линейно-алгебраического метода мы при переходе от полиномов $\mathcal{P}_{\mathbf{x}}$ к полиномам $\mathcal{P}'_{\mathbf{x}}$ могли апеллировать к такому соотношению, то переменные в мономах имели бы исключительно первые степени. Это

бы означало, что размерность пространства, оценивающая мощность интересующей нас совокупности, не превосходит

$$\sum_{i=0}^{p-1} C_n^i \sim C_n^{n/4} = (1,754 \dots + o(1))^n,$$

т. е. предложение 5 было бы ничем не лучше предложения 4. Собственно, теорема Франкла—Уилсона, переведенная на язык $(0, 1)$ -векторов, так и доказывается. Беда наступает при добавлении к нулям и единицам всего лишь одной отрицательной координаты. С точки зрения метода это провал: первыми степенями в мономах не отделаться, причем вторых степеней сразу образуется так же много, как если бы в векторах было порядка $\frac{n}{4}$ минус единиц (ср. теорему 9); в результате и размерность пространства полиномов катастрофически увеличивается — с $(1,754 \dots + o(1))^n$ до $(1,852 \dots + o(1))^n$. Однако предложение 5 свидетельствует о том, что иногда бороться с проблемой можно. К сожалению, предлагаемые там средства слишком кустарны, и применять их при работе с теоремой 9 бессмысленно. В то же время ясно, что нечто делать все равно необходимо, а с этого мы и начали раздел.

Итак мы поняли что, вероятнее всего, теорема 9 не вполне удовлетворительна. Тем не менее, хорошо бы еще осознать, к чему, вообще, стоит стремиться: насколько большой может быть совокупность \mathcal{F} из теоремы?

Сейчас, наконец, мы приведем пример достаточно большой совокупности попарно неортогональных векторов

$$\mathcal{F} \subset \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

где k_{-1}, k_0, k_1 — параметры из теоремы 9. Напомним, что

$$n = 2p, \quad k_{-1} + k_1 = p, \quad k_{-1} = \left\lfloor \frac{p}{2} \right\rfloor$$

(p — нечетное простое). Однако простота и возникающие в связи с ней целые части суть просто важные атрибуты метода. Посему, как и в случае с совокупностями множеств, мы пренебрежем деталями и исключительно для удобства будем считать, что n делится на 24,

$$k_{-1} + k_1 = \frac{n}{2}, \quad k_{-1} = \frac{n}{4}:$$

с точностью до мелочей, это и есть то, что нам требуется. Дабы сделать прозрачным происхождение нашей будущей конструкции, мы напомним сначала идею, которой мы воспользовались при построении совокупности подмножеств множества \mathcal{R}_n , демонстрировавшей

точность теоремы Франкла—Уилсона. Только теперь рассуждать мы будем не в терминах множеств, а в эквивалентных терминах $(0, 1)$ -векторов. Действовали мы так (см. п. 2.3): разбили множество координатных позиций на две части и взяли все $(0, 1)$ -векторы, имеющие как в первой, так и во второй части заданные наперед количества единичных координат. При этом мы следили за тем, чтобы минимальное скалярное произведение наших векторов (минимальная мощность пересечения множеств) было строго больше запрещенной величины и, стало быть, заведомо ей не равнялось. Это минимальное произведение складывалось, конечно, из соответствующих минимумов в обеих частях разбиения. Именно потому в той конкретной ситуации разумно было мощности частей определить как $n/2$, а количества единичных координат в них задать выражениями $[3n/8] + 1$ и $n/2 - [3n/8] - 1$. Там, по счастью, и оптимальность указанного выбора имела место за счет теоремы Франкла—Уилсона—Альсведе—Хачатряна, причем мы несколько раз подчеркнули близость задач о запрете одной мощности пресечения t и всех мощностей, величин t не превосходящих (задач о функциях $m(n, k, t)$ и $f(n, k, t)$). Ввиду всего этого кажется естественным и в нынешней ситуации реализовать аналогичную программу. Цифр раньше было две (0 и 1); разбивали мы множество координат на два куска, и получался оптимум. Почему бы и тут не поступить так же? Цифр стало три ($-1, 0$ и 1); разобьем мы как-нибудь координатные позиции на три группы, зафиксируем заранее количества координат той или иной величины да и рассмотрим все $(-1, 0, 1)$ -векторы, у которых и в первой, и во второй, и в третьей группах — те самые заданные наперед количества координат определенного вида. Лишь бы сумма минимальных скалярных произведений векторов, образованных координатами из соответствующих групп, была больше нуля (мы же с ортогональностью боремся). Чем черт не шутит — глядишь, и здесь оптимум получится.

Строго постановка задачи выглядит следующим образом. Пусть $m_1, m_2, m_3 \in \mathbb{N} \cup \{0\}$ таковы, что $m_1 + m_2 + m_3 = n$. Это будут мощности упомянутых выше групп в разбиении множества координатных позиций. Мы разрешили им обращаться в нуль для пущей общности.

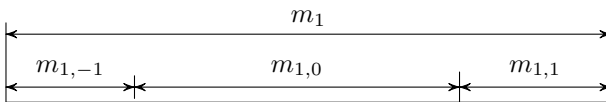


Рис. 3

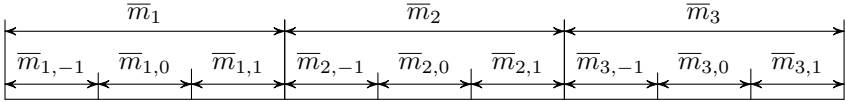


Рис. 4

Пусть, далее, $m_{1,-1}, m_{1,0}, m_{1,1}$ — тоже неотрицательные целые (возможно, равные нулю), в сумме дающие m_1 . Эти числа сыграют роль наперед заданных количеств координат соответствующей величины ($-1, 0$ или 1), расположенных в первой координатной группе каждого вектора строящейся совокупности (см. рис. 3). Аналогично определяются $m_{2,-1}, m_{2,0}, m_{2,1}$ (их сумма равна m_2) и $m_{3,-1}, m_{3,0}, m_{3,1}$ (их сумма есть m_3). Кроме того,

$$m_{1,-1} + m_{2,-1} + m_{3,-1} = \frac{n}{4}, \quad m_{1,1} + m_{2,1} + m_{3,1} = \frac{n}{4}$$

и

$$m_{1,0} + m_{2,0} + m_{3,0} = \frac{n}{2}$$

(общие количества координат данного вида совпадают с нашими k_{-1}, k_0 и k_1 соответственно, см. рис. 4). И дополнительно, если положить $\underline{s}_i = \min(\mathbf{x}, \mathbf{y})$, где $i \in \{1, 2, 3\}$, а минимум берется по всем векторам \mathbf{x}, \mathbf{y} из совокупности

$$\mathcal{F}_i = \{\mathbf{x} = (x_1, \dots, x_{m_i})\}$$

$$x_j \in \{-1, 0, 1\}, \quad |\{j: x_j = \nu\}| = m_{i,\nu}, \quad \nu \in \{-1, 0, 1\},$$

то $\underline{s}_1 + \underline{s}_2 + \underline{s}_3 > 0$. Все уже сказано, и в свете этого понятно, откуда берется совокупность

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

$$= \{\mathbf{x} = (x_1, \dots, x_n): x_i \in \{-1, 0, 1\}, \quad |\{i \in \{1, \dots, m_1\}: x_i = \nu\}| = m_{1,\nu},$$

$$|\{i \in \{m_1 + 1, \dots, m_1 + m_2\}: x_i = \nu\}| = m_{2,\nu},$$

$$|\{i \in \{m_1 + m_2 + 1, \dots, n\}: x_i = \nu\}| = m_{3,\nu}, \quad \nu \in \{-1, 0, 1\}\}$$

и почему в ней содержатся только нужные нам и к тому же попарно неортогональные векторы. Немного странно выглядят, быть может, аргументы совокупности \mathcal{F} , но ведь остальные через них выражаются: скажем,

$$m_3 = n - m_1 - m_2, \quad m_{3,-1} = \frac{n}{4} - m_{1,-1} - m_{2,-1} \quad \text{и т. д.}$$

Сама задача состоит в максимизации по шести независимым параметрам величины $|\mathcal{F}|$. Например, при

$$m_1 = m_2 = \frac{n}{3}, \quad m_{1,-1} = \frac{5n}{24} + 1, \quad m_{1,0} = \frac{n}{8} - 1, \\ m_{2,-1} = \frac{n}{24} - 1, \quad m_{2,0} = \frac{n}{8} + 1$$

все в порядке (недаром же у нас n на 24 делилось), и мы имеем

$$|\mathcal{F}| = C_{n/3}^{5n/24+1} C_{n/3}^{n/6} C_{n/6}^{n/24-1} C_{n/3}^{n/12} = (2,08 \dots + o(1))^n.$$

Последнее равенство стандартно, и каждый сам может его обосновать.

Как видно, мощность построенной совокупности довольно велика. Конечно, мы взяли параметры едва ли не наугад, но, если повозиться с ними подольше, станет ясно, что особенно больших-то совокупностей и нет. Короче, на данном пути до $(2,46 \dots + o(1))^n$ вряд ли доберется получиться. С другой стороны, связь нашей конструкции с построением Альсведе и др. мотивирует следующую гипотезу.

Гипотеза 2. *Самая большая совокупность попарно неортогональных $(-1, 0, 1)$ -векторов с параметрами k_{-1}, k_0, k_1 из теоремы 9 находится в рамках описанной выше процедуры. Ее мощность есть*

$$\max P(m_{1,-1}, m_{1,0}, m_{1,1}) P(m_{2,-1}, m_{2,0}, m_{2,1}) P(m_{3,-1}, m_{3,0}, m_{3,1}),$$

где максимум берется по всем допустимым значениям параметров, из которых шесть — независимые.

В свою очередь, верна, по-видимому,

Гипотеза 3. *Упомянутый в гипотезе 2*

$$\max P(m_{1,-1}, m_{1,0}, m_{1,1}) P(m_{2,-1}, m_{2,0}, m_{2,1}) P(m_{3,-1}, m_{3,0}, m_{3,1})$$

равен $(c + o(1))^n$, где $c < 2,4628 \dots$

Вторая гипотеза не столь интересна: найти максимум можно даже перебором. А вот первая весьма примечательна. Ведь что бы нам, в действительности, мешало обобщить конструкцию и осуществлять разбиение множества координатных позиций не на три, а на четыре, пять и т. д. частей? Параметров стало бы больше, и откуда такая уверенность, что это не приведет к дальнейшим усилениям результатов? Но мы уже дали соответствующую мотивировку: в теореме Альсведе и др. тоже можно было не ограничиваться разбиениями \mathcal{R}_n на две группы, однако там и двух хватило. Есть, есть шанс, что гипотеза 2 правильная. И этот шанс значителен.

В этом разделе мы столкнулись с разнообразными применениями линейно-алгебраического метода. В следующем разделе мы обсудим обобщения теоремы 9 гораздо более детально.

3.5. Вокруг теоремы 9

Прежде всего мы приведем достаточно общий результат, являющийся аналогом результата из теоремы 9. Конечно, и он подлежит дальнейшим уточнениям, но ведь ни для кого, наверное, не секрет, что любой факт можно обобщать до бесконечности: тем не менее, отнюдь не всякий раз эта деятельность осмысленна. Мы будем апеллировать к обозначениям

$$\Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

$$\underline{\Sigma}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1), \quad \bar{\Sigma}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

которые были введены нами в п. 3.1. Если в теореме 9 речь шла о совершенно конкретных параметрах k_{-1}, k_0, k_1 , то теперь они смогут принимать абсолютно любые значения. За счет линейно-алгебраического метода доказывается

Теорема 10. Пусть q — это такое число вида $q = p^\alpha$ (p — простое, $\alpha \geq 1$), что

$$\bar{\Sigma}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - 2q < \underline{\Sigma}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1).$$

Тогда мощность произвольной подсовокупности векторов в

$$\Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

у которой скалярное произведение любых двух элементов не равно

$$\bar{\Sigma}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - q,$$

не превосходит величины

$$\sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2},$$

где

$$\mathcal{A} = \{(m_1, m_2): m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq q - 1\}.$$

Нет сомнений, что после того, как мы обосновали теорему 9 и предложение 4, заинтересованному читателю уж точно не составит труда убедиться в справедливости последнего утверждения, коль скоро, вместо q вида p^α , в нем будет фигурировать просто $q = p$. Впрочем, и со степенями простых мы кое-где сталкивались (предложение 2), так что мы бы рекомендовали теорему 10 для самостоятельного доказательства. В любом случае, возможность работы не только с p , но и с q является первым тривиальным свидетельством общности теоремы. Второй не менее очевидный факт, подтверждающий широту результата, мы, собственно, упоминали: параметры k_{-1}, k_0, k_1 ничем не регламентированы. Правда, хорошо бы еще понять, почему теорема 9 есть

частный случай теоремы 10. Это-то тоже важно. Действительно, если

$$k_1 + k_{-1} = p, \quad \text{а} \quad k_{-1} = \left\lfloor \frac{p}{2} \right\rfloor$$

(p — нечетное простое), то

$$\begin{aligned} \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) &= k_1 + k_{-1} = p, \\ \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) &= -2 \left\lfloor \frac{p}{2} \right\rfloor. \end{aligned}$$

При $q = p$ имеем

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - 2q = -p < \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

т. е. нужное неравенство выполнено. Но при таком q оценка из теоремы 10 совпадает с оценкой из теоремы 9, и все в порядке.

Недостаток у теоремы 10 тот же, что и у теоремы Франкла—Уилсона: мы не умеем работать с произвольным q . Однако в п. 2.4 мы детально обсудили аналогичную ситуацию и пришли к выводу, что, хотя бороться с проблемой нужно, она не столь глобальна: простые числа и тем более их степени достаточно плотны в натуральном ряде, и, в частности, чисел вида

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - q, \quad q = p^\alpha,$$

на отрезке

$$\left[\underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1), \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) \right]$$

весьма много.

Теперь мы проследим одной простой, но крайне важный для нас в дальнейшем эффект. Пусть параметры k_{-1}, k_0, k_1 фиксированы. Обозначим через M мощность совокупности $\Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)$:

$$M = |\Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)| = P(k_{-1}, k_0, k_1).$$

Положим $D = D(q)$ равным величине оценки из теоремы 10. Очевидно, что если мы желаем с какой-либо целью подобрать q , при котором отношение M/D максимально, то нам достаточно минимизировать D (так как M от q не зависит). В свою очередь, величина D тем меньше, чем меньше q , и, стало быть, с точки зрения максимума дроби M/D необходимо применять теорему 10 с минимальным $q = p^\alpha$, дающим неравенство

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - 2q < \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1).$$

Спрашивается, насколько маленьким может оказаться такое q ? Понятно, что в идеале оно должно не более чем на единицу отличаться

от величины

$$\frac{1}{2}(\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)) \quad \text{и т. д.}$$

К сожалению, так будет не всегда, ведь q — это обязательно степень простого. Тем не менее, мы знаем (см. п. 2.4), что, например, между x и $x + O(x^{38/61})$ заведомо есть простое число. Это означает, что $q = p^\alpha$ непременно имеет вид

$$\frac{1}{2}(\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)) + O\left(\left(\frac{1}{2}\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - \frac{1}{2}\underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)\right)^{38/61}\right).$$

Правда, если величина

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)$$

не стремится к бесконечности, то смысл «о большого» как остаточного члена в асимптотике теряется. Эта тонкость исчезает, коль скоро, скажем, $k_1 = k_1(n) \rightarrow \infty$ и $k_{-1} = k_{-1}(n) \rightarrow \infty$ при $n \rightarrow \infty$. Так было, кстати, в рамках теоремы 9, и там величина запрета была подобрана в нынешнем смысле оптимально: если в обозначениях теоремы 9 взять $q < p$, то $q \leq p - 1$ и

$$\begin{aligned} \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - 2q &\geq -p + 2 > \\ &> \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = -2\left[\frac{p}{2}\right]. \end{aligned}$$

Заметим, что при постоянных k_{-1}, k_0, k_1 гораздо более значим перебор конкретных q . Например, если $k_{-1} = k_1 = 4, k_0 = 8$, то

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = 8, \quad \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = -8,$$

и в теореме 10 можно брать любое q из множества $\{9, 11, 13, \dots\}$. Наименьшее q здесь, между прочим, не просто, а наибольшее есть, по сути, $q = 16$, так как при $q > 16$ и запрещать нечего:

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - q < -8 = \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1).$$

До сих пор мы обсуждали задачи с $(0, 1)$ - и $(-1, 0, 1)$ -векторами. Но ведь не сошелся же на них мир клином, в самом деле. Почему бы не разрешить координатам наших векторов принимать любые значения? Пусть b_1, \dots, b_r — произвольные вещественные числа, а k_{b_1}, \dots, k_{b_r} — произвольные натуральные, в сумме дающие n (n — как обычно, размерность). Рассмотрим совокупность векторов

$$\begin{aligned} \Sigma = \Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}) &= \{\mathbf{x} = (x_1, \dots, x_n) : \\ x_i \in \{b_1, \dots, b_r\}, |\{i: x_i = b_1\}| &= k_{b_1}, \dots, |\{i: x_i = b_r\}| = k_{b_r}\}. \end{aligned}$$

Таким образом, числа b_1, \dots, b_r как раз играют роль значений координат наших векторов, а числа k_{b_1}, \dots, k_{b_r} суть количества координат данной величины в каждом векторе из Σ . Понятно, в частности, почему мы потребовали, чтобы $k_{b_1} + \dots + k_{b_r} = n$. Ясно, вместе с тем, что мы имеем прямое обобщение прежней деятельности. Скажем, если $r = 2, b_1 = 0, b_2 = 1$, то речь идет о науке из второй главы, а если $r = 3, b_1 = -1, b_2 = 0, b_3 = 1$, то мы возвращаемся к только что изученному нами кругу вопросов. Заметим, что величине r (количеству типов координат) ничто не мешает зависеть от n . Например, даже ситуация, в которой $r = n, b_1 = 1, b_2 = 2, \dots, b_r = n$, вполне осмысленна (здесь, без сомнения, $k_{b_1} = \dots = k_{b_r} = 1$). При этом, как видно, и сами числа b_1, \dots, b_r не обязаны быть константами типа $0, 1, -1$ и т. д. Заметим еще, что

$$|\Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})| = P(k_{b_1}, \dots, k_{b_r}) = \frac{n!}{k_{b_1}! \cdot \dots \cdot k_{b_r}!},$$

и это полезно иметь в виду.

Положим, как обычно,

$$\begin{aligned} \bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}) &= \max_{\mathbf{x}, \mathbf{y} \in \Sigma} (\mathbf{x}, \mathbf{y}), \\ \underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}) &= \min_{\mathbf{x}, \mathbf{y} \in \Sigma} (\mathbf{x}, \mathbf{y}). \end{aligned}$$

По аналогии с теоремами 3 и 10 может быть доказана

Теорема 11. Пусть b_1, \dots, b_r — целые, а q — это такое число вида $q = p^\alpha$ (p — простое, $\alpha \geq 1$), что

$$\bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}) - 2q < \underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}).$$

Тогда мощность произвольной подсовкупности векторов в

$$\Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}),$$

у которой скалярное произведение любых двух элементов не равно

$$\bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}) - q,$$

не превосходит величины

$$\sum_{(m_1, \dots, m_{r-1}) \in \mathcal{A}} C_n^{m_1} \cdot C_{n-m_1}^{m_2} \cdot \dots \cdot C_{n-m_1-\dots-m_{r-2}}^{m_{r-1}},$$

где

$$\mathcal{A} = \{(m_1, \dots, m_{r-1}) : m_1, \dots, m_{r-1} \in \mathbb{N} \cup \{0\}, m_1 + \dots + m_{r-1} \leq n, m_1 + 2m_2 + \dots + (r-1)m_{r-1} \leq q-1\}.$$

Формулировка теоремы 11 мало отличается от формулировки теоремы 10, и это неудивительно: линейно-алгебраический язык к настоящему времени развит весьма и весьма хорошо. Собственно, если в теореме 11 положить $r = 3$, то с точностью до значений величин

$$\begin{aligned} & \bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}), \\ & \underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}) \end{aligned}$$

получится теорема 10. Однако, если мы пожелаем понять, насколько силен результат теоремы 11, то, как и в п. 3.3, нам придется вычислять асимптотику $(r - 1)$ -кратной суммы. Когда $r - 1 = 2$, это еще терпимо, но при $r > 3$ — это тяжелая задача. Для случаев $r = 4$, $b_1 = 0, \dots, b_4 = 3$ и $r = 5$, $b_1 = 0, \dots, b_5 = 4$ (k_{b_i} — совершенно любые) ее недавно решила И. М. Шитова.

Аналогом теоремы 4 служит

Теорема 12. Пусть b_1, \dots, b_r — целые, а q — это число вида $q = p^\alpha$ (p — простое, $\alpha \geq 1$). Тогда мощность произвольной подсовокупности векторов в

$$\Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}),$$

у которой скалярное произведение любых двух элементов не сравнимо с

$$\bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})$$

по модулю q , не превосходит величины

$$\sum_{(m_1, \dots, m_{r-1}) \in A} C_n^{m_1} \cdot C_{n-m_1}^{m_2} \cdot \dots \cdot C_{n-m_1-\dots-m_{r-2}}^{m_{r-1}},$$

где A такое же, как и в теореме 11.

Теоремы 10, 11 и 12 допускают различные обобщения, уточнения и переформулировки. Это почти бескрайнее поле деятельности, порой с чересчур громоздкими результатами, и мы не станем в него углубляться.

Остается еще один важный тип проблем, которого, обсуждая свойства совокупности

$$\Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}),$$

мы пока не касались. Речь идет о задачах, аналогичных задаче про величину $f(n, k, t)$ (теорема Франкла—Уилсона—Альсведе—Хачатряна) и задаче, в связи с которой мы высказали гипотезы 2 и 3. Иными словами, мы хотим понять, насколько большой может быть совокупность

$$\mathcal{F} \subset \Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}),$$

коль скоро мы предполагаем, что скалярное произведение любых двух векторов $\mathbf{x}, \mathbf{y} \in \mathcal{F}$ не меньше какой-нибудь наперед заданной величины

$$t \in [\bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}), \underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})].$$

К несчастью (а может, и к счастью), в рамках этой тематики не сделано практически ничего. Что ж, нужно заполнить такой существенный пробел. Формулируя гипотезу 2, мы очень подробно и тщательно комментировали вероятный способ построения максимальной совокупности $(-1, 0, 1)$ -векторов (с $k_{-1} = k_1 = n/4$ и пр.), в которой все попарные скалярные произведения положительны. Сейчас мы предложим некоторую достаточно общую конструкцию, которая также сможет, по-видимому, претендовать на роль оптимальной. Естественно, параметров в ней будет еще больше (ср. раздел 3.4), но мы их столь детально комментировать уже не станем. Смысл их очень легко будет понять, сопоставляя их определение с похожим определением из раздела 3.4.

Итак, пусть b_1, \dots, b_r — целые, k_{b_1}, \dots, k_{b_r} — какие угодно, а функция $r = r(n)$ — либо не «очень быстро» растет, либо и вовсе постоянна (гипотеза об оптимальности нижеследующей конструкции более правдоподобна при $r = \text{const}$, хотя есть шанс, что от константы удастся потом оторваться). Зафиксируем

$$t \in [\bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}), \underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})].$$

Рассмотрим сперва произвольные неотрицательные целые m_1, \dots, m_r , для которых что $m_1 + \dots + m_r = n$ (ср. §3.4, где $r = 3$). Составим из них для краткости дальнейшей записи «вектор» $\mathbf{m} = (m_1, \dots, m_r)$. Возьмем, далее, любые числа m_{i,b_j} , $i, j \in \{1, \dots, r\}$, из которых можно (опять-таки для краткости) составить матрицу

$$M = \begin{pmatrix} m_{1,b_1} & m_{1,b_2} & \dots & m_{1,b_r} \\ m_{2,b_1} & m_{2,b_2} & \dots & m_{2,b_r} \\ \vdots & \vdots & \ddots & \vdots \\ m_{r,b_1} & m_{r,b_2} & \dots & m_{r,b_r} \end{pmatrix}$$

и которые удовлетворяют следующими условиям:

1. Все элементы матрицы M — неотрицательные целые.
2. Сумма элементов, стоящих в i -й строке матрицы M , равна m_i , $i = 1, \dots, r$.
3. Сумма элементов, стоящих в j -м столбце матрицы M , равна k_{b_j} , $j = 1, \dots, r$.

4 (вытекает из 2 и 3). Сумма всех элементов матрицы \mathbf{M} равна n .

5. Положим

$$\mathcal{F}_i = \{ \mathbf{x} = (x_1, \dots, x_{m_i}) : \\ x_j \in \{b_1, \dots, b_r\}, |\{j: x_j = \nu\}| = m_{i,\nu}, \nu \in \{b_1, \dots, b_r\} \}, \\ \underline{s}_i = \min_{\mathbf{x}, \mathbf{y} \in \mathcal{F}_i} (\mathbf{x}, \mathbf{y}), \quad i = 1, \dots, r.$$

Тогда выполнено неравенство $\underline{s}_1 + \dots + \underline{s}_r \geq t$.

Определим совокупность векторов

$$\mathcal{F} \subset \Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})$$

как

$$\mathcal{F} = \mathcal{F}(\mathbf{m}, \mathbf{M}) = \{ \mathbf{x} = (x_1, \dots, x_n) : x_i \in \{b_1, \dots, b_r\}, \\ |\{i \in \{1, \dots, m_1\} : x_i = \nu\}| = m_{1,\nu}, \\ |\{i \in \{m_1 + 1, \dots, m_1 + m_2\} : x_i = \nu\}| = m_{2,\nu}, \dots \\ \dots, |\{i \in \{m_1 + \dots + m_{r-1} + 1, \dots, n\} : x_i = \nu\}| = m_{r,\nu}, \nu \in \{b_1, \dots, b_r\} \}.$$

Конструкция завершена. Ясно, что условие 5 влечет неравенство $(\mathbf{x}, \mathbf{y}) \geq t$, коль скоро $\mathbf{x}, \mathbf{y} \in \mathcal{F}$. Все остальные условия лишь обеспечивают корректность задания параметров, в результате чего типичный вектор из \mathcal{F} выглядит так же, как вектор, изображенный на рис. 5 (ср. рис. 3 и 4). Подчеркнем еще раз, что мы высказываем гипотезу:

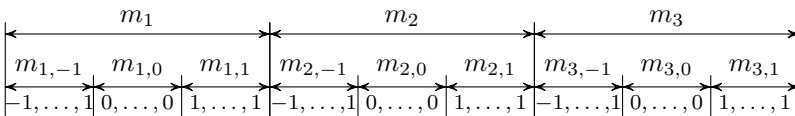


Рис. 5

Гипотеза 4. Самая большая совокупность

$$\mathcal{F} \subset \Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}),$$

в которой скалярное произведение любых двух векторов не меньше t , находится с помощью описанной выше процедуры. Ее мощность есть

$$\max_{\mathbf{m}, \mathbf{M}} P(m_{1,b_1}, \dots, m_{1,b_r}) \cdot \dots \cdot P(m_{r,b_1}, \dots, m_{r,b_r}),$$

где максимум берется по всем допустимым значениям параметров.

Задачи

1. Попытайтесь усилить результат предложения 3, т.е. оценку $|\mathcal{F}| \leq 70$. Как величина $\max |\mathcal{F}|$ оценивается снизу?
2. Аккуратнее оценивая размерность пространства полиномов, возникающих в доказательстве предложения 2, убедитесь в том, что оценка $\max |\mathcal{F}| \leq 157$, фактически фигурирующая в предложении, может быть заменена на $\max |\mathcal{F}| \leq 148$. Возможны ли дальнейшие продвижения в рамках линейно-алгебраического метода?
3. Докажите теоремы 10, 11 и 12.
4. Докажите или опровергните гипотезу 3.
5. Найдите асимптотику суммы $\sum_{k=0}^{\lfloor n/2 \rfloor} C_{n-k+1}^k$. Чему равно ее точное значение?

4

Применение полученных результатов в комбинаторной геометрии

4.1. Постановки основных задач

В предыдущих главах мы тщательно изучили один из красивейших и нетривиальнейших аспектов линейно-алгебраического метода в комбинаторике. Разумеется, мы уже имели немало шансов убедиться в исключительной силе и широте применения метода; немало глубоких и интересных задач мы решили уже с его помощью. Однако у придирчивого читателя все равно может возникнуть вопрос: *«Хорошо. Задачи о скалярных произведениях векторов, безусловно, увлекательны, и нет сомнений, что они лежат едва ли не в основе классической комбинаторики. Пересекать множества — замечательно. Но не висит ли все это в воздухе? Не остается ли вся эта деятельность замкнутой в себе? Какие, право слово, могут быть у нее приложения?»* На первый взгляд, читатель прав, и использование накопленного нами материала в рамках какой-либо иной науки кажется маловероятным. Тем не менее, такая наука есть, и носит она не менее классический характер, чем та чистая комбинаторика, о которой до сих пор шла речь.

В последней фразе мы недаром употребили эпитет «чистая» по отношению к слову «комбинаторика». Дело в том, что обещанная наука, в которой удивительным образом применяются теоремы о запрещенных скалярных произведениях, называется «комбинаторной геометрией». Эта наука лежит на стыке комбинаторных и геометрических исследований. Имея, как правило, глубоко геометрические постановки задач, она во многом комбинаторна, и, в частности, различные методы *чистой* комбинаторики работают при решении ее проблем в полную силу.

Комбинаторная геометрия возникла, по-видимому, еще в начале XX века. Однако в самостоятельную дисциплину она оформилась лишь к середине того же столетия. Сейчас это бурно развивающийся раздел математики, крайне популярный во всем мире. Нет никакой возможности перечислить хотя бы малую долю его задач. Но есть

в нем задачи, которые определили, по сути, весь ход его становления, лежали в его основе и без которых, стало быть, о нем и говорить нельзя. Это задачи Борсука и Нельсона—Эрдёша—Хадвигера.

Сформулируем сначала задачу Нельсона—Эрдёша—Хадвигера. Представим себе, что мы разбили пространство \mathbb{R}^n на χ частей:

$$\mathbb{R}^n = V_1 \sqcup \dots \sqcup V_\chi,$$

причем расстояние между любыми двумя точками в каждой из частей не равно единице:

$$|\mathbf{x} - \mathbf{y}| \neq 1 \quad \text{для всех } \mathbf{x}, \mathbf{y} \in V_i, i \in \{1, \dots, \chi\}.$$

Априори неясно даже, возможно ли такое разбиение, но оно возможно, и в этом очень легко убедиться (см. [6]). Задача состоит в отыскании минимального χ , при котором разбиение осуществимо. Это минимальное χ принято обозначать через $\chi(\mathbb{R}^n)$ и называть *хроматическим числом вещественного евклидова пространства*. Многие знают, что в переводе с греческого «хроматический» — это «цветной». Ничего странного в подобной терминологии нет. Словами можно сказать, что $\chi(\mathbb{R}^n)$ — это *минимальное число цветов, в которые можно так раскрасить все точки пространства, чтобы между точками одного цвета не было расстояния 1*. Действительно, каждое V_i и есть «цвет». Просто аналитически удобнее рассуждать посредством дизъюнктивных объединений, а практически приятнее говорить о «раскрасках» — с них обычно и начинают.

Точкам одного цвета мы *запретили* отстоять друг от друга на расстояние 1; евклидово расстояние однозначно задается своим скалярным произведением, и что-то подсказывает нам, что мы не уйдем с правильного пути, коль скоро попытаемся в дальнейшем применить результаты предшествующих глав к решению задачи Нельсона—Эрдёша—Хадвигера. Правда, пока мы этим заниматься не станем, но заметим только, что величина «запрещенного расстояния» (каковая у нас равна единице) на самом деле ни малейшей роли при определении хроматического числа не играет: пространство \mathbb{R}^n гомотетично самому себе, и если мы научимся раскрашивать его, «минуя», скажем, расстояние $a > 0$ внутри каждого из цветов, то и раскраска без одноцветных точек на любом другом расстоянии $b > 0$ нам обеспечена; достаточно в надлежащее число раз сжать или растянуть все векторы в пространстве. Это простое наблюдение нам пригодится.

Теперь перейдем к постановке проблемы Борсука. Рассмотрим произвольное ограниченное множество Ω в \mathbb{R}^n . Определим *диаметр* мно-

жества Ω :

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

Понятие диаметра вполне естественно, ибо оно отлично согласуется с аналогичным понятием для шара. Вместе с тем, мы берем супремум расстояний, а не максимум, так как заранее нам не сказано, замкнуто ли Ω . Впрочем, без ограничения общности можно считать, конечно, что оно замкнуто и, более того, выпукло: известно ведь, что диаметр множества и его выпуклой оболочки совпадают (см. [7]).

Постараемся представить Ω в виде

$$\Omega = \Omega_1 \sqcup \dots \sqcup \Omega_f,$$

где каждое множество Ω_i , $i = 1, \dots, f$, является частью Ω , имеющей строго меньший диаметр, чем все Ω : $\text{diam } \Omega_i < \text{diam } \Omega$ для всех i . Обозначим через $f(\Omega)$ минимум среди всех f , для которых упомянутое представление возможно. Проблема Борсука состоит в том, чтобы найти $f(n) = \min_{\Omega} f(\Omega)$. Понятно, что вкратце вопрос Борсука следует задавать так: *каково минимальное число $f(n)$ частей меньшего диаметра, на которые может быть разбито произвольное ограниченное множество в \mathbb{R}^n ?* Заметим, что здесь взятие минимумов и максимумов, а не точных нижних и верхних граней совершенно уместно. Кроме того, мы вольны рассматривать только (замкнутые, выпуклые) множества диаметра 1; тут объяснение такое же, как при постановке проблемы Нельсона—Эрдёша—Хадвигера (гомотетичность \mathbb{R}^n самому себе).

Смотрите: вот и в проблеме Борсука мы имеем дело с разбиением чего-то на части, которые, в свою очередь, чего-то «запрещенного» не содержат. Если раньше мы так раскрашивали все пространство, чтобы внутри цветов не было точек на запрещенном расстоянии, то теперь мы фактически так раскрашиваем каждое множество в пространстве, чтобы в рамках цветов (и их замыканий) не было векторов, диаметрально противоположных с точки зрения исходного множества. Ясно, что задачи Нельсона—Эрдёша—Хадвигера и Борсука крайне близки и что, по-видимому, ко второй из них тоже должна применяться техника прошлых глав.

Вообще, можно даже рассматривать серию красивых промежуточных проблем, на концах которой, так сказать, расположены наши задачи. В самом деле, определим $\chi(n, a, d)$ как минимальное число частей, на которые можно так разбить произвольное множество диаметра d в \mathbb{R}^n , чтобы внутри каждой из частей (и их замыканий) не было точек на расстоянии $a \in [0, d]$. Понятно, что при $a \rightarrow 0$ мы

имеем аналог задачи Нельсона—Эрдёша—Хадвигера, а при $a \rightarrow d$ — аналог проблемы Борсука. Автор настоящей брошюры и М. М. Китяев занимались оценками величины $\chi(n, a, d)$, и на этом пути возникло немало интересных наблюдений. Впрочем, нам бы для начала надо с классическими вопросами разобраться, и мы не станем более говорить об указанных обобщениях.

Итак, проблемы близки. Именно поэтому не может не удивлять тот факт, что они не только появились совершенно независимо и притом в разное время, но еще и существовали долгие годы порознь, без какого-либо взаимного влияния.

Проблема Борсука возникла в 1933 году, и была она мотивирована деятельностью своего автора в области *топологии*. Известный польский тополог Кароль Борсук верил, что $f(n) = n + 1$, и, оказавшись его гипотеза правильной, мы бы имели сейчас нетривиальное альтернативное определение размерности пространства. К сожалению, гипотеза ошибочна, но это мы уже забегаем вперед. Главное, что очень долго проблема Борсука привлекала внимание геометров, оставляя вполне равнодушными комбинаторов, и в результате были установлены весьма глубокие геометрические факты, которые, однако ж, ни доказать гипотезу, ни опровергнуть ее так и не помогли.

В то же время проблема Нельсона—Эрдёша—Хадвигера была предложена в 1950 году, и ею, наоборот, занимались исключительно специалисты в области комбинаторики, многие из которых (включая, между прочим, и знакомых нам Франкла с Уилсоном) довольно слабо ориентировались в геометрии. Собственно, только после появления теорем Франкла и Уилсона открылась заслонка; и даже тогда потребовалось более десяти лет, чтобы линейно-алгебраический метод был, наконец, замечен геометрами и адекватно ими использован. Можно говорить о том, что история совместного существования столь, очевидно, близких проблем насчитывает не более двадцати-тридцати лет. То ли ее надо вести с 1981 года (года появления в печати теорем Франкла—Уилсона), то ли с 1993 года, когда возникли первые контрпримеры к гипотезе Борсука. В любом случае, именно линейно-алгебраический метод послужил тем связующим звеном, которое окончательно состыковало проблемы; именно благодаря ему мы имеем сейчас великое множество любопытнейших результатов относительно обеих проблем — результатов, которые еще и еще раз красноречиво свидетельствуют об исключительной близости задач. В этом нам предстоит вскоре убедиться.

Подробно мы об истории задач Борсука и Нельсона—Эрдёша—Хадвигера писать, естественно, не будем. Истории эти крайне много-

гранны и в чем-то почти детективны даже, но ведь не о них наша книга. К тому же о проблеме Нельсона—Эрдёша—Хадвигера мы написали целую брошюру [6], а о проблеме Босука — другую брошюру (см. [7]). Кроме того, есть недавние наши обзоры — [8] (об обеих проблемах) и [15] (о проблеме Борсука). Впрочем, кое-что мы все же скажем в соответствующих разделах, но это будет уже лишь по необходимости.

4.2. Задача Нельсона—Эрдёша—Хадвигера

Итак, мы уже знаем, что такое хроматическое число пространства. Между прочим, это самое число зачастую возникает и в рамках олимпиадной деятельности; только там оно обычно рассматривается в простейшем случае — в случае евклидовой плоскости. С одной стороны, такое рассмотрение ведет, конечно, к значительному упрощению задачи, но в том и специфика олимпиад. С другой стороны, даже отыскание величины $\chi(\mathbb{R}^2)$ представляет огромную трудность. Практически каждый школьник, потратив от силы день-два на размышление, без сомнения, установит неравенство

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

Однако трагедия науки Нельсона—Эрдёша—Хадвигера состоит в том, что никто ничего лучшего не знает. Всем, разумеется, понятно, что хроматическое число прямой равно двум, а вот что делать с задачей на плоскости уже неизвестно. Это, действительно, позор, но ведь и на \mathbb{R}^2 мир клином не сошелся. В то же время ясно, что при $n \geq 3$ будет только хуже. В конце концов, мы ведь не обязаны отыскать точное значение $\chi(\mathbb{R}^n)$ для любого n (а как хотелось бы!), нам бы, стало быть, хоть *оценки* для хроматического числа поточнее найти. Вот, скажем, в \mathbb{R}^3 есть на данный момент неравенства

$$6 \leq \chi(\mathbb{R}^3) \leq 15.$$

Зазор еще более обескураживающий, чем тот, что мы имели при $n = 2$. Но при $n \rightarrow \infty$ так ли уж сильно этот зазор растет? Можно ли надеяться, что в асимптотике разрыв между верхней и нижней оценками не будет катастрофически велик? Постепенно мы придем к выводу, что ответ на последний вопрос, скорее, положителен, и это здорово.

Сперва мы заметим, что верхняя оценка хроматического числа с ростом n — самая лучшая из ныне известных нам — имеет вид $\chi(\mathbb{R}^n) \leq (3 + o(1))^n$. Ее доказали Дэвид Ларман и Клаус А. Роджерс еще в 1972 году. Их технология никакого отношения к комбинаторике не имела (речь шла о разбиениях пространства и о так называемых

плотнейших упаковках шаров), и мы на ней не останавливаемся: нас интересуют приложения линейно-алгебраического метода.

А вот что можно сказать о нижних оценках? Далее мы изложим абсолютно естественный и простой подход к их получению. Ничего, так сказать, более умного (или, если хотите, заумного) человечество пока не измыслило, да оно в некотором роде и хорошо. Дело в том, что, по-видимому, где-то в рамках этого подхода уже находится оптимум, просто нам не удастся его изловить. Соображения, в пользу последнего заявления, апеллируют к слишком сложной и далеко в стороне от нас стоящей науке, так что читателю придется поверить нам на слово. Сам же подход объяснить совсем легко.

Предположим, что мы нашли в пространстве некоторую конечную совокупность векторов Σ , имеющую мощность M . Ну, это-то вряд ли проблема. Допустим еще, что, какова бы ни была подсовокупность \mathcal{F} в Σ , в которой расстояние между любыми двумя элементами не равно заданному наперед числу a , ее мощность не превосходит некоторого $D < M$. Утверждается, что тогда

$$\chi(\mathbb{R}^n) \geq \frac{M}{D}.$$

Это утверждение мгновенно вытекает из принципа Дирихле: если бы $\chi < M/D$ цветов было достаточно для раскраски пространства, то тем более их было бы достаточно для раскраски Σ , при которой в Σ нет одноцветных точек, отстоящих друг от друга на расстояние a ; но тогда по упомянутому принципу нашелся бы цвет, в котором больше D векторов; значит, «внутри» этого цвета (внутри соответствующей совокупности $\mathcal{F} \subset \Sigma$, $|\mathcal{F}| > D$) образовалась бы пара векторов на запрещенном расстоянии, и мы имели бы противоречие.

Вот и вся идея. Отловим мы в \mathbb{R}^n совокупность векторов Σ , подберем величину a запрета так, чтобы верхняя оценка на мощность максимальной подсовокупности $\mathcal{F} \subset \Sigma$, свободной от «запрещенных пар» векторов, была в сравнении с мощностью самой Σ как можно меньше, и вперед: чем большим окажется отношение M/D , тем для нас лучше. Ничего не напоминает? Да ведь мы именно этим в главах 2, 3 и занимались! Даже в тех же обозначениях. Помните, в разделе 3.5 мы рассуждали про величину M/D ? Так это она и есть. Все было, оказывается, учтено заранее. Заметим, что совокупность Σ , отвечающая описанным параметрам M , D и a , называется в нашей науке (M, D, a) -критической конфигурацией, и перейдем к применению теорем о скалярных произведениях.

Следствие из теоремы 1. *Имеет место неравенство $\chi(\mathbb{R}^n) \geq cn^2$ с некоторым постоянным $c > 0$.*

История этого следствия, как ни странно, довольно запутанна. В 1972 году Д. Ларман и К. А. Роджерс написали замечательную статью, в которой доказали множество нижних оценок для хроматических чисел в «малых» (фиксированных) размерностях (типа $n \leq 24$) и ту самую неулучшенную до сих пор верхнюю оценку, о которой мы говорили выше. Вместе с тем они объявили, что могут установить неравенство

$$\chi(\mathbb{R}^n) \geq c' \frac{n^2}{\log n}.$$

Разумеется, все свои нижние оценки они обосновывали за счет построения тех или иных (M, D, a) -критических конфигураций. Только вот теоремы Ж. Надя они не знали. По-видимому, еще до того, как эта статья была опубликована, ее результаты стали известны Полу Эрдешу и Вере Шош. Именно они подсказали Ларману и Роджерсу обратиться к теореме Надя, и те (со ссылкой на всю «троицу помощников») дописали к статье дополнение, которое мы сейчас изложим.

Доказательство следствия из теоремы 1. Пусть \tilde{M} — совокупность всевозможных трехэлементных подмножеств \mathcal{R}_n , фактически фигурирующая в теореме, а Σ — отвечающая ей совокупность $(0, 1)$ -векторов. В теореме множествам запрещается пересекаться по одному общему элементу. Это соответствует запрету скалярного произведения 1 у векторов из Σ , и, поскольку скалярный квадрат каждого такого вектора равен трем, можно смело говорить о запрещенном расстоянии $a = 2$ в конфигурации, образованной элементами совокупности Σ . Понятно, что

$$|\Sigma| = C_n^3 \sim \frac{1}{6}n^3 = M,$$

и конфигурация станет критической, коль скоро мы укажем для нее величину D . Эта величина дается в теореме: $D = n' \sim n$, — и мы имеем оценку

$$\chi(\mathbb{R}^n) \geq \frac{M}{D} \sim \frac{1}{6}n^2.$$

Следствие (с константой $c \approx 1/6$) доказано. \square

Аналогичным путем устанавливается оценка $\chi(\mathbb{R}^n) \geq cn^3$. Она получается из рассмотрения совокупности пятиэлементных подмножеств \mathcal{R}_n , которым запрещено пересекаться по двум общим элементам. Помните, мы говорили, что до появления линейно-алгебраического метода даже с такими множествами было крайне тяжело иметь дело? Все-таки в 1978 году Ларман справился с ними и показал, что в качестве c можно взять нечто вроде одной стотысячной. Однако мы с вами знаем уже, что в указанной конфигурации и $D = C_n^2$ работает

$(m(n, 5, 2) \leq C_n^2)$; M там, очевидно, есть C_n^5 , и, стало быть, даже $c \approx 1/60$ вполне подойдет.

Следствие из теоремы 2. *Имеет место неравенство*

$$\chi(\mathbb{R}^n) \geq (1,139 \dots + o(1))^n.$$

Вот оно, так сказать, величие линейно-алгебраического метода во всей своей красе. Экспоненциальность роста хроматического числа заподозрил еще в семидесятые годы Эрдёш, но, не появившись метода и соответствующих теорем о пересечениях множеств, гипотеза Эрдёша так и осталась бы неподтвержденной. Между прочим, уже результат последнего следствия свидетельствует о том, что с ростом n , как мы и обещали, зазор между верхней и нижней оценками величины $\chi(\mathbb{R}^n)$ заведомо не запределен. Разница лишь в значениях констант, стоящих в основаниях экспонент. Конечно, и ее устранение — важная и интересная проблема, но принципиально и сейчас понятно, как устроена жизнь.

Доказательство следствия из теоремы 2. Пусть $n = 4p$, $k = 2p$ (p — простое), а $\tilde{\mathcal{M}}$ — это совокупность всевозможных k -элементных подмножеств \mathcal{R}_n , фактически фигурирующая в теореме. Беря в качестве Σ совокупность $(0, 1)$ -векторов, отвечающих множествам из $\tilde{\mathcal{M}}$, получаем, с очевидностью, (M, D, a) -критическую конфигурацию, у которой

$$a = \sqrt{2p}, \quad M = C_n^k, \quad D \leq 2C_{n-1}^{p-1}.$$

В разделе 2.3, рассуждая о значении теоремы Франкла—Уилсона, мы пришли к выводу, что $M = (2 + o(1))^n$, $D = (1,754 \dots + o(1))^n$. Таким образом,

$$\chi(\mathbb{R}^n) \geq \frac{M}{D} = (1,139 \dots + o(1))^n,$$

и, казалось бы, все в порядке. Ан нет: n ведь у нас не любое. Вдруг при других n оценка резко ухудшится, и мы останемся лишь с тем, что называется «омега-результатом»?

Тут на помощь приходят наши знания о частоте появления простых в натуральном ряде. В самом деле, пусть n совершенно произвольно. Выберем максимальное простое число p , при котором $n' = 4p \leq n$. Ввиду наших прежних наблюдений

$$\chi(\mathbb{R}^{n'}) \geq (1,139 \dots + o(1))^{n'}.$$

Ясно тогда, что тем более $\chi(\mathbb{R}^n) \geq (1,139 \dots + o(1))^{n'}$. А как выглядит n' ? Безусловно, выбранное нами p не превосходит $n/4$. Однако, будучи *максимальным*, оно оценивается снизу как $n/4 - O(n^{38/61})$, т. е.

$$p = \frac{n}{4} + O(n^{38/61}),$$

и, стало быть, $n' = n + O(n^{38/61})$. Значит,

$$\chi(\mathbb{R}^n) \geq (1,139 \dots + o(1))^{n'} = (1,139 \dots + o(1))^n,$$

и теперь уж точно проблем нет. Правда, $o(1)$ могло ухудшиться, но да Бог с ним: когда главный член асимптотики неизвестен, рано беспокоиться об остатках. Следствие доказано. \square

Следствие из теоремы 3. *Имеет место неравенство*

$$\chi(\mathbb{R}^n) \geq (1,207 \dots + o(1))^n.$$

Теорема 3 более обща, нежели теорема 2, и понятно, что ее следствие должно было оказаться более сильным. На самом деле с помощью $(0, 1)$ -векторов и теорем об их скалярных произведениях ничего лучшего уже не добиться. Мы не станем обосновывать последнее утверждение, да оно и вытекает почти мгновенно из доказательства следствия, которое мы проведем ниже.

Доказательство следствия из теоремы 3. Положим в теореме 3 $k = [k'n]$, причем для технического удобства пускай $k' \in (0, 1/2)$. Рассмотрим минимальное p , при котором $k - 2p < 0$ ($k - 2p \leq -1$). Последнее условие очень нам знакомо. Помните, в разделе 3.5 мы в аналогичной ситуации убедились в том, что такой выбор параметров приводит к максимизации отношения M/D ? Правда, там речь шла о $(-1, 0, 1)$ -векторах, и мы еще не знали, в чем смысл самого отношения, но все те же рассуждения пригодятся и теперь. Конечно, можно относиться к параметрам чисто формально: ну, выбрали их как-то — и повезло, победителей не судят. Тем не менее, на таком пути вряд ли следует ожидать возникновения самостоятельных результатов. В общем, мы рекомендуем читателю вникнуть в соответствующую часть раздела 3.5 и осознать, почему нынешние параметры подобраны именно так, а не иначе.

Пусть, далее, в теореме $t = k - p$. Имеем неравенство

$$2t + 1 = 2k - 2p + 1 = k + ((k - 2p) + 1) \leq k,$$

которое, в силу теоремы, означает, что

$$m(n, k, t) \leq C_n^{k-t-1} = C_n^{p-1}.$$

Рассмотрим совокупность Σ , состоящую из всевозможных $(0, 1)$ -векторов, у которых k ненулевых координат. Запретим этим векторам иметь скалярное произведение t , и Σ , конечно же, станет автоматически (M, D, a) -критической конфигурацией с $a = \sqrt{2p}$, $M = C_n^k$, $D = C_n^{p-1}$. Отсюда следует, что

$$\chi(\mathbb{R}^n) \geq \frac{M}{D} = \frac{C_n^k}{C_n^{p-1}},$$

но $k = [k'n]$ у нас произвольно, и мы вольны написать

$$\chi(\mathbb{R}^n) \geq \max_{k'} \frac{M}{D} = \max_{k'} \frac{C_n^k}{C_n^{p-1}}.$$

Остается оценить максимум. Подобные операции мы проделывали, но на этот раз есть своя специфика, и мы проведем соответствующие рассуждения достаточно подробно.

Для аккуратности следовало бы поступить так же, как мы поступили в разделе 3.3: рассмотреть три случая — два «крайних» ($k' \approx 0$ и $k' \approx 1/2$) и один «центральный», затем за счет простых соображений убедиться в том, что в крайних случаях величиной $(1,207\dots + o(1))^n$ и не пахнет, а потом, наконец, изучить случай центральный, расписывая факториалы по формуле Стирлинга, пренебрегая сомножителями субэкспоненциального порядка и дифференцируя оставшуюся функцию по k' . Но во-первых, однажды мы эту программу реализовали; во-вторых, крайние случаи, действительно, просты; а в третьих, найдем мы в центральном случае k' , на котором достигается обещанное значение дроби M/D — и чудесно: убедиться в том, что лучшего не добиться, читатель сумеет и сам.

Итак, ограничимся центральным случаем. Возьмем сперва C_n^k :

$$C_n^{[k'n]} = \frac{\sqrt{2\pi n}^n e^{-n}}{\sqrt{2\pi[k'n]}[k'n]^{[k'n]} e^{-[k'n]} \sqrt{2\pi(n-[k'n])} (n-[k'n])^{n-[k'n]} e^{[k'n]-n}}.$$

После сокращения экспонент и стандартного собирания различных «паразитических» сомножителей полиномиального порядка в один отдельный, получается выражение вида

$$C_n^k = \frac{P(n)}{((k')^{k'}(1-k')^{1-k'})^n} = \left(\frac{1}{(k')^{k'}(1-k')^{1-k'}} + o(1) \right)^n.$$

Теперь обратимся к C_n^{p-1} . С точностью до всякой «ерунды» имеем:

$$C_n^{p-1} = Q(n) \frac{n^n}{p^p(n-p)^{n-p}}.$$

Здесь и далее важно то, что $p = \frac{k'n}{2} + O(n^{38/61})$ (ср. раздел 3.5). Если обозначить $O(n^{38/61})$ через ε_n , то, например,

$$p^p = \left(\frac{k'n}{2} + \varepsilon_n \right)^{k'n/2 + \varepsilon_n} = \left(\frac{k'n}{2} \right)^{k'n/2} o(e^n).$$

В результате

$$C_n^{p-1} = \left(\frac{1}{\left(\frac{k'}{2} \right)^{\frac{k'}{2}} \left(1 - \frac{k'}{2} \right)^{1 - \frac{k'}{2}}} + o(1) \right)^n.$$

Таким образом, мы, по сути, должны найти максимум дроби

$$f(k') = \frac{\left(\frac{k'}{2}\right)^{k'/2} \left(1 - \frac{k'}{2}\right)^{1 - \frac{k'}{2}}}{(k')^{k'} (1 - k')^{1 - k'}}, \quad k' \in \left(0, \frac{1}{2}\right).$$

Он достигается на том же k' , что и максимум выражения

$$g(k') = \frac{k'}{2} \ln \frac{k'}{2} + \left(1 - \frac{k'}{2}\right) \ln \left(1 - \frac{k'}{2}\right) - k' \ln k' - (1 - k') \ln(1 - k').$$

Приравниваем производную функции g к нулю. Возникает квадратное уравнение, корни которого суть

$$k'_{1,2} = \frac{2 \pm \sqrt{2}}{2}.$$

Большой корень нам не подходит, так как он вылезает за пределы интервала, на котором живет k' . Если же подставить меньший корень в функцию f , то получится в аккурат 1,207... Следствие доказано. \square

Следствие из теоремы 10. *Имеет место неравенство*

$$\chi(\mathbb{R}^n) \geq (1,239 \dots + o(1))^n.$$

Последнее неравенство чуть лучше, чем то, которое мы вывели из теоремы 3, да это и немудрено: «степеней свободы»-то у нас теперь еще больше.

Доказательство следствия из теоремы 10. Пусть $k_{-1} = [k'_{-1}n]$, $k_1 = [k'_1n]$, причем $k'_{-1} + k'_1 < \frac{1}{2}$, $k'_\nu > 0$ ($\nu \in \{-1, 1\}$) и $k'_{-1} < k'_1$ (ср. начало доказательства предыдущего следствия). Ясно тогда, что

$$k_0 = n - [k'_{-1}n] - [k'_1n] \sim (1 - k'_{-1} - k'_1)n. \quad (1)$$

Рассмотрим совокупность

$$\Sigma = \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1),$$

появляющуюся в теореме 10. Понятно, что в наших предположениях

$$\begin{aligned} \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) &= k_{-1} + k_1, \\ \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) &= -2k_{-1}. \end{aligned}$$

Возьмем, стало быть, руководствуясь прежними соображениями, изложенными еще в разделе 3.5, минимальное простое число p , для которого

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - 2p < \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1).$$

В этом случае, как мы знаем

$$p = \frac{\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)}{2} + \\ + O\left(\left(\frac{\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) - \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)}{2}\right)^{38/61}\right),$$

т. е.

$$p = \frac{3k_{-1} + k_1}{2} + O\left(\left(\frac{3k_{-1} + k_1}{2}\right)^{38/61}\right). \quad (2)$$

По теореме 10 совокупность Σ есть (M, D, a) -критическая конфигурация с

$$a = \sqrt{2p}, \quad M = P(k_{-1}, k_0, k_1), \quad D = \sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2},$$

где

$$\mathcal{A} = \{(m_1, m_2) : m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq p - 1\}.$$

Разумеется, $\chi(\mathbb{R}^n) \geq M/D$, и, более того, за счет произвольности параметров, определяющих значения M и D , мы можем искать $\max_{k'_{-1}, k'_1} M/D$. Это утомительная задача, но мы уже имеем все необходимые ингредиенты для ее решения. Посему мы не станем в очередной раз вдаваться в технические детали, загромождая книгу ненужными выкладками, которые к настоящему моменту любой читатель должен уметь проделать сам; мы лишь изложим надлежащую последовательность знакомых нам действий.

Сперва находим асимптотику для M . Благодаря выбору параметров (см. (1)) и привычной нам аналитической возне с формулой Стирлинга она имеет вид

$$M = \left(\frac{1}{(k'_{-1})^{k'_{-1}} (k'_1)^{k'_1} (1 - k'_{-1} - k'_1)^{1 - k'_{-1} - k'_1}} + o(1) \right)^n.$$

Асимптотика для D ищется точно так же, как и ее аналог в разделе 3.3: выделяется три случая, оптимум всегда лежит в центральном из них, и т. д. При этом надо учитывать, конечно, соотношение (2). В результате получается

$$D = \left(\frac{1}{A^A B^B C^C} + o(1) \right)^n,$$

где

$$A = \frac{2 + 9k'_{-1} + 3k'_1 - \sqrt{(2 + 9k'_{-1} + 3k'_1)^2 - 12(3k'_{-1} + k'_1)^2}}{12}, \\ B = \frac{3k'_{-1} + k'_1}{2} - 2A, \quad C = 1 + A - \frac{3k'_{-1} + k'_1}{2}.$$

Заметим, что при $k'_{-1} = k'_1 = 1/4$ величина A есть попросту $(5 - \sqrt{13})/12$ (ср. раздел 3.3).

Остается фактически вычислить максимум дроби

$$f(k'_{-1}, k'_1) = \frac{A^A B^B C^C}{(k'_{-1})^{k'_{-1}} (k'_1)^{k'_1} (1 - k'_{-1} - k'_1)^{1 - k'_{-1} - k'_1}}$$

и убедиться в том, что он равен $1,239\dots$ В принципе, можно сделать это на компьютере, пробегая области, в которых живут параметры k'_{-1} и k'_1 , с достаточно маленьким шагом. Можно попытаться составить систему

$$\begin{cases} \frac{\partial f(k'_{-1}, k'_1)}{\partial k'_{-1}} = 0, \\ \frac{\partial f(k'_{-1}, k'_1)}{\partial k'_1} = 0. \end{cases}$$

К сожалению, жуткие уравнения, которые здесь возникнут, все равно придется запускать в компьютер. В конечном счете и на таком пути появится вождеденная константа $1,239\dots$ Так или иначе, следствие доказано. \square

Если очень постараться, то можно удостовериться в том, что следствие неулучшаемо. Иными словами, за счет $(-1, 0, 1)$ -векторов и линейно-алгебраического метода в его нынешнем состоянии константу $1,239$ не превзойти. Правда, гипотеза 3 оставляет некоторую надежду.

Заметим, что если бы мы работали не с теоремой 10, а с теоремой 9 — ее частным случаем, то мы бы пришли к оценке

$$\chi(\mathbb{R}^n) \geq \frac{M}{D} = \frac{2,8284\dots}{2,4628\dots} = 1,148\dots$$

Это хуже, чем результат, вытекающий из теоремы 3, но лучше, чем его аналог, обусловленный теоремой 2.

Любопытно, что из теоремы 11 вывести более сильные следствия тоже не удастся. Конечно, когда разрешенных величин координат больше, аналитическая часть деятельности становится убийственно сложной. Тем не менее кое-что на этом пути посчитано, но неравенство

$$\chi(\mathbb{R}^n) \geq (1,239\dots + o(1))^n$$

уточнению пока не поддается. По-видимому, это еще одно косвенное подтверждение того, что как ни глубок линейно-алгебраический метод, а улучшать его нужно.

4.3. Задача Борсука

Как мы уже говорили, эта наука возникла из гипотезы Борсука о равенстве величины $f(n)$ числу $n + 1$. Мы даже успели заметить, что гипотеза оказалась неверна. Сейчас мы поймем, что неверна она, так сказать, катастрофически. Вообще, результатов относительно проблемы исторически было получено очень много, и, поскольку проблема целиком до сих пор не решена (это тоже станет постепенно ясно), они продолжают появляться и ныне. Но до «катастрофы» (т. е. до 1993 года, когда Джефф Кан и Гил Калаи построили первый контрпример к гипотезе) ситуация, тем не менее, казалась безнадежной, а именно, самая лучшая верхняя оценка величины $f(n)$ выглядела так:

$$f(n) \leq \left(\sqrt{\frac{3}{2}} + o(1) \right)^n.$$

По сравнению с гипотетической линейной функцией $n + 1$ упомянутая экспонента — это просто «пощечина общественному вкусу». А ведь и ее отыскивали лишь в 1988 году с помощью весьма продвинутой техники. Сделал это израильский математик Одед Шрамм. Отметим, что его результат был иначе передоказан в 1991 году Жаном Бургейном и Йорамом Линденштрауссом и что он и сейчас остается сильнейшим из известных (см. [7]).

Теперь мы изложим общий подход, который позволяет доказывать весьма отличные от гипотетических нижние оценки для $f(n)$ и, соответственно, строить контрпримеры к гипотезе Борсука. Фактически идея этого подхода содержалась и в работе Кана—Калаи. Однако автор настоящей брошюры значительно обобщил и доработал ее, за счет чего в конечном итоге и результаты «первопроходцев» удалось улучшить. Естественно, в основе идеи — все тот же линейно-алгебраический пласт комбинаторных фактов.

Пусть

$$\Sigma = \Sigma(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})$$

— это некоторая совокупность векторов, описанная в разделе 3.5. Рассмотрим отвечающие ей величины

$$\bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}), \quad \underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})$$

и предположим, что для какого-то

$$a \in [\underline{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r}), \bar{s}(\{b_1, \dots, b_r\}^n; k_{b_1}, \dots, k_{b_r})]$$

и какого-то D выполнено следующее утверждение.

Утверждение 1. *Какова бы ни была подсовокупность векторов \mathcal{F} в Σ , в которой скалярное произведение любых двух элементов не равно a , ее мощность не превосходит D .*

Очень похоже на критическую конфигурацию, но куда ее при-
ткнуть, пока не ясно. При этом опять-таки вполне разумно считать,
что

$$M = |\Sigma| = P(k_{b_1}, \dots, k_{b_r}), \quad D < M.$$

Допустим, далее, что

$$(b_1 k_{b_1} + \dots + b_r k_{b_r})^2 - an \geq 0.$$

Тогда можно зафиксировать любой корень λ уравнения

$$n\lambda^2 - 2(b_1 k_{b_1} + \dots + b_r k_{b_r})\lambda + a = 0.$$

Возьмем произвольный вектор $\mathbf{x} = (x_1, \dots, x_n)$ из Σ и, полагая $\tilde{x}_i = x_i - \lambda$, $i = 1, \dots, n$, рассмотрим новый вектор

$$\mathbf{x} * \mathbf{x} = (\tilde{x}_1^2, \tilde{x}_1 \tilde{x}_2, \dots, \tilde{x}_1 \tilde{x}_n, \tilde{x}_2 \tilde{x}_1, \tilde{x}_2^2, \dots, \tilde{x}_2 \tilde{x}_n, \dots, \tilde{x}_n \tilde{x}_1, \dots, \tilde{x}_n^2).$$

Иными словами, мы в определенном порядке попарно перемножаем «уменьшенные» координаты вектора \mathbf{x} , получая, тем самым, вектор размерности n^2 . В результате возникает совокупность векторов Σ^* , и мы будем предполагать, что отображение, породившее ее из Σ , взаимнооднозначно (биективно), т.е. что для любых $\mathbf{x}, \mathbf{y} \in \Sigma$ векторы $\mathbf{x} * \mathbf{x}$, $\mathbf{y} * \mathbf{y}$ не совпадают. Читателю остается лишь с известной легкостью осознать, что подобное свойство не есть исключение и что выполнение его напрямую зависит от значений параметров b_1, \dots, b_r и пр. В любом случае, $|\Sigma| = |\Sigma^*| = M$. При этом очень важно заметить, что размерность совокупности Σ^* на самом деле не превосходит

$$m = \frac{n(n+1)}{2},$$

ведь в каждом $\mathbf{x} * \mathbf{x} \in \Sigma^*$ координаты с номерами $\{i, j\}$ и $\{j, i\}$ ($i \neq j$) совпадают: $\tilde{x}_i \tilde{x}_j = \tilde{x}_j \tilde{x}_i$.

Имеет место

Лемма 7. *Если $\mathbf{x}, \mathbf{y} \in \Sigma$ и $(\mathbf{x}, \mathbf{y}) = a$, то векторы $\mathbf{x} * \mathbf{x}$, $\mathbf{y} * \mathbf{y}$ реализуют диаметр совокупности Σ^* .*

Доказательство леммы 7. Пожонглируем сперва скалярным произведением векторов $\mathbf{x} * \mathbf{x}$, $\mathbf{y} * \mathbf{y}$:

$$\begin{aligned} (\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y}) &= \sum_{i=1}^n \sum_{j=1}^n (x_i - \lambda)(x_j - \lambda)(y_i - \lambda)(y_j - \lambda) = \\ &= \left(\sum_{i=1}^n (x_i - \lambda)(y_i - \lambda) \right)^2 = \left(\sum_{i=1}^n x_i y_i - \lambda \sum_{i=1}^n x_i - \lambda \sum_{i=1}^n y_i + n\lambda^2 \right)^2. \end{aligned}$$

Каков бы ни был вектор из Σ , сумма его координат всегда равна $b_1 k_{b_1} + \dots + b_r k_{b_r}$, и, стало быть,

$$\begin{aligned} \left(\sum_{i=1}^n x_i y_i - \lambda \sum_{i=1}^n x_i - \lambda \sum_{i=1}^n y_i + n\lambda^2 \right)^2 &= \\ &= ((\mathbf{x}, \mathbf{y}) - 2(b_1 k_{b_1} + \dots + b_r k_{b_r})\lambda + n\lambda^2)^2. \end{aligned}$$

Если, как и в условии леммы, $(\mathbf{x}, \mathbf{y}) = a$, то тем самым, ввиду выбора параметра λ , мы имеем $(\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y}) = 0$.

В то же время

$$|\mathbf{x} * \mathbf{x} - \mathbf{y} * \mathbf{y}|^2 = (\mathbf{x} * \mathbf{x}, \mathbf{x} * \mathbf{x}) + (\mathbf{y} * \mathbf{y}, \mathbf{y} * \mathbf{y}) - 2(\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y}).$$

Очевидно,

$$\begin{aligned} (\mathbf{x} * \mathbf{x}, \mathbf{x} * \mathbf{x}) &= (\mathbf{y} * \mathbf{y}, \mathbf{y} * \mathbf{y}) = \\ &= (b_1^2 k_{b_1} + \dots + b_r^2 k_{b_r} - 2(b_1 k_{b_1} + \dots + b_r k_{b_r})\lambda + n\lambda^2)^2. \end{aligned}$$

Следовательно, максимальное расстояние между векторами из Σ^* достигается, коль скоро их скалярное произведение минимально. Но это произведение, будучи полным квадратом, разумеется, неотрицательно, причем, как мы знаем, нулю оно равно в точности при $(\mathbf{x}, \mathbf{y}) = a$. Лемма доказана. \square

Предположим, что мы разбили Σ^* на $f < M/D$ частей меньшего диаметра:

$$\Sigma^* = \Omega_1^* \sqcup \dots \sqcup \Omega_f^*.$$

Благодаря биективности соответствия между Σ^* и Σ мы имеем разбиение

$$\Sigma = \Omega_1 \sqcup \dots \sqcup \Omega_f,$$

где, в частности, $|\Omega_i| = |\Omega_i^*|$, $i = 1, \dots, f$. По известному принципу Дирихле («ящики с кроликами») найдется такое i , что

$$|\Omega_i| \geq \frac{|\Sigma|}{f} = \frac{M}{f} > D.$$

В силу утверждения 1 в Ω_i есть пара векторов \mathbf{x}, \mathbf{y} со скалярным произведением a . Но лемма 7 говорит, что тогда диаметр Ω_i^* совпадает с диаметром всей совокупности Σ^* . Полученное противоречие свидетельствует о том, что $f(m) \geq M/D$. Однако нетрудно догадаться, что, как и прежде, последнее отношение будет иметь у нас вид

$$\frac{M}{D} = (\gamma + o(1))^n, \quad \gamma > 1.$$

В таком случае

$$f(m) \geq (\gamma + o(1))^n = (\gamma\sqrt{2} + o(1))^{\sqrt{m}}$$

(мы не забываем, что $m = \frac{n(n+1)}{2} \sim \frac{n^2}{2}$, т. е. $n \sim \sqrt{2}\sqrt{m}$).

Изложение общего подхода завершено. В дальнейшем нам останется только надлежащим способом подобрать параметры совокупности Σ , величины a и λ , а также найти значение D , доказав утверждение типа утверждения 1, и убедиться в экспоненциальности роста дроби M/D . Снова мы постараемся действовать оптимально.

Заметим прежде, что первая оценка, полученная на более или менее сходном пути Каном и Калаи, выражалась неравенством

$$f(n) \geq (1,203 \dots + o(1))^{\sqrt{n}}.$$

Она опиралась на $(0, 1)$ -векторы и была впоследствии улучшена автором настоящей брошюры. Заметим также, что и от нее, и от самого сильного известного результата все-таки весьма далеко до верхней оценки Шрамма. Однако и гипотезой более не пахнет. Впрочем, неэффективность значения $o(1)$ мешает осознанию величины размерности, в которой гипотеза начинает нарушаться, но об этом мы поговорим позже. Сейчас мы докажем теорему.

Теорема 13. *Выполнена оценка*

$$f(n) \geq \left(\left(\frac{2}{\sqrt{3}} \right)^{\sqrt{2}} + o(1) \right)^{\sqrt{n}} = (1,2255 \dots + o(1))^{\sqrt{n}}.$$

Доказательство теоремы 13. Будем действовать в соответствии с заявленным планом. Пусть $\delta \in \left(0, \frac{1}{2}\right)$ — параметр, по которому в конечном итоге будет произведена оптимизация. Возьмем нечетное простое число p , ближайшее к величине $[\delta n]$. Как мы прекрасно знаем, $p \sim \delta n$. Положим

$$k_{-1} = \left\lfloor \frac{p}{2} \right\rfloor, \quad k_1 = p - k_{-1}, \quad k_0 = n - p$$

и рассмотрим совокупность

$$\Sigma = \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1).$$

Зависимость от δ мы нигде явно не указываем, но и не забываем про нее. Заметим, что $k_{-1} < k_1$ ввиду нечетности p , хотя в то же время, конечно, $k_{-1} \approx k_1$. Ясно, что в нашей ситуации

$$\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = p, \quad \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) > -p.$$

Таким образом, нужное нам «утверждение 1» при $a = 0$ вытекает из теоремы 10, в которой $q = p$. Величина D имеет, соответственно, вид

$$D = D(\delta) = \sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2},$$

где

$$\mathcal{A} = \{(m_1, m_2): m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq p - 1\}.$$

Разумеется, у нас $(-k_{-1} + k_1)^2 - 0 \cdot n \geq 0$, а впрочем, и так понятно, что $\lambda = 0$ есть корень уравнения

$$n\lambda^2 - 2(-k_{-1} + k_1)\lambda + 0 = 0.$$

Поскольку $k_{-1} < k_1$, переход от Σ к Σ^* биективен, и, стало быть, с этим тоже проблем нет. В результате мы получаем оценку

$$f(m) \geq M/D,$$

где, естественно,

$$m = \frac{n(n+1)}{2}, \quad M = |\Sigma| = M(\delta).$$

Далее следуют противные аналитические выкладки, которые мы проделывали уже столько раз, что их вполне можно опустить. Смысл в том, что при каждом δ величины M и D суть экспоненты, причем отношение их также растет показательно, т. е., как мы и ожидали, неравенство таково:

$$f(m) \geq \max_{\delta} \frac{M(\delta)}{D(\delta)} = \max_{\delta} (\gamma(\delta) + o(1))^n$$

(мы помним, что $p \sim \delta n$). Остается найти максимум, но и такая процедура нас нисколько теперь не пугает. Любопытно, что здесь корень уравнения, задающего необходимое условие экстремума, ищется явно:

$$\delta = 1 - \frac{1}{\sqrt{3}}.$$

По-прежнему такое δ и впрямь реализует максимум (проверьте все сказанное!), так что, подставляя его в $\gamma(\delta)$, мы и приходим к оценке

$$f(m) \geq \left(\left(\frac{2}{\sqrt{3}} \right)^{\sqrt{2}} + o(1) \right)^{\sqrt{m}} = (1,2255 \dots + o(1))^{\sqrt{m}}.$$

Теорема доказана. \square

Замечание 1. Мы говорили, что «первопроходцы» — Кан и Калаи — работали при доказательстве своей оценки для $f(n)$ с $(0, 1)$ -векторами. В теореме 13 использованы $(-1, 0, 1)$ -векторы, которые, как и в случае задачи о хроматическом числе, дают более сильный результат. Интересно, что добавление общности (усложнение структуры Σ) к успеху пока не привело (теорема 11 не помогает). Это опять свидетельствует о наличии задела для отыскания новых фактов в будущем.

Замечание 2. Когда мы имели дело с хроматическим числом, оптимизация велась по параметрам k_{-1}, k_1 . Естественно, возникает вопрос: почему бы теперь нам не поступить так же? Ведь в доказательстве теоремы 13 мы варьировали сумму $k_{-1} + k_1$, полагая при этом, что $k_{-1} \approx k_1$, и в результате один параметр оказался, по существу, не использован. Разве мы на этом не проиграли? Ответ таков: да, возможно, и проиграли, но тут уж ничего не попишешь. В чем беда? Сейчас мы попробуем понять это.

Примем соотношения $k_{-1} < k_1$ и $k_{-1} + k_1 < 1/2$ как данность. Они для нас стандартны и носят лишь технический характер, упрощая подсчет максимальных и минимальных скалярных произведений векторов из Σ . В таком случае

$$\begin{aligned}\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) &= k_{-1} + k_1, \\ \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) &= -2k_{-1}.\end{aligned}$$

В нашем распоряжении есть только теорема 10: она сильнее других, а ничего лучшего мы, к сожалению, не знаем. В разделе 3.5 мы замечали фактически, что теорема 10 раскрывается в полную силу, коль скоро величина запрещенного скалярного произведения a максимально близка к дроби

$$\frac{\bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) + \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1)}{2}.$$

У нас эта дробь превращается в $\frac{k_1 - k_{-1}}{2}$. Тогда уравнение на λ записывается в виде

$$n\lambda^2 - 2(k_1 - k_{-1})\lambda + a = 0,$$

где $a \approx (k_1 - k_{-1})/2$. Очевидно, что уравнение разрешимо лишь при $a \approx 0$ (т.е. при $k_{-1} \approx k_1$), и его корень есть как раз $\lambda \approx 0$. Жесткой связи между параметрами в рамках нашей технологии и впрямь не избежать.

Сразу же возникает встречный вопрос. Ладно, тут все ясно. Но зачем же мы тогда весь огород городили, если λ непременно равно нулю? Да, действительно, в рамках нынешнего подхода наши усилия

ни к чему. Однако в следующем разделе мы изложим удивительную технику — так называемый «метод альтернирования», — и для нее ненулевые значения λ понадобятся. Опять-таки, все учтено заранее.

Замечание 3. Предположим все-таки, что $\lambda = 0$. Помните, в доказательстве леммы 7 мы апеллировали к тому факту, что сумма координат любого вектора из Σ есть одно и то же число? В нынешнем предположении в этом нет необходимости. В частности, при $\lambda = 0$ метод сработает и для совокупностей $(-1, 0, 1)$ -векторов, в каждом элементе которых фиксировано лишь число ненулевых координат: сказано, что $k_{-1} + k_1 = k$, но сами k_ν никак не регламентированы. Лишь бы аналог утверждения 1 имел место.

Обсудим контрпримеры к гипотезе Борсука. Разумеется, начиная с какого-то n , они есть, но вот с какого? У Кана и Калаи гипотеза впервые нарушалась при $n = 2014$ и всюду далее оказывалась неверна. Дальнейшая история вопроса напоминала историю мировых рекордов в каком-нибудь виде спорта (см. [7]).

Последние результаты, полученные с помощью $(0, 1)$ -векторов, принадлежали автору этой брошюры, который опроверг гипотезу при $n \geq 561$, и Бернульф Вайсбаху, сумевшему уменьшить эту оценку на единицу. Затем наступило затишье, нарушенное серией работ Айке Хинрихса, Олега Пихурко и Христиана Рихтера, показавших в итоге, что Борсук заведомо ошибался в случае $n \geq 298$. Этот факт опирался на так называемые «минимальные векторы решетки Лича». Наука о такого сорта конфигурациях выходит далеко за рамки нашей темы, и мы ее даже не попытаемся объяснять здесь. Вместе с тем, не станем мы рассказывать и о « $(0, 1)$ -контрпримерах»: они нам доступны, но не в том наша цель.

Главное, что никто пока не знает, справедлива ли гипотеза при $n < 298$ (известно только, что при $n \leq 3$ она верна), и что забавным образом $(-1, 0, 1)$ — совокупности мы еще в этой связи не упоминали. Казалось бы, в асимптотике оценки, полученные за счет таких совокупностей, куда точнее оценок, вытекающих из рассмотрения $(0, 1)$ -векторов. Разве не значит это, что и контрпримеры проще находить, используя три координаты? Нет, к сожалению, все упирается в конкретный вид бесконечно малых слагаемых в основаниях наших экспонент, и этот вид при малых n «забывает» первый член асимптотики. Однако не все так скверно. В разделе 3.4 у нас была гипотеза 1, и мы сейчас покажем, что если она верна, то контрпримеры к предположению Борсука возникают уже в размерности 136.

Рассмотрим совокупность $(-1, 0, 1)$ -векторов Σ_1 , фигурирующую в гипотезе 1. Мы знаем, что $M = |\Sigma_1| = 1\,647\,360$. Правда, в Σ_1

количество единиц и минус единиц у каждого вектора не определено, но мы положим $a = \lambda = 0$ и сошлемся на замечание 3. Тогда

$$m = \frac{16(16+1)}{2} = 136,$$

и нетрудно видеть, что отображение $\Sigma_1 \mapsto \Sigma_1^*$ взаимнооднозначное. При этом гипотеза говорит нам, что $D < 12\,000$. Следовательно,

$$f(136) \geq \frac{M}{D} > \frac{1\,647\,360}{12\,000} = 137,28,$$

т.е. $f(136) \geq 138$, и контрпример у нас в кармане.

В двух последних разделах мы установили самые точные нижние оценки для $f(n)$ и $\chi(\mathbb{R}^n)$. В разделе 4.4 мы покажем, как нетривиально можно одну из этих оценок чуть-чуть улучшить.

4.4. О числах Борсука и Нельсона—Эрдёша—Хадвигера

Мы знаем, что

$$\chi(\mathbb{R}^n) \geq (1,239 \dots + o(1))^n, \quad f(n) \geq (1,2255 \dots + o(1))^{\sqrt{n}},$$

и ничего лучшего нам доказать не удастся. Разумеется, мы не можем даже предположить, как выглядит правильная оценка для $\chi(\mathbb{R}^n)$ или $f(n)$. Однако в любом случае она есть нечто вроде

$$\chi(\mathbb{R}^n) \geq (\tilde{\chi} + o(1))^n, \quad f(n) \geq (\tilde{f} + o(1))^{\sqrt{n}},$$

где заведомо

$$1,239 \dots \leq \tilde{\chi} = \tilde{\chi}(n) \leq 3, \quad 1,2255 \dots \leq \tilde{f} = \tilde{f}(n) \leq \left(\sqrt{\frac{3}{2}}\right)^{\sqrt{n}}.$$

Последнее неравенство особенно неприятно, но и в первом зависимость от n вполне уместно подчеркнуть. Короче говоря, все, что есть в нашем распоряжении,—это тот факт, что $\tilde{\chi}(n) \geq 1,239 \dots$ и $\tilde{f}(n) \geq 1,2255 \dots$. В частности,

$$\tilde{\chi}(n) + \tilde{f}(n) \geq 1,239 \dots + 1,2255 \dots$$

Казалось бы, что нового в таком сложении? Понятно, что раз каждая функция (\tilde{f} — число Борсука, $\tilde{\chi}$ — число Нельсона—Эрдёша—Хадвигера) больше некоторой величины, то и сумма функций оценивается соответственно. Ан нет: автор настоящей брошюры разработал *метод альтернирования*, который в рамках данной задачи привел к совершенно неожиданному результату. А именно, справедлива

Теорема 14. *Существует такое постоянное $\delta > 0$ и найдутся такие бесконечные последовательности n_i, ν_i размерностей, что*

$$\tilde{\chi}(n_i) + \tilde{f}(\nu_i) \geq 1,239 \dots + 1,2255 \dots + \delta.$$

Иными словами, оценку каждого числа в отдельности мы уточнять не умеем, но можем показать, что хотя бы одно из этих чисел на самом деле слегка больше. Это, безусловно, свидетельствует о поразительной близости задач Борсука и Нельсона—Эрдёша—Хадвигера. Само число δ вычисляется в явном виде, и по ходу доказательства мы объясним, как это делается.

Доказательство теоремы 14. Сперва мы изложим основную идею. Именно в ней состоит суть метода. Мы докажем следующую альтернативу:

Альтернатива 1. *Либо $\tilde{\chi}(n_i) \geq u_1$, либо $\tilde{f}(\nu_i) \geq u_2$ с некоторыми u_1, u_2 и $n_i, \nu_i, i = 1, 2, \dots$*

Из альтернативы сразу же вытекает, что либо

$$\tilde{\chi}(n_i) + \tilde{f}(\nu_i) \geq u_1 + 1,2255 \dots,$$

либо

$$\tilde{\chi}(n_i) + \tilde{f}(\nu_i) \geq u_2 + 1,239 \dots$$

Дабы оценка суммы наших величин сделалась безусловной, нужно искать u_1, u_2 , для которых

$$u_1 + 1,2255 \dots = u_2 + 1,239 \dots$$

Естественно, мы будем стремиться при этом к тому, чтобы u_1 было строго больше (на $\delta > 0$), чем 1,239, а u_2 — строго больше, чем 1,2255. И результат к тому же хочется получить, по возможности, оптимальный. Все это, впрочем, детали; главное — альтернатива. Доказательство альтернативы 1 мы распишем для пущей прозрачности по шагам.

Шаг 1. Возьмем n, k_{-1}, k_0, k_1 такими же, как в доказательстве следствия из теоремы 10 (см. раздел 4.2). Рассмотрим совокупность

$$\Sigma = \Sigma(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1).$$

Тогда

$$\bar{s} = \bar{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = k_{-1} + k_1,$$

$$\underline{s} = \underline{s}(\{-1, 0, 1\}^n; k_{-1}, k_0, k_1) = -2k_{-1},$$

$$M = |\Sigma| = (M_0 + o(1))^n, \quad M_0 = M_0(k_{-1}, k_0, k_1) = \text{const} > 1$$

(см. следствие из теоремы 10).

Шаг 2. Выберем минимальное простое p , удовлетворяющее неравенству $\bar{s} - 3p < \underline{s}$. Это для нас совершенно стандартная операция, и понятно, что, как обычно,

$$p \sim \frac{\bar{s} - \underline{s}}{3} = \frac{k_1 + 3k_{-1}}{3}.$$

Однако кое-что все же не так. Дело в том, что прежде (скажем, в следствии из теоремы 10) p было асимптотически равно половине разности между максимальным и минимальным скалярными произведениями. Теперь же речь идет о трети той же величины. Очевидно, за этим скрывается некая хитрость: разумеется, чем p меньше, тем для нас лучше (см. следующий шаг), но ведь в том-то и беда, что до сих пор мы p подбирали оптимально. С чего бы это вдруг нам такая удача улыбнулась? Смысл в том, что мы не будем доказывать в дальнейшем никаких «абсолютных» утверждений; мы лишь обоснуем «условную» альтернативу. Именно это поможет нам уменьшить p и не только ничего на том не потерять, но даже слегка выиграть.

Шаг 3. Положим

$$D = \sum_{(m_1, m_2) \in \mathcal{A}} C_n^{m_1} C_{n-m_1}^{m_2},$$

где

$$\mathcal{A} = \{(m_1, m_2): m_1, m_2 \in \mathbb{N} \cup \{0\}, m_1 + m_2 \leq n, m_1 + 2m_2 \leq p - 1\}.$$

В доказательстве следствия из теоремы 10 было формально точно такое же D . Однако нынешняя величина заведомо меньше своей тезки, поскольку значение p , как мы уже отмечали на шаге 2, уменьшилось. Мы знаем, что величины типа D обычно оказываются в знаменателе дроби, увеличить которую мы всеми силами стремимся. Еще яснее, стало быть, то, о чем мы говорили на предыдущем шаге. Только опять-таки трудно угадать, как мы всем этим воспользуемся. Что ж, всему свое время. В любом случае,

$$D = (D_0 + o(1))^n, \quad D_0 = D_0(k_{-1}, k_0, k_1) = \text{const} < M_0.$$

Последнее утверждение доказывается стандартно (см. раздел 4.2), и мы на нем более подробно останавливаться не будем.

Шаг 4. Найдем решение $\rho_0 = \rho_0(k_{-1}, k_0, k_1)$ уравнения

$$1,2255 \dots + \frac{M_0}{\rho_0} = 1,239 \dots + \left(\frac{\rho_0}{D_0}\right)^{\sqrt{2}}$$

на интервале (D_0, M_0) . Нетрудно видеть, что при любых k_{-1}, k_0, k_1 такое решение существует и единственно. Само уравнение выглядело бы

угрожающе, если бы не описанная нами с самого начала общая идея доказательства. В действительности, величина M_0/ρ_0 сыграет впоследствии роль u_1 , а величина $(\rho_0/D_0)^{\sqrt{2}}$ — роль u_2 . Положим $\rho = \rho_0^n$.

Шаг 5. Рассмотрим произвольную подсовокупность векторов \mathcal{F} в Σ , обладающую тем свойством, что

$$(\mathbf{x}, \mathbf{y}) \neq \bar{s} - p \quad \text{при всех } \mathbf{x}, \mathbf{y} \in \mathcal{F}.$$

Поскольку в Σ скалярное произведение очень даже часто равняется $\bar{s} - 2p$, применить линейно-алгебраический метод для отыскания верхней оценки мощности \mathcal{F} не удастся. А нам того и не слишком хотелось: так или иначе, но следующая альтернатива, без сомнения, выполнена.

Альтернатива 2. Либо $|\mathcal{F}| \leq \rho$, либо найдется такое $W \subset \Sigma$, что в W нет пар векторов со скалярным произведением $\bar{s} - p$ и, тем не менее, $|W| > \rho$.

Далее мы убедимся в том, что если верен первый вариант альтернативы 2, то

$$\tilde{\chi}(n) \geq u_1 = \frac{M_0}{\rho_0};$$

если же в силе второй вариант, то

$$\tilde{f}(m) \geq u_2 = \left(\frac{\rho_0}{D_0}\right)^{\sqrt{2}}$$

с некоторым $m = m(n)$. Как только мы это сделаем, теорема будет, по сути, доказана.

Шаг 6. Итак, обратимся к первому варианту альтернативы 2. В этом случае очевидно, что Σ есть $(M, \rho, \sqrt{2p})$ -критическая конфигурация в \mathbb{R}^n (в совокупности Σ расстояние $\sqrt{2p}$ однозначно задается скалярным произведением $\bar{s} - p$). Значит,

$$\chi(\mathbb{R}^n) \geq \frac{M}{\rho} = \left(\frac{M_0}{\rho_0} + o(1)\right)^n = (u_1 + o(1))^n,$$

т. е. как раз $\tilde{\chi}(n) \geq u_1$, и все в порядке. Что же будет в противном случае?

Шаг 7. Пусть теперь $W \subset \Sigma$ свободно от пар векторов, имеющих скалярное произведение $\bar{s} - p$, и в то же время $|W| > \rho$. Имеет место

Лемма 8. Какова бы ни была совокупность векторов $Q \subset W$, скалярное произведение любых двух элементов которой не совпадает с $\bar{s} - 2p$, ее мощность не превосходит D .

Доказательство леммы 8. Ясно, что в Q нет пар векторов как со скалярным произведением $\bar{s} - p$ ($Q \subset W$), так и со скалярным

произведением $\bar{s} - 2p$ (условие леммы). Вместе с тем, $\bar{s} - 3p < \underline{s}$, и, стало быть,

$$(\mathbf{x}, \mathbf{y}) \not\equiv \bar{s} \pmod{p} \quad \text{при всех } \mathbf{x}, \mathbf{y} \in Q.$$

Применима теорема 12, которая и влечет за собой наше утверждение. \square

Шаг 8. В раздел 4.3 был изложен общий подход к построению оценок для $f(m)$ ($m = n(n+1)/2$). Там требовались совокупность Σ , величины a (запрещенное скалярное произведение в том контексте), λ (параметр перехода от Σ к Σ^* , т.е. от размерности n к размерности m) и D (размер оценки в утверждении 1), и нужна была уверенность в том, что переход от Σ к Σ^* биективен. В нашем случае роль Σ исполнит W (с биекцией тут проблем нет), и мы положим $a = \bar{s} - 2p$. Число λ отыщется автоматически, а D — это то самое D , что сопутствует нам по ходу доказательства: лемма 8 и есть, конечно, нужный нам аналог утверждения 1. Надо только следить за тем, чтобы $(k_1 - k_{-1}) - (\bar{s} - 2p)n$ не было меньше нуля (см. раздел 4.3); иначе λ найти не удастся.

В результате

$$f(m) \geq \frac{|W|}{D} = \left(\frac{\rho_0}{D_0} + o(1) \right)^n = \left(\left(\frac{\rho_0}{D_0} \right)^{\sqrt{2}} + o(1) \right)^{\sqrt{m}},$$

т.е. $\tilde{f} \geq u_2$, и снова все получается.

Шаг 9. Альтернатива 1 (а вместе с ней и теорема 14) практически доказана. Остается лишь оптимизировать по k_{-1}, k_0, k_1 значения u_1, u_2 . Это и приведет к искомым неравенствам. Дело это, однако ж, довольно муторное, и мы предоставляем его читателю. \square

Замечание 4. Подход, использованный нами, весьма универсален. С его помощью можно доказывать оценки не только на сумму чисел Борсука и Нельсона—Эрдёша—Хадвигера, но и, скажем, на их произведение. Вообще, можно брать любую функцию $g = g(x, y)$, которая монотонна по каждому из своих аргументов при $x \geq 1$ и $y \geq 1$, и для $g(\tilde{x}, \tilde{f})$ всегда отыщется нетривиальная оценка (лучшая, чем $g(\tilde{x}, \tilde{f}) \geq g(1, 239 \dots, 1, 2255 \dots)$).

4.5. О хроматических числах с несколькими запретами

До сих пор мы использовали теорему 12 лишь в весьма специальном виде. Это несколько огорчительно, ведь в соответствии со всеми классическими канонами ружье, висящее на стене, не может не выстрелить. По счастью, и нам каноны нарушать не придется:

есть задача, появившаяся до теоремы 12, но без последней теоремы не решаемая.

Речь идет о *хроматическом числе пространства \mathbb{R}^n с несколькими запрещенными расстояниями*, которое определяется практически так же, как и $\chi(\mathbb{R}^n)$; только теперь точкам одного цвета запрещено отстоять друг от друга на каждое расстояние $a_i > 0$ из множества $\{a_1, \dots, a_t\}$ различных вещественных чисел. Соответственно, новое хроматическое число обозначается

$$\chi(\mathbb{R}^n, \{a_1, \dots, a_t\}).$$

Величина $\chi(\mathbb{R}^n, \{a_1, \dots, a_t\})$ зависит от слишком многих параметров. Правда, один из них без ограничения общности можно считать равным единице (гомотетичность пространства самому себе). Но это не очень помогает. Посему рассматривают, как правило,

$$\hat{\chi}(\mathbb{R}^n, t) = \max_{a_1, \dots, a_t} \chi(\mathbb{R}^n, \{a_1, \dots, a_t\}).$$

П. Эрдёш был инициатором рассмотрения такой величины, и он знал, например, что

$$\hat{\chi}(\mathbb{R}^2, t) \geq ct\sqrt{\log t}, \quad c > 0.$$

Нас будет в большей мере интересовать ситуация, когда $n \rightarrow \infty$, причем, вообще говоря, одновременно $t = t(n) \rightarrow \infty$. В этом случае упомянутая в разделе 4.2 оценка

$$\chi(\mathbb{R}^n) \leq (3 + o(1))^n$$

заведомо влечет за собой неравенство

$$\hat{\chi}(\mathbb{R}^n, t) \leq (3 + o(1))^{tn}.$$

Ужасно, но никто его пока не улучшил, хотя, по-видимому, сделать это не так уж трудно. Зато самую точную нижнюю оценку здесь дает

Теорема 15. *Существуют константы $c_1, c_2 > 0$, с которыми выполнено неравенство*

$$\hat{\chi}(\mathbb{R}^n, t) \geq (c_1 t)^{c_2 n}.$$

Разумеется, константы можно пытаться вычислить явно и притом предельно аккуратно, но это очень скучно. К тому же пока у нас в наличии колоссальный зазор в оценках:

$$(c_1 t)^{c_2 n} \leq \hat{\chi}(\mathbb{R}^n, t) \leq (3 + o(1))^{tn},$$

ведь если, например, $t \asymp \log n$, то мы имеем

$$e^{O(n \log \log n)} \leq \hat{\chi}(\mathbb{R}^n, t) \leq e^{O(n \log n)},$$

что скверно. Похоже, что улучшать надо именно верхнюю оценку, а потому тем более не стоит гнаться за константами в нижней. Итак, мы будем выписывать в доказательстве вполне огромные постоянные, не обращая внимания на их величину.

Доказательство теоремы 15. Сейчас мы воспользуемся идеей, на которой были основаны все рассуждения в разделе 4.2: мы введем понятие $(M, D, \{a_1, \dots, a_t\})$ -критической конфигурации. В сущности, ясно, что это такое. Это совокупность векторов Σ в \mathbb{R}^n , имеющая мощность M и обладающая тем свойством, что любая подсовокупность $\mathcal{F} \subset \Sigma$, в которой $|\mathbf{x} - \mathbf{y}| \notin \{a_1, \dots, a_t\}$ ($\mathbf{x}, \mathbf{y} \in \mathcal{F}$), состоит не более чем из D элементов. Разумеется, коль скоро такая совокупность Σ найдена,

$$\hat{\chi}(\mathbb{R}^n, t) \geq \chi(\mathbb{R}^n, \{a_1, \dots, a_t\}) \geq \frac{M}{D},$$

и нужно чтобы последнее отношение оказалось побольше. Ниже мы отдельно рассмотрим четыре различных случая, в каждом из которых построим свою критическую конфигурацию. При этом мы будем всякий раз считать, что $n \geq n_0$, т. е. размерность достаточно велика. Каким следует брать n_0 , будет видно из контекста.

Случай 1. Пусть $t \leq 2^{10\,000}$. Жуткая константа, но мы другого и не обещали. Понятно, что, каковы бы ни были a_1, \dots, a_t ,

$$\hat{\chi}(\mathbb{R}^n, t) \geq \chi(\mathbb{R}^n, \{a_1, \dots, a_t\}) \geq \chi(\mathbb{R}^n) \geq (1,239 \dots + o(1))^n.$$

Однако t не превосходит константы, и, значит, мы вольны написать

$$\hat{\chi}(\mathbb{R}^n, t) \geq (1,239 \dots + o(1))^n = (\nu_1 t)^{\mu_1 n}.$$

Первый случай был тривиальным, и понадобился он лишь затем, чтобы мы могли считать величину t достаточно большой. Это удобно при дальнейших выкладках. Следующий случай самый сложный, и именно в нем нужна линейная алгебра.

Случай 2. Пусть $2^{10\,000} < t \leq 2^{100} n^2$. Вот первый момент, когда важно, что $n > n_0$: иначе таких t не будет. Введем дополнительные параметры. Положим

$$u = \left\lceil \frac{1}{2} \log_2 t \right\rceil - 100, \quad v = \left\lfloor \frac{n}{2^u} \right\rfloor.$$

Заметим, что

$$u \leq \frac{1}{2} \log_2(2^{100} n^2) - 100 = 50 + \log_2 n - 100 < \lfloor \log_2 n \rfloor,$$

и, стало быть, $2^u < n$, а $v \geq 1$. Все оценки сделаны с огромным запасом, и это лишний раз свидетельствует о крайней небрежности в выборе параметров.

Рассмотрим совокупность векторов

$$\Sigma = \Sigma(\{0, 1, \dots, 2^u\}^n; n - v2^u, v, v, \dots, v)$$

(см. раздел 3.5). Совокупность определена корректно, так как $v \geq 1$, $n - v2^u \geq 0$ (нулевых координат в векторах из Σ , вообще говоря, может и не быть, но это значения не имеет) и $n - v2^u + v + \dots + v = n$.

В дальнейшем мы поймем, что Σ — это $(M, D, \{a_1, \dots, a_t\})$ -критическая конфигурация с некоторыми a_1, \dots, a_t и надлежащим M/D . Пока же заведомо ясно, что

$$M = |\Sigma| = P(n - v2^u, v, v, \dots, v) = \frac{n!}{(n - v2^u)!(v!)^{2^u}}.$$

Выражение для M выглядит довольно-таки страшно. Однако нам нужна его нижняя оценка, и сейчас мы ее приведем. Обратимся к помощи легкого неравенства

$$M = \frac{n!}{(n - v2^u)!(v!)^{2^u}} \geq \frac{(v2^u)!}{(v!)^{2^u}}$$

и общих неравенств

$$\left(\frac{a}{e}\right)^a \leq a! \leq e\left(\frac{a}{2}\right)^a,$$

которые каждый без особого труда докажет по индукции. Тогда

$$(v2^u)! \geq \left(\frac{v2^u}{e}\right)^{v2^u}, \quad (v!)^{2^u} \leq \left(e\left(\frac{v}{2}\right)^v\right)^{2^u},$$

ввиду чего

$$\frac{(v2^u)!}{(v!)^{2^u}} \geq 2^{uv2^u} e^{-v2^u - 2^u} 2^{v2^u}.$$

Очевидно, $v \geq \frac{n}{2^{u+1}}$. Следовательно, $uv2^u \geq \frac{un}{2}$. В то же время

$$e^{-v2^u - 2^u} 2^{v2^u} = e^{-v2^u - 2^u + v2^u \ln 2} > e^{-\frac{1}{2}v2^u - 2^u},$$

поскольку $\ln 2 > \frac{1}{2}$. В свою очередь

$$-\frac{1}{2}v2^u - 2^u = -2^u\left(\frac{1}{2}v + 1\right).$$

Но $\frac{1}{2}v + 1 \leq 2v$ ($v \geq 1$), т. е.

$$-\frac{1}{2}v2^u - 2^u \geq -v2^{u+1} \geq -2n.$$

Таким образом,

$$M \geq 2^{un/2} e^{-2n},$$

и это уже вполне обозримо.

Как и в разделе 3.5, определим

$$\bar{s} = \bar{s}(\{0, 1, \dots, 2^u\}^n; n - v2^u, v, v, \dots, v).$$

Нетрудно видеть, что

$$\bar{s} = v(1^2 + 2^2 + \dots + (2^u)^2) = \left[\frac{n}{2^u} \right] \frac{2^u(2^u + 1)(2^{u+1} + 1)}{6}.$$

Здесь мы пользуемся известной формулой для суммы квадратов натуральных чисел.

Пусть p — это наименьшее нечетное простое, для которого $p > \bar{s}/t$. В силу известного постулата Бертрана (см. раздел 2.4) $p \leq 2\bar{s}/t$. Правда, хорошо бы еще проверить, что $\bar{s}/t > 3$ (иначе постулат неприемлем). В самом деле,

$$\bar{s} \geq \frac{1}{12} \frac{n}{2^u} 2^{3u+1} = \frac{1}{12} n 2^{2u+1}.$$

Далее,

$$2u + 1 \geq 2 \left(\frac{1}{2} \log_2 t - 101 \right) + 1 = \log_2 t - 201.$$

Значит,

$$\frac{1}{12} n 2^{2u+1} \geq \frac{1}{12} n t \frac{1}{2^{201}} > 3,$$

и все в порядке. Опять-таки запас прочности у нас колоссальный.

Положим

$$\begin{aligned} a_1 &= \sqrt{2p}, & a_2 &= \sqrt{4p}, \dots, & a_t &= \sqrt{2tp}, \\ a'_1 &= \bar{s} - p, & a'_2 &= \bar{s} - 2p, \dots, & a'_t &= \bar{s} - tp. \end{aligned}$$

Число p подобрано так, что $a'_t < 0$. Беря в качестве \underline{s} аналог одноименной величины из раздела 3.5 (применительно к нынешней ситуации) и замечая, что $\underline{s} > 0$, приходим к выводу, что для $\mathbf{x}, \mathbf{y} \in \Sigma$ условия

$$\begin{aligned} |\mathbf{x} - \mathbf{y}| &\notin \{a_1, \dots, a_t\}, \\ (\mathbf{x}, \mathbf{y}) &\notin \{a'_1, \dots, a'_t\} \end{aligned}$$

и

$$(\mathbf{x}, \mathbf{y}) \not\equiv \bar{s} \pmod{p}$$

равносильны. В таком случае теорема 12 показывает, что Σ — это $(M, D, \{a_1, \dots, a_t\})$ -критическая конфигурация с

$$D \leq \sum_{(m_1, \dots, m_{2u}) \in \mathcal{A}} C_n^{m_1} \cdot C_{n-m_1}^{m_2} \cdot \dots \cdot C_{n-m_1-\dots-m_{2u-1}}^{m_{2u}},$$

где

$$\mathcal{A} = \{(m_1, \dots, m_{2^u}) : m_1, \dots, m_{2^u} \in \mathbb{N} \cup \{0\}, m_1 + \dots + m_{2^u} \leq n, \\ m_1 + 2m_2 + \dots + 2^u m_{2^u} \leq p - 1\}.$$

В действительности, оценка на D — это оценка количеством мономов от n переменных, таких, что их степени не выше $p - 1$, а степень каждой конкретной переменной в них не выше 2^u (убедитесь в этом). Ясно, что таких мономов не больше, чем $\sum_{i=0}^{p-1} C_n^i (2^u)^i$: C_n^i — это число способов выбрать переменные, которые войдут в моном, а $(2^u)^i$ — это количество вариантов возведения каждой из фиксированных i переменных в одну из 2^u возможных степеней.

Получаем оценку

$$D < \sum_{i=0}^{p-1} C_n^i (2^u)^i < 2^{up} 2^n.$$

У нас $p \leq 2\bar{s}/t$, причем $t \geq 2^{2u+200}$. Следовательно,

$$p \leq \frac{2n2^u(2^u+1)(2^{u+1}+1)}{2^u2^u2^{200}6} < \frac{n}{6}.$$

Таким образом,

$$\hat{\chi}(\mathbb{R}^n, t) \geq \chi(\mathbb{R}^n, \{a_1, \dots, a_t\}) \geq \frac{M}{D} \geq 2^{\frac{un}{2}} e^{-2n} 2^{-\frac{un}{6} - n} \geq 2^{\frac{un}{6}} = (\nu_2 t)^{\mu_2 n}.$$

Здесь в последнем неравенстве важно, что u достаточно велико, а это обусловлено оценкой $t > 2^{10000}$. Случай разобран.

Случай 3. Тут мы предполагаем, что

$$\max\{2^{10000}, 2^{100} n^2\} < t \leq n^{2.5} \quad (n > n_0).$$

Тогда мы апеллируем к соображению из случая 1:

$$\hat{\chi}(\mathbb{R}^n, t) \geq \hat{\chi}(\mathbb{R}^n, t')$$

при $t' < t$ (например, при $t' = 2^{100} n^2$). Иными словами,

$$\hat{\chi}(\mathbb{R}^n, t) \geq (\nu_2 t')^{\mu_2 n} = (\nu_3 t)^{\mu_3 n}$$

(мы пользуемся тем, что $t \leq n^\alpha$ с фиксированным α).

Случай 4. Пусть $t > n^{2.5}$. Введем следующие обозначения. Через \mathbb{Z}_+^n мы обозначим множество всех n -мерных векторов, имеющих неотрицательные целые координаты; через $B \subset \mathbb{R}^n$ мы обозначим шар радиуса $\sqrt{t/2}$ с центром в начале координат:

$$B = \left\{ \mathbf{x} = (x_1, \dots, x_n) : x_1^2 + \dots + x_n^2 \leq \frac{t}{2} \right\}.$$

Положим $S = B \cap \mathbb{Z}_+^n$. Рассмотрим набор чисел

$$\{a_1, \dots, a_{t'}\} = \{a > 0: a = |\mathbf{x} - \mathbf{y}|, \mathbf{x}, \mathbf{y} \in S\}.$$

Если считать, что

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

то, разумеется,

$$0 < |\mathbf{x} - \mathbf{y}|^2 = (x_1 - y_1)^2 + \dots + (x_n - y_n)^2 \leq x_1^2 + \dots + x_n^2 + y_1^2 + \dots + y_n^2 \leq t.$$

Вместе с тем $|\mathbf{x} - \mathbf{y}|^2 \in \mathbb{Z}$, и, значит, $t' \leq t$, т. е., как обычно,

$$\hat{\chi}(\mathbb{R}^n, t) \geq \hat{\chi}(\mathbb{R}^n, t').$$

Но S — это $(M, D, \{a_1, \dots, a_{t'}\})$ -критическая конфигурация, у которой, тривиальным образом, $D = 1$. Что же до M , то с ним дела обстоят так:

$$M = |S| \geq V_n(\gamma\sqrt{t})^n,$$

где $\gamma > 0$ — постоянная, а V_n — объем единичного n -мерного шара. Последний имеет порядок β^n/n^n , где $\beta > 0$ (см. [10]), ввиду чего

$$\hat{\chi}(\mathbb{R}^n, t) \geq M \geq \left(\delta \frac{\sqrt{t}}{n}\right)^n, \quad \delta > 0.$$

Однако $n < t^{0,4}$, и, стало быть,

$$\hat{\chi}(\mathbb{R}^n, t) \geq (\delta t^{0,1})^n = (\nu_4 t)^{\mu_4 n}.$$

Для завершения доказательства остается лишь положить

$$c_1 = \min\{\nu_1, \dots, \nu_4\},$$

$$c_2 = \min\{\mu_1, \dots, \mu_4\},$$

так что всегда $\hat{\chi}(\mathbb{R}^n, t) \geq (c_1 t)^{c_2 n}$. Теорема доказана. \square

4.6. Вокруг задачи Нельсона—Эрдёша—Хадвигера

В предыдущих разделах мы рассказали о многих интересных и важных задачах комбинаторной геометрии, возникающих в связи с проблемами Борсука и Нельсона—Эрдёша—Хадвигера. Естественно, линейно-алгебраический метод применялся нами в полную силу, и мы даже привели нетривиальное его уточнение (см. раздел 4.4). Однако классических вопросов о раскрасках пространств еще на порядок больше. Конечно, мы говорили однажды, что истории этих вопросов мы будем касаться лишь по случаю, отсылая читателя к известному

набору брошюр и обзоров. И тем не менее, кое-что не осветить здесь, пожалуй, нельзя: во-первых, результаты абсолютно свежие и в упомянутых источниках не содержатся; а во-вторых, сам круг задач исключительно любопытен и своеобразен. Опять-таки большая часть результатов основана на линейной алгебре.

Некоторые читатели наверняка знают, что в математике существует обобщенное понятие расстояния—так называемая *метрика*. Это понятие совершенно разумно и отвечает начальной интуиции (см. [6] и [9]). Мы дадим сейчас его определение. Пусть X —это произвольное множество объектов, называемое «пространством». Функция $\rho = \rho(\cdot, \cdot)$ двух аргументов пространства X (скажем, x, y)—это метрика (расстояние между x и y), коль скоро выполнены следующие три свойства:

1. $\rho(x, y) \geq 0$, и $\rho(x, y) = 0$ тогда и только тогда, когда $x = y$.
2. $\rho(x, y) = \rho(y, x)$.
3. $\rho(x, y) \leq \rho(x, z) + \rho(z, y)$.

Во всех свойствах стоило бы поставить кванторы «для любого» по каждой из букв x, y, z , но это и так ясно. Смысл очень простой: разумеется, расстояние должно быть неотрицательным, и вряд ли оно может быть положительным при $x = y$ или же нулевым при $x \neq y$; далее, нам безразлично, откуда начинать мерить расстояние—от x к y или наоборот (свойство 2—симметрия); наконец, и аналог неравенства треугольника (свойство 3) в особых комментариях не нуждается.

В конечном итоге пару (X, ρ) принято именовать *метрическим пространством*. Вообще-то, такое пространство имеет право быть сколь угодно вычурным, но мы о таких ситуациях рассуждать не станем. Даже X состоит подчас из не вполне удобоваримых элементов. Для наших целей хватит $X = \mathbb{R}^n$ и $X = \mathbb{Q}^n$. В первом случае речь идет, как обычно, о вещественном арифметическом пространстве, во втором—о его рациональном подмножестве, т. е. о совокупности векторов, имеющих рациональные координаты. Очень важно, что пока и \mathbb{R}^n , и \mathbb{Q}^n суть лишь наборы «точек»: никакого расстояния на них еще нет. И если раньше мы тотчас же заявляли, что расстояние евклидово (см. §4.1), то теперь мы попытаемся вычислять его по иным, более общим, формулам.

Пусть $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$ и, кроме того,

$$\mathbf{x} = (x_1, \dots, x_n), \quad \mathbf{y} = (y_1, \dots, y_n) \in X.$$

Фиксируем $p \in [1, \infty)$ (p — это некоторое вещественное число; не думайте, что оно простое) и рассмотрим функцию l_p :

$$l_p(\mathbf{x}, \mathbf{y}) = \sqrt[p]{|x_1 - y_1|^p + \dots + |x_n - y_n|^p}.$$

Понятно, что

$$l_2(\mathbf{x}, \mathbf{y}) = |\mathbf{x} - \mathbf{y}|,$$

т. е. мы имеем прямое обобщение евклидова расстояния. Проверить же, что все три свойства метрики выполнены при любом p , ничего не стоит. Введенную нами метрику иногда называют *гёльдеровской*, и она исключительно часто возникает в науке.

Зададимся вопросом: что будет, если, допустим, перейти к пределу при $p \rightarrow \infty$ в выражении $\sqrt[p]{3^p + 5^p}$? Ответ на вопрос очевиден: получится 5. Оно и всегда так:

$$\lim_{p \rightarrow \infty} \sqrt[p]{|x_1 - y_1|^p + \dots + |x_n - y_n|^p} = \max_{i=1, \dots, n} |x_i - y_i|.$$

Такое замечание позволяет нам определить l_p и при $p = \infty$:

$$l_\infty(\mathbf{x}, \mathbf{y}) = \max_{i=1, \dots, n} |x_i - y_i|.$$

Нетрудно убедиться в том, что это тоже метрика. Ее зачастую называют *чебышёвской* или *экстремальной*.

Всё, больше никаких пространств и метрик нам не потребуется, и мы ограничимся изучением пар (X, l_p) , коль скоро $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$. Это, впрочем, не означает, что другими вопросами никто не занимается: просто нам и без того информации будет предостаточно.

В 1976 году М. Бенда и М. Перлес, следуя духу задачи Нельсона—Эрдёша—Хадвигера, сформулировали понятие *хроматического числа метрического пространства* (X, ρ) с множеством запрещенных расстояний \mathcal{H} : это минимальное число цветов, в которые можно так раскрасить все элементы X , чтобы элементы, отстоящие друг от друга на любое расстояние (в смысле метрики) $a \in \mathcal{H}$, оказались разноцветными. Говоря более подробно, мы должны разбить X на части X_1, \dots, X_χ таким образом, чтобы для любого $i \in \{1, \dots, \chi\}$ и для любых $x, y \in X_i$ было выполнено соотношение $\rho(x, y) \notin \mathcal{H}$. При этом искомая величина — обозначим ее

$$\chi((X, \rho), \mathcal{H})$$

— есть наименьшее χ , при котором указанное разбиение осуществимо. Понятно, что

$$\chi((\mathbb{R}^n, l_2), \{a\}) = \chi(\mathbb{R}^n) \quad \text{при любом } a > 0.$$

Точно так же

$$\chi((\mathbb{R}^n, l_2), \{a_1, \dots, a_t\}) = \chi(\mathbb{R}^n, \{a_1, \dots, a_t\}).$$

Раньше мы для краткости не вводили лишние параметры, ведь и так ясно было, о какой метрике идет речь. Теперь же мы будем выписывать всё, что только можно. Полезно сразу же подчеркнуть, что $\chi((\mathbb{Q}^n, l_p), \{a\})$ зависит от величины a , в отличие от своего «вещественного» аналога.

Отметим, что \mathcal{H} вполне может быть и бесконечным. В таком случае хроматическое число устроено крайне нетривиально, и линейная алгебра помогает мало. Тем не менее, мы скажем и об этом пару слов, но пока ограничимся рассмотрением конечных множеств запретов. Доказывать мы ничего не станем; мы лишь приведем результаты и прокомментируем их. Имеет место

Теорема 16. *Выполнены следующие оценки.*

1. Если $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$ и $a > 0$, то

$$\chi((X, l_2), \{a\}) \leq (3 + o(1))^n.$$

2. Если $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$, $a > 0$ и $p \in [1, \infty)$, то

$$\chi((X, l_p), \{a\}) \leq (5 + o(1))^n.$$

3. Если $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$, $p \in [1, \infty)$ и \mathcal{H} любое,

$$\chi((X, l_p), \mathcal{H}) \leq (5 + o(1))^{n|\mathcal{H}|}.$$

Если $p = 2$, то пятерку в основании можно заменить тройкой.

4. При любых $a > 0$ и $p \in [1, \infty)$

$$\chi((\mathbb{R}^n, l_p), \{a\}) \geq (1,207\dots + o(1))^n,$$

5. При любом $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$

$$\chi((X, l_1), \{a\}) \geq (1,365\dots + o(1))^n,$$

в то время как $a \in \mathbb{R}$ при $X = \mathbb{R}^n$ и $a \in \mathbb{Q}$ при $X = \mathbb{Q}^n$ (всегда, конечно, $a > 0$).

6. При любом $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$,

$$\chi((X, l_\infty), \{1\}) = 2^n.$$

7. Если $a > 0$ и $a \in \mathbb{Q}$, то

$$\chi((\mathbb{Q}^n, l_2), \{a\}) \geq (1,173\dots + o(1))^n.$$

8. Существует такое $a \in \mathbb{R}$, что

$$\chi((\mathbb{Q}^n, l_2), \{a\}) \geq (1,239 \dots + o(1))^n.$$

9. Существует такая бесконечная последовательность размерностей n_i , что

$$\chi((\mathbb{Q}^{n_i}, l_2), \{a\}) \geq (1,239 \dots + o(1))^{n_i}$$

при любом $a \in \mathbb{Q}$.

10. Для каждого $p \in [1, \infty)$ существует такое $\varepsilon(p) > 0$, что

$$\chi((\mathbb{Q}^n, l_p), \{a\}) \geq (1 + \varepsilon + o(1))^n$$

для любого положительного рационального a . При этом $\varepsilon(p) \rightarrow 0$, коль скоро $p \rightarrow \infty$.

11. Для каждого t найдутся положительные постоянные c_1, c_2 и множество \mathcal{H} , $|\mathcal{H}| = t$, с которыми

$$\chi((X, l_p), \mathcal{H}) \geq (c_1 t)^{c_2 n},$$

коль скоро $X \in \{\mathbb{R}^n, \mathbb{Q}^n\}$ любое, $a \in \{1, 2\}$.

Пункт 1 теоремы 10 доказан Д. Ларманом и К. А. Роджерсом в 1972 году, пункт 2 — Дж.-Х. Канг и З. Фюреди в 2004 году, пункт 4 — П. Франклом и Р. М. Уилсоном в 1981 году, пункты 5, 7 — А. М. Райгородским (2000—2004). Пункт 3 есть непосредственное следствие пунктов 1 и 2.

Перейдем к комментариям. Пункты 1, 2, 3 теоремы доказываются за счет геометрической техники, связанной с разбиениями пространств и упаковкой множеств в них. Пункты 4, 5 и 7—11 основаны на линейно-алгебраических результатах. Например, пункт 4 ничем, по сути, не отличается от следствия из теоремы 3 (см. раздел 4.2). Пункты 8 и 9 апеллируют к следствию из теоремы 10 (см. раздел 4.2), а пункт 11 аналогичен факту из предыдущего раздела. Остальные пункты (за исключением пункта 6, доказательство которого мы оставляем читателю) суть нетривиальные модификации следствий из теорем 3 и 10: их уже так лихо не доказать, но читатель может попробовать сделать и это.

Если внимательно посмотреть на оценки, в которых фигурирует \mathbb{Q}^n , станет ясно, что главная тонкость в них — это возможность (или невозможность) выбора в них произвольного запрещенного состояния (множества запретов). Скажем, в пункте 7 результат весьма общий: a — любое рациональное. Однако из-за этого слегка страдает оценка, ведь, как свидетельствуют пункты 8 и 9, иногда неравенство из пункта 7 улучшаемо. Тем не менее, нужно либо жестко зафиксировать a , пожертвовав прежней общностью, либо, сохраняя

произвольность выбора запрета, пожертвовать большинством размерностей. Между прочим, хоть условие $a \in \mathbb{Q}$ и вредит (пункт 7), все же работать с произвольным (а не специально подобранным, как в пункте 8) $a \in \mathbb{R}$ еще тяжелее, и мы об этом просто не станем рассказывать. В то же время проблема произвольности рационального запрета особенно хорошо видна в случае, когда этот запрет не один. Если в пункте 11 дополнительно потребовать, чтобы \mathcal{H} состояло только из рациональных чисел, то линейная алгебра не поможет. Нужно будет привлекать технику так называемых случайных графов, и это уже совершенно иная наука.

Интересно, что хроматическое число рационального пространства оценивается снизу хуже, чем его «вещественный» аналог. Разумеется, это вполне ожидаемо, ведь раскрасить подмножество легче, чем все множество ($\mathbb{Q}^n \subset \mathbb{R}^n$). Однако любопытно то, что в «малых» размерностях дела с \mathbb{Q}^n обстоят не столь трагично, как с \mathbb{R}^n : известно, например, что

$$\chi((\mathbb{Q}^2, l_2), \{1\}) = \chi((\mathbb{Q}^3, l_2), \{1\}) = 2,$$

т. е. такой проблемы, какую мы имели для

$$\chi(\mathbb{R}^2) = \chi((\mathbb{R}^2, l_2), \{1\}),$$

здесь и в помине нет. Вместе с тем, ничего более сильного в асимптотике, чем тривиальное неравенство

$$\chi((\mathbb{Q}^n, l_2), \{1\}) \leq \chi((\mathbb{R}^n, l_2), \{1\}) \leq (3 + o(1))^n$$

(см. пункты 1 и 2 теоремы), никто пока не придумал. Таким образом, в малой размерности зазор между верхними и нижними оценками хроматического числа больше в вещественном случае, а при растущем n — в рациональном.

Приглядимся к нижним оценкам величины $\chi((\mathbb{R}^n, l_p), \{1\})$. Зависимость от p константы, стоящей в правой части каждой такой оценки, изображена на рис. 6. Эта зависимость крайне нерегулярна, что наводит на мысль о сравнительном несовершенстве тех методов, которыми мы пользуемся. Что ж, все еще впереди.

Что же можно сказать, если $|\mathcal{H}| = \infty$? Безусловно, сказать можно так много, что деваться от подобного избытия информации будет некуда. На самом деле, наука здесь крайне обширная и многогранная. Однако, поскольку к теме нашей книги она отношения не имеет, мы позволим себе только несколько слов об одном из ее интереснейших аспектов.

Итак, пусть $\mathcal{H} = \{a_i\}_{i=1}^{\infty}$. Таким образом, речь пойдет о счетных последовательностях запретов, хотя, разумеется, запрещенные рассто-

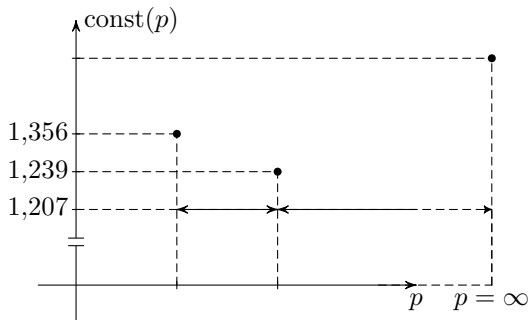


Рис. 6

яния могли бы и в континуальное множество сложиться. Предположим дополнительно, что

$$\frac{a_{i+1}}{a_i} \geq 1 + \frac{1}{d} \quad \text{для любого } i.$$

Это значит, что последовательность должна расти не медленнее, чем геометрическая прогрессия. Говорят тогда, что эта последовательность *лакунарна*. Смысл понятен: с увеличением номера i значение a_i , как минимум, экспоненциально возрастает, и между соседними членами последовательности возникают «дыры» (лакуны), по которым и дано название. Спрашивается, например: как велико может быть число $\chi((\mathbb{R}^n, l_2), \mathcal{H})$? Это замечательная проблема. Известно, что

$$d \leq \max_{\mathcal{H}} \chi((\mathbb{R}^1, l_2), \mathcal{H}) \leq 9d^2,$$

где $d \geq 3$ — «степень» (коэффициент) лакунарности каждой последовательности \mathcal{H} из области, по которой берется максимум. Нижняя оценка проста (докажите ее), а верхняя получена за счет методов аналитической теории чисел, и принадлежит она Н. Г. Мощевитину и Р. К. Ахунжанову. Как видно, проблема нетривиальна даже на прямой. Но с плоскостью и вовсе чудеса творятся: никто не знает даже, конечно ли соответствующее хроматическое число при произвольном \mathcal{H} . Техника там отнюдь не комбинаторная. Наука, к которой она относится, называется эргодической теорией, и здесь у нас нет возможности о ней говорить.

Заметим для пущей ясности, что если последовательность может быть «сублакунарна», т. е. если a_i может расти как $o(e^n)$, то проблемы нет: существуют сублакунарные \mathcal{H} , для которых хроматическое число $\chi((\mathbb{R}^1, l_2), \mathcal{H})$ бесконечно.

Задачи

1. Попробуйте получить какие-нибудь оценки величины $\chi(n, a, d)$, упомянутой в разделе 4.1.
2. Можно ли улучшить оценку $\chi(\mathbb{R}^n) \geq (1,239 \dots + o(1))^n$ с помощью линейной алгебры?

3. (*Теорема Райгородского.*) Докажите, что

$$\hat{\chi}(\mathbb{R}^n, 2) \geq (1,439 \dots + o(1))^n.$$

4. (*Теорема Райгородского.*) Докажите, что существуют $a_1, a_2 \in \mathbb{R}$, с которыми выполняется неравенство

$$\chi((\mathbb{R}^n, l_1), \{a_1, a_2\}) \geq (1,607 \dots + o(1))^n.$$

5. Попробуйте вычислить константы в теореме 15, сделав это как можно аккуратнее.

6. Попробуйте улучшить оценку $\hat{\chi}(\mathbb{R}^n, t) \leq (3 + o(1))^{tn}$.

7. Докажите теорему 16.

8. (*Теорема Райгородского.*) С помощью альтернирования покажите, что существуют числа a_1, \dots, a_t , с которыми справедливо неравенство $\chi(\mathbb{R}^n, \{a_1, \dots, a_t\}) \geq (c_1 t)^{c_2 n}$, причем

$$1 + \frac{\gamma_1}{t} \leq \frac{a_{i+1}}{a_i} \leq 1 + \frac{\gamma_2}{\log t}.$$

Здесь $i \in \{1, \dots, t-1\}$, $\gamma_1, \gamma_2 > 0$.

9. (*Теорема Райгородского.*) С помощью альтернирования улучшите одну из оценок: $\hat{\chi}(\mathbb{R}^n, 2) \geq (1,439 \dots + o(1))^n$ и

$$\max_{a_1, a_2 \in \mathbb{Q}} \chi((\mathbb{R}^n, l_2), \{a_1, a_2\}) \geq (1,173 \dots + o(1))^n.$$

5 || Теория Рамсея

5.1. Круг задач и формулировка результата

В настоящей главе мы рассмотрим приложение группы комбинаторных результатов, полученных нами с помощью линейно-алгебраического метода, еще к одной классической задаче. Задача эта содержится в рамках целой замечательной и крайне популярной в настоящее время теории — *теории Рамсея*. Основной (и притом самый общий) вопрос теории: *если дано некоторое множество объектов, верно ли, что его можно так разбить на куски, чтобы некоторые из этих кусков содержали (или не содержали) конфигурацию заданного типа?* Ниже мы для пущей ясности приведем несколько наиболее важных примеров конкретных рамсеевских проблем. В результате станет видно, насколько разнообразна, нетривиальна и глубока теория.

Самым близким нам примером является, конечно, уже изученная нами задача Нельсона—Эрдёша—Хадвигера. Действительно, в этой задаче в роли «объектов» выступают точки пространства \mathbb{R}^n (или даже элементы произвольного метрического пространства (X, ρ)). «Запрещенная конфигурация» объектов, которую не должны содержать куски искомого разбиения, — это пара точек на расстоянии 1. Кажется, тут и сомнений быть не может. Заметим, что, рассмотренная в рамсеевском ключе, проблема хроматического числа допускает красивое обобщение, состоящее в том, что точкам одного цвета запрещается образовывать множество вершин некоторого многогранника — скажем, симплекса или параллелепипеда. В таком случае задача приобретает новый оттенок. П. Франкл, В. Рёдл и др. занимались ею, но мы сейчас об их результатах говорить не будем.

Любопытно, что проблема Борсука носит не совсем рамсеевский характер. Мы не имеем права утверждать, что речь в ней идет о разбиении произвольного множества точек в \mathbb{R}^n на части, внутри которых нет каких-либо определенных конструкций. Хотелось бы, конечно, сказать, что в упомянутых частях должны отсутствовать точки, расстояние между которыми равно диаметру исходного множества, но это неверно: в открытом шаре радиуса $1/2$ нет диаметрально противоположных векторов, и все же диаметр его, будучи точной верхней гранью расстояний, равен единице. Посему следует требовать того,

чтобы не только в самих частях разбиения, но и в их *замыканиях* не было паразитических точек. Вот тогда все будет честно. Беда лишь в том, что замыкания частей «чуть-чуть» пересекаются (по границам)¹⁾, и это портит картину, коль скоро мы пытаемся подогнать ее под теорию Рамсея. Однако если ограничиться рассмотрением конечных множеств точек в пространстве (каковые, между прочим, доставляют контрпримеры к гипотезе Борсука), то для них рамсеевость будет иметь место.

Вот совсем другая и ничуть не менее актуальная область исследований. В 1926 году Б. Л. Ван дер Варден доказал теорему: *как бы мы ни разбивали множество натуральных чисел на конечное число частей, найдется часть, содержащая сколь угодно длинные арифметические прогрессии*. Иными словами, если дано разбиение

$$\mathbb{N} = N_1 \sqcup \dots \sqcup N_k, \quad (1)$$

то существует такое $i \in \{1, \dots, k\}$, что для любого l можно подобрать прогрессию a_1, \dots, a_l , все элементы которой принадлежат N_i . Подчеркнем, что для разных l прогрессии будут, вообще-то, разными, т. е. выражение «сколь угодно длинные» нельзя сократить до слова «бесконечные». Тем не менее, факт поразительный, и с него началась целая эпоха в теории Рамсея, к каковой этот факт, без сомнения, относится. Доказывается он с помощью методов теории чисел, да это и немудрено (см. [4], [12]). Мы не можем удержаться от того, чтобы не изложить вкратце следствия ван-дер-варденовской теоремы, хотя наша цель в дальнейшем и будет иной. Скажем, что множество $A \subset \mathbb{N}$ имеет *положительную верхнюю плотность*, если

$$\limsup_{n \rightarrow \infty} \frac{|\{i \in (A \cap \{1, \dots, n\})\}|}{n} > 0.$$

Очевидно, что в разбиении (1) одна из частей непременно имеет положительную верхнюю плотность. Лишь в 1975 году Э. Семереди доказал, что любое множество такой плотности содержит сколь угодно длинную арифметическую прогрессию. Естественно, теорема Ван дер Вардена есть простое следствие утверждения Семереди. Наконец, вездесущий Эрдеш высказал такую гипотезу: *если ряд*

$$\sum_{i=1}^{\infty} \frac{1}{a_i}$$

¹⁾ Отметим, что, граница — это не так уж мало: у счетного множества рациональных точек на континуальном отрезке $[0, 1]$ граница — это весь отрезок.

расходится ($a_i \in \mathbb{N}$), то в последовательности чисел a_i есть сколь угодно длинная арифметическая прогрессия. Из гипотезы вытекает и результат Семереди, и тем более результат Ван дер Вардена. Гипотеза исключительно красива и важна, но никто ее пока доказать не может. Дабы почувствовать всю ее универсальность и трудность, достаточно заметить, что из нее следует существование сколь угодно длинных прогрессий в множестве простых чисел. В самом деле, мы знаем, что количество простых, величина которых не превосходит $x \in \mathbb{R}$, асимптотически равно $x/\ln x$ (см. раздел 2.4). Это значит, что верхняя плотность множества простых равна нулю. Вместе с тем, если мы занумеруем все простые в порядке возрастания, то i -е простое будет иметь вид $a_i \sim i \ln i$. По известному интегральному признаку ряд из величин $1/(i \ln i)$ расходится, и гипотеза применима. Не правда ли, удивительно? Впрочем, буквально год назад именно для простых a_i гипотезу подтвердили Б. Грин и Т. Тао, которые этим прославились. Общий же случай стоит неприступно.

Перейдем, собственно, к постановке нашей главной на данном этапе задачи. Для этого нам потребуется вспомнить, что такое *граф*. Мы будем считать, что граф — это пара $G = (V, E)$, где V — некоторое множество объектов (у нас оно будет всегда конечным, хотя это не

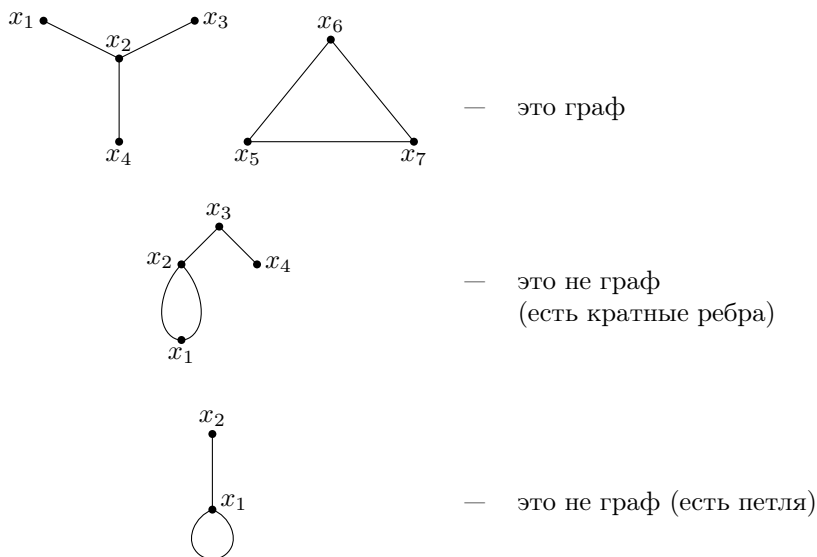


Рис. 7

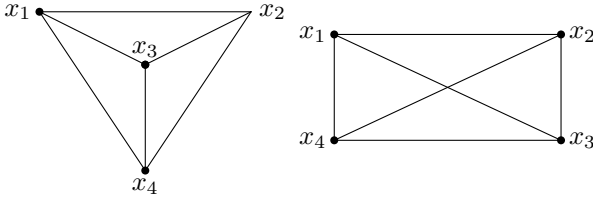


Рис. 8

обязательно), называемое *множеством вершин* графа, а E — некоторая совокупность пар элементов из V , называемая *множеством ребер* графа: $x \in V$ — вершина G ; $(x, y) \in E$ — ребро G . При этом каждая пара (x, y) встречается в E не более одного раза (в графе нет *кратных ребер*), пара (x, x) не принадлежит E (в графе нет *петель*), и ребро (x, y) отождествляется с ребром (y, x) (в графе нет *ориентации*, т. е. ребра суть неупорядоченные пары вершин). Зачастую (конечные) графы изображают на плоскости. Это удобно для понимания определения (см. рис. 7), но это же и приводит к различным тонкостям, связанным с тем, что один и тот же граф можно совершенно по-разному расположить на картинке: скажем, в одном случае ребра графа будут пересекаться только по вершинам, а в другом появятся какие-нибудь «перекрестки» (см. рис. 8). Это — вопрос о *планарности* графа (см. [6], [11]). Нас подобные геометрические вопросы сейчас волновать не должны, и мы будем интерпретировать граф исключительно комбинаторно.

Граф $G = (V, E)$ называется *полным*, если $|E| = C_{|V|}^2$, т. е. в графе каждые две вершины соединены ребром. Если в полном графе n вершин, то он обозначается K_n (см. рис. 9). Говорят, что $G' = (V', E')$ — это *подграф* графа $G = (V, E)$ ($G' \subseteq G$), если $V' \subseteq V$ и $E' \subseteq E$. Множество $I \subseteq V$ называется *независимым множеством вершин* графа $G = (V, E)$, коль скоро ни одна пара (x, y) с $x, y \in I$ не принадлежит E , т. е. на I нет ребер графа G (см. рис. 5.1). В графе может быть куча независимых множеств вершин, но, поскольку он конечен, среди этих множеств заведомо есть те, у которых вершин больше всего. Обозначим мощность каждого из таких «максимальных» независимых множеств через $\alpha(G)$ и назовем эту величину *числом независимости* графа G (см. рис. 5.1, на котором изображен

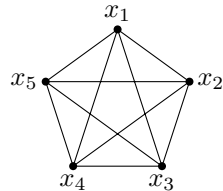


Рис. 9

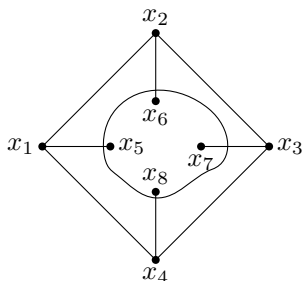


Рис. 10

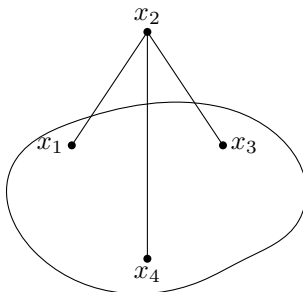


Рис. 11

граф с числом независимости 3). Независимое множество вершин — это как бы «пустой» подграф в G . По аналогии можно рассматривать полные подграфы, выбирать из них те, у которых самое большое количество вершин, и обозначать это количество через $\omega(G)$ (см. рис. 12, на котором показан граф с $\omega(G) = 4$). Обозначим, наконец, через \bar{G} граф, «дополнительный» к графу $G = (V, E)$, т. е. граф, у которого множество вершин — V (то же, что и у G), а в множество ребер входят те и только те пары (x, y) с $x, y \in V$, которые E не принадлежат (см. рис. 13). Ясно, что $\alpha(G) = \omega(\bar{G})$ и наоборот.

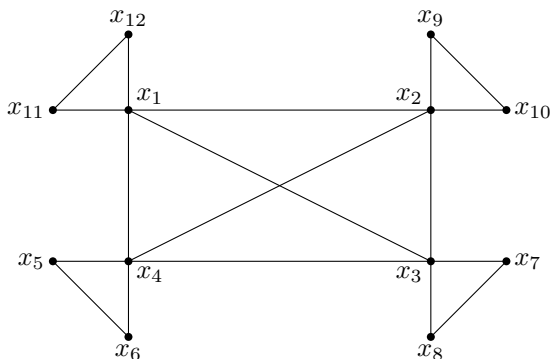


Рис. 12

Пусть s и t — натуральные числа. Скажем, что *число Рамсея* $R(s, t)$ — это минимальное $n \in \mathbb{N}$, такое, что при любой раскраске множества ребер графа K_n в два цвета (синий и красный) либо найдется $K_s \subseteq K_n$, у которого все ребра синие, либо отыщется

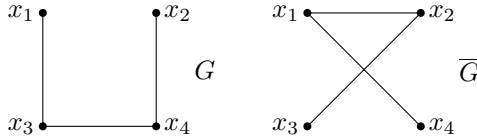


Рис. 13

$K_t \subseteq K_n$, у которого все ребра красные. Можно сказать и иначе: $R(s, t)$ — это минимальное $n \in \mathbb{N}$, такое, что для любого графа G , имеющего n вершин, одновременно $\omega(G) \geq s$ и $\omega(\bar{G}) \geq t$. Очевидно, определения эквивалентны: раскрасить ребра K_n в синий и красный цвета — это все равно что взять граф на n вершинах, объявить его ребра синими, а ребра дополнительного графа — красными (см. рис. 14).

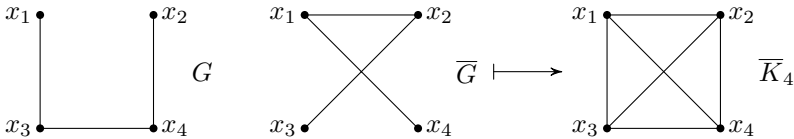


Рис. 14

Понятно сразу, что

$$R(s, t) = R(t, s), \quad R(s, 1) = 1, \quad R(s, 2) = s.$$

Первое утверждение совсем тривиально, а второе содержит логическую тонкость, которую мы поясним фразой «все крокодилы в реке Тумча синие» (если у графа одна вершина, то ребрами там не пахнет, а стало быть, и цвет у них какой угодно). Все: больше точных результатов нет. Известно только, что

$$\begin{aligned} R(3, 3) &= 6, & R(3, 4) &= 9, & R(3, 5) &= 14, \\ R(4, 4) &= 18, & R(3, 6) &= 18, & R(3, 7) &= 23. \end{aligned}$$

Впрочем, изначально не ясно даже, конечно ли число Рамсея. Оно таки конечно, но мы этого доказывать не станем. Мы лишь предложим читателю схему необходимых действий, реализовав которую, он сам поймет, что все в порядке. Действительно, сперва следует установить рекуррентное неравенство

$$R(s, t) \leq R(s, t-1) + R(s-1, t). \quad (2)$$

Обосновывать неравенство надо посредством индукции по параметрам s, t . Затем полезно вспомнить простое тождество

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1},$$

из которого ввиду оценки (2) и начальных условий

$$R(s, 1) = R(1, t) = 1$$

мгновенно вытекает соотношение

$$R(s, t) \leq C_{s+t-2}^{s-1}.$$

В частности,

$$R(s, s) \leq C_{2s-2}^{s-1} \sim \frac{4^s}{\sqrt{4\pi s}}.$$

Последняя оценка была усилена в 2006 году Д. Конлоном:

$$R(s, s) \leq \exp\left\{-c \frac{\log^2 s}{\log \log s}\right\} 4^s s^{-1/2}, \quad c > 0,$$

и пока это самое точное, что мы знаем.

Что касается нижних оценок для $R(s, t)$, то и они, конечно же, найдены. Позднее мы будем, в основном, интересоваться величиной $R(s, s)$ («диагональным» числом Рамсея), и потому, не желая перегружать книгу излишней информацией, мы приведем результаты лишь для такой величины. А для нее наилучшим в настоящее время является неравенство, доказанное Дж. Спенсером в 1975 году:

$$R(s, s) \geq \frac{\sqrt{2}}{e} s 2^{s/2} (1 + o(1)).$$

Таким образом, по существу,

$$(\sqrt{2} + o(1))^s \leq R(s, s) \leq (4 + o(1))^s,$$

и зазор, несомненно, велик. Устранение или хотя бы уменьшение зазора — сложная проблема, и не в ее обсуждении наша цель. Имеется вот еще какая тонкость. Дело в том, что упомянутая выше нижняя оценка получена с помощью мощного *вероятностного метода* в комбинаторике. Мы не станем, конечно, объяснять детали, но смысл в том, что существование искомого объекта (в данном случае — раскраски ребер полного графа) доказывается путем некоего «усреднения» (см. [14]). В результате, мы определенно знаем, что нужный объект где-то есть, но как он выглядит — понятия не имеем: ни малейшего представления о его внутренней структуре у нас, к сожалению, нет. И вроде бы хорошо, что объект отыскался — оценка-то у нас в кармане — да вот

и поглядеть на него все же не мешало бы. А это не удастся. Соответственно, возникает новая задача — придумать *явную* конструкцию, которая давала бы как можно лучшую нижнюю оценку для $R(s, s)$. Поразительно, но это очень тяжело, и тут один из самых мощных результатов принадлежит П. Франклу и Р. М. Уилсону, которые в 1981 году доказали следующую теорему.

Теорема 17 (П. Франкл, Р. М. Уилсон). *Можно предъявить конкретную конструкцию, показывающую, что*

$$R(s, s) \geq \exp\left\{\gamma(s) \frac{\ln^2 s}{\ln \ln s}\right\},$$

где $\gamma(s) \asymp \text{const}$.

Теорема обосновывается за счет линейной алгебры, и мы подробно изложим ее доказательство в следующем разделе. Заметим лишь, что на сей раз суть теоремы именно в ее конкретности (новое преимущество нашего основного метода), а не в величине оценки. С ней-то как раз все исключительно, на первый взгляд, плохо: она ведь даже не экспоненциальна. Но такова уж специфика комбинаторных задач. Зачастую неявные оценки куда сильнее явных, однако это не снижает значимости последних. Впрочем, никто не утверждает, что бороться с возникшей трудностью не нужно. Еще как нужно. А пока — чем богаты, тем и рады. Все-таки без линейной алгебры у нас и того не было бы.

Прежде чем переходить к доказательству теоремы, мы сформулируем еще один (неявный, но любопытный) результат. А именно, для $R(s, 3)$ найдена «почти асимптотика»:

$$\left(\frac{1}{162} + o(1)\right) \frac{s^2}{\log s} \leq R(s, 3) \leq (1 + o(1)) \frac{s^2}{\log s}.$$

Чуть-чуть бы подтянуть, и готово дело. Нижнюю оценку доказал Дж. Х. Ким в 1995 году, а верхняя принадлежит фактически М. Айтаи, Й. Комлошу и Э. Семереди, которые получили свой результат в 1980 году.

5.2. Доказательство теоремы 17

Доказательство. Мы стремимся показать, что $R(s, s) \geq m = m(s)$, где конкретный вид функции m пока значения не имеет. Для этого нам достаточно построить такой граф G на m вершинах, что и $\omega(G) < s$, и $\alpha(G) < s$. Таким образом, мы как бы получим отрицание второго определения диагонального числа Рамсея, и все

будет в порядке. С высоты наших знаний граф строится крайне просто.

Возьмем произвольное $q = p^\beta$, где p — простое число (знакомое начало), и положим

$$n = q^3, \quad k = q^2 - 1.$$

Пусть V — это совокупность всех возможных k -элементных подмножеств множества \mathcal{R}_n (см. главу 2), т. е. $|V| = C_n^k$. Рассмотрим граф $G = (V, E)$, где

$$E = \{(M, N) : M, N \in V, |M \cap N| \not\equiv -1 \pmod{q}\}.$$

Очевидно,

$$|M \cap N| \not\equiv k \pmod{q},$$

когда (M, N) — ребро. Тогда теорема 4 немедленно дает оценку

$$\omega(G) \leq C_n^{q-1} < C_n^q.$$

С другой стороны, если $I \subset V$ — независимое множество, то

$$|M \cap N| \equiv -1 \pmod{q}$$

для любых $M, N \in I$, т. е.

$$|M \cap N| \in \{q-1, 2q-1, \dots, q^2-1\}.$$

Следовательно, если мы положим

$$r = q, \quad l_1 = q-1, \quad \dots, \quad l_r = q^2-1,$$

то теорема 5 даст нам неравенство

$$\alpha(G) \leq \sum_{i=0}^r C_n^i,$$

которое легко превратить в оценку

$$\alpha(G) < (q+1)C_n^q.$$

Итак, мы имеем совершенно конкретный граф, у которого

$$\omega(G) < C_n^q \quad \text{и} \quad \alpha(G) < (q+1)C_n^q.$$

Пусть

$$s = (q+1)C_n^q = (q+1)C_{q^3}^q, \quad m = |V| = C_n^k = C_{q^3}^{q^2-1}.$$

Остается понять, как m выражается через s . Иными словами, мы докажем теорему, если убедимся в том, что

$$m = \exp \left\{ \gamma(s) \frac{\ln^2 s}{\ln \ln s} \right\}$$

с некоторым $\gamma(s) \asymp 1$.

Воспользуемся очевидной оценкой $C_n^k \leq n^k$ и неравенством

$$C_n^k = \frac{n(n-1)\cdots(n-k+1)}{k!} \geq \frac{n^k}{k^k} \left(1 - \frac{k}{n}\right)^k.$$

Тогда

$$\begin{aligned} s &= (q+1)C_{q^3}^q \leq (q+1)q^{3q} \leq q^{4q}, \\ s &\geq (q+1)\frac{q^{3q}}{q^q} \left(1 - \frac{1}{q^2}\right)^q \geq q^q. \end{aligned}$$

Значит,

$$s = q^{\gamma_1(q)q},$$

где $\gamma_1 \asymp 1$. Аналогично доказывается, что

$$m = q^{\gamma_2(q)q^2}, \quad \gamma_2 \asymp 1.$$

Ясно, что

$$\begin{aligned} \ln^2 s &= (\gamma_1 q \ln q)^2, \\ \ln \ln s &= \ln q + O(\ln \ln q). \end{aligned}$$

Следовательно,

$$\frac{\ln^2 s}{\ln \ln s} \asymp q^2 \ln q,$$

т. е. можно подобрать $\gamma(s) \asymp 1$ так, что

$$\exp\left\{\gamma(s)\frac{\ln^2 s}{\ln \ln s}\right\} = \exp\{\gamma_2(q)q^2 \ln q\} = m.$$

Теорема почти доказана. Маленькая тонкость состоит в том, что пока мы имеем результат лишь при тех s , которые имеют вид $s = (q+1)C_{q^3}^q$ с $q = p^\beta$. Борьба с этим можно исходя из известных нам фактов о распределении простых (и их степеней) в натуральном ряде. Делается это так же, как при доказательстве следствия из теоремы 2, и здесь мы выкладки опускаем. \square

Можно вычислить более аккуратно значение $\gamma(s)$ в теореме. Однако смысла в том большого нет: все равно оценка неэкспоненциальна, и потому куда важнее увеличивать порядок роста показателя экспоненты, а не константу при нем. Интересно, что здесь даже $(-1, 0, 1)$ -векторы не помогают. Попробуйте убедиться в этом.

Задачи

1. Докажите, что $R(3, 3) = 6$. Попробуйте найти как можно лучшие верхние и нижние оценки для $R(4, 5)$ и $R(3, 8)$.
2. Докажите, что для любого $\varepsilon > 0$ и $s \geq 3$ найдется такая константа $c(\varepsilon, s)$, что при достаточно большом t либо

$$R(s, t) < c(\varepsilon, s)R(s-1, t)\frac{t}{\log t},$$

либо

$$R(s, t) < R(s-2, t)t^\varepsilon.$$

Что отсюда следует?

6 || Задача об отклонении

6.1. Постановка задачи и краткий исторический экскурс

Сейчас мы в некотором роде вернемся к объектам, с которых начинали нашу книгу. Действительно, мы рассмотрим множество \mathcal{R}_n и произвольную совокупность $\mathcal{M} = \{M_1, \dots, M_s\}$ его подмножеств. На сей раз, впрочем, мы никак не регламентируем мощности множеств $M_i \in \mathcal{M}$. Да и задача теперь совсем иная. Отныне нас будет интересовать построение раскрасок элементов \mathcal{R}_n в два цвета (скажем, синий и красный), при которых в каждом множестве совокупности \mathcal{M} число синих и красных элементов «примерно» одно и то же. Чуть позже мы дадим более точную постановку проблемы, но уже ясно, что проблема весьма нетривиальна и многогранна. В самом деле, если совокупность \mathcal{M} состоит из попарно непересекающихся множеств, то, очевидно, существует такая раскраска, что разница между количеством синих и красных элементов в каждом из множеств $M_i \in \mathcal{M}$ не превосходит единицы (если же мощности множеств четные, то и вовсе говорить не о чем; см. рис. 15). На другом «конце» находится ситуация, когда \mathcal{M} содержит все возможные подмножества \mathcal{R}_n ($|\mathcal{M}| = 2^n$). В этих условиях какую бы раскраску мы ни взяли, заведомо отыщется полностью синее или полностью красное множество (причем оно будет далеко не одиноким). Таким образом, проблема есть, и она нуждается в четкой формализации.

Говорить о синих и красных цветах приятно, но для математических целей не всегда удобно. Посему мы обозначим произвольную раскраску (в конечном итоге раскрасок 2^n) через χ и будем интерпретировать ее как отображение множества \mathcal{R}_n на множество n -мерных $(-1, 1)$ -векторов $\{-1, 1\}^n$: $\chi(i) \in \{-1, 1\}$, $i \in \mathcal{R}_n$. В таком ключе синий цвет элемента — это, допустим, 1, а красный цвет — это -1 , соответственно. Или наоборот, неважно. Введем *отклонение раскраски* χ на

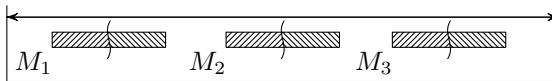


Рис. 15

множестве $M \in \mathcal{M}$, полагая его равным

$$\text{disc}(\chi, M) = \left| \sum_{i \in M} \chi(i) \right|.$$

Понятно, что чем меньше отклонение, тем меньше разница между количеством элементов красного и синего цветов в множестве M . И термин «отклонение», стало быть, не случаен. Немного смущает его обозначение disc , но и оно легко объяснимо: оно происходит от слова *discrepancy*, имеющего латинский корень и означающего в аккурат ‘разброс’, ‘уклонение’.

Положим, далее,

$$\text{disc}(\chi, \mathcal{M}) = \max_{M \in \mathcal{M}} \text{disc}(\chi, M).$$

Последняя величина есть, естественно, *отклонение раскраски χ на совокупности множеств \mathcal{M}* . Она измеряет степень глобального разброса и показывает, насколько хороша или плоха раскраска всей совокупности в целом.

Нас же волнует, безусловно, «самая хорошая» раскраска. Разумеется, она однозначно характеризуется тем, что минимизирует значение $\text{disc}(\chi, \mathcal{M})$ для данной совокупности \mathcal{M} . Иными словами, мы рассмотрим величину

$$\text{disc}(\mathcal{M}) = \min_{\chi} \text{disc}(\chi, \mathcal{M}).$$

Если эта величина ограничена некоторым числом значит, то *существует* раскраска с соответствующим отклонением на совокупности \mathcal{M} . Иначе — *любая* раскраска отклоняется слишком сильно. Вот и задача: оценить как можно точнее (при различных условиях) величину $\text{disc}(\mathcal{M})$. Более того, интересно понять, как ведет себя (в зависимости от n , s и, возможно, каких-нибудь других параметров)

$$\max \text{disc} = \max_{\mathcal{M}} \text{disc}(\mathcal{M}) = \max_{\mathcal{M}} \min_{\chi} \max_{M \in \mathcal{M}} \left| \sum_{i \in M} \chi(i) \right|,$$

где внешний максимум берется по всем совокупностям с фиксированными параметрами. Опять-таки, коль скоро $\max \text{disc} \leq t$, *всякая* совокупность допускает раскраску, отклонение которой не больше t . В противном случае *имеется* совокупность, у которой любая раскраска чересчур «разбросана».

Большинство результатов относительно величины $\max \text{disc}$ доказывается с помощью *вероятностного метода в комбинаторике*. Мы приведем несколько формулировок такого сорта, но обосновывать, естественно, ничего не будем. У нас, как известно, иная цель. И так, во-первых, выполнена

Теорема 18. *Для любой совокупности \mathcal{M} имеет место оценка*

$$\text{disc}(\mathcal{M}) \leq \sqrt{2n \ln(2s)}.$$

Эта теорема простая, но нам она, ввиду специфики нашей деятельности, все равно не по зубам (теорию вероятностей мы вполне можем не знать). Стоит, однако ж, прояснить ее смысл. Суть теоремы в том, что если, скажем, $s \asymp n$, а мощности множеств из \mathcal{M} равны, например, $[n/2]$, то отклонение с определенностью меньше величины порядка $\sqrt{n \log n}$, которая ничтожно мала по сравнению с $[n/2]$ («почти» половина каждого множества синяя и «почти» половина красная). Более того, параметры можно широко варьировать, и вывод будет тем же (величина отклонения останется равной «о малому» от мощности представителей совокупности \mathcal{M}). Иногда теорему 18 можно усилить. В 1985 году Дж. Спенсер доказал следующий факт.

Теорема 19 (Дж. Спенсер). *Для любой совокупности*

$$\mathcal{M} = \{M_1, \dots, M_n\}$$

имеет место оценка

$$\text{disc}(\mathcal{M}) \leq 5,32\sqrt{n}.$$

Иными словами, если количество множеств в совокупности совпадает с числом элементов в множестве, которому все это хозяйство принадлежит, то, вместо неравенства

$$\text{disc}(\mathcal{M}) \leq \sqrt{2n \ln(2n)},$$

возникает неравенство $\text{disc}(\mathcal{M}) \leq 5,32\sqrt{n}$, что в логарифм раз точнее. Теорема 19 снова вероятностная (там удобно использовать замечательное понятие *энтропии*), и мы ее не доказываем.

Можно приводить и некоторые другие верхние оценки, но нам хватит того, что есть. Интересно, например, насколько точна теорема 19. Может, и она допускает улучшения? Иначе говоря, верно ли, что $\max \text{disc} \asymp \sqrt{n}$ при $s = n$? Оказывается, ответ на поставленный вопрос положителен.

Теорема 20. *Существует бесконечная последовательность \mathcal{R}_{n_i} и совокупности $\mathcal{M} = \{M_1, \dots, M_{n_i}\}$, для которых*

$$\text{disc}(\mathcal{M}) \geq \frac{\sqrt{n}}{2}.$$

Эту теорему мы докажем в следующем разделе с помощью изящного линейно-алгебраического подхода. Наконец, мы докажем исключительно красивую теорему, принадлежащую Дж. Беку и Т. Фиале.

В самом деле, пусть $\deg_i(\mathcal{M})$ — это количество множеств из \mathcal{M} , содержащих фиксированный элемент $i \in \mathcal{R}_n$, а

$$\deg(\mathcal{M}) = \max_{i \in \mathcal{R}_n} \deg_i(\mathcal{M}).$$

(Обозначение происходит от английского слова *degree* — ‘степень’.) Тогда выполнена

Теорема 21 (Дж. Бек и Т. Фиала). *Если $\deg(\mathcal{M}) < t$, то*

$$\text{disc}(\mathcal{M}) \leq 2t - 1.$$

Утверждение поразительное, так как никаких условий на количество множеств в \mathcal{M} и пр. оно не предполагает; лишь бы степень совокупности как-то оценивалась (а она ведь всегда чему-нибудь равна!).

6.2. Доказательство теоремы 20

Доказательство. Сперва нам потребуются нетривиальные сведения из линейной алгебры.

Матрицы Адамара. Квадратную матрицу размера $n \times n$ мы назовем *матрицей Адамара*, если все ее элементы суть плюс и минус единицы, а строки ее попарно ортогональны. Априори не ясно даже, существует ли такая матрица, но заведомо понятно, что с тем же успехом можно было потребовать попарную ортогональность ее столбцов (вышло бы эквивалентное определение) и что домножение всех элементов любой строки (любого столбца) матрицы Адамара на -1 сохраняет «адамаровость». Упомянутые факты позволяют считать, что, скажем, все элементы первого столбца и первой строки матрицы Адамара суть единицы. Обозначим такую матрицу H_1 .

Теперь о существовании матриц Адамара. Гипотеза, которая до сих пор не доказана, состоит в том, что эти матрицы существуют при $n = 1$, $n = 2$ и $n = 4k$. Известно, тем не менее, достаточно много. Так, например, установлено существование матриц при $n = 2^k$, $n = p^k + 1$, где p простое, а n делится на 4, при $n = 92, 116, 172$ и при различных других специальных значениях n (см. [13]). В конечном счете множество тех n , для которых матрицы Адамара железно найдутся, «плотно» в том смысле, что для любого $\varepsilon > 0$ между n и $n(1 + \varepsilon)$ есть порядок матрицы Адамара.

Основная лемма. Пусть $n_1 < n_2 < n_3 < \dots$, где n_i — порядок матрицы Адамара. Рассмотрим для каждого $n = n_i$ матрицу H_1 порядка n . Возьмем, кроме того, матрицу J , состоящую из одних единиц,

и положим

$$H^* = \frac{H_1 + J}{2}$$

(H^* — это $(0, 1)$ -матрица). Считая, что $\mathbf{x} = (x_1, \dots, x_n)$ — это вектор в \mathbb{R}^n , определим его норму в метрике l_p как

$$|\mathbf{x}|_p = \sqrt[p]{|x_1|^p + \dots + |x_n|^p}$$

при $p \in [1, \infty)$ и как

$$|\mathbf{x}|_p = \max_i |x_i|$$

при $p = \infty$. Выполнена

Лемма 9. *Для любого вектора \mathbf{x} , координаты которого суть плюс и минус единицы, имеет место оценка*

$$|H^* \mathbf{x}|_\infty \geq \frac{\sqrt{n}}{2}.$$

Доказательство леммы 9. Рассмотрим произвольный вектор

$$\mathbf{x} = (x_1, \dots, x_n)$$

из формулировки леммы. Тогда

$$H_1 \mathbf{x} = x_1 \mathbf{h}_1 + \dots + x_n \mathbf{h}_n,$$

где \mathbf{h}_i — вектор-столбцы матрицы H_1 . Полагая $H_1 \mathbf{x} = (L_1, \dots, L_n)$, имеем

$$L_1^2 + \dots + L_n^2 = |H_1 \mathbf{x}|_2^2 = x_1^2 |\mathbf{h}_1|_2^2 + \dots + x_n^2 |\mathbf{h}_n|_2^2 = n + \dots + n = n^2,$$

поскольку векторы \mathbf{h}_i попарно ортогональны. Значит, некоторое L_i^2 оценивается снизу величиной n , и, стало быть, $|H_1 \mathbf{x}|_\infty \geq \sqrt{n}$.

Хорошо. Пусть $h_{i,j}$, $i, j = 1, \dots, n$, — элементы матрицы H_1 . Тогда

$$L_1 + \dots + L_n = \sum_{i=1}^n \sum_{j=1}^n x_j h_{i,j} = \sum_{j=1}^n x_j \left(\sum_{i=1}^n h_{i,j} \right) = x_1 n = \pm n,$$

поскольку сумма элементов матрицы H_1 , стоящих в первой строке, есть, очевидно, n , а сумма элементов в остальных строках равна нулю (числа единиц и минус единиц в них одинаковы, ведь они должны быть ортогональны первой строке, в которой одни единицы).

Положим, далее,

$$\lambda = x_1 + \dots + x_n,$$

так что $J \mathbf{x} = (\lambda, \dots, \lambda)$. Соответственно,

$$(H_1 + J) \mathbf{x} = (L_1 + \lambda, \dots, L_n + \lambda).$$

Следовательно,

$$|(H_1 + J)\mathbf{x}|_2^2 = \sum_{i=1}^n (L_i + \lambda)^2 = \sum_{i=1}^n (L_i^2 + 2L_i\lambda + \lambda^2) = n^2 \pm 2n\lambda + n\lambda^2.$$

У нас n четно, так как матриц Адамара нечетного порядка, конечно же, не бывает (исключение составляет вырожденный случай $n = 1$). Величина λ , будучи, стало быть, суммой четного числа плюс и минус единиц, есть тогда четное целое. Квадратичная форма $n^2 \pm 2n\lambda + n\lambda^2$ достигает минимума (по λ) при $\lambda = \pm 1$, но, как мы выяснили только что, λ обязано быть четным, и посему реальный минимум находится в $\lambda \in \{-2, 0, 2\}$. Это рассуждение влечет оценку

$$|(H_1 + J)\mathbf{x}|_2^2 \geq n^2.$$

Как это уже было однажды, последнее неравенство означает, что

$$|(H_1 + J)\mathbf{x}|_\infty \geq \sqrt{n},$$

т. е. $|H^*\mathbf{x}| \geq \sqrt{n}/2$, и лемма доказана. \square

Завершение доказательства теоремы. Обозначим строки матрицы H^* через $\mathbf{g}_1, \dots, \mathbf{g}_n$. Это $(0, 1)$ -векторы, которые мы стандартным способом волны превратить в множества M_1, \dots, M_n из \mathcal{R}_n . Возникает совокупность $\mathcal{M} = \{M_1, \dots, M_n\}$, и нам остается понять, что для нее

$$\text{disc}(\mathcal{M}) \geq \frac{\sqrt{n}}{2}.$$

Пусть χ — это произвольная раскраска. Ей однозначно соответствует $(-1, 1)$ -вектор \mathbf{x} , состоящий из «цветов». Нетрудно видеть, что

$$|H^*\mathbf{x}|_\infty = \text{disc}(\chi, \mathcal{M}).$$

В самом деле,

$$H^*\mathbf{x} = ((\mathbf{g}_1, \mathbf{x}), \dots, (\mathbf{g}_n, \mathbf{x})),$$

но

$$(\mathbf{g}_\nu, \mathbf{x}) = \sum_{i \in M_\nu} \chi(i), \quad \nu = 1, \dots, n,$$

и все в порядке. Раскраска χ была выбрана, по сути, наугад, и потому

$$\text{disc}(\mathcal{M}) = \min_{\chi} \text{disc}(\chi, \mathcal{M}) = \min_{\mathbf{x}} |H^*\mathbf{x}|_\infty \geq \frac{\sqrt{n}}{2}$$

ввиду леммы 9. Теорема доказана. \square

Отметим, что из теоремы немедленно следует справедливость неравенства

$$\text{disc}(\mathcal{M}) \geq c\sqrt{n}, \quad c > 0,$$

при любых n . Здесь главное — упомянутая выше плотность порядков матриц Адамара.

Замечание о матрицах Адамара. Как мы поняли, доказывая теорему, строки матрицы H_1 , начиная со второй ($n \geq 2$), должны содержать ровно половину единиц и половину минус единиц. Из этого, в частности, следовала четность порядка адамаровой матрицы. Однако, сверх того, эти строки обязаны быть ортогональны друг другу ($n \geq 3$), т. е. множества единиц в них (и, соответственно, множества минус единиц) не могут пересекаться иначе, нежели по $n/4$ общим элементам. Таким образом, суть гипотезы о существовании матриц Адамара при $n = 4k$ именно в достаточности указанного условия; необходимость же его очевидна. В то же время в терминах совокупностей множеств гипотеза переформулируется крайне симпатично. В самом деле, речь идет фактически о построении совокупности

$$\mathcal{M} = \{M_1, \dots, M_{n-1}\},$$

состоящей из $(n/2)$ -элементных подмножеств в \mathcal{R}_n (этих подмножеств $n-1$) и обладающей свойством: любые два множества в \mathcal{M} имеют в пересечении ровно $n/4$ элементов. Не правда ли, что-то это напоминает? Да, конечно: мы совершенно неожиданно для самих себя пришли к постановке вопроса, обратного к тому, который столь детально обсуждали в начале книги. Там мы хотели, помимо всего прочего, запретить $(n/2)$ -элементным множествам пересекаться по множеству мощности $n/4$. Теперь же мы только такое пересечение им и разрешаем.

6.3. Доказательство теоремы 21

Доказательство. Зафиксируем произвольную совокупность множеств \mathcal{M} , у которой

$$\text{deg}(\mathcal{M}) < t.$$

Для удобства будем считать, что

$$\mathcal{M} = \{M_1, \dots, M_s\} \quad \text{и что } M_i \subset \mathcal{R}_n, \quad i = 1, \dots, s,$$

хотя значения параметров n и s на дальнейшие выкладки никак не повлияют. Наша основная цель — построить раскраску χ , при которой

$$\text{disc}(\chi, \mathcal{M}) \leq 2t - 1.$$

Если мы этой цели достигнем, все будет в порядке. Желая достичь успеха в нашем начинании, мы, естественно, обязаны сделать так, чтобы для каждого $M \in \mathcal{M}$ было выполнено неравенство

$$\text{disc}(\chi, M) \leq 2t - 1.$$

И тут еще полезно заметить, что раскраску можно интерпретировать как вектор $\mathbf{x} = (x_1, \dots, x_n) \in \{-1, 1\}^n$, в терминах которого

$$\text{disc}(\chi, M) = \left| \sum_{i \in M} x_i \right|.$$

В результате наша задача сведется к отысканию такого $(-1, 1)$ -вектора, что для всякого $M \in \mathcal{M}$ последняя сумма не превосходит $2t - 1$.

Осуществлять заявленную программу мы будем в рамках *индуктивного процесса*. Сперва мы положим $x_1 = \dots = x_n = 0$. Нет сомнений, что вектор $\mathbf{x} = (x_1, \dots, x_n)$ вовсе не является искомым. Затем с помощью линейно-алгебраических соображений мы станем преобразовывать начальный вектор. Дабы свести к минимуму громоздкость обозначений, мы всякий раз будем называть новоиспеченный вектор именем его предшественника (т.е. «именем» $\mathbf{x} = (x_1, \dots, x_n)$), хотя, разумеется, он уже не будет состоять из одних нулей. В результате некоторого количества однотипных шагов мы и получим тот \mathbf{x} , который нам нужен. Заметим, что на каждом шаге координаты вектора \mathbf{x} не будут выходить за пределы отрезка $[-1, 1]$: $x_i \in [-1, 1]$, $i = 1, \dots, n$ (это заведомо так на «старте», а после мы просто правильно организуем наш процесс). Для каждого \mathbf{x} и $M \in \mathcal{M}$ назовем величину $\sum_{i \in M} x_i$ *суммой множества M* : это оправдано, поскольку лишь для завершающего \mathbf{x} эта сумма будет (с точностью до знака) равна отклонению; иначе это некоторое промежуточное рабочее число (вообще говоря, даже не целое).

Опишем произвольный (очередной) шаг процесса. Например, шаг, состоящий в переходе от вектора

$$\mathbf{x} = (x_1, \dots, x_n) = (0, \dots, 0)$$

к его потомку. Итак, пусть

$$\mathbf{x} = (x_1, \dots, x_n) \in [-1, 1]^n,$$

причем найдутся $x_i \neq \pm 1$. Соответственно, назовем элемент $i \in \mathcal{R}_n$ *плавающим*, если для него x_i еще не равняется ± 1 ; иначе назовем его *фиксированным*. Понятно, что на первом шаге все элементы в \mathcal{R}_n плавающие, а стремимся мы к тому, чтобы они «поголовно» стали фиксированными. Скажем, что множество $M \in \mathcal{M}$ *активно*, коль

скоро в нем не менее t плавающих элементов; иначе множество *пассивно*. Между прочим, пассивные множества имеются и на первом шаге: это множества, мощность которых $< t$. В конечном итоге все множества сделаются пассивными (да в них и вовсе плавающих элементов не будет). Преобразовывать мы будем только плавающие элементы; как только элемент зафиксирован, мы на него перестаем обращать внимание.

Некоторые плавающие элементы могут не входить ни в какое множество из \mathcal{M} ; в частности, есть, конечно же, плавающие элементы в каждом активном множестве, но есть и плавающие элементы, ни одному активному множеству не принадлежащие. С последними мы поступим просто: если i «плавает», но активного множества, которое бы его содержало, нет, то мы положим $x'_i = 1$ или $x'_i = -1$ наобум, а затем заменим нынешнее x_i на x'_i , сохраняя прежнее «имя» координаты. Разумеется, новые x_i станут тогда фиксированными, и их мы более рассматривать не будем.

Пусть, наконец, i_1, \dots, i_k — плавающие элементы, каждый из которых содержится по крайней мере в одном активном множестве. Обозначим сами активные множества через M_{j_1}, \dots, M_{j_l} .

Утверждение 2. *Выполнено неравенство $k > l$.*

Доказательство утверждения 2. Возьмем сумму

$$\sum_{\nu=1}^l \sum_{i_\mu \in M_{j_\nu}} 1,$$

т. е. мы фактически сперва производим суммирование по всем активным множествам, а затем смотрим, сколько плавающих элементов в каждом из них ($\mu \in \{1, \dots, k\}$). С одной стороны,

$$\sum_{\nu=1}^l \sum_{i_\mu \in M_{j_\nu}} 1 \geq \sum_{\nu=1}^l t = lt$$

ввиду активности M_{j_ν} , $\nu = 1, \dots, l$. С другой стороны, порядки суммирования можно менять местами, и тогда

$$\sum_{\nu=1}^l \sum_{i_\mu \in M_{j_\nu}} 1 = \sum_{\mu=1}^k \sum_{\{\nu: i_\mu \in M_{j_\nu}\}} 1 < \sum_{\mu=1}^k t = kt,$$

поскольку

$$\sum_{\{\nu: i_\mu \in M_{j_\nu}\}} 1 \leq \deg(\mathcal{M}) < t.$$

Таким образом, $lt < kt$, и утверждение доказано. \square

Пусть $\mathbf{x} = (x_1, \dots, x_n)$ — вектор, который мы имеем на данном этапе (мы не забываем, что кое-какие простейшие преобразования мы уже успели совершить). Заметим, что в самом начале процесса сумма каждого активного множества равнялась нулю. Предположим, что в результате всех пертурбаций и для нынешнего \mathbf{x} аналогичные суммы нулевые. Сейчас мы осуществим шаг индукции, так что для нового вектора \mathbf{x} , который в его конце появится, это свойство сохранится. Собственно, это и есть ключевой момент доказательства.

Введем вещественные переменные y_{i_1}, \dots, y_{i_k} , отвечающие (все еще) плавающим элементам i_1, \dots, i_k (т.е. элементам, которые входят в активные множества; остальные уже были зафиксированы ранее). Рассмотрим систему уравнений

$$\begin{cases} \sum_{i \in M_{j_1}} z_i = 0, \\ \dots\dots\dots \\ \sum_{i \in M_{j_l}} z_i = 0, \end{cases}$$

где $z_i = y_i$, если $i = i_\mu$ ($\mu = 1, \dots, k$), и $z_i = x_i$ в противном случае. Таким образом, наша система состоит из l уравнений и зависит от k неизвестных. В силу утверждения 2 эта система недоопределена, т.е. размерность пространства ее решений не меньше одного. Следовательно, у системы есть целая прямая решений. К тому же надлежащие координаты вектора \mathbf{x} ввиду сделанного нами предположения индукции удовлетворяют системе (суммы активных множеств были нулевыми). Значит, упомянутая прямая решений может быть параметризована в виде

$$x'_{i_\mu} = x_{i_\mu} + \lambda u_{i_\mu}, \quad \mu = 1, \dots, k.$$

(Здесь λ пробегает всю прямую, а u_{i_μ} — некоторая константа.)

Возьмем минимальное λ , при котором хотя бы одна величина x'_{i_μ} равна плюс или минус единице. Поскольку все x_i у нас принадлежали отрезку $[-1, 1]$, это возможно сделать. Заменим x_{i_1}, \dots, x_{i_k} на $x'_{i_1}, \dots, x'_{i_k}$. При этом число плавающих элементов заведомо уменьшится, новые x_i не выйдут за пределы отрезка $[-1, 1]$, а суммы активных множеств (если таковые еще есть в наличии), как мы и обещали, продолжают быть равными нулю. Шаг индукции (процесса) завершен.

За конечное число шагов мы, очевидно, избавимся от всех плавающих элементов и построим некоторый вектор $\mathbf{x} \in \{-1, 1\}^n$ (некоторую раскраску χ). Остается понять, что будет с отклонением. В действительности, мы сначала освободимся от активных множеств и лишь

потом уничтожим плавающие элементы (утверждение 2), фиксируя их на решающем этапе (когда все множества пассивны) произвольным образом. До того, как множество становится пассивным (включая момент «деактивации»), его сумма равна нулю. Но затем не более $t-1$ элементов в нем претерпит изменения (см. определение активного множества). Измениться же элемент может, как максимум, на двойку (оставаясь все время на отрезке $[-1, 1]$). Это значит, что в самом конце процесса модуль суммы любого множества (равный отклонению) не превосходит в аккурат $2t-1$. Теорема доказана. \square

Гипотеза 5. Теорему 21 можно значительно усилить, а именно, верна, по-видимому, оценка

$$\text{disc}(\mathcal{M}) \leq c\sqrt{t}, \quad c > 0.$$

Гипотеза нетривиальна, и похоже, что для ее подтверждения потребуется сочетание линейно-алгебраического и вероятностного методов.

6.4. Дополнение 1. «Свойство В» Эрдёша

Сейчас мы скажем буквально несколько слов о задаче, которую нельзя не упомянуть в связи с проблемами отклонения. Она отнюдь не линейно-алгебраическая, но просто без нее картина не будет полной.

Вот какой возникает вопрос. Пусть даны величины $s, k \in \mathbb{N}$. Верно ли, что для любой совокупности k -элементных множеств

$$\mathcal{M} = \{M_1, \dots, M_s\}$$

существует раскраска множества

$$\mathcal{R}_n = M_1 \cup \dots \cup M_s$$

в два цвета, при которой каждое $M_i \in \mathcal{M}$ неодноцветно? Иными словами, речь не идет, как прежде, о «качестве» раскраски: дай Бог, чтобы при ней хотя бы полностью синих или полностью красных множеств не было! К сожалению, мы знаем (см. начало главы), что ответ на вопрос отрицательный. Разумеется, об этом знал и Поль Эрдёш, который в начале 60-х годов прошлого века предложил следующую «правильную» постановку проблемы. Во-первых, он ввел так называемое «свойство В» (В латинское) совокупности. Он сказал, что совокупность обладает *свойством В*, если для нее упомянутая выше раскраска все-таки существует. Во-вторых же (и это главное), он рассмотрел величину $m(k)$, равную максимуму среди всех s , при которых

любая совокупность мощности s , состоящая из k -элементных множеств, обладает свойством В. Сам Эрдёш в 1961—1962 годах доказал утверждения, которые мы объединим в теорему 22.

Теорема 22 (П. Эрдёш). *Имеют место оценки*

$$2^{k-1} \leq m(k) \leq (1 + o(1)) \frac{e \ln 2}{4} k^2 2^k.$$

Теорема доказывается вероятностными средствами. Видно, что зазор между нижней и верхней оценками невелик. Однако и его стоит устранять. Этим занимался Дж. Бек, который в 1978 году установил неравенство

$$m(k) \geq c \left(\frac{k}{\log k} \right)^{1/3} 2^k, \quad c > 0$$

(тоже вероятность), и только в 2000 году оценку Бека уточнили:

$$m(k) \geq c' \left(\frac{k}{\log k} \right)^{1/2} 2^k, \quad c' > 0.$$

Последний результат принадлежит Дж. Радхакришнану и А. Сринивасану. Он исключительно красив и алгоритмичен, но, к несчастью, снова не алгебраичен. Хотелось бы отослать читателя к первоисточнику, да он крайне малодоступен (как в плане наличия журнала в библиотеках, так и в плане прозрачности изложения); единственная же книга (английская), где он понятно изложен, до сих пор толком не издана и тем более на русский не переведена. Придется подождать.

Любопытно, что верхнюю оценку Эрдёша никому улучшить не удастся, а вообще, никто даже не решается высказать гипотезу о том, каким должен быть правильный порядок роста величины $m(k)$.

Сейчас очень многие занимаются различными нетривиальными обобщениями свойства В. Наибольших успехов в этом плане достиг, пожалуй, Д. А. Шабанов. Он установил, в частности, весьма хорошие оценки на величину $m_t(k)$, которая отличается от классической тем, что предполагает выполнение нового свойства V_t . В рамках этого свойства всякое множество обязано содержать не менее t элементов каждого из цветов ($m(k) = m_1(k)$). Если $t \sim k/2$, то речь опять идет об отклонении, и это особенно интересно.

6.5. Дополнение 2.

Матрицы Адамара и проблема Борсука

В роли одного из основных линейно-алгебраических инструментов этой главы выступили матрицы Адамара. Сейчас мы расскажем

еще об одном их любопытном применении, и речь пойдет о проблеме Борсука, с которой мы уже имели возможность как следует познакомиться в предшествующей части нашей книги.

Вероятно, читатель помнит, что гипотеза Борсука, вокруг которой и строилась соответствующая проблема, была опровергнута в первую очередь за счет рассмотрения совокупностей векторов, имеющих координаты 0 и 1. Правда, самые хорошие нижние оценки величины $f(n)$ потребовали добавления минус единиц в качестве потенциальных компонент упомянутых векторов, но это несущественно. Главное, что некоторые весьма простые конструкции уже давали крайне неожиданные контрпримеры. Возникает абсолютно естественный вопрос: а всякие ли конструкции подобного типа, действительно, способны свидетельствовать о том, что $f(n) > n+1$? И проще всего, конечно же, обсуждать этот вопрос в случае $(0, 1)$ -векторов. Только его еще нужно разумным образом формализовать. Скажем, понятно, что векторы с одной единицей и $n-1$ нулем заведомо к опровержению гипотезы Борсука не приводят. А как бы поставить в задачу максимально общем виде?

Из определенных технических соображений нам легче будет в дальнейшем иметь дело не с $(0, 1)$ -, а с $(-1, 1)$ -векторами: ясно ведь, что одна ситуация без труда преобразуется в другую. Возьмем произвольную совокупность Σ в \mathbb{R}^n , состоящую, стало быть, из векторов, у которых все координаты суть плюс и минус единицы. Очевидно, ее диаметр не превосходит величины $2\sqrt{n}$. Давайте считать, что он равен какому-то числу

$$d \in \{0, 2, \sqrt{8}, \dots, \sqrt{4n}\}$$

(квадрат расстояния между $(-1, 1)$ -векторами всегда кратен четырем). Таким образом, у нас есть два фиксированных параметра — размерность n и диаметр совокупности d . Пусть $f(n, d)$ — это *минимальное число частей меньшего диаметра, на которые может быть разбита произвольная совокупность Σ с параметрами n и d* . Более подробно: мы представляем каждую совокупность Σ в виде

$$\Sigma = \Sigma_1 \sqcup \dots \sqcup \Sigma_f, \quad \text{diam } \Sigma_i < \text{diam } \Sigma \text{ при всех } i \in \{1, \dots, f\},$$

а затем находим $f(\Sigma) = \min f$ и $f(n, d) = \max f(\Sigma)$ (ср. определение $f(n)$ в разделе 4.1).

Разумеется, $f(n) \geq f(n, d)$ для любого d , и вопрос в том, когда можно гарантировать, что $f(n, d) \leq n+1$. Иными словами, нас интересует, при каких d мы не сумеем построить контрпример на основе « (n, d) -параметрических» Σ .

Итак, вопрос поставлен. Заметим, во-первых, что в нем мы слегка отступили от наших прежних канонов. А именно, мы не стали фиксировать количество единиц в каждом векторе совокупности, порождающей величину $f(n, d)$; это-то количество вольно быть любым. Отныне нас беспокоит, помимо размерности, исключительно значение диаметра. Что, впрочем, и неудивительно. Заметим, далее, что результатов про $f(n, d)$ крайне много, но окончательным пока не пахнет. Один из таких (нетривиальных, но частных) фактов мы и обоснуем вскоре посредством матриц Адамара. Кое-какие близкие утверждения мы сформулируем после этого, а кое-что отправится в раздел задач.

Для удобства мы перейдем на язык теории графов. Пусть $G = (V, E)$ — граф. Назовем его *хроматическим числом* минимальное количество цветов $\chi(G)$, в которые можно так раскрасить множество V , чтобы вершины, соединенные ребром из E , оказались разноцветными. Видно, что $\chi(G)$ очень похоже на $\chi(\mathbb{R}^n)$ и пр. Это не случайно (см. [6]), но нам это не важно.

Рассмотрим граф

$$\mathcal{H}(n, d) = (\mathcal{V}(n), \mathcal{E}(n, d)),$$

у которого множество вершин состоит из всевозможных $(-1, 1)$ -векторов, а ребрами соединены те и только те вершины, расстояние между которыми равно d . Такой граф обычно называют *графом расстояний*, но иногда присваивают ему имя Хэмминга. Последнее обстоятельство связано с тем, что этот граф имеет непосредственное отношение к теории кодирования и, в частности, к неким *кодам Хэмминга*.

Фиксируем произвольную совокупность Σ с параметрами n и d . Ей также можно сопоставить граф $G = (V, E)$, у которого $V = \Sigma$, а ребра соединяют диаметрально противоположные вершины. Этот граф называется *графом диаметров*. Замечательно то, что, во-первых, $f(\Sigma) = \chi(G)$ (убедитесь в этом) и, во-вторых, G является подграфом в $\mathcal{H}(n, d)$. Отсюда следует, что, желая оценить сверху $f(n, d)$, мы можем поценивать для начала $\chi(\mathcal{H}(n, d))$: ясно ведь, что, какова бы ни была совокупность Σ , $\chi(G) \leq \chi(\mathcal{H}(n, d))$, а стало быть, то же неравенство верно и для $f(n, d)$. Справедлива

Теорема 23 (Н. Алон). Пусть $l \leq n$ таково, что существует матрица Адамара H_l порядка l . Пусть, кроме того,

$$d > 2\sqrt{n - \sqrt{l}}.$$

Тогда

$$f(n, d) \leq \chi(\mathcal{H}(n, d)) \leq 2l.$$

Прежде чем доказывать теорему, поясним ее смысл. В самом деле, если $l \approx n/2$, то матрица Адамара найдется и мы достигаем цели: $f(n, d) \leq n+1$. При этом d может быть любым таким, что квадрат его больше $4n - c\sqrt{n}$. Это значит, что, дабы опровергнуть гипотезу Борсука, нам нет смысла брать совокупности, имеющие слишком большой диаметр (близкий к максимально допустимому). Для сравнения скажем, что все контрпримеры фактически используют совокупности с $d^2 \sim \lambda n$, $\lambda < 4$.

Доказательство теоремы 23. Рассмотрим $\mathcal{H}(n, d) = (\mathcal{V}(n), \mathcal{E}(n, d))$ и матрицу Адамара H_l , $l \leq n$, которая по условию существует. На сей раз вид этой матрицы нам безразличен, и для нас важно лишь то, что, скажем, ее столбцы $\mathbf{v}_1, \dots, \mathbf{v}_l$ образуют (по определению) ортогональный базис в пространстве \mathbb{R}^l .

Возьмем множество $\{\pm \mathbf{v}_1, \dots, \pm \mathbf{v}_l\}$. Его мощность равна $2l$. Занумеруем его элементы в каком-нибудь порядке:

$$\{\pm \mathbf{v}_1, \dots, \pm \mathbf{v}_l\} = \{\mathbf{u}_1, \dots, \mathbf{u}_{2l}\}.$$

Например, мы вольны считать, что

$$\mathbf{u}_{2i-1} = \mathbf{v}_i, \quad \mathbf{u}_{2i} = -\mathbf{v}_i, \quad i = 1, \dots, l.$$

Присвоим каждому \mathbf{u}_i свой «цвет» (всего, таким образом, получится $2l$ цветов). Зафиксируем произвольный вектор $\mathbf{x} \in \mathcal{V}(n)$. Его размерность n , и мы «укоротим» его, сохраняя в новом векторе \mathbf{x}' только первые l его координат: если $\mathbf{x} = (x_1, \dots, x_n)$, то $\mathbf{x}' = (x_1, \dots, x_l)$. Понятно, что в множестве

$$\{t: t = |\mathbf{x}' - \mathbf{u}_i|, \quad i = 1, \dots, 2l\}$$

есть минимальные элементы (множество конечно). Предположим, что они отвечают каким-то $\mathbf{u}_a, \mathbf{u}_b, \dots$. Как мы помним, $\mathbf{u}_a, \mathbf{u}_b, \dots$ имеют некоторые цвета. Раскрасим \mathbf{x}' , а вслед за ним и \mathbf{x} , в любой (для определенности первый по величине индекса a, b, \dots) из них. В результате всё $\mathcal{V}(n)$ окажется раскрашенным в $2l$ цветов по принципу: какой вектор \mathbf{u}_i к «обрубку» данной вершины ближе, такой и цвет у этой вершины (если же ближайших векторов несколько, то цвет выбирается «хронологически» минимальным).

Чтобы доказать теорему, необходимо удостовериться, что одноцветные вершины из $\mathcal{V}(n)$ не могут быть соединены ребром из $\mathcal{E}(n, d)$. Если нам это удастся, то мы и впрямь увидим, что $\chi(\mathcal{H}(n, d)) \leq 2l$.

Итак, мы хотим убедиться в том, что, коль скоро $\mathbf{x}, \mathbf{y} \in \mathcal{V}(n)$ покрашены одинаково, расстояние между ними не превосходит

$$r = 2\sqrt{n - \sqrt{l}}$$

(мы не забываем, что по условию теоремы $d > r$, а ребра в аккурат расстоянием d и порождены).

Мы скажем, что векторы

$$\mathbf{x} = (x_1, \dots, x_k), \quad \mathbf{y} = (y_1, \dots, y_k),$$

лежащие в пространстве некоторой размерности k , имеют t общих координат, если найдутся различные i_1, \dots, i_t , для которых $x_{i_1} = y_{i_1}, \dots, x_{i_t} = y_{i_t}$ (остальные же компоненты разнятся).

Допустим, мы доказали, что у одноцветных \mathbf{x}' , \mathbf{y}' не менее \sqrt{l} общих координат. Тогда у соответствующих одноцветных $\mathbf{x}, \mathbf{y} \in \mathcal{V}(n)$ тем более $t \geq \sqrt{l}$ координат с номерами i_1, \dots, i_t совпадают. Это значит, что

$$\begin{aligned} |\mathbf{x} - \mathbf{y}| &= \sqrt{|x_{i_1} - y_{i_1}|^2 + \dots + |x_{i_t} - y_{i_t}|^2 + \dots} = \\ &= \sqrt{|x_{j_1} - y_{j_1}|^2 + \dots + |x_{j_{n-t}} - y_{j_{n-t}}|^2}, \end{aligned}$$

где

$$\{j_1, \dots, j_{n-t}\} = \{1, \dots, n\} \setminus \{i_1, \dots, i_t\}.$$

Однако $|x_{j_\nu} - y_{j_\nu}|^2 = 4$, $\nu = 1, \dots, n-t$, и $n-t \leq n - \sqrt{l}$, т.е.

$$|\mathbf{x} - \mathbf{y}| \leq \sqrt{4(n - \sqrt{l})} = r,$$

и «по модулю» исходного допущения все в порядке.

Докажем это допущение. Возьмем \mathbf{x}' , \mathbf{y}' , цвет которых отвечает одному и тому же

$$\mathbf{u}' \in \{\mathbf{u}_1, \dots, \mathbf{u}_{2l}\}.$$

Убедимся в том, что \mathbf{u}' имеет как с \mathbf{x}' , так и с \mathbf{y}' не менее $(1/2)(l + \sqrt{l})$ общих координат. Ясно, что, как только мы это сделаем, допущение будет обосновано (см. рис. 16).

Достаточно работать, скажем, с \mathbf{u}' и \mathbf{x}' . Разложим \mathbf{x}' по ортогональному базису $\mathbf{v}_1, \dots, \mathbf{v}_l$:

$$\mathbf{x}' = \sum_{i=1}^l \lambda_i \mathbf{v}_i.$$

Тогда

$$l = |(\mathbf{x}', \mathbf{x}')| \leq \sum_{i=1}^l |\lambda_i| |(\mathbf{v}_i, \mathbf{x}')| \leq \sum_{i=1}^l |\lambda_i| \sqrt{|\mathbf{v}_i|_2 |\mathbf{x}'|_2}.$$

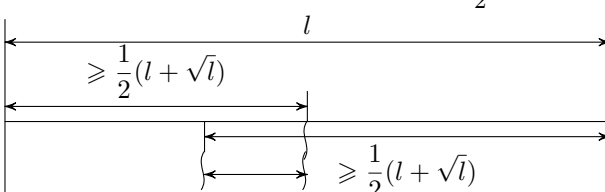
$$\begin{aligned}
 x' &= \left(\begin{array}{cccc|cccc} 1 & 1 & \dots & 1 & -1 & -1 & \dots & -1 \\ 1 & 1 & \dots & 1 & -1 & -1 & \dots & -1 \end{array} \middle| \begin{array}{cccc} 1 & \dots & 1 & -1 & \dots & -1 \end{array} \right) \\
 u' &= \left(\begin{array}{cccc|cccc} 1 & 1 & \dots & 1 & -1 & -1 & \dots & -1 \\ \leftarrow \hline \hline \rightarrow \end{array} \middle| \begin{array}{cccc} -1 & \dots & -1 & 1 & \dots & 1 \end{array} \right) \\
 &\geq \frac{1}{2}(l + \sqrt{l}) \\
 y' &= \left(\begin{array}{cccc|cccc} -1 & -1 & \dots & -1 & 1 & 1 & \dots & 1 \\ -1 & -1 & \dots & -1 & 1 & 1 & \dots & 1 \end{array} \middle| \begin{array}{cccc} -1 & \dots & -1 & 1 & \dots & 1 \end{array} \right) \\
 u' &= \left(\begin{array}{cccc|cccc} 1 & 1 & \dots & 1 & -1 & -1 & \dots & -1 \\ \leftarrow \hline \hline \rightarrow \end{array} \middle| \begin{array}{cccc} -1 & \dots & -1 & 1 & \dots & 1 \end{array} \right) \\
 &\geq \frac{1}{2}(l + \sqrt{l})
 \end{aligned}$$


Рис. 16

(Последняя оценка вытекает из неравенства Коши—Буняковского—Шварца.) Следовательно,

$$l \leq \sum_{i=1}^l |\lambda_i| \sqrt{l},$$

т. е.

$$\sum_{i=1}^l |\lambda_i| \geq \sqrt{l},$$

и, стало быть, по принципу Дирихле есть такое i , что

$$|\lambda_i| \geq \frac{1}{\sqrt{l}}.$$

В то же время

$$\lambda_i = \frac{(\mathbf{x}', \mathbf{v}_i)}{(\mathbf{v}_i, \mathbf{v}_i)} = \frac{(\mathbf{x}', \mathbf{v}_i)}{l}.$$

(Как раз здесь используется ортогональность и, соответственно, адямаровость.) Значит, либо с $\mathbf{u} = \mathbf{v}_i$, либо с $\mathbf{u} = -\mathbf{v}_i$ мы имеем

$$\frac{(\mathbf{x}', \mathbf{u})}{l} = |\lambda_i| \geq \frac{1}{\sqrt{l}}.$$

Иными словами, для данного

$$\mathbf{u} \in \{\mathbf{u}_1, \dots, \mathbf{u}_{2l}\}$$

выполнена оценка $(\mathbf{x}', \mathbf{u}) \geq \sqrt{l}$.

Утверждение 3. Векторы \mathbf{x}' и \mathbf{u} имеют

$$t \geq \frac{1}{2}(l + \sqrt{l})$$

общих координат.

Доказательство утверждения 3. Предположим противное. Тогда

$$(\mathbf{x}', \mathbf{u}) = t - (l - t) = 2t - l < \sqrt{l}.$$

Противоречие, и утверждение у нас в кармане. \square

Утверждение показывает, в частности, что вектор \mathbf{u} расположен весьма близко к вектору \mathbf{x}' . Но вектор \mathbf{u}' лежит заведомо не дальше. Таким образом, опять-таки ввиду утверждения, общих координат у \mathbf{x}' и \mathbf{u}' по крайней мере $(1/2)(l + \sqrt{l})$. Теорема 23 доказана. \square

Мы поняли, что если диаметр совокупности $(0, 1)$ -векторов велик (асимптотически равен своему максимально возможному значению), то такая совокупность удовлетворяет гипотезе Борсука. А что если этот диаметр, напротив, пренебрежимо мал? Й. Петерсен показал в своей дипломной работе, что при достаточно больших n всякая совокупность n -мерных $(0, 1)$ -векторов, имеющая диаметр 2, разбивается на $n + 1$ часть меньшего диаметра. Дж. Мак-Кэммонд усилил этот результат: из его оценок следует, что существует такое $c > 0$, при котором, едва лишь d берется меньшим величины $c \sqrt[n]{\log n}$, гипотеза Борсука для « $(0, 1)$ -совокупностей» размерности n и диаметра d оказывается верной ($n > n_0(d)$).

Задачи

1. Попробуйте найти значения или получить какие-нибудь оценки величин $m(1), m(2), \dots, m(10)$.
2. Пусть даны две матрицы — матрица $A = (a_{i,j})$ размера $m \times m$ и матрица $B = (b_{r,s})$ размера $n \times n$. Назовем их *прямым произведением* матрицу C , имеющую размер $mn \times mn$ и вид

$$C = \begin{pmatrix} a_{1,1}B & \dots & a_{1,m}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \dots & a_{m,m}B \end{pmatrix}.$$

Докажите, что если A и B — матрицы Адамара, то их прямое произведение также адамарово.

3. Пусть $\mathbf{v}_1, \dots, \mathbf{v}_s \in \mathbb{R}^n$, а числа $x_1, \dots, x_s \in [-1, 1]$ таковы, что $\sum_{i=1}^s x_i \mathbf{v}_i = 0$. Предположим, что, более того,

$$|\{i: x_i \notin \{-1, 1\}\}| \leq n.$$

Иными словами, мы считаем, что, когда s велико, «почти все» x_i суть плюс и минус единицы. Разумеется, при $s \leq n$ это свойство выполняется с очевидностью (достаточно положить $x_i = 0$, $i = 1, \dots, s$), а вот в случае $s > n$ мы пока лишь верим, что такое возможно.

Пусть $\mathbf{v}_{s+1} \in \mathbb{R}^n$. Используя идеи Бека—Фиалы, докажите, что существуют $x'_1, \dots, x'_s, x'_{s+1}$, для которых

- $\sum_{i=1}^{s+1} x'_i \mathbf{v}_i = 0$;
- все x'_i лежат на отрезке $[-1, 1]$;
- $|\{i: x'_i \notin \{-1, 1\}\}| \leq n$;
- $x'_i = x_i$ для всех $x_i \in \{-1, 1\}$.

Таким образом, вы осуществите индукцию. С ее помощью вы сможете обосновать теорему И. Барани—В. Гринберга: *пусть $p \in [1, \infty)$, а $\mathbf{v}_1, \dots, \mathbf{v}_s$ — произвольные векторы в пространстве, обладающие свойством $|\mathbf{v}_i|_p \leq 1$, $i = 1, \dots, s$; тогда найдутся такие числа $x_1, \dots, x_s \in \{-1, 1\}$, что*

$$\left| \sum_{i=1}^t x_i \mathbf{v}_i \right|_p \leq 2n \quad \text{для любого } t \in \{1, \dots, s\}.$$

4. Будем раскрашивать элементы множества \mathcal{R}_n не в два, а в три цвета — скажем, красный, желтый и зеленый. Коль скоро дана некоторая совокупность $\mathcal{M} = \{M_1, \dots, M_s\}$ подмножеств в \mathcal{R}_n и фиксирована какая-нибудь трехцветная раскраска χ , обозначим через $\chi_{\text{кж}}(M_i)$ ($i \in \{1, \dots, s\}$) модуль разности между количествами красных и желтых элементов в $M_i \in \mathcal{M}$. Аналогично введем величины $\chi_{\text{кз}}(M_i)$ и $\chi_{\text{жз}}(M_i)$. Назовем *экстремальным отклонением раскраски χ на множестве $M \in \mathcal{M}$* выражение

$$\text{disc}_\infty(\chi, M) = \max\{\chi_{\text{кж}}(M), \chi_{\text{кз}}(M), \chi_{\text{жз}}(M)\}.$$

Сообразно этому определим $\text{disc}_\infty(\chi, \mathcal{M})$, $\text{disc}_\infty(\mathcal{M})$ и $\max \text{disc}_\infty$. Найдите какие-нибудь аналоги теорем 20, 21 для последних величин. Сделайте то же самое для похожих величин $\text{disc}_p(\chi, M)$, $\text{disc}_p(\mathcal{M})$ и $\max \text{disc}_p$, полагая

$$\text{disc}_p(\chi, M) = |(\chi_{\text{кж}}(M), \chi_{\text{кз}}(M), \chi_{\text{жз}}(M))|_p$$

при $p \in [1, \infty)$ (*отклонение в метрике l_p*).

5. Докажите неравенство

$$\chi(\mathcal{H}(n, d)) \leq 2^{n-d^2/4+1}.$$

6. Докажите, что если $d^2/4$ нечетно, то $\chi(\mathcal{H}(n, d)) \leq 2$.

7. Докажите, что $\max_d f(n, d) \leq n + 1$, коль скоро $n \leq 6$. Попытайтесь улучшить этот результат, продолжая его на размерности $n > 6$.

8. Попробуйте сформулировать и доказать какой-нибудь нетривиальный аналог теоремы 23 для $(-1, 0, 1)$ -векторов. Что можно здесь сделать похожего на задачи 5–7?

7 || Теорема Эрдёша—Гинзбурга—Зива и ее окрестности

7.1. Классический результат

В 1961 году П. Эрдёш, А. Гинзбург и А. Зив доказали следующую замечательную теорему.

Теорема 24 (П. Эрдёш, А. Гинзбург, А. Зив). Пусть $n \geq 1$ — произвольное натуральное число, а последовательность a_1, \dots, a_{2n-1} состоит из каких-либо целых (не обязательно различных) чисел. Тогда найдется такое

$$I \subset \{1, \dots, 2n - 1\},$$

что

$$|I| = n \quad \text{и} \quad \sum_{i \in I} a_i \equiv 0 \pmod{n}.$$

Теорема утверждает, что в любом множестве из не менее чем $2n - 1$ целых чисел отыщется подмножество мощности n , сумма элементов которого делится на n . Это красивое наблюдение в определенном смысле можно отнести к теории Рамсея (см. главу 5), но мы решили обсудить его отдельно. Сама теорема 24 доказывается достаточно просто, и мы могли бы сформулировать ее даже в качестве упражнения. Однако в таком случае мы бы упустили шанс продемонстрировать суть некоторого подхода, нетривиальные вариации на тему которого нам понадобятся в дальнейшем.

К настоящему времени результат Эрдёша—Гинзбурга—Зива сделался столь классическим и «кормится» вокруг него так много народу, что различных его доказательств известно немало. Мы же приведем сейчас рассуждение Н. Циммермана, которое опирается на соображения, весьма часто встречавшиеся нам на страницах этой книги, — соображения линейной алгебры. Более того, в конечном счете мы придем к аналогу изученной нами полиномиальной техники, и это особенно любопытно.

Доказательство теоремы 24. Рассмотрим случай $n = p$, где p — простое. Пусть

$$J = \{1, \dots, 2p - 1\}.$$

Положим

$$S = \sum_{I \subset J, |I|=p} \left(\sum_{i \in I} a_i \right)^{p-1}.$$

Если мы раскроем скобки в определении S , то мы получим линейную комбинацию мономов вида

$$a_1^{k_1} \cdot \dots \cdot a_{2p-1}^{k_{2p-1}},$$

где $k_i \geq 0$, $i \in J$, и

$$\sum_{i \in J} k_i = p - 1.$$

Понятно, в частности, что количество j различных сомножителей в каждом из таких мономов не превосходит $p - 1$ (очень знакомая технология!). Заметим теперь, что те и только те переменные внешнего суммирования (p -элементные подмножества в J) влияют на коэффициент данного монома, которые содержат все индексы i , отвечающие сомножителям a_i в мономе. Множеств $I \subset J$ такого типа, очевидно, в точности C_{2p-1-j}^{p-j} штук. Нетрудно проверить, что последняя величина делится на p . С другой стороны, ясно, что каждое из упомянутых I дает один и тот же вклад в обсуждаемый коэффициент, и, стало быть, сам этот коэффициент сравним с нулем по модулю p . И так для любого монома. Значит, $S \equiv 0 \pmod{p}$.

Предположим, что утверждение теоремы неверно, т. е. не существует подмножества I в J , которое имело бы мощность p и давало сравнение $\sum_{i \in I} a_i \equiv 0 \pmod{p}$. Тогда для каждого $I \subset J$ мы имеем в силу малой теоремы Ферма (см. [2]) соотношение

$$\left(\sum_{i \in I} a_i \right)^{p-1} \equiv 1 \pmod{p}.$$

Однако таких $I \subset J$ ровно C_{2p-1}^{p-1} штук. Следовательно,

$$S \equiv C_{2p-1}^{p-1} \equiv 1 \pmod{p}.$$

Возникает противоречие, и теорема для простого n доказана. \square

Основной смысл результата мы прояснили, а перенести его на произвольные значения n читатель наверняка сумеет самостоятельно (см. задачи).

Практически очевидно, что теорему, по существу, улучшить нельзя. Иными словами, можно придумать такое множество a_1, \dots, a_{2n-2} , что в нем никакое n -элементное подмножество не суммируется в ноль

по модулю n . Достаточно рассмотреть набор из $n - 1$ нуля и $n - 1$ единицы.

Обозначим через $f(n, d)$ минимальное натуральное число с таким свойством: среди любых $f(n, d)$ (не обязательно различных) векторов в \mathbb{R}^d , имеющих неотрицательные целые координаты (то есть векторов в \mathbb{N}^d), найдется n таких, что сумма их координат с каждым фиксированным номером делится на n . Иначе говоря, $f(n, 1) = 2n - 1$, и мы имеем дело с обобщением науки Эрдеша—Гинзбурга—Зива на d -мерный случай. Сразу же легко заметить, что $f(n, d) \geq 1 + 2^d(n - 1)$. Действительно, нужно просто взять последовательность из всех 2^d $(0, 1)$ -векторов, каждый из которых берется с кратностью $n - 1$. По теореме 24 последняя оценка достигается, коль скоро $d = 1$. А. Кемниц высказал гипотезу, что та же оценка точна и при $d = 2$, т. е. что $f(n, 2) = 4n - 3$. Гипотезу долгое время никому не удавалось доказать. Для нескольких конкретных значений n ее справедливость установили сам Кемниц и Х. Харборт. Затем Н. Алон и М. Дубинер в 1993 году показали, что $f(n, 2) \leq 6n - 5$. Этот результат был улучшен до $f(n, 2) \leq 4n - 2$ Л. Роньяи в 2000 году. Таким образом, до гипотезы оставалось совсем чуть-чуть, и рубеж был преодолен: буквально полгода назад Х. Райхер получил неравенство $f(n, 2) \leq 4n - 3$.

В следующих разделах мы докажем теоремы Роньяи и Райхера с помощью линейно-алгебраического метода. И сперва нам потребуются пара чисто алгебраических фактов.

7.2. Вспомогательные факты

Теорема 25 (Э. Варнинг). Пусть F_q — это поле из $q = p^r$ элементов (см. [5]). Здесь p — простое, а r — натуральное. Предположим, что многочлен f из $F_q[x_1, \dots, x_n]$ имеет степень меньше n . Тогда число решений уравнения $f(x_1, \dots, x_n) = 0$ в пространстве $F_q^n = F_q \times \dots \times F_q$ делится на p .

Доказательство теоремы 25. Положим

$$g(x_1, \dots, x_n) = 1 - (f(x_1, \dots, x_n))^{q-1}.$$

Ввиду условия теоремы степень g строго меньше, чем $n(q - 1)$. Понятно, что, коль скоро $(\alpha_1, \dots, \alpha_n) \in F_q^n$,

$$g(\alpha_1, \dots, \alpha_n) = 1, \quad \text{если } f(\alpha_1, \dots, \alpha_n) = 0,$$

и

$$g(\alpha_1, \dots, \alpha_n) = 0, \quad \text{если } f(\alpha_1, \dots, \alpha_n) \neq 0.$$

Отсюда следует, что число решений уравнения $f(x_1, \dots, x_n) = 0$ в F_q^n есть $\sum g(\alpha_1, \dots, \alpha_n)$, где суммирование распространяется на все векторы $(\alpha_1, \dots, \alpha_n) \in F_q^n$. Таким образом, нам осталось показать, что

$$\sum g(\alpha_1, \dots, \alpha_n) = 0.$$

Раскроем скобки в определении g и рассмотрим произвольный моном вида $Cx_1^{i_1} \dots x_n^{i_n}$. В результате суммирования по векторам из F_q^n получится выражение

$$\sum_{\alpha_1, \dots, \alpha_n \in F_q} \alpha_1^{i_1} \dots \alpha_n^{i_n} = \left(\sum_{\alpha_1 \in F_q} \alpha_1^{i_1} \right) \dots \left(\sum_{\alpha_n \in F_q} \alpha_n^{i_n} \right).$$

Если некоторое i_ν равно нулю, то соответствующая сумма есть q , а это ноль в F_q , и все в порядке. Иначе пользуемся тем, что какое-то i_ν меньше $q-1$ за счет ограничения, наложенного на степень многочлена в формулировке теоремы. В этом случае найдется такое $a \in F_q^*$, что $a^{i_\nu} \neq 1$. Поскольку умножение на a дает перестановку элементов F_q , имеем

$$\sum_{\alpha_\nu \in F_q} \alpha_\nu^{i_\nu} = \sum_{\alpha_\nu \in F_q} a^{i_\nu} \alpha_\nu^{i_\nu}.$$

Но $a^{i_\nu} \neq 1$, и, значит, $\sum_{\alpha_\nu \in F_q} \alpha_\nu^{i_\nu} = 0$. Итак, в любом случае

$$\left(\sum_{\alpha_1 \in F_q} \alpha_1^{i_1} \right) \dots \left(\sum_{\alpha_n \in F_q} \alpha_n^{i_n} \right) = 0.$$

Наше рассуждение верно для каждого монома, так что окончательно получаем $\sum g(\alpha_1, \dots, \alpha_n) = 0$, и теорема доказана. \square

Теорема 26 (К. Шевалле). Пусть $f \in F_q[x_1, \dots, x_n]$ — полином, имеющий степень меньше n . Предположим,

$$f(0, 0, \dots, 0) = 0.$$

Тогда существует такой вектор

$$(\alpha_1, \dots, \alpha_n) \in F_q^n \setminus \{(0, 0, \dots, 0)\},$$

что $f(\alpha_1, \dots, \alpha_n) = 0$.

Доказательство теоремы 26. Поскольку $f(0, 0, \dots, 0) = 0$, одно решение уже есть. Но по теореме 25 число таких решений делится на p , и, значит, оно не меньше $p \geq 2$. Теорема доказана. \square

Заметим, что результат последней теоремы легко переносится на случай, когда решается система полиномиальных уравнений с n неизвестными: надо только потребовать, чтобы сумма степеней полиномов была меньше n , и промодифицировать определение g в теореме 25. Такое наблюдение нам тоже пригодится.

7.3. Доказательство оценки Роньяи $f(n, 2) \leq 4n - 2$

Доказательство. Мы будем работать с простым $n = p$. Поскольку результат очевиден при $p = 2$ (принцип Дирихле), мы можем считать, что p нечетно. Докажем лемму.

Лемма 10. Пусть p — простое число, а векторы

$$\mathbf{b}_1 = (a_{1,1}, a_{1,2}), \mathbf{b}_2 = (a_{2,1}, a_{2,2}), \dots, \mathbf{b}_{3p} = (a_{3p,1}, a_{3p,2})$$

образуют такую последовательность в F_p^2 , что

$$\mathbf{b}_1 + \mathbf{b}_2 + \dots + \mathbf{b}_{3p} = (0, 0) \in F_p^2.$$

Тогда найдется такое p -элементное подмножество I множества $\{1, \dots, 3p\}$, что

$$\sum_{i \in I} \mathbf{b}_i = (0, 0) \in F_p^2.$$

Доказательство леммы 10. Рассмотрим в F_p следующую систему с $3p - 1$ переменной x_1, \dots, x_{3p-1} :

$$\begin{cases} \sum_{i=1}^{3p-1} a_{i,1} x_i^{p-1} = 0, \\ \sum_{i=1}^{3p-1} a_{i,2} x_i^{p-1} = 0, \\ \sum_{i=1}^{3p-1} x_i^{p-1} = 0. \end{cases}$$

Эта система полиномиальна, и сумма степеней полиномов, которые в нее входят, равна $3(p-1) < 3p-1$. В то же время

$$x_1 = x_2 = \dots = x_{3p-1} = 0$$

— решение системы, и, значит, по замечанию, сделанному нами после доказательства теоремы Шевалле, есть и другое, нетривиальное, решение. Пусть $J \subset \{1, 2, \dots, 3p-1\}$ — это множество индексов, соответствующих ненулевым элементам такого решения.

С учетом малой теоремы Ферма (см. [2]) из первых двух уравнений следует, что

$$\sum_{i \in J} \mathbf{b}_i = (0, 0) \in F_p^2.$$

Аналогично третье уравнение показывает, что $|J| \in \{p, 2p\}$. Если $|J| = p$, то мы можем взять в качестве искомого I само J ; если же

$|J| = 2p$, то с тем же успехом берется $I = \{1, \dots, 3p\} \setminus J$. Лемма доказана. \square

Вернемся к доказательству оценки Роньяи. Положим $m = 4p - 2$, и пусть $\mathbf{v}_1 = (a_1, b_1)$, $\mathbf{v}_2 = (a_2, b_2)$, \dots , $\mathbf{v}_m = (a_m, b_m)$ — последовательность векторов в F_p^2 .

Если мы докажем существование такого подмножества J в множестве $\{1, \dots, m\}$, что $|J| \in \{p, 3p\}$ и $\sum_{j \in J} \mathbf{v}_j = (0, 0)$, то останется применить лемму 10 и все будет в порядке. Предположим, однако, противное.

Рассмотрим p -й элементарный симметрический многочлен от переменных x_1, \dots, x_m

$$\sigma(x_1, x_2, \dots, x_m) = \sum_{I \subset \{1, \dots, m\}, |I|=p} \prod_{i \in I} x_i$$

и следующий многочлен из $F_p[x_1, \dots, x_m]$:

$$P(x_1, \dots, x_m) = \left(\left(\sum_{i=1}^m a_i x_i \right)^{p-1} - 1 \right) \times \left(\left(\sum_{i=1}^m b_i x_i \right)^{p-1} - 1 \right) \times \\ \times \left(\left(\sum_{i=1}^m x_i \right)^{p-1} - 1 \right) \cdot (\sigma(x_1, \dots, x_m) - 2).$$

Если число ненулевых координат в векторе

$$\mathbf{c} = (c_1, \dots, c_m) \in \{0, 1\}^m$$

равно $2p$, то $\sigma(\mathbf{c}) = C_{2p}^p$, и это есть 2 в F_p , так что на векторе $(x_1, \dots, x_m) = \mathbf{c}$ последний сомножитель в F_p обнуляется. Если число единиц в \mathbf{c} есть p или $3p$, то

$$\left(\left(\sum_{i=1}^m a_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m b_i x_i \right)^{p-1} - 1 \right) = 0$$

ввиду нашего изначального предположения. Наконец, третий сомножитель в P исчезает, коль скоро число единиц в \mathbf{c} не делится на p .

Таким образом, P обращается в ноль на всех векторах из $\{0, 1\}^m$, кроме вектора $\mathbf{0} = (0, \dots, 0)$. В свою очередь, $P(\mathbf{0}) = 2$. Заметим, что степень P не превосходит $3(p-1) + p = 4p - 3$.

Теперь мы проводим весьма знакомую процедуру. А именно, мы раскрываем скобки и записываем тем самым наш полином P в виде линейной комбинации мономов. Далее, степени всех переменных в каждом из таких мономов мы заменяем на единицу. Возникает новый полином Q . Понятно, что как функция на $\{0, 1\}^m$ полином Q

ничем не отличается от полинома P . Более того, и его степень не может превысить $4p - 3$. Однако нетрудно показать, что Q обязан иметь вид $2(1 - x_1)(1 - x_2) \dots (1 - x_m)$ (убедитесь в этом самостоятельно). Возникает противоречие, так как последний полином имеет степень $m = 4p - 2 > 4p - 3$. Оценка Роньяи доказана. \square

7.4. Доказательство оценки Райхера $f(n, 2) \leq 4n - 3$

Доказательство. Как и в предыдущем разделе, мы считаем, что $n = p > 2$. Следуя Райхеру, введем для пушей четкости и краткости изложения некоторые обозначения. Итак, p — это всюду далее нечетное простое число. Сравнения по модулю p (являющиеся равенствами в F_p) мы будем записывать, не указывая величину модуля, т. е. выражения $a \equiv b \pmod{p}$ и $a \equiv b$ для нас отныне значат одно и то же. Большими латинскими буквами (например, J, X и т. д.) мы будем кодировать множества целых точек на плоскости. Иными словами, $J \subset \mathbb{N}^2$, $X \subset \mathbb{N}^2$ и пр. Суммы (покоординатные) векторов из подобных множеств мы представим в виде $\sum J$, $\sum X$, ... Наконец, через $(n|X)$ мы обозначим число таких n -элементных подмножеств в X , что сумма векторов в каждом из них есть $(0, 0)$ по модулю p . Как и в разделе 7.3, мы прибегнем к помощи теорем Варнинга, Шевалле и замечания к ним. Даже лемма 10 нам пригодится. Сейчас мы также приведем серию лемм.

Лемма 11. Если $|J| = 3p - 3$, то

$$1 - (p - 1|J) - (p|J) + (2p - 1|J) + (2p|J) \equiv 0.$$

Доказательство леммы 11. Пусть (a_n, b_n) -векторы из J ($1 \leq n \leq 3p - 3$). Применим теорему Варнинга к системе (см. замечание к теореме Шевалле) вида

$$\left\{ \begin{array}{l} \sum_{n=1}^{3p-3} a_n x_n^{p-1} \equiv 0, \\ \sum_{n=1}^{3p-3} b_n x_n^{p-1} \equiv 0, \\ \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1} \equiv 0. \end{array} \right.$$

Теорема и впрямь применима, поскольку количество переменных в системе (их $3p - 2$) на единицу больше суммарной степени многочленов, формирующих систему. Мы знаем, таким образом, что число решений системы делится на p . Осталось показать, что оно же сравнимо с

$$1 - (p - 1|J) - (p|J) + (2p - 1|J) + (2p|J).$$

Разобьем множество решений системы на два класса: к первому отнесем все наборы (x_1, \dots, x_{3p-2}) , у которых $x_{3p-2} \equiv 0$; ко второму — все наборы с $x_{3p-2} \not\equiv 0$. Нетрудно проверить, что первый класс состоит из

$$1 + (p-1)^p(p|J) + (p-1)^{2p}(2p|J) \equiv 1 - (p|J) + (2p|J) \quad (1)$$

решений, а второй класс включает ровно

$$(p-1)^p(p-1|J) + (p-1)^{2p}(2p-1|J) \equiv -(p-1|J) + (2p-1|J) \quad (2)$$

решений. В самом деле, если, скажем, в J есть какое-нибудь подмножество

$$(a_{i_1}, b_{i_1}), \dots, (a_{i_p}, b_{i_p}),$$

суммирующееся в ноль по модулю p , то ему отвечают решения, у которых на позициях с номерами i_1, \dots, i_p стоят произвольные ненулевые вычеты по модулю p , а на остальных позициях расположены нули. Таковых решений, очевидно, $(p-1)^p(p|J)$, и т. д.

Складывая правые части выражений (1), (2), получаем в точности утверждение леммы. \square

Лемма 12а. Если $|J| \in \{3p-2, 3p-1\}$, то

$$1 - (p|J) + (2p|J) \equiv 0.$$

Лемма 12б. Если $|J| \in \{3p-2, 3p-1\}$, то $(p|J) \equiv 0$ влечет $(2p|J) \equiv -1$.

Лемма 12а доказывается точно так же, как и лемма 11 (только в системе не будет x_{3p-2}^{p-1}), а лемма 12б является ее тривиальным следствием.

Лемма 13. Если $|X| = 4p-3$, то

$$-1 + (p|X) - (2p|X) + (3p|X) \equiv 0 \quad (a)$$

и

$$(p-1|X) - (2p-1|X) + (3p-1|X) \equiv 0. \quad (b)$$

Доказательство стандартно, и мы его не приводим.

Лемма 14. Если $|X| = 4p-3$, то

$$3 - 2(p-1|X) - 2(p|X) + (2p-1|X) + (2p|X) \equiv 0.$$

Доказательство леммы 14. Лемма 11 дает сравнение

$$\sum (1 - (p-1|I) - (p|I) + (2p-1|I) + (2p|I)) \equiv 0,$$

где суммирование идет по всем подмножествам I в X , имеющим мощность $3p-3$. Легко видеть, что последняя сумма совпадает с выражением

$$C_{4p-3}^{3p-3} - C_{3p-2}^{2p-2}(p-1|X) - C_{3p-3}^{2p-3}(p|X) + C_{2p-2}^{p-2}(2p-1|X) + C_{2p-3}^{p-3}(2p|X).$$

Действительно, если есть, скажем, $(p - 1)$ -элементное подмножество в X , суммирующееся в ноль, то оно содержится как раз в C_{3p-2}^{2p-2} множествах $I \subset X$. И так далее.

Остается надлежащим образом упростить биномиальные коэффициенты по модулю p , но это уже совсем не сложно, и читатель справится с этим без нашей помощи. Лемма доказана. \square

Лемма 15. Если $|X| = 4p - 3$ и $(p|X) = 0$, то

$$(p - 1|X) \equiv (3p - 1|X).$$

Доказательство леммы 15. Пусть χ — это число разбиений $X = A \sqcup B \sqcup C$, удовлетворяющих условиям

$$\begin{aligned} |A| = p - 1, \quad |B| = p - 2, \quad |C| = 2p; \\ \sum A \equiv (0, 0), \quad \sum B \equiv \sum X, \quad \sum C \equiv (0, 0). \end{aligned}$$

Ясно, что

$$\chi \equiv \sum_A (2p|X \setminus A),$$

где суммирование распространяется на все допустимые множества A . У нас, однако, $(p|X) = 0$, так что тем более $(p|X \setminus A) = 0$, и по лемме 12b $(2p|X \setminus A) \equiv -1$. Значит,

$$\chi \equiv \sum_A -1 \equiv -(p - 1|X).$$

Аналогично

$$\chi \equiv \sum_B (2p|X \setminus B) \equiv \sum_{X \setminus B} -1 \equiv -(3p - 1|X).$$

Лемма доказана. \square

Перейдем непосредственно к результату Райхера. Допустим, $|X| = 4p - 3$ и $(p|X) = 0$. Сложим сравнения, полученные в леммах 13 (пункты (а) и (б)), 14 и 15. Окажется, что $2 - (p|X) + (3p|X) \equiv 0$. Следовательно, либо $(p|X) \not\equiv 0$ (что невозможно), либо $(3p|X) \not\equiv 0$, т.е. $(3p|X) > 0$. Но ввиду леммы 10 последнее условие опять-таки влечет неравенство $(p|X) > 0$, и деваться нам больше некуда. Противоречие, и оценка $f(p, 2) \leq 4p - 3$ доказана. \square

Задачи

1. Докажите теорему Эрдёша—Гинзбурга—Зива и ее двумерные обобщения для непростых n .

2. Докажите, что $f(n, d) \leq 1 + n^d(n - 1)$.
3. (теорема Алона—Фридланда—Калаи). С помощью теоремы Шевалле докажите, что если к множеству ребер 4-регулярного графа $G = (V, E)$ добавить еще одно ребро, обе вершины которого принадлежат V , то новый граф G' будет содержать 3-регулярный подграф. Граф называется k -регулярным, если из каждой его вершины выходит ровно k ребер.

Литература

- [1] *Aigner M., Ziegler G.M.* Proofs from THE BOOK. Berlin: Springer-Verlag, 1998.
- [2] *Виноградов И. М.* Основы теории чисел. М.; Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003.
- [3] *Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б.* Введение в теорию чисел. М.: Изд-во МГУ, 1995.
- [4] *Грэхем Р.* Начала теории Рамсея. М.: Мир, 1984.
- [5] *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
- [6] *Райгородский А. М.* Хроматические числа. М.: МЦНМО, 2003.
- [7] *Райгородский А. М.* Проблема Борсука. М.: МЦНМО, 2006.
- [8] *Райгородский А. М.* Проблема Борсука и хроматические числа некоторых метрических пространств // УМН. Т. 56. 2001. Вып. 1. С. 107–146.
- [9] *Скворцов В. А.* Примеры метрических пространств. М.: МЦНМО, 2002.
- [10] *Фиштенгольц Г. М.* Курс дифференциального и интегрального исчисления. М.; Ижевск: Физматлит, 2003.
- [11] *Харари Ф.* Теория графов. М.: Мир, 1973.
- [12] *Хинчин А. Я.* Три жемчужины теории чисел. М.: Эдиториал УРСС, 2004.
- [13] *Холл М.* Комбинаторика. М.: Мир, 1970.
- [14] *Эрдёш П., Спенсер Дж.* Вероятностные методы в комбинаторике. М.: Мир, 1976.
- [15] *Raigorodskii A. M.* The Borsuk partition problem: the seventieth anniversary // Mathematical Intelligencer. V. 26. 2004. № 4. P. 4–12.

А. М. Райгородский

ЛИНЕЙНО-АЛГЕБРАИЧЕСКИЙ МЕТОД В КОМБИНАТОРИКЕ

Подписано в печать 18.06.2007 г. Формат $60 \times 90 \frac{1}{16}$.
Бумага офсетная № 1. Печать офсетная. Печ. л. 8,5. Тираж 1000 экз.
Заказ № .

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (495)-241-74-83.

Отпечатано с готовых диапозитивов в ФГУП «Полиграфические ресурсы».

Книги издательства МЦНМО можно приобрести
в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. (495) 241-72-85. E-mail: biblio@mccme.ru
