Вероятность и линейная алгебра в комбинаторике

А.М. Райгородский

1 Введение

Современная комбинаторика - это весьма многогранная и бурно развивающаяся наука. Только за последние десятилетия в ней возникло множество новых и важных, но зачастую крайне далеких друг от друга разделов. В результате все труднее становится увидеть комбинаторику в целом, почувствовать единство комбинаторных проблем, осознать подлинные взаимосвязи между ними. Вместе с тем, неограниченное дробление любой, сколь угодно содержательной, науки в конечном счете лишь вредит ей. Необходима серьезная база, на основе которой набор разрозненных задач и наблюдений сформировался бы в цельную дисциплину. И тут огромную роль играет база методологическая. Возникают мощные методы, позволяющие дать ответы на самые различные вопросы и служащие, таким образом, естественными инструментами для цементирования науки: отныне значительная часть ее разделов, которые, на первый взгляд, совсем не коррелировали между собой, группируется вокруг единого метода, и этот метод не только ведет к решению прежних частных задач, но еще и выступает как катализатор к созданию новых нетривиальных и глубоко взаимосвязанных проблем. В комбинаторике можно выделить несколько таких общих и действительно важных методов. Если речь идет о подсчете числа комбинаций тех или иных объектов (т.е. о так называемой "перечислительной комбинаторике"), то, конечно, нужно в первую очередь упоминать метод производящих функций (см. [1], [2]). Нас, однако, будут в большей мере интересовать "экстремальные" задачи комбинаторики - задачи, в рамках которых требуется находить различные экстремальные характеристики какой-либо

совокупности объектов (например, максимальное число попарно пересекающихся подмножеств конечного множества и пр.). И здесь наиболее существенны методы, связанные с применением идей теории вероятностей и алгебры.

Разумеется, нельзя сказать, кто был первым, применившим, скажем, вероятностные соображения для решения какой-нибудь комбинаторной задачи. Некоторые авторы еще в начале XX века догадались, что вычисление средних значений "случайных величин" бывает весьма полезным в комбинаторике. Тем не менее, именно выдающийся венгерский математик П. Эрдеш (1913 - 1996) занялся в пятидесятые годы систематическим развитием вероятностного метода, и потому именно его - создателя венгерской школы современного комбинаторного анализа, человека, внесшего неоценимый вклад в становление комбинаторики (в том числе и вероятностной), - принято считать основателем метода.

Что же касается алгебраического метода, тут есть своя большая история. Мы не станем, однако, вдаваться ни в какие исторические подробности, отсылая заинтересованного читателя к другим источникам (см. [3], [4], [5], [6], [7], [8], [9]). Заметим лишь, что для нас будет актуален линейно-алгебраический аспект алгебраического метода, о чем подробнее ниже.

В серии из четырех лекций мы предполагаем рассказать о нескольких ярких задачах комбинаторики и комбинаторной геометрии. На их примере мы проиллюстрируем ряд основополагающих подходов вероятностного и линейно-алгебраического характера. Именно за счет этих методов задачи окажутся неожиданно близкими и тесно друг с другом связанными, хотя априори было бы трудно увидеть их естественную и глубокую близость. Для большей доступности изложения мы приведем в главе Дополнение набор необходимых определений из теории вероятностей, линейной алгебры, теории графов и математического анализа, так что читатель, не совсем знакомый с соответствующей терминологией, сможет получить всю недостающую ему информацию, не обращаясь к внешним источникам; впрочем, вспомогательную литературу по предметам мы также упомянем. В конце каждой лекции мы сформулируем некоторое количество задач, среди которых будут как чисто учебные, так и исследовательские - еще не решенные.

2 Лекция 1. Задачи о пересечениях множеств

2.1 Постановки задач и формулировки некоторых результатов

В 60-ые годы XX века начала активно развиваться наука об экстремальных свойствах совокупностей подмножеств конечного множества. Эти совокупности часто называют также "гиперграфами", имея в виду, что граф задается *конечным множеством* вершин и совокупностью пар вершин - ребер (см. дополнение): понятно, что, рассматривая вместо двухэлементных абы какие подмножества множества вершин, мы получаем обобщение графа - "сверхграф", гиперграф. Мы изучим здесь две на вид очень похожие задачи упомянутого типа. Обе они имеют значительное количество приложений, просты по своим постановкам и крайне, однако ж, нетривиальны.

Итак, пусть $\mathcal{R}_n = \{a_1, a_2, \ldots, a_n\}$ - произвольное множество, состоящее из n элементов. Можно считать без ограничения общности, что $\mathcal{R}_n = \{1, 2, \ldots, n\}$ есть просто отрезок натурального ряда. Рассмотрим какую-нибудь совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$, образованную (различными) k - элементными подмножествами M_i (k - сочетаниями), $i = 1, \ldots, s$, множества $\mathcal{R}_n$, $0 \leq k \leq n$. Очевидно, $s \leq C_n^k$, и тут никаких проблем нет. Возникает вопрос: а что, если мы запретим множествам из совокупности $\mathcal{M}$ иметь попарные пересечения той или иной мощности? Как это повлияет на размер s самой совокупности? Наиболее изучены две ситуации. В первом случае мы потребуем, чтобы любые два множества из $\mathcal{M}$ пересекались не менее, чем по $t \leq k$, общим элементам. Во втором случае нам важно будет лишь отсутствие пар множеств $M_i, M_j \in \mathcal{M}$, которые бы пересекались ровно по t элементам из $\mathcal{R}_n$. Положим, соответственно,

$$f(n,k,t) = \max\{s = |\mathcal{M}| : \forall\, i,j \in \{1,\ldots,s\} \;\; |M_i \cap M_j| \geq t\},$$

$$m(n,k,t) = \max\{s = |\mathcal{M}| : \forall\, i,j \in \{1,\ldots,s\} \;\; |M_i \cap M_j| \neq t\}.$$

Отыскание величин $m(n,k,t), f(n,k,t)$ - крайне сложная, красивая и богатая приложениями задача (см. лекции 2 и 3). Ниже мы приведем две яркие и показательные теоремы относительно этих величин.

Теорема 1 (П. Эрдеш, Ч. Ко и Р. Радо). *Если* $n < 2k$, *то* $f(n,k,1) = C_n^k$; *иначе* $f(n,k,1) = C_{n-1}^{k-1}$.

Теорема 2 (П. Франкл и Р.М. Уилсон). *Пусть* p - *простое число,* $n = 4p$, $k = 2p$, $t = p$. *Тогда* $m(n,k,t) \leq 2C_{n-1}^{p-1}$.

Обе теоремы носят достаточно специфический характер. Тем не менее, в них уже содержится вся суть происходящего, а некоторую историю, связанную с ними, и более общие формулировки мы приведем в параграфе 2.4. Сейчас мы заметим лишь, что результат теоремы 1 окончательный, тогда как в теореме 2 приводится только оценка сверху. На самом деле, эта оценка практически неулучшаема (см. задачи). Более того, она, на первый взгляд, абсолютно неожиданна. Действительно, если аккуратно применить формулу Стирлинга $m! = \sqrt{2\pi m}\left(\frac{m}{e}\right)^m(1 + o(1))$, $m \to \infty$ (см. дополнение), к каждому из факториалов, фигурирующих в известной записи выражений C_n^k и $2C_{n-1}^{p-1}$, то нетрудно увидеть, что в первом случае мы имеем дело с величиной $(2 + o(1))^n$, а во втором - с величиной $(1.754... + o(1))^n$. Это означает, что, едва мы запретили всего один вариант пересечения множеств в совокупности (разрешено ведь все, что угодно; лишь бы множества не пересекались по p общим элементам), и сразу же от тривиальной оценки $s \leq (2+o(1))^n$ мы пришли к экспоненциально меньшему неравенству $s \leq (1.754... + o(1))^n$. Трудно поверить, что буквально один запрет столь сильно ограничивает свободу в построении совокупности $\mathcal{M}$; однако это так.

Теорему 1 мы докажем в следующем параграфе, а теорему 2 - в параграфе 2.3.

2.2 Доказательство теоремы 1

Начнем с замечания, что случай $n < 2k$ очевиден. В самом деле, при данных условиях просто не существует непересекающихся множеств, так что и впрямь $f(n,k,1) = C_n^k$. Далее, во втором случае нижняя оценка $f(n,k,1) \geq C_{n-1}^{k-1}$ тоже практически очевидна. Достаточно рассмотреть совокупность множеств, каждый элемент которой содержит, например, единицу:

$$\mathcal{M} = \{M \subset \mathcal{R}_n : |M| = k,\ 1 \in M\}.$$

Понятно, что $|\mathcal{M}| = C_{n-1}^{k-1}$, и все в порядке. В свою очередь, верхнюю оценку можно, в принципе, получить различными способами, но мы при-

меним самый естественный и показательный из них - вероятностный. Этот способ формально предложил Д. Катона в 1972 году, хотя нам представляется, что подобная идея должна сразу же прийти в голову всякому, желающему обосновать теорему Эрдеша - Ко - Радо.

Зафиксируем произвольную совокупность $\mathcal{M}$, состоящую из попарно пересекающихся множеств, и рассмотрим вспомогательную конструкцию: положим $A_s = \{s, s+1, \ldots, s+k-1\}$, $s = 1, \ldots, n$. Здесь суммирование понимается по модулю n, так что $A_s \subset \mathcal{R}_n$ и $|A_s| = k$. Нетрудно заметить, что из множеств A_s не более k попадает в $\mathcal{M}$. Действительно, если допустить, что какое-то A_s принадлежит $\mathcal{M}$, то остальные множества A_t, которые пересекаются с A_s и, тем самым, имеют право лежать в $\mathcal{M}$, можно разбить на пары вида (A_{s-i}, A_{s+k-i}), $i = 1, \ldots, k-1$. Таких пар $k-1$ штука, и из каждой мы вольны добавить в $\mathcal{M}$ не более одного элемента. Вместе с исходным $A_s \in \mathcal{M}$ получится в аккурат не более k множеств типа A_s в нашей совокупности, и утверждение доказано.

Теперь рассмотрим *случайный* элемент $i \in \mathcal{R}_n$ и *случайную* перестановку σ на множестве $\mathcal{R}_n$. В обоих случаях случайность мы понимаем в смысле классического определения вероятности (см. дополнение), так что вероятность каждого конкретного i есть $P(i) = \frac{1}{n}$, а вероятность любого σ равна $P(\sigma) = \frac{1}{n!}$ (различных перестановок $n!$, и их мы считаем равновероятными). При этом, разумеется, выбор элемента мы осуществляем независимо от выбора перестановки. Рассмотрим множество $A_{i,\sigma} = \{\sigma(i), \sigma(i+1), \ldots, \sigma(i+k-1)\}$, по-прежнему определяя сложение по модулю n. Множество $A_{i,\sigma}$ вложено в $\mathcal{R}_n$, имеет мощность k, и образовано оно перестановкой элементов множества A_i. Несложно убедиться в том, что множество $A_{i,\sigma}$ есть случайное k - элементное подмножество $\mathcal{R}_n$ опять-таки в классическом смысле, т.е. что вероятность $P(A_{i,\sigma})$ возникновения того или иного множества $A_{i,\sigma}$ совпадает с величиной $\frac{1}{C_n^k}$.

С одной стороны, ввиду сделанных наблюдений ясно, что $P(A_{i,\sigma} \in \mathcal{M}) = \frac{|\mathcal{M}|}{C_n^k}$. С другой стороны, если мы фиксируем на время перестановку, то условная вероятность $P(A_{i,\sigma} \in \mathcal{M}|\sigma)$ не превосходит $\frac{k}{n}$. Это вытекает из нашего рассуждения про попадание в $\mathcal{M}$ множеств вида A_s. Понятно ведь, что и среди "переставленных" множеств $A_{s,\sigma}$ при данном σ не более k лежат в $\mathcal{M}$. Пользуясь формулой полной вероятности (см. дополнение), получаем

$$P(A_{i,\sigma} \in \mathcal{M}) = \sum_{\sigma} P(A_{i,\sigma} \in \mathcal{M}|\sigma)P(\sigma) \leq \sum_{\sigma} \frac{k}{n}\frac{1}{n!} = \frac{k}{n}.$$

Таким образом, $\frac{|\mathcal{M}|}{C_n^k} \le \frac{k}{n}$, откуда $|\mathcal{M}| \le \frac{k}{n} C_n^k = C_{n-1}^{k-1}$, и теорема доказана.

В заключение следует отметить, что приведенное "вероятностное" доказательство вполне можно было изложить на языке "количественном", сравнивая не вероятности, а мощности. Подобное замечание не может не прийти в голову всякому, кто внимательно следит за нашим рассуждением. Замечание это вполне правомочно, но возразить на него можно так. Конечно, *простейшие* вероятностные соображения суть соображения взятия среднего арифметического, и потому их ничего не стоить перевести на количественный язык. Тем не менее, такие соображения лежат лишь на самой верхушке огромного айсберга, который мы называем "вероятностным методом". Современная теория вероятностей гораздо тоньше и многограннее, нежели "вероятность классическая". Техника, разработанная в ее рамках, сложна, многопланова, и апеллирует она подчас к таким понятиям, которые крайне трудно, а главное, совершенно неестественно представлять чисто комбинаторно. Нет смысла пытаться "дерандомизировать" вероятностные инструменты, относительно которых имеется огромная литература; разве что такого рода дерандомизация помогает кому-то на первых порах лучше осознать метод. Однако в конечном итоге затея изживает себя.

2.3 Доказательство теоремы 2

Зафиксируем произвольную совокупность $\mathcal{M}$, удовлетворяющую условиям теоремы, и разобьем ее на две части: $\mathcal{M} = \mathcal{M}_1 \bigsqcup \mathcal{M}_2$. Здесь

$$\mathcal{M}_1 = \{M \in \mathcal{M} : M \subset \mathcal{R}_{n-1}\}.$$

Нетрудно видеть, что при каждом $i \in \{1,2\}$ для любых $M, N \in \mathcal{M}_i$ выполнено: $|M \bigcap N| \equiv 0 \pmod p$ тогда и только тогда, когда $M = N$ (по условию $|M \bigcap N| \neq p$, и любые два множества теперь пересекаются). Мы докажем ниже, что $|\mathcal{M}_1| \le C_{n-1}^{p-1}$. Из нашего рассуждения будет понятно, как обосновать аналогичную оценку $|\mathcal{M}_2| \le C_{n-1}^{p-1}$ (читатель сам без труда проделает необходимые выкладки), и в результате мы получим утверждение теоремы.

Рассмотрим совокупность векторов

$$V = \{\mathbf{x} = (x_1, \ldots, x_{n-1}) : x_i \in \{0,1\},\ x_1 + \ldots + x_{n-1} = k = 2p\}.$$

Ясно, что множествам из $\mathcal{M}_1$ однозначно отвечают некоторые из этих векторов: если $M \in \mathcal{M}_1$, то соответствующий $\mathbf{x} \in V$ имеет коорди-

наты $x_i = 1$, коль скоро $i \in M$, и $x_i = 0$, коль скоро $i \notin M$. При этом условие "$|M \bigcap N| \equiv 0 \pmod p$ тогда и только тогда, когда $M = N$" превращается в условие "$(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod p$ тогда и только тогда, когда $\mathbf{x} = \mathbf{y}$"; скобками мы обозначаем обычное скалярное произведение векторов (см. дополнение). Пусть $V_1 = \{\mathbf{x}_1, \ldots, \mathbf{x}_s\} \subset V$ есть точный образ совокупности $\mathcal{M}_1$ в совокупности V. Нам нужно доказать, что $|V_1| \leq C_{n-1}^{p-1}$.

Каждому вектору $\mathbf{x} \in V$ сопоставим некоторый многочлен $F_{\mathbf{x}}$ от $n-1$ переменной. Коэффициенты этого многочлена будем считать принадлежащими множеству (полю) $\mathbb{Z}_p$ классов вычетов по модулю p (см. дополнение). Иными словами, возьмем следующий $F_{\mathbf{x}} \in \mathbb{Z}_p[y_1, \ldots, y_{n-1}]$:

$$F_{\mathbf{x}}(\mathbf{y}) = \prod_{i=1}^{p-1}(i - (\mathbf{x}, \mathbf{y})),$$

где $\mathbf{y} = (y_1, \ldots, y_{n-1})$. Имеет место простая лемма.

Лемма 1. *Для любых $\mathbf{x}, \mathbf{y} \in V$ значение $F_{\mathbf{x}}(\mathbf{y})$ сравнимо с нулем по модулю p тогда и только тогда, когда $(\mathbf{x}, \mathbf{y}) \not\equiv 0 \pmod p$.*

Лемма очевидна, и мы ее не доказываем. Теперь раскроем скобки в определении каждого многочлена $F_{\mathbf{x}}$, т.е. запишем $F_{\mathbf{x}}$ в виде линейной комбинации одночленов. Получится некоторое выражение вида

$$F_{\mathbf{x}}(\mathbf{y}) = \sum c_{i_1,\ldots,i_q} y_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot y_{i_q}^{\alpha_{i_q}}.$$

Здесь $q \leq p-1$, и, более того, $\alpha_{i_1} + \ldots + \alpha_{i_q} \leq p-1$, причем $1 \leq \alpha_{i_\nu} \leq p-1$, $\nu = 1, \ldots, q$; вместе с тем $1 \leq i_1 < \ldots < i_q \leq n-1$. Положим

$$\tilde{F}_{\mathbf{x}}(\mathbf{y}) = \sum c_{i_1,\ldots,i_q} y_{i_1} \cdot \ldots \cdot y_{i_q},$$

т.е. "обрежем" все степени переменных y_ν. Возникает новый многочлен $\tilde{F}_{\mathbf{x}} \in \mathbb{Z}_p[y_1, \ldots, y_{n-1}]$, и этот многочлен замечательным образом удовлетворяет условию леммы 1: просто его значения на векторах $\mathbf{y} \in V$ совпадают со значениями многочлена $F_{\mathbf{x}}$ на тех же векторах ($y_i^m = y_i$ для всех i и всех $m \geq 1$, ведь у нас $y_i \in \{0, 1\}$).

Обозначим через d размерность пространства, образованного многочленами $\tilde{F}_{\mathbf{x}}$, $\mathbf{x} \in V$ (см. дополнение).

Лемма 2. *Имеет место неравенство $|\mathcal{M}_1| = |V_1| \leq d$.*

Доказательство леммы 2. Рассмотрим многочлены $\tilde{F}_{\mathbf{x}_1}, \ldots, \tilde{F}_{\mathbf{x}_s}$, отвечающие векторам из V_1. Покажем, что они линейно независимы над $\mathbb{Z}_p$ (см. дополнение). Для этого достаточно убедиться в том, что тождество

$$c_1\tilde{F}_{\mathbf{x}_1}(\mathbf{y}) + \ldots + c_s\tilde{F}_{\mathbf{x}_s}(\mathbf{y}) \equiv 0 \pmod{p} \ \forall\, \mathbf{y} \in V$$

выполнено, только если

$$c_1 \equiv c_2 \equiv \ldots \equiv c_s \equiv 0 \pmod{p}.$$

Пусть $\mathbf{y} = \mathbf{x}_i$, $i = 1, \ldots, s$. Тогда $(\mathbf{x}_i, \mathbf{y}) \equiv 0 \pmod{p}$, и $\tilde{F}_{\mathbf{x}_i}(\mathbf{y}) \not\equiv 0 \pmod{p}$ по лемме 1. В то же время за счет условия "$(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{p}$ тогда и только тогда, когда $\mathbf{x} = \mathbf{y}$" $(\mathbf{x}, \mathbf{y} \in V_1)$ имеем $(\mathbf{x}_j, \mathbf{y}) \not\equiv 0 \pmod{p}$ для любого $j \neq i$, и, стало быть, $\tilde{F}_{\mathbf{x}_j}(\mathbf{y}) \equiv 0 \pmod{p}$ опять-таки по лемме 1. Поскольку p - простое число, наше тождество вкупе со сделанными наблюдениями влечет сравнение $c_i \equiv 0 \pmod{p}$. Сравнение верно для каждого i, и линейная независимость многочленов доказана. Отсюда, в свою очередь, следует утверждение леммы.

Подчеркнем, что именно при доказательстве леммы простота p была актуальна. Больше она нам нигде не понадобится.

Остается понять, почему $d \leq C_{n-1}^{p-1}$. В пространстве, порожденном многочленами $\tilde{F}_{\mathbf{x}}$, $\mathbf{x} \in V$, можно выбрать естественный базис (см. дополнение), состоящий из одночленов вида $y_{i_1} \cdot \ldots \cdot y_{i_q}$, $0 \leq q \leq p-1$, $1 \leq i_1 < \ldots < i_q \leq n-1$. Очевидно, таких одночленов $\sum\limits_{i=0}^{p-1} C_{n-1}^{i}$. Однако на V все эти одночлены можно линейно выразить через одночлены старшей степени (степени $p-1$). В самом деле, рассмотрим, для примера, одночлен $y_1 \cdot \ldots \cdot y_{p-2}$. Домножим его на сумму всех переменных $y_1, \ldots, y_{n-1}$, каковая на V совпадает с величиной $k = 2p$. Получим (на V) цепочку соотношений

$$2py_1 \cdot \ldots \cdot y_{p-2} = (y_1 + \ldots + y_{n-1})y_1 \cdot \ldots \cdot y_{p-2} = y_1^2 y_2 \cdot \ldots \cdot y_{p-2} + \ldots +$$

$$+y_1 \cdot \ldots \cdot y_{p-3}y_{p-2}^2 + y_1 \cdot \ldots \cdot y_{p-2}y_{p-1} + \ldots + y_1 \cdot \ldots \cdot y_{p-2}y_{n-1} =$$

$$= (p-2)y_1y_2 \cdot \ldots \cdot y_{p-2} + y_1 \cdot \ldots \cdot y_{p-2}y_{p-1} + \ldots + y_1 \cdot \ldots \cdot y_{p-2}y_{n-1}.$$

Следовательно,

$$(p+2)y_1y_2 \cdot \ldots \cdot y_{p-2} = y_1 \cdot \ldots \cdot y_{p-2}y_{p-1} + \ldots + y_1 \cdot \ldots \cdot y_{p-2}y_{n-1},$$

т.е. мы и впрямь линейно выразили одночлен $y_1 \cdot \ldots \cdot y_{p-2}$ через одночлены степени $p-1$. Аналогично (с использованием индукции) можно поступить и в отношении других одночленов. Окончательно получаем $d \le C_{n-1}^{p-1}$, и теорема доказана.

2.4 Несколько слов об истории задач

Теорему 1 П. Эрдеш, Ч. Ко и Р. Радо доказали еще в 1938 году. Однако, как говорил впоследствии Эрдеш, в те времена тематика задач о пересечениях множеств была не слишком популярна, и потому работа была опубликована только в 1961 году. Любопытно, что за прошедшие с момента доказательства до момента публикации годы проблематика "гиперграфов" стала куда популярнее: на сегодняшний день статья Эрдеша - Ко - Радо - едва ли не одна из самых цитируемых в области.

На самом деле, Эрдеш, Ко и Радо доказали нечто гораздо большее, а именно: для любых k, t найдется такое $n_0(k,t)$, что при всех $n \ge n_0(k,t)$ выполнено $f(n,k,t) = C_{n-t}^{k-t}$. Конечно, результат вполне ожидаемый (см. §2.2); не ясно лишь, почему он не всегда верен. В действительности, все далеко не так просто, как могло бы показаться на первый взгляд, и значение $f(n,k,t)$ отнюдь не для любых n,k,t достигается на всем понятной конструкции (ср. §2.2). Общую конструкцию мы приведем ниже, но пока мы ведь даже не знаем, что из себя представляет $n_0(k,t)$. В 1977 году П. Франкл доказал, что $n_0(k,t) = (k-t+1)(t+1)$ при $k \ge 15$. Досадное ограничение на k устранил семь лет спустя Р.М. Уилсон. Таким образом, начиная с 1984 года, оставался открытым вопрос, что же происходит, коль скоро $n < (k-t+1)(t+1)$; например, что будет, если величины n,k,t устроены так же, как в теореме 2? И только в 1996 году на поставленный вопрос был дан окончательный ответ.

Теорема 3 (Р. Алсведе и Л. Хачатрян). *Пусть $r \in \mathbb{N}$ таково, что*

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

(при $r=0$ считаем правую часть цепочки неравенств бесконечной). Тогда $f(n,k,t) = |\mathcal{F}_r|$, где

$$\mathcal{F}_r = \{F \subset \mathcal{R}_n : |F| = k,\ |F \cap \{1,\ldots,t+2r\}| \ge t+r\}.$$

Во-первых, легко видеть, что все параметры в теореме 3 определены корректно. Во-вторых, понятно, что при $r = 0$ мы имеем в точности результат, доказанный Эрдешем - Ко - Радо, причем $n_0(k,t)$ ровно то, которое нашли Франкл и Уилсон. Наконец, ясно, что с теоремой Алсведе - Хачатряна задача про $f(n,k,t)$ оказалась полностью решенной. Впрочем, мысль человеческая не стоит на месте, и теперь крайне актуальны два направления исследований. С одной стороны, рассматривается величина

$$f(n,k,t,r) =$$

$$= \max\{|\mathcal{M}| : \forall\, M \in \mathcal{M}\ \ |M| = k,\, \forall\, M_1, \ldots, M_r \in \mathcal{M}\ \ |M_1 \cap \ldots \cap M_r| \geq t\}.$$

Иными словами, теперь не парам множеств мы запрещаем пересекаться меньше, чем по t, элементам, а произвольным их наборам мощности r; при $r = 2$ мы возвращаемся к уже изученной задаче. Мы не станем цитировать здесь известные результаты относительно $f(n,k,t,r)$; только заметим, что даже при $r = 3$ до отыскания соответствующей величины исключительно далеко.

Другая задача, естественным образом обобщающая решенную, может быть поставлена так (ср. §2.3). Пусть $\mathcal{M}$ - это совокупность n - мерных векторов, координаты которых принимают значения из фиксированного множества чисел $\{b_1, \ldots, b_r\}$, причем количество координат той или иной величины в каждом векторе одно и то же - скажем, l_i координат величины b_i, $i = 1, \ldots, r$ $(l_1 + \ldots + l_r = n)$. Положим

$$f(n; b_1, \ldots, b_r; l_1, \ldots, l_r; t) = \max\{|\mathcal{M}| : \forall\, \mathbf{x}, \mathbf{y} \in \mathcal{M}\ \ (\mathbf{x}, \mathbf{y}) \geq t\}.$$

Очевидно, $f(n; 1, 0; k, n-k; t) = f(n,k,t)$. Уже при $r = 3$, $b_1 = -1, b_2 = 0, b_3 = 1$ задача не решена.

Теперь о задаче для $m(n,k,t)$. Общая формулировка теоремы Франкла - Уилсона (теоремы 2) звучит так.

Теорема 4 (П. Франкл и Р.М. Уилсон). *Пусть $k - t$ - это 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 $m(n,k,t) \leq C_n^d C_{n-d}^{t-d} / C_k^d$.*

Понятно, что теорема применима к значительно большему количеству параметров, и все же остается недоумение: мы опять-таки существенно ограничиваем себя условием, что $k - t$ - степень простого числа. Неужели нельзя от этого условия избавиться? Это сложный вопрос, на

который никто до сих пор не знает ответа. Известно, например, что при $n = 4t$ (t любое)

$$\max\{|\mathcal{M}| : \forall\, M, N \in \mathcal{M} \;\; |M \cap N| \neq t\} \leq (1.99)^n,$$

но это гораздо хуже результата

$$m(4p, 2p, p) \leq 2C_{n-1}^{p-1} \leq (1.754 + o(1))^n.$$

Дальнейшие нетривиальные аспекты деятельности весьма похожи на те, что были заложены нами в определения величин

$$f(n, k, t, r), \quad f(n; b_1, \ldots, b_r; l_1, \ldots, l_r; t).$$

Аналогично можно, разумеется, определить и величины

$$m(n, k, t, r), \;\; m(n; b_1, \ldots, b_r; l_1, \ldots, l_r; t).$$

Первая величина исследована пока совсем мало, а вот относительно второй величины значительное количество результатов было получено автором данной брошюры. Тем не менее, и с ней далеко не все ясно.

Задачи.

1. Докажите, что $m(4p, 2p, p) \geq (1.754... + o(1))^n$, $n = 4p$.

2. Докажите вариант теоремы 2, заменив простое p на степень простого p^α.

3. С помощью линейной алгебры докажите оценку $m(n, 3, 1) \leq n$. Можно ли эту оценку уточнить?

4. С помощью линейной алгебры докажите оценку $m(n, 5, 2) \leq C_n^2$. Можно ли эту оценку уточнить?

5. Докажите теорему 4.

6. (*Теорема Франкла - Уилсона*) Пусть $\mathcal{M} = \{M_1, \ldots, M_s\}$ - произвольная совокупность семиэлементных подмножеств множества $\mathcal{R}_n$, обладающая свойством:

$$\left| M_i \bigcap M_j \right| \in \{0, 2, 3, 5, 6\}$$

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

7. Пусть

$$V = \{\mathbf{x} = (x_1, \ldots, x_{16}) : x_i \in \{-1, 0, 1\},\ |\{i : x_i = \pm 1\}| = 8\}.$$

Предположим, $W \subset V$ таково, что для любых $\mathbf{x}, \mathbf{y} \in W$ скалярное произведение $(\mathbf{x}, \mathbf{y})$ не равно нулю. Найдите или хотя бы оцените $\max |W|$.

3 Лекция 2. Проблемы Борсука и Нелсона - Эрдеша - Хадвигера

3.1 Постановки проблем и формулировки теорем

В этой лекции мы расскажем о приложениях изученной нами техники к двум классическим задачам комбинаторной геометрии - проблеме Борсука и проблеме Нелсона - Эрдеша - Хадвигера.

Первая задача, поставленная К. Борсуком в 1933 году, состоит в отыскании минимального числа $f(n)$ частей меньшего диаметра, на которые может быть разбито произвольное ограниченное множество в евклидовом пространстве $\mathbb{R}^n$. Если говорить чуть более развернуто, то нужно сперва для каждого ограниченного $\Omega \subset \mathbb{R}^n$ ввести величину

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

где $\operatorname{diam}\Omega = \sup\limits_{\mathbf{x},\mathbf{y}\in\Omega} |\mathbf{x}-\mathbf{y}|$, а $|\mathbf{x}-\mathbf{y}|$ - евклидово расстояние между векторами. Соответственно, $f(n) = \max\limits_{\Omega} f(\Omega)$.

Проблема Э. Нелсона - П. Эрдеша - Г. Хадвигера сформировалась на рубеже 40-ых - 50-ых годов XX века, и сводится она к нахождению так называемого хроматического числа $\chi(\mathbb{R}^n)$ евклидова пространства. Здесь

$$\chi(\mathbb{R}^n) = \min\left\{\chi : \mathbb{R}^n = V_1 \bigsqcup \ldots \bigsqcup V_\chi,\ \forall\, i\, \forall\, \mathbf{x}, \mathbf{y} \in V_i\ \ |\mathbf{x}-\mathbf{y}| \neq 1\right\}.$$

Иначе говоря, хроматическое число пространства - это минимальное количество цветов, в которые можно так раскрасить все точки $\mathbb{R}^n$, чтобы между одноцветными точками не было расстояния 1.

История обеих задач и смежных с ними вопросов исключительно богата и к тому же драматична. Имеется обширная литература, по которой можно ознакомиться со всеми тонкостями проблематики (см. [8], [10], [11], [12], [13], [14], [15]), и мы не будем здесь тратить время на исторические отступления. Скажем буквально несколько слов, достаточных для того, чтобы создать общее представление о задачах.

Во-первых, заметим, что в проблеме Борсука можно вполне считать все множества имеющими диаметр 1; напротив, ничто не мешает нам в задаче о хроматическом числе запретить точкам одного цвета отстоять друг от друга на любое заданное наперед расстояние: однородность пространства показывает, что ни $f(n)$, ни $\chi(\mathbb{R}^n)$ от подобных модификаций не пострадают. Кстати, величину "одноцветного" расстояния, которую мы запрещаем в проблеме Нелсона - Эрдеша - Хадвигера, так и называют *запрещенным расстоянием.*

Далее, проблема Борсука выросла из гипотезы того же автора, который предположил, что $f(n) = n + 1$. Если бы гипотеза подтвердилась, то это был бы крупный успех, так как возникло бы новое определение размерности. К сожалению, в 1993 году Дж. Кан и Г. Калаи показали, что $f(n) \geq (1.203... + o(1))^{\sqrt{n}}$, и это дало контрпримеры к гипотезе в размерностях $n \geq 2014$. Сейчас известно, что гипотеза верна при $n \leq 3$ и неверна при $n \geq 298$. До сих пор вопрос о том, что происходит в размерностях $n \in [4, 297]$, остается открытым. Что до же до величины $f(n)$, то на данный момент наилучшие ее оценки таковы:

$$(1.2255... + o(1))^{\sqrt{n}} \leq f(n) \leq \left(\sqrt{\frac{3}{2}} + o(1)\right)^n.$$

Нижняя оценка получена в 1999 году автором этой брошюры, а верхняя установлена О. Шраммом в 1988 году. Самое в этой истории удивительное, что гипотеза верна для множеств с гладкой границей, т.е., если граница Ω непрерывно дифференцируема, то $f(\Omega) \leq n + 1$. Казалось бы, как близко от гладких тел до любых: осталось только надлежащую аппроксимацию построить. Ан нет, и мы увидим, что уже конечные множества точек в пространстве дают контрпримеры.

В проблеме Нелсона - Эрдеша - Хадвигера наиболее "трагичен" тот факт, что даже при $n = 2$ хроматическое число не найдено. Известно лишь, что $4 \leq \chi(\mathbb{R}^n) \leq 7$, причем обе оценки практически тривиальны. Нас, однако, будет больше интересовать здесь случай растущей размер-

ности. На данном этапе установлены неравенства

$$(1.239... + o(1))^n \leq \chi(\mathbb{R}^n) \leq (3 + o(1))^n.$$

Первое из них принадлежит автору брошюры, второе доказано в 1972 году Д. Ларманом и К.А. Роджерсом.

В принципе, близость двух проблем видна уже по их постановкам; однако долгое время они существовали порознь: люди, занимавшиеся одной задачей, редко имели достаточное представление о другой. Именно создание П. Франклом и Р.М. Уилсоном линейно-алгебраического метода, рассмотренного нами в прошлой лекции, привело к возникновению единой почвы для решения задач, и это лишний раз подтверждает наш основной тезис. Задачи оказались настолько близкими, что недавно автором был получен, грубо говоря, такой результат: либо $\chi(\mathbb{R}^n) \geq (1.25... + o(1))^n$, либо $f(n) \geq (1.25... + o(1))^{\sqrt{n}}$, т.е. мы не знаем пока, как улучшить прежние результаты $\chi(\mathbb{R}^n) \geq (1.239... + o(1))^n$, $f(n) \geq (1.2255... + o(1))^{\sqrt{n}}$, но мы можем гарантировать существенное улучшение хотя бы одного из них (см. [16]).

В настоящей брошюре мы докажем следующие две теоремы.

Теорема 5 (П. Франкл и Р.М. Уилсон). *Имеет место неравенство* $\chi(\mathbb{R}^n) \geq (1.139... + o(1))^n$.

Теорема 6 (А.М. Райгородский). *Гипотеза Борсука неверна при всех* $n \geq 561$.

Обе теоремы дают не самые сильные результаты среди известных, но и они уже весьма близки к наилучшим. К тому же в них заложена суть подхода, а наша задача здесь состоит в первую очередь в усвоении существа дела. Теорему 5 мы докажем в §3.2, теорему 6 - в §3.3.

3.2 Доказательство теоремы 5

Пусть p - простое число, $n = 4p$. Рассмотрим в $\mathbb{R}^n$ совокупность векторов

$$V = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \{0, 1\},\ x_1 + \ldots + x_n = 2p\}.$$

Понятно, что $|V| = C_n^{2p}$. Предположим, мы раскрасили все $\mathbb{R}^n$ в $\chi < \frac{C_n^{2p}}{2C_{n-1}^{p-1}}$ цветов с запретом расстояния $\sqrt{2p}$. Тогда и на V ушло не больше χ красок. Значит, найдется цвет, в который покрашено $> 2C_{n-1}^{p-1}$ векторов из

V. По теореме 2 Франкла - Уилсона в рамках данного цвета есть пара векторов со скалярным произведением p. Однако расстояние между такими векторами равно $\sqrt{2p}$, и это противоречит исходному предположению о раскраске. Следовательно,

$$\chi(\mathbb{R}^n) \geq \frac{C_n^{2p}}{2C_{n-1}^{p-1}} = \frac{(2+o(1))^n}{(1.754...+o(1))^n} = (1.139...+o(1))^n.$$

Все бы хорошо, да одна беда: n не всякое, но лишь равное учетверенному простому. Как быть? Нужно вспомнить, что простые числа встречаются довольно часто в натуральном ряду, а хроматическое число, очевидно, монотонно растет с увеличением размерности. Итак, пусть n - произвольное натуральное число. Рассмотрим максимальное простое p, для которого $n' = 4p < n$. Понятно, что $p < \frac{n}{4}$. Однако в аналитической теории чисел, которая занимается, в частности, изучением распределения простых чисел, есть теорема, утверждающая, что при $n \to \infty$ для подходящего $\varphi(n) = o(n)$ найдется простое число p на интервале $\left(\frac{n}{4} - \varphi(n), \frac{n}{4}\right)$ (см. [17]). В результате имеем

$$\chi(\mathbb{R}^n) \geq \chi(\mathbb{R}^{n'}) \geq (1.139...+o(1))^{n'} \geq$$

$$\geq (1.139...+o(1))^{n-\varphi(n)} = (1.139...+o(1))^n.$$

Теорема доказана.

3.3 Доказательство теоремы 6

Здесь мы также прибегнем к помощи линейной алгебры; однако на сей раз повозиться придется значительно больше.

Положим $n = 36$ и рассмотрим совокупность векторов

$$\Sigma = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \{-1, 1\},\ x_1 = x_2 = x_3 = 1,\ x_1 \cdot \ldots \cdot x_n = 1\}.$$

Иными словами, Σ состоит из всех возможных 36-мерных (-1,1) - векторов, у которых первые три координаты равны единице и среди оставшихся тридцати трех положительных координат четное число. Понятно, что $|\Sigma| = 2^{32}$. Имеют место две очевидные леммы.

Лемма 3. *Для любых* $\mathbf{x}, \mathbf{y} \in \Sigma$ *выполнено* $(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod 4$.

Лемма 4.
а) *Для любых* $\mathbf{x}, \mathbf{y} \in \Sigma$ *имеем* $(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod 9$ *тогда и только тогда, когда либо* $\mathbf{x} = \mathbf{y}$, *либо* $(\mathbf{x}, \mathbf{y}) = 0$;
б) *Для любых* $\mathbf{x}, \mathbf{y} \in \Sigma$ *имеем* $(\mathbf{x}, \mathbf{y}) \equiv 4 \pmod 9$ *тогда и только тогда, когда* $(\mathbf{x}, \mathbf{y}) = 4$.

Каждому вектору $\mathbf{x} \in \Sigma$ поставим в соответствие многочлен $F_{\mathbf{x}} \in \mathbb{Q}[y_4, \ldots, y_n]$:

$$F_{\mathbf{x}}(\mathbf{y}) = \frac{1}{9} \prod_{i=1,\, i\neq 4}^{8} (i - (\mathbf{x}, \mathbf{y})).$$

Здесь $\mathbf{y} = (1, 1, 1, y_4, \ldots, y_n)$, так что в самом деле $F_{\mathbf{x}}$ зависит лишь от тридцати трех последних переменных. Кроме того, коэффициенты многочлена на сей раз рациональны. Тем не менее, легко доказать следующую лемму.

Лемма 5.
а) *Для любых* $\mathbf{x}, \mathbf{y} \in \Sigma$ *имеем* $F_{\mathbf{x}}(\mathbf{y}) \in \mathbb{Z}$;
б) *Если* $\mathbf{x}, \mathbf{y} \in \Sigma$ *таковы, что* $(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod 9$, *то* $F_{\mathbf{x}}(\mathbf{y}) \not\equiv 0 \pmod 3$;
в) *Если* $\mathbf{x}, \mathbf{y} \in \Sigma$ *таковы, что* $(\mathbf{x}, \mathbf{y}) \not\equiv 0 \pmod 9$ *и* $(\mathbf{x}, \mathbf{y}) \not\equiv 4 \pmod 9$, *то* $F_{\mathbf{x}}(\mathbf{y}) \equiv 0 \pmod 3$;

Доказательство леммы мы оставляем читателю. С многочленами же $F_{\mathbf{x}}$ мы проделаем знакомую нам процедуру: раскроем скобки и обрежем степени переменных. Только теперь, желая добиться успеха, достигнутого нами в аналогичной ситуации ранее, мы должны пользоваться тем фактом, что $y_i^2 = 1$, коль скоро мы имеем дело с произвольной координатой вектора из Σ. Напомним, что в §2.3 мы работали с нулями и единицами, так что там речь шла о тождестве $y_i^2 = y_i$. В любом случае новые многочлены, которые мы также обозначим $\tilde{F}_x$, удовлетворяют лемме 5, и размерность пространства, порожденного этими многочленами, не превосходит величины $\sum_{k=0}^{7} C_{33}^k$ (естественный базис в данном пространстве составляют одночлены, которые зависят от тридцати трех переменных, имеют суммарную степень по всем переменным не выше семи и степень не выше единицы по каждой отдельной переменной).

Лемма 6. *Какова бы ни была совокупность векторов* $Q = \{\mathbf{x}_1, \ldots,$

$\mathbf{x}_s\} \subset \Sigma$, *у которой скалярное произведение любых двух различных элементов не сравнимо ни с нулем, ни с четырьмя по модулю девять, ее мощность удовлетворяет неравенству* $s = |Q| \leq \sum\limits_{k=0}^{7} C_{33}^k$.

Доказательство леммы 6. Достаточно установить линейную независимость многочленов $\tilde{F}_{\mathbf{x}_1}, \ldots, \tilde{F}_{\mathbf{x}_s}$ над $\mathbb{Q}$ (см. дополнение и ср. §2.3). Для этого же нужно проверить, что тождество

$$c_1\tilde{F}_{\mathbf{x}_1}(\mathbf{y}) + \ldots + c_s\tilde{F}_{\mathbf{x}_s}(\mathbf{y}) = 0 \ \ \forall\, \mathbf{y} \in \Sigma$$

выполнено, только если

$$c_1 = c_2 = \ldots = c_s = 0.$$

Сперва домножим тождество на общий знаменатель рациональных (по определению) чисел $c_1, \ldots, c_s$. В результате мы вольны считать, не теряя общности, что $c_1, \ldots, c_s \in \mathbb{Z}$. Далее, вспомним, что имеет место пункт **а)** леммы 5. Он означает, что мы также не ограничим общность, полагая $c_1, \ldots, c_s \in \mathbb{Z}_3$ и понимая отныне равенство нулю в нашем тождестве как сравнение по модулю 3 (мы просто вынесем "за скобки" максимальную степень тройки, делящую каждый из наших коэффициентов, коль скоро, конечно, не все c_i равны нулю; но в последнем случае и делать нечего, все и без того в порядке). Итак, остается показать, что с необходимостью

$$c_1 \equiv c_2 \equiv \ldots \equiv c_s \equiv 0 \pmod 3.$$

Как и в §2.3, возьмем $\mathbf{y} = \mathbf{x}_i$. Тогда $(\mathbf{x}_i, \mathbf{y}) = 36 \equiv 0 \pmod 9$, и в силу пункта **б)** леммы 5 $\tilde{F}_{\mathbf{x}_i}(\mathbf{y}) \not\equiv 0 \pmod 3$. В то же время по условию $(\mathbf{x}_j, \mathbf{y}) \not\equiv 0 \pmod 9$ и $(\mathbf{x}_j, \mathbf{y}) \not\equiv 4 \pmod 9$ $(j \neq i)$, так что за счет утверждения **в)** леммы 5 $\tilde{F}_{\mathbf{x}_j}(\mathbf{y}) \equiv 0 \pmod 3$. Следовательно, для каждого i величина c_i обязана делиться на 3, и лемма 6 доказана.

Осуществим некоторую "надстройку" над Σ. Это и будет множеством, доставляющим контрпример к гипотезе Борсука. Итак, каждому вектору $\mathbf{x} = (x_1, \ldots, x_n) \in \Sigma$ сопоставим вектор

$$\mathbf{x} * \mathbf{x} = (x_i \cdot x_j), \ i = 2, \ldots, n, \ j = 4, \ldots, n,$$

т.е.

$$\mathbf{x} * \mathbf{x} = (x_2x_4, x_2x_5, \ldots, x_2x_n, x_3x_4, \ldots, x_3x_n, x_4^2, \ldots, x_4x_n, \ldots, x_nx_4, \ldots, x_n^2).$$

Получится новая совокупность векторов Σ^*, элементы которой находятся, как нетрудно видеть, во взаимно однозначном соответствии с элементами совокупности Σ (и, в частности, $|\Sigma^*| = 2^{32}$). Очевидно, что $\Sigma^* \subset \mathbb{R}^m$ с $m = (n-1)(n-3)$. Однако, на самом деле, можно сказать гораздо больше: Σ^* лежит в подпространстве пространства $\mathbb{R}^m$, имеющем размерность $d \leq C_{n-3}^2 + (n-3) = 561$, так что в конечном счете $\Sigma^* \subset \mathbb{R}^d$. Наше утверждение вытекает из линейных соотношений $x_i^2 = 1$, $x_i x_j = x_j x_i$, $x_2 x_j = x_3 x_j$, $x_2 x_3 = 1$, которые верны для координат любого вектора $\mathbf{x} * \mathbf{x} \in \Sigma^*$.

Лемма 7. *Диаметр совокупности Σ^* достигается на тех и только тех векторах $\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y}$, для которых либо $(\mathbf{x}, \mathbf{y}) = 0$, либо $(\mathbf{x}, \mathbf{y}) = 4$.*

Доказательство леммы 7. Известно, что (см. дополнение)

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

Вместе с тем

$$(\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y}) = \sum_{i=2}^{n} \sum_{j=4}^{n} x_i x_j y_i y_j = \left(\sum_{i=2}^{n} x_i y_i \right) \left(\sum_{j=4}^{n} x_i y_i \right) =$$

$$= ((\mathbf{x}, \mathbf{y}) - 1)((\mathbf{x}, \mathbf{y}) - 3)$$

(мы не забываем, что первые три координаты каждого вектора из Σ фиксированы). Таким образом,

$$|\mathbf{x} * \mathbf{x} - \mathbf{y} * \mathbf{y}|^2 = 2(n-1)(n-3) - 2(\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y}),$$

и максимум достигается, коль скоро скалярное произведение минимально. А оно минимально (ввиду леммы 3) тогда и только тогда, когда либо $(\mathbf{x}, \mathbf{y}) = 0$, либо $(\mathbf{x}, \mathbf{y}) = 4$. Лемма 7 доказана.

Предположим, мы разбили Σ^* на $f < \frac{2^{32}}{\sum_{k=0}^{7} C_{33}^k}$ частей меньшего диаметра:

$$\Sigma^* = \Omega_1^* \bigsqcup \ldots \bigsqcup \Omega_f^*.$$

Тогда найдется такая часть Ω_i^*, что $|\Omega_i^*| > \sum_{k=0}^{7} C_{33}^k$. Рассмотрим прообраз Ω_i множества Ω_i^* в Σ. Как мы знаем, его элементы находятся

во взаимно однозначном соответствии с векторами из Ω_i^*. Стало быть, $|\Omega_i| > \sum\limits_{k=0}^{7} C_{33}^k$. По лемме 6 в Ω_i есть два различных вектора $\mathbf{x}, \mathbf{y}$, у которых либо $(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod 9$, либо $(\mathbf{x}, \mathbf{y}) \equiv 4 \pmod 9$. Однако в силу леммы 4 либо $(\mathbf{x}, \mathbf{y}) = 0$, либо $(\mathbf{x}, \mathbf{y}) = 4$. И в том, и в другом случае на векторах $\mathbf{x} * \mathbf{x}, \mathbf{y} * \mathbf{y} \in \Omega_i^*$ достигается диаметр совокупности Σ^* (см. лемму 7), а это противоречит нашему изначальному предположению. Получается, что

$$f(561) \geq f(\Sigma^*) \geq \frac{2^{32}}{\sum\limits_{k=0}^{7} C_{33}^k} \approx 758 > 562.$$

Контрпример к гипотезе Борсука мы построили фактически при всех $d \in [561, 756]$. Однако легко распространить конструкцию и на большие размерности. Читателю предлагается самостоятельно сделать это, хотя имеется и ссылка на статью, в которой соответствующий результат был получен тогдашними школьниками А. Гайфуллиным и Д. Гуревичем (см. [18]). Теорема 6 доказана.

Задачи.

8. Докажите, что величины $\chi(\mathbb{R}^n)$ и $f(n)$ конечны.

9. (*Теорема Д. Лармана, К.А. Роджерса, П. Эрдеша и В. Шош*) Из результата задачи 3 выведите оценку $\chi(\mathbb{R}^n) \geq cn^2$, $c > 0$.

10. (*Теорема Д. Лармана*) Из результата задачи 4 выведите оценку $\chi(\mathbb{R}^n) \geq cn^3$, $c > 0$.

11. (*Теорема Д. Лармана и К.А. Роджерса*) Докажите, что $\chi(\mathbb{R}^{11}) \geq 19$.

12. Пусть $B \subset \mathbb{R}^n$ - шар. Докажите, что $f(B) \leq n + 1$. Можно ли разбить шар на n частей меньшего диаметра?

13. (*Теорема Б. Вайссбаха*) Попытайтесь слегка модифицировать доказательство теоремы 6 с тем, чтобы опровергнуть гипотезу Борсука в размерности 560.

14. Пусть V - произвольная совокупность n - мерных (0,1) - векторов. При каких n можно утверждать, что $f(V) \leq n + 1$?

4 Лекция 3. Числа Рамсея

4.1 Определения и формулировки результатов

Наука, которую принято называть "теорией Рамсея", начала бурно развиваться еще в первой половине XX века. Нельзя сказать, чтобы сам Рамсей, опубликовавший замечательную и, по существу, эпохальную статью в 1930 году, был именно основателем науки; и до него различные аспекты проблематики не раз рассматривались многими авторами. Все же результат Рамсея явился одной из главных вех в формировании теории. Если говорить совсем общо, теория Рамсея состоит в отыскании "неизбежных закономерностей" внутри хаоса. Чуть более конкретно можно сформулировать основную задачу этой науки следующим образом: требуется доказать, что, как бы мы ни разбили некоторую совокупность объектов на части, найдется часть, содержащая определенную подструктуру. Одна из классических теорем теории Рамсея принадлежит Б.Л. Ван дер Вардену: *при любом разбиении натурального ряда на конечное число частей в некоторой части есть сколь угодно длинные арифметические прогрессии* (см. [19]). По теории Рамсея имеется обширная литература (см., например, [1], [4], [20], [21]), и мы не станем даже пытаться охватить в этой лекции все многообразие "рамсеевских" задач. Нас будет интересовать именна та задача, которую впервые рассмотрел сам Рамсей в своей основополагающей работе 1930 года. Перейдем же к ее постановке.

Пусть K_n - это полный граф на n вершинах (см. дополнение). Для каждой пары натуральных s, t определим *число Рамсея* $R(s,t)$ как минимальное $n \in \mathbb{N}$, такое, что при любой раскраске ребер K_n в красный и синий цвета либо найдется $K_s \subseteq K_n$, у которого все ребра красные, либо найдется $K_t \subseteq K_n$, у которого все ребра синие. Понятно, что и здесь речь идет о наличии "регулярной подструктуры" в сколь угодно "хаотическом" разбиении множества ребер полного графа на две части ("раскрасить" и "разбить" суть синонимы в нашем контексте). Утверждение о том, что $R(3,3) = 6$, многие знают со школы. Звучит оно обычно так: "среди любых шести человек либо трое друг с другом знакомы, либо трое друг с другом не знакомы". Здесь ребрам красного цвета отвечают, например, пары знакомых людей, а ребрам синего цвета - пары незнакомых. В этой связи удобно переформулировать задачу следующим образом. Мы скажем, что $R(s,t)$ - это минимальное $n \in \mathbb{N}$, такое,

что у любого графа $G = (V, E)$ на n вершинах либо $\omega(G) \geq s$, либо $\alpha(G) \geq t$ (см. дополнение). Отметим, что по понятным причинам число $R(s, s)$ принято называть "диагональным".

Первый же вопрос, который возникает в связи с числами Рамсея, - это вопрос о корректности их определения: почему, собственно, такое минимальное n существует? Сразу ясно, конечно, что проблем нет с величинами $R(1, t) = 1$ ("все крокодилы в реке Дубна красные") и $R(2, t) = t$. Однако отыскание величины $R(3, t)$ - задача уже крайне нетривиальная, и лишь в 1995 году Ким "дожал" ее, установив, что

$$\left(\frac{1}{162} + o(1)\right) \frac{t^2}{\ln t} \leq R(3, t) \leq (1 + o(1)) \frac{t^2}{\ln t}.$$

Разумеется, здесь нет точной формулы, как при $s = 1$, $s = 2$. Тем не менее, результат совершенно выдающийся. Между прочим, нижняя оценка, которая, собственно, и принадлежит Киму, получена с помощью весьма тонких вероятностных соображений. Там и "псевдослучайные графы", и "мартингалы", и многие другие исключительно продвинутые инструменты. Естественно, мы не станем излагать в этой брошюре соответствующее рассуждение, занимающее в оригинальной журнальной статье четверть сотни страниц. Нам еще будет, о чем поговорить. Впрочем, слегка более слабое неравенство, нежели неравенство Кима, мы вкратце обсудим.

Что касается чисел $R(s, t)$, $s \geq 4$, то тут все покрыто мраком. Однако кое-что (и даже, скорее, многое) известно. Например, мы знаем, что $R(s, t)$ всегда существует. Первым, установившим это, был сам Рамсей, но его верхние оценки чересчур громоздки, и мы их не приводим. Зато в 1934 году П. Эрдеш и Г. Секереш доказали следующую теорему.

Теорема 7 (П. Эрдеш и Г. Секереш). *Имеет место рекуррентное неравенство*

$$R(s, t) \leq R(s - 1, t) + R(s, t - 1).$$

Теорема Эрдеша - Секереша имеет несложное доказательство, и мы оставляем его читателю. Нетрудно заметить, исходя из классического комбинаторного тождества $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$, что вкупе с начальными условиями $R(1, s) = R(s, 1) = 1$ рекуррентное неравенство влечет оценку

$R(s,t) \leq C_{s+t-2}^{s-1}$. В частности, диагональное число Рамсея не превосходит величины $C_{2s-2}^{s-1} \sim \frac{4^s}{c\sqrt{s}}$, где $c > 0$ - абсолютная постоянная, легко выводимая из формулы Стирлинга.

Поразительно то, что за прошедшие с момента публикации статьи Эрдеша - Секереша 72 года, неравенство $R(s,s) \leq \frac{4^s}{c\sqrt{s}}$ никто, по сути, не улучшил. Это, несколько позорное, обстоятельство, должно только подстегивать нас к борьбе с проблемой. Впрочем, кое-что доказано. На данный момент самый сильный результат принадлежит Д. Конлону, который показал буквально год назад, что

$$R(s,s) \leq e^{-\gamma \frac{\ln^2 s}{\ln \ln s}} \cdot 4^s, \ \ \gamma > 0.$$

Пафос оценки в том, что функция $e(s) = e^{\gamma \frac{\ln^2 s}{\ln \ln s}}$ стремится к бесконечности быстрее любого полинома (так что эта оценка куда лучше неравенства с корнем из s в знаменателе), а ее слабость обусловлена тем, что как $\sqrt{s}$, так и $e(s)$ - функции, бесконечно малые в сравнении с экспонентой 4^s, ввиду чего в обоих случаях мы могли бы записать неравенство так: $R(s,s) \leq (4 + o(1))^s$. Когда мы работали с проблемами Борсука и Нелсона - Эрдеша - Хадвигера, нас не слишком заботил вид "о малого", а теперь вот поди ж ты - ковыряемся и с ним; не от "хорошей жизни" это. Отметим еще, что фунцкия $e(s)$ совершенно неожиданно проявится в ином контексте ниже. Скорее всего, то будет простое совпадение, да кто знает?

Коль скоро с верхними оценками мы более или менее разобрались, интересовать нас будут отныне оценки нижние. Насколько, так сказать, плох или хорош результат Конлона? Сейчас мы сформулируем две теоремы: результат первой из них, как мы увидим ниже, слегка слабее результата второй; для нас же актуальны будут прежде всего методы доказательства, к каковым мы, безусловно, обратимся чуть позже.

Теорема 8 (П. Эрдеш). *Если n и s таковы, что $C_n^s 2^{1-C_s^2} < 1$, то $R(s,s) > n$.*

Теорема 9 (Дж. Спенсер). *Если n и s таковы, что $e(C_s^2 C_n^{s-2} + 1)2^{1-C_s^2} < 1$, то $R(s,s) > n$. Здесь $e = 2.71...$ - основание натурального логарифма.*

Имею место следствия.

Следствие из теоремы 8. *При $s \geq 3$ выполнена оценка $R(s,s) >$*

$\left[2^{\frac{s}{2}}\right]$.

Следствие из теоремы 9. *Выполнена оценка* $R(s,s) > \frac{\sqrt{2}}{e}(1 + o(1))s2^{\frac{s}{2}}$.

Теорема 8 была доказана Эрдешем в 1947 году, а теорема 9 получена Спенсером лишь примерно 30 лет спустя. Видно, что разница между результатами опять-таки (как и в случае верхних оценок) не слишком велика: и в том, и в другом случае речь идет о неравенстве вида $R(s,s) \geq (\sqrt{2} + o(1))^s$, причем спенсеровское неравенство вовсе никак до сих пор не улучшено. Итак,

$$(\sqrt{2} + o(1))^2 \leq R(s,s) \leq (4 + o(1))^s,$$

или, более точно,

$$\frac{\sqrt{2}}{e}(1 + o(1))s2^{\frac{s}{2}} \leq R(s,s) \leq e^{-\gamma\frac{\ln^2 s}{\ln\ln s}} \cdot 4^s.$$

Любое новое усиление оценок будет здесь огромным достижением!

Теорему 8 мы докажем в §4.2, теорему 9 - в §4.3. Несколько слов о том, как выводить из теорем следствия, мы скажем в §4.4. В §4.5 мы обсудим нижнюю оценку для $R(3,t)$.

4.2 Доказательство теоремы 8

Нам нужно показать, что при нашем n существует раскраска ребер K_n в красный и синий цвета, при которой все полные подграфы K_s графа K_n неодноцветны (т.е. содержат и синие, и красные ребра). Существование раскраски мы докажем с помощью теории вероятностей.

Присвоим каждому ребру тот или иной цвет с вероятностью $\frac{1}{2}$, причем такого рода случайную раскраску ребра мы будем осуществлять независимо от того, как раскрашены любые другие ребра. Иначе говоря, мы считаем все раскраски ребер K_n в два цвета равновероятными, так что, если χ - некоторая конкретная раскраска, то вероятность ее возникновения есть $P(\chi) = 2^{-C_n^2}$.

Пусть $K_n = (V,E)$, где $V = \{1,\ldots,n\}$. Для каждого $S \subset V$, $|S| = s$, введем событие (см. дополнение) A_S, состоящее в том, что все ребра полного графа K_s с множеством вершин S одноцветны. Очевидно,

$P(A_S) = 2^{1-C_s^2}$. Следовательно,

$$P\left(\bigcup_{S\subset V} A_S\right) \leq \sum_{S\subset V} P(A_S) = C_n^s 2^{1-C_s^2}.$$

Условие теоремы дает нам оценку

$$P\left(\bigcup_{S\subset V} A_S\right) < 1,$$

и, стало быть, $P\left(\bigcap\limits_{S\subset V} \overline{A_S}\right) > 0$ (черта означает отрицание события). Но в событии $\bigcap\limits_{S\subset V} \overline{A_S}$ лежат именно те раскраски, которые нам нужны. Раз вероятность этого события положительна, то и соответствующие раскраски существуют. Теорема доказана.

Отметим, что опять-таки ничего не стоило доказать теорему не на вероятностном, а на количественном языке. Тем не менее, соображения теории вероятностей тут уже как нельзя кстати, и мы убедимся в силе метода при доказательстве теоремы 9. Там вероятность раскроется во всей своей красе.

4.3 Доказательство теоремы 9

Здесь мы воспользуемся центральным понятием теории вероятностей - понятием независимости событий. Окажется, что если события $A_1, \ldots,$ A_m "не слишком сильно" зависимы, то при некоторых условиях легко оценить снизу величину $P\left(\bigcap\limits_i \overline{A_i}\right)$; а мы помним, что такая величина крайне полезна при решении нашей задачи. В действительности, от этой величины и деться некуда. Конечно, можно было бы пытаться расписать ее по "формуле включений и исключений" (см., например, [1]), но это весьма неблагодарное и малоперспективное занятие. Вместо него как раз и применяется тот мощный инструмент, о котором сейчас пойдет речь.

Пусть $A_1, \ldots, A_m$ - события на каком-то вероятностном пространстве $(\Omega, \mathcal{F}, P)$. Мы скажем, что A_i "независимо со всеми остальными событиями, кроме, быть может, d", если найдутся события $A_{i_1}, \ldots, A_{i_{m-d}}$,

$d = 0, 1, 2, \ldots$, от совокупности которых A_i не зависит (см. дополнение). Если $d = 0$, то мы приходим к обычной независимости в совокупности, и, чем больше d, тем степень совокупной зависимости наших событий в некотором смысле выше. Имеет место замечательная лемма, которую, вообще-то, следовало бы называть теоремой (да так уж сложилось).

Лемма 8 (Л. Ловас). *Пусть $A_1, \ldots, A_m$ - события на каком-то вероятностном пространстве $(\Omega, \mathcal{F}, P)$. Предположим, $P(A_i) \leq p$ для любого i. Допустим, далее, каждое A_i независимо со всеми остальными событиями, кроме, быть может, d, причем $ep(d+1) < 1$ (здесь $e = 2.71...$). Тогда $P\left(\bigcap_i \overline{A_i}\right) > 0$.*

Лемму 8 называют "Локальной леммой Ловаса". Она была доказана в середине 70-ых годов XX века, и за прошедшие с тех пор 30 лет она нашла великое множество разнообразных применений (см. [4]). Мы не станем доказывать лемму здесь, отсылая читателя к соответствующей литературе. Заметим только, что при желании читатель вполне может доказать лемму и сам. Заметим также, что загадочная константа e в формулировке существенна и ничем меньшим ее в общем случае заменить нельзя. Впрочем, обоснование этого факта совсем нетривиально, и оно-то уж точно выходит за рамки данной брошюры.

Применим локальную лемму к нашей ситуации. У нас в роли событий выступают множества раскрасок A_S, определенные в предыдущем параграфе. Там же мы фактически доказали, что $p = 2^{1-C_s^2}$. Остается разобраться с величиной d. Однако ясно, что любое A_S не зависит от совокупности тех $A_{S'}$, у которых $|S \cap S'| \leq 1$ (просто тогда у соответствующих полных графов нет общих ребер, и легко проверить, что раскраска любого из них никак не влияет на раскраску другого). Отсюда следует, что d есть, напротив, количество таких подмножеств $S' \subset V$ (см. §4.2), что $|S \cap S'| \geq 2$. Понятно, что $d \leq C_s^2 C_n^{s-2}$, и теорема 9 доказана.

Заметим сперва, что оценку величины d мы слегка огрубили. Проверьте самостоятельно (ср. §4.4), что это нас смущать не должно. Далее, мы знаем (и мы убедимся в этом в следующем параграфе), что теорема 9 не многим сильнее теоремы 8. Казалось бы, и что после этого проку в локальной лемме? Стоило ли ее так хвалить? А дело в том, что в данной-то конкретной ситуации зависимостей среди наших событий именно что полно, и это, к сожалению, вредит. В §4.5 мы увидим, что бывает иначе:

к оценке числа $R(3,t)$ локальная лемма куда как более применительна, нежели чем к оценке диагонального числа.

4.4 Обсуждение следствий из теорем 8 и 9

Совсем просто выводится следствие из теоремы 8. В самом деле, $C_n^s < \frac{n^s}{s!}$, и, коль скоро,

$$n = \left[2^{\frac{s}{2}}\right] \leq 2^{\frac{s}{2}},$$

мы имеем $C_n^s < \frac{2^{\frac{s^2}{2}}}{s!}$. Значит,

$$C_n^s 2^{1-C_s^2} < \frac{2^{\frac{s^2}{2}}}{s!} \cdot 2^{1-\frac{s^2}{2}+\frac{s}{2}} = \frac{2^{1+\frac{s}{2}}}{s!}.$$

Нетрудно видеть, что $\frac{2^{1+\frac{s}{2}}}{s!} < 1$ при $s \geq 3$.

Аналитическая возня со вторым следствием носит слегка более противный характер, но, по существу, деятельность абсолютно аналогичная. Мы оставляем ее читателю в качестве несложного и, на наш взгляд, полезного упражнения.

4.5 Обсуждение нижней оценки для $R(3,t)$

В этом параграфе мы обсудим оценку $R(3,t) \geq c\frac{t^2}{\ln^2 t}$, $c > 0$. Эта оценка чуть слабее точного неравенства Кима (см. 4.1), но отличие в логарифм раз в определенном смысле не слишком существенно, а теорему Кима нам здесь все равно не изложить. Для доказательства оценки потребуется более общий вариант локальной леммы Ловаса, нежели тот, который содержится в лемме 8. В свою очередь, лемма 8 окажется частным случаем леммы 9, которую мы сформулируем ниже. Заметим сразу, что без леммы Ловаса ничего лучшего, чем неравенство $R(3,t) \geq ct$, $c > 0$, установить, по сути, нельзя. Таким образом, сейчас мы, наконец, получим весьма значимую апологию метода.

Пусть $A_1, \ldots, A_m$ - события на некотором вероятностном пространстве $(\Omega, \mathcal{F}, P)$. Введем понятие *ориентированного графа (орграфа) зависимостей*, а именно, рассмотрим любой орграф $G = (V, E)$, у которого $V = \{A_1, \ldots, A_m\}$ и каждое событие A_i не зависит от совокупности событий (см. дополнение), с которыми оно не соединено ребрами. Иными словами, если $j_1, \ldots, j_k$ - это все индексы, для которых $\{A_i, A_{j_\nu}\} \notin E$

(подчеркнем, что порядок элементов в паре $\{A_i, A_{j_\nu}\}$ важен), то A_i не зависит от совокупности событий $A_{j_1}, \ldots, A_{j_k}$. Из определения видно, что, вообще говоря, орграф зависимостей задается неоднозначно. Однако зависимости между событиями он отлично улавливает: уж коли A_i и A_j, например, зависимы, то непременно в орграфе появится и ребро $\{A_i, A_j\}$, и ребро $\{A_j, A_i\}$. Более того, существуют тонкие ситуации, когда ребра "туда-обратно" вести не обязательно. Это связано с различиями в понятиях, скажем, попарной и совокупной независимости (см. задачу 21). Для пущей ясности приведем простой и в то же время наиболее актуальный для нас пример. Положим $n = 5$, $s = 3$ в обозначениях §4.2 и рассмотрим события A_S, которые фигурируют в том же параграфе. Занумеруем эти события в следующем порядке:

$$S_1 = \{1,2,3\},\ S_2 = \{1,2,4\},\ S_3 = \{1,2,5\},\ S_4 = \{1,3,4\},\ S_5 = \{1,3,5\},$$

$$S_6 = \{1,4,5\},\ S_7 = \{2,3,4\},\ S_8 = \{2,3,5\},\ S_9 = \{2,4,5\},\ S_{10} = \{3,4,5\}.$$

Понятно (ср. §4.3), что на рисунке 1 изображен наиболее естественный орграф зависимостей для событий $A_{S_1}, \ldots, A_{S_{10}}$. Теперь мы готовы сформулировать общий случай леммы Ловаса.

Лемма 9 (Л. Ловас). *Пусть $A_1, \ldots, A_m$ - события на каком-то вероятностном пространстве $(\Omega, \mathcal{F}, P)$ и $G = (V, E)$ - любой орграф их зависимостей. Предположим, $x_1, \ldots, x_m$ таковы, что $x_i \in [0,1)$, $i = 1, \ldots, m$, и*

$$P(A_i) \le x_i \cdot \prod_{j:\{A_i,A_j\}\in E} (1 - x_j),\ \ i = 1, \ldots, m.$$

Тогда

$$P\left(\bigcap_i \overline{A_i}\right) \ge \prod_{i=1}^{m} (1 - x_i).$$

В лемме дается явная оценка интересующей нас вероятности, но нам, как правило, по-прежнему важно только следствие: $P\left(\bigcap_i \overline{A_i}\right) > 0$. По понятным причинам лемма 8 называется "симметричным случаем" леммы 9: в ней все события равнозначимы с точки зрения оценок их вероятностей. Нетрудно вывести лемму 8 из леммы 9. Нужно рассмотреть

два случая (см. лемму 8): $d = 0$ (события независимы в совокупности) и $d \geq 1$. В первом случае мы сразу же имеем

$$P\left(\bigcap_i \overline{A_i}\right) = \prod_{i=1}^{m}(1 - P(A_i)) \geq \prod_{i=1}^{m}(1-p) = (1-p)^m \geq \left(1 - \frac{1}{e}\right)^m > 0.$$

(Предпоследнее неравенство вытекает из условия $ep = ep(d+1) < 1$.) Во втором же случае мы построим такой орграф зависимостей, что $|\{j : \{A_i, A_j\} \in E\}| \leq d$ (это можно сделать за счет условия леммы 8), и положим $x_i = \frac{1}{d+1} < 1$. Тогда, в самом деле,

$$P(A_i) \leq p < \frac{1}{d+1} \cdot \frac{1}{e} = \frac{x_i}{e} < x_i \left(1 - \frac{1}{d+1}\right)^d \leq x_i \cdot \prod_{j:\{A_i,A_j\}\in E}(1 - x_j),$$

так что применима лемма 9, и все в порядке.

Лемма 9 доказывается с помощью индукции (задача 17), но мы доказательство не приводим.

Как же из леммы 9 получить неравенство $R(3,t) \geq c\frac{t^2}{\ln^2 t}$? Действовать нужно по схеме параграфов 4.2, 4.3. Там раскраски были равновероятными; здесь же имеется очевидный априорный дисбаланс: мы стремимся найти либо синий $K_3 \subset K_n$ ("треугольник"), либо красный $K_t \subset K_n$. Понятно, что неразумно теперь присваивать ребрам цвета с одинаковыми вероятностями. Будем считать, что синий цвет возникает с вероятностью $p \in [0,1]$, а красный - с вероятностью $1-p$, соответственно ("над каждым ребром" подбрасываем монету со смещенным центром тяжести: выпадает решка - красим ребро в красный цвет, выпадает орел - красим его в синий цвет; бросания монеты независимы в совокупности). При этом мы пока не знаем, чему равно p; мы подберем его позже из соображений некоторой оптимизации. Более того, p может вполне зависеть от n.

Введем для каждого $T \subset V = \{1, \ldots, n\}$, $|T| = 3$, (ср. §4.2, 4.3) событие A_T, состоящее в том, что все ребра треугольника с вершинами в T синие; аналогично введем события B_S для $S \subset V$, $|S| = t$ ("все ребра красные"). Очевидно, $P(A_T) = p^3$, $P(B_S) = (1-p)^{C_t^2}$. Построим орграф зависимостей для событий A_T, B_S, соединяя их ребрами (в обоих направлениях) тогда и только тогда, когда соответствующие полные графы имеют хотя бы одно общее ребро (события зависимы). Понятно, что любая вершина вида A_T соединена с $3(n-3) < 3n$ вершинами вида

$A_{T'}$ и с $\leq C_n^t$ вершинами вида B_S; точно так же любая B_S смежна с $C_t^2(n-t) < \frac{t^2 n}{2}$ вершинами A_T и с $\leq C_n^t$ вершинами $B_{S'}$. Допустим, мы нашли такие $p = p(n) \in [0,1]$, $x = x(n) \in [0,1)$ и $y = y(n) \in [0,1)$, что

$$p^3 \leq x(1-x)^{3n}(1-y)^{C_n^t},$$

$$(1-p)^{C_t^2} \leq y(1-x)^{\frac{t^2 n}{2}}(1-y)^{C_n^t}.$$

Тогда применима лемма 9 с

$$m = C_n^3 + C_n^t,\ x_1 = \ldots = x_{C_n^3} = x,\ x_{C_n^3+1} = \ldots = x_m = y.$$

Из леммы 9 следует оценка

$$P\left(\bigcap_T \overline{A_T} \bigcap \bigcap_S \overline{A_S}\right) > 0,$$

которая как раз и означает наличие хотя бы одной раскраски ребер графа K_n, оставляющей неодноцветными и все треугольники, и все K_t в K_n. В итоге $R(3,t) > n$.

Остается оптимально подобрать параметры $p(n), x(n), y(n), t(n)$; оптимальность меряется, конечно, величиной $n(t)$, которая должна быть не меньше $c\frac{t^2}{\ln^2 t}$. Это муторная аналитическая задача, и мы напишем здесь ее решение, не обосновывая его оптимальность. Проверить же, что оно удовлетворяет нашим условиям, большого труда, по-видимому, не составит. Итак:

$$p = \frac{c_1}{\sqrt{n}},\ x = \frac{c_2}{n^{3/2}},\ y = \frac{c_3}{e^{\sqrt{n}\ln^2 n}},\ t = c_4\sqrt{n}\ln n$$

с подходящими $c_1, \ldots, c_4 > 0$. В результате $n = c_5\frac{t^2}{\ln^2 t}$, и оценка доказана.

4.6 Явные нижние оценки диагональных чисел Рамсея

Мы видели в параграфах 4.2, 4.3 и 4.5, сколь мощен и широко применим вероятностный метод. Однако есть одно "но". Дело в том, что всякий раз, апеллируя к теории вероятностей, мы фактически лишь обосновывали существование интересующего нас объекта. В данном случае речь шла, по сути, об отыскании графа G, у которого одновременно малы и

$\omega(G)$, и $\alpha(G)$ (см. §4.1). А как выглядит подобный граф? Да, он где-то есть, но всего графов на n вершинах $2^{C_n^2}$, и поди, отыщи иголку в стоге сена: уже при $n = 10$ перебор необозрим. Конечно, если мы случайно "ткнем" в один из графов, то с огромной вероятностью мы получим то, что нам нужно. Но что, если не получим? Мы хотим определенности, и к тому же нас интересует структура "рамсеевского" графа. Ну, найдем мы такой граф при $n = 10$, найдем при $n = 100$, да ведь все равно не ясно, как устроена общая ситуация. Таким образом, крайне важна "дерандомизация", конструктивизация результатов Эрдеша, Спенсера и пр. Оказывается, на этом пути все совсем печально. Самая лучшая явная нижняя оценка диагонального числа Рамсея была установлена в 1981 году П. Франклом и Р.М. Уилсоном, но она крайне далека от того, к чему мы стремимся.

Теорема 10 (П. Франкл и Р.М. Уилсон). *Можно явно указать граф, свидетельствующий о том, что*

$$R(s,s) > \left(e^{\frac{1}{4}} + o(1)\right)^{\frac{\ln^2 s}{\ln\ln s}}.$$

Вот она где, функция $e(s)$, проявилась-то. Вряд ли, конечно, это нечто большее, нежели совпадение, но все возможно. Ужас же положения в том, что $e(s) = o\left(e^s\right)$, а это значит, что конструктивная оценка несравнимо хуже оценки вероятностной. Тем не менее, это все, что у нас есть; что называется, "чем богаты". И здесь как раз работает наш второй метод - метод линейно-алгебраический.

4.7 Доказательство теоремы 10

Пусть q - простое число. Рассмотрим

$$V = \{\mathbf{x} = (x_1, \ldots, x_{q^3}) : x_i \in \{0,1\},\ x_1 + \ldots + x_{q^3} = q^2\},$$

$$E = \{\{\mathbf{x},\mathbf{y}\} : \mathbf{x},\mathbf{y} \in V,\ (\mathbf{x},\mathbf{y}) \equiv 0 \pmod q\}.$$

Положим $G = (V, E)$. Это и есть искомый граф. Чтобы доказать это, достаточно установить неравенства $\omega(G) \le qC_{q^3}^q$ и $\alpha(G) \le qC_{q^3}^q$. В самом деле, тогда для $s = qC_{q^3}^q$ и $n = C_{q^3}^{q^2}$ как раз выполнено соотношение

$$n = \left(e^{\frac{1}{4}} + o(1)\right)^{\frac{\ln^2 s}{\ln\ln s}},$$

и теорема доказана. Осталось пояснить, откуда взялись неравенства и как возникло соотношение.

Для обоснования неравенств нужно воспользоваться линейной независимостью некоторых многочленов. В случае $\alpha(G)$ можно взять многочлены $F_{\mathbf{x}} \in \mathbb{Z}_q[y_1, \ldots, y_{q^3}]$, $\mathbf{x} \in V$, вида

$$F_{\mathbf{x}}(\mathbf{y}) = \prod_{i=1}^{q-1}(i - (\mathbf{x}, \mathbf{y})), \ \ \mathbf{y} = (y_1, \ldots, y_{q^3}),$$

и обрезать их степени по правилу $y_i^2 = y_i$. В случае же $\omega(G)$ полезны многочлены $F_{\mathbf{x}} \in \mathbb{R}[y_1, \ldots, y_{q^3}]$ вида

$$F_{\mathbf{x}}(\mathbf{y}) = (\mathbf{x}, \mathbf{y})((\mathbf{x}, \mathbf{y}) - q)((\mathbf{x}, \mathbf{y}) - 2q) \cdot \ldots \cdot ((\mathbf{x}, \mathbf{y}) - q^2 + q).$$

Мы оставляем читателю (теперь уже в качестве несложного упражнения) доказательство линейной независимости выписанных полиномов и, как следствие, обоснование неравенств $\alpha(G) \leq qC_{q^3}^q$, $\omega(G) \leq qC_{q^3}^q$.

Теперь несколько слов о выражении n через s. Распишем сперва s:

$$s = qC_{q^3}^q = \frac{q \cdot q^3(q^3-1) \cdot \ldots \cdot (q^3 - q + 1)}{q!} = \frac{q^{3q}\left(1 - \frac{1}{q^3}\right) \cdot \ldots \cdot \left(1 - \frac{q-1}{q^3}\right)}{(q-1)!}.$$

Понятно, что

$$\left(1 - \frac{q-1}{q^3}\right)^q \leq \left(1 - \frac{1}{q^3}\right) \cdot \ldots \cdot \left(1 - \frac{q-1}{q^3}\right) \leq \left(1 - \frac{1}{q^3}\right)^q.$$

В свою очередь, и правая, и левая части неравенства стремятся к единице при $q \to \infty$. Таким образом, $s = \frac{q^{3q}(1+o(1))}{(q-1)!}$. За счет формулы Стирлинга получаем

$$s = \frac{q^{2q}e^{q-1}(1 + o(1))}{\sqrt{2\pi(q-1)}} = q^{2q(1+o(1))}.$$

Аналогично доказывается, что $n = q^{q^2(1+o(1))}$. Далее, $\ln s = 2q(1 + o(1)) \ln q$, так что $\ln \ln s = (1 + o(1)) \ln q$, а $\ln^2 s = 4q^2(1 + o(1)) \ln^2 q$. Следовательно,

$$\left(e^{\frac{1}{4}} + o(1)\right)^{\frac{\ln^2 s}{\ln \ln s}} = q^{q^2(1+o(1))} = n,$$

и все доказано.

Отметим, что мы опять-таки получили результат только при некоторых s. Тем не менее, соображения плотности распределения простых чисел в натуральном ряду (см. §3.2) позволяют справиться с этой проблемой. Попробуйте убедиться в этом самостоятельно.

Задачи.

15. Найдите $R(3,4), R(4,4), R(4,5), R(3,5), R(5,5)$.

16. С помощью локальной леммы Ловаса докажите, что

$$R(4,t) \geq t^{2.5+o(1)}.$$

Какая оценка получится, если не использовать локальную лемму?

17. Попытайтесь доказать локальную лемму.

18. С помощью вероятностных методов попробуйте получить как можно лучшие нижние оценки для произвольного числа Рамсея $R(s,t)$.

19. Что будет, если в доказательстве теоремы 10 положить

$$V = \{\mathbf{x} = (x_1, \ldots, x_{2q^2}) : x_i \in \{0,1\},\ x_1 + \ldots + x_{2q^2} = q^2\},$$

$$E = \{\{\mathbf{x},\mathbf{y}\} : \mathbf{x},\mathbf{y} \in V,\ (\mathbf{x},\mathbf{y}) \equiv 0 \pmod{q}\}?$$

Попробуйте убедиться в том, что параметры в доказательстве подобраны в некотором смысле оптимально.

20. Попытайтесь получить какие-нибудь явные оценки для произвольных чисел $R(s,t)$.

21. Пусть $\Omega = [0,1]^2$, $\mathcal{F}$ состоит из всех множеств $B \subset \Omega$, "площадь" которых мы можем измерить (точнее, $\mathcal{F}$ - сигма-алгебра борелевских подмножеств квадрата), а $P(B)$ - это и есть "площадь" (мера) B. Рассмотрим A_1, A_2, A_3, изображенные на рисунке 2. Приведите пример орграфа зависимостей для этих событий. Каково минимальное число ребер в таком орграфе?

5 Лекция 4. Раскраски гиперграфов

5.1 Определения и формулировки результатов

В этой лекции мы вернемся к изучению свойств совокупностей $\mathcal{M} = \{M_1, \ldots, M_s\}$ подмножеств конечного множества $\mathcal{R}_n$ (см. §2.1), которые, как мы помним, задают гиперграфы $H = (V, E)$ с $V = \mathcal{R}_n$ и $E = \mathcal{M}$. Основная наша задача будет состоять в том, чтобы так или иначе раскрасить вершины гиперграфа (элементы $\mathcal{R}_n$) в два цвета; при этом всякий раз мы будем, по существу, требовать неодноцветности ребер (множеств из $\mathcal{M}$). Прежде всего рассмотрим задачу "об отклонении".

Любую раскраску $\mathcal{R}_n$ в два цвета мы будем интерпретировать как отображение $\chi : \mathcal{R}_n \mapsto \{-1, 1\}$. Для каждого $M \in \mathcal{M}$ рассмотрим величину

$$\chi(M) = \sum_{i \in M} \chi(i),$$

которая равна разности количества "красных" и "синих" вершин в ребре M гиперграфа $(\mathcal{R}_n, \mathcal{M})$. *Отклонением совокупности* $\mathcal{M}$ *в раскраске* χ назовем выражение

$$\operatorname{disc}(\mathcal{M}, \chi) = \max_{M \in \mathcal{M}} |\chi(M)|,$$

а просто под *отклонением* $\mathcal{M}$ будем понимать число

$$\operatorname{disc}(\mathcal{M}) = \min_{\chi} \operatorname{disc}(\mathcal{M}, \chi).$$

Таким образом, речь идет об отыскании ситуации, в которой даже самое "неравномерно раскрашенное" множество в совокупности раскрашено все же не слишком неравномерно. Отметим, что обозначение disc происходит от английского слова "discrepancy", имеющего, впрочем, латинский корень; слово вполне корректно отражает смысл термина.

Замечательным образом при решении задач об отклонении работают и вероятностный, и линейно-алгебраический методы. К сожалению, линейная алгебра, которую следовало бы использовать здесь, требует введения многих дополнительных понятий, выходящих за рамки данного краткого курса лекций. Посему мы изложим лишь вероятностный аспект проблематики. Однако, формулируя результаты, мы скажем, какие из них апеллируют к линейно-алгебраической технологии, и дадим соответствующие ссылки.

Теорема 11. *Пусть* $\mathcal{M} = \{M_1, \ldots, M_s\}$, $M_i \subset \mathcal{R}_n$. *Тогда*

$$\operatorname{disc}(\mathcal{M}) \leq \sqrt{2n \ln(2s)}.$$

Теорема 11 доказывается с помощью несложного вероятностного соображения, которое мы приведем в §5.2. Заметим, что результат не зависит от мощностей множеств $M \in \mathcal{M}$. Тем не менее, модельной ситуацией может служить та, в рамках которой мощность каждого элемента совокупности имеет порядок n. Тогда при не очень больших s (скажем, при $s \leq n^k$, где k любое фиксированное) мы имеем отличную оценку отклонения: ее величина есть всего лишь $c\sqrt{n \ln n}$, что бесконечно мало по сравнению с $|M|$. Мы, так сказать, можем гарантировать, что "почти половина" всех элементов каждого M в некоторой раскраске имеет красный цвет и "почти половина" - синий. При $s = n$ теорема 11 допускает важное усиление.

Теорема 12 (Дж. Спенсер). *Пусть* $\mathcal{M} = \{M_1, \ldots, M_n\}$, $M_i \subset \mathcal{R}_n$. *Тогда*

$$\operatorname{disc}(\mathcal{M}) \leq 6\sqrt{n}.$$

Иными словами, теорема 12, полученная Спенсером в 1985 году, позволяет устранить логарифмический сомножитель под корнем. Эта теорема достаточно нетривиальна. Ее доказательство также носит вероятностный характер, но оно уже для нас немного сложновато, и мы не станем излагать его здесь, сославшись на книгу [4], которая совсем скоро должна выйти по-русски в издательстве "Мир".

Оценка теоремы 12 практически точна.

Теорема 13. *Существует такая совокупность* $\mathcal{M} = \{M_1, \ldots, M_n\}$, $M_i \subset \mathcal{R}_n$, *что*

$$\operatorname{disc}(\mathcal{M}) \geq c\sqrt{n}$$

с некоторым $c > 0$.

Поразительно, но и тут не обошлось как без вероятности, так и без линейной алгебры. Вероятностные соображения мы изложим в §5.3, а линейную алгебру см. в [4]. Отметим, наконец, что с помощью линейно-алгебраического метода доказывается стоящая несколько особняком теорема 14.

Теорема 14 (Т. Фиала). *Положим*

$$\deg \mathcal{M} = \max_{i \in \mathcal{R}_n} |\{M \in \mathcal{M} : i \in M\}|.$$

Если $\deg \mathcal{M} \leq t$, *то*

$$\operatorname{disc}(\mathcal{M}) \leq 2t - 1.$$

Теорема особенно замечательна тем, что мы никак не используем в ней ни величину n, ни величину $s = |\mathcal{M}|$.

Очень близка к задаче об отклонении задача о так называемом "свойстве B", которое в начале 60-ых годов XX века ввел П. Эрдеш. Мы скажем вслед за Эрдешем, что гиперграф $H = (\mathcal{R}_n, \mathcal{M})$ обладает свойством B, если его вершины можно так раскрасить в два цвета, чтобы все его ребра оказались неодноцветными. То есть отныне нас не волнует отклонение: лишь бы хоть сколько-то вершин в каждом ребре имело красный цвет и хоть сколько-то - синий. Мы скажем, что гиперграф k - *равномерен*, коль скоро все его ребра $M \in \mathcal{M}$ имеют одну и ту же мощность k. Определим $m(k)$ как максимум среди таких $m \in \mathbb{N}$, что любой k - равномерный гиперграф (число вершин которого значения не имеет) обладает свойством B.

Теорема 15 (П. Эрдеш). *Имеют место оценки*

$$2^{k-1} \leq m(k) \leq \frac{e \ln 2}{4} k^2 2^k.$$

Обе оценки в теореме получаются с помощью теории вероятностей. Никаких, однако, новых идей в них не содержится, причем нижняя оценка практически тривиальна. Посему мы оставляем теорему 15 читателю в качестве упражнения. Заметим, что теорема Эрдеша неоднократно улучшалась, но всякий раз улучшение касалось оценки $m(k) \geq 2^{k-1}$. Самый сильный результат на данном этапе принадлежит Радхакришнану и Сринивасану: $m(k) \geq c\sqrt{\frac{n}{\ln n}} 2^n$. Этот результат апеллирует к "рандомизированным алгоритмам" в теории вероятностей, и его изложение также выходит за рамки этих лекций. Заметим, что, хотя нынешний зазор между верхними и нижними оценками величины $m(k)$ совсем невелик, устранение его - весьма важная и популярная задача. Однако пока, несмотря ни на какие усилия, полному решению она не поддается.

5.2 Доказательство теоремы 11

Пусть фиксирована произвольная совокупность $\mathcal{M} = \{M_1, \ldots, M_s\}$ на $\mathcal{R}_n$. Нам нужно найти такую раскраску χ, что $|\chi(M)| \leq \sqrt{2n \ln(2s)}$ для любого $M \in \mathcal{M}$. Построим, как обычно, случайную раскраску и докажем, что с положительной вероятностью она обладает надлежащим свойством. В данном случае мы будем считать все раскраски равновероятными, т.е. каждое $\chi(i)$ мы будем, если угодно, рассматривать как случайную величину (см. дополнение), принимающую свои значения ± 1 с вероятностью $\frac{1}{2}$; при этом случайные величины $\chi(1), \ldots, \chi(n)$ независимы в совокупности. Понятно, что $M\chi(i) = 0$, $D\chi(i) = 1$, и применима центральная предельная теорема (см. дополнение). Тогда, полагая $\alpha = \sqrt{2n \ln(2s)}$ и $|M| = k$, имеем

$$P(|\chi(M)| > \alpha) = P\left(\left|\sum_{i \in M} \chi(i)\right| > \alpha\right) =$$

$$P\left(\frac{\left|\sum\limits_{i \in M} \chi(i)\right|}{\sqrt{k}} > \frac{\alpha}{\sqrt{k}}\right) \sim \frac{2}{\sqrt{2\pi}} \int_{-\infty}^{\frac{\alpha}{\sqrt{k}}} e^{-\frac{x^2}{2}} dx.$$

Последний интеграл оценивается сверху величиной

$$2e^{-\frac{\alpha^2}{2k}} \leq 2e^{-\frac{\alpha^2}{2n}} = \frac{1}{s}.$$

Получается, что при достаточно больших n выполнено неравенство

$$P(|\chi(M)| > \alpha) < \frac{1}{s}.$$

Значит,

$$P(\exists\, M \in \mathcal{M} : |\chi(M)| > \alpha) \leq sP(|\chi(M)| > \alpha) < 1,$$

т.е.

$$P(\forall\, M \in \mathcal{M} : |\chi(M)| \leq \alpha) > 0,$$

и при $n \to \infty$ теорема доказана. В действительности, можно установить аналогичные неравенства и при малых n (см., например, [22]), но мы этого делать не будем. На наш взгляд, суть доказательства в применении классического аппарата теории вероятностей, а закапываться в дебри науки сейчас не стоит.

5.3 Доказательство теоремы 13

Здесь мы тоже будем слегка неаккуратны в выкладках, но суть мы постараемся отразить верно. Станем теперь искать не случайную раскраску, а случайную совокупность $\mathcal{M} = \{M_1, \ldots, M_n\}$ подмножеств $\mathcal{R}_n$. Нам хочется, чтобы в итоге для любой раскраски χ отклонение этой совокупности в данной раскраске было больше $c\sqrt{n}$. Построим случайную матрицу U размера $n \times n$, элементы которой суть нули и единицы. Каждому элементу матрицы мы присваиваем то или иное значение с вероятностью $\frac{1}{2}$ независимо от остальных. Понятно, что строки матрицы U вполне можно интерпретировать как подмножества $\mathcal{R}_n$. Конечно, некоторые строки могут совпасть, но нам от этого только лучше: если у маленькой совокупности (различных) множеств большое отклонение, то с увеличением совокупности оно только вырастет.

Пусть χ - произвольная раскраска $\mathcal{R}_n$. Тогда она кодируется вектором $\chi = (\chi(1), \ldots, \chi(n))$. Более того, координаты вектора $(L_1, \ldots, L_n)$, возникающего в результате умножения матрицы U на вектор-столбец χ^T, суть величины $L_i = \chi(M_i)$, коль скоро мы продолжаем считать строки U множествами $M_1, \ldots, M_n \in \mathcal{M}$. Если допустить, что у χ половина координат отрицательна, а половина положительна (что, вообще говоря, конечно, не так), то нетрудно видеть (см. дополнение), что $L_i = \xi - \eta$, где обе величины ξ, η имеют одинаковое биномиальное распределение с $\frac{n}{2}$ испытаниями и "вероятностью успеха" $\frac{1}{2}$. Можно показать, что асимптотически распределение L_i нормально с параметрами 0 и $\frac{\sqrt{n}}{2}$ (см. дополнение). В этом случае мы выбираем λ так, чтобы

$$\frac{1}{\sqrt{2\pi}} \int\limits_{-\lambda}^{\lambda} e^{-\frac{x^2}{2}} dx < \frac{1}{2},$$

и тогда

$$P(|L_i| < \lambda\sqrt{n}/2) < \frac{1}{2}.$$

На самом деле, то же неравенство выполнено и для χ с неодинаковыми количествами отрицательных и положительных координат, но мы не станем обосновывать здесь данный тезис: заинтересованный читатель сам без труда сделает это. Для нас главное, что величины L_i независимы в совокупности (это обусловлено независимостью выбора элементов ма-

трицы U), а значит,

$$P(\forall\, i\ |L_i| < \lambda\sqrt{n}/2) < \left(\frac{1}{2}\right)^n.$$

Отсюда следует, что

$$P(\exists\, \chi\ \forall\, i\ |L_i| < \lambda\sqrt{n}/2) < 1,$$

т.е.

$$P(\forall\, \chi\ \exists\, i\ |L_i| \geq \lambda\sqrt{n}/2) > 0,$$

и теорема доказана.

Задачи.

22. Найдите $m(2), m(3), m(4)$.

23. Докажите оценку Эрдеша $m(k) \geq 2^{n-1}$.

24. С помощью локальной леммы Ловаса докажите следующую теорему: пусть H - k - равномерный гиперграф, у которого каждое ребро пересекается с не более, чем d, другими ребрами; тогда при $e(d+1) \leq 2^{k-1}$ гиперграф обладает свойством B.

6 Дополнение

6.1 Теория вероятностей

6.1.1 Классическое определение вероятности и схема Бернулли

Классическое определение вероятности имеет многовековую историю, и интуитивно оно понятно каждому. Два события *несовместны*, если одно исключает другое. Например, монета при случайном падении на стол не может одновременно выпасть "орлом" и "решкой" кверху. События $A_1, \ldots, A_n$ образуют *полную группу*, если хотя бы одно из них обязательно произойдет: события "монета упала решкой кверху" и "монета упала кверху орлом" образуют полную группу (на ребро монета

не встанет). События считаются *равновероятными* из интуитивных соображений. Скажем, естественно предположить, что при случайном извлечении шара из урны, содержащей один белый и один черный шар, вероятность достать черный шар равна вероятности вытянуть белый. Пусть $\omega_1, \ldots, \omega_n$ образуют полную группу Ω попарно несовместных равновероятных событий (например, $n = 6$, ω_i - "на игральной кости, сделанной из однородного материала, выпало i очков"). Тогда вероятность $P(\omega_i)$ полагается равной $\frac{1}{n}$. События $\omega_1, \ldots, \omega_n$ называются *элементарными*; из них, как из кирпичиков, складываются более сложные события: $A = \omega_{i_1} \cup \ldots \cup \omega_{i_k}$. Понятно, что вероятность $P(A)$ должна равняться $\frac{k}{n}$. Это просто доля тех (равновероятных) событий, которые "благоприятствуют" выполнению A. Скажем, событию A - "на игральной кости выпало четное число очков" - благоприятствуют три элементарных события, и потому $P(A) = \frac{3}{6} = \frac{1}{2}$. Множество всех событий обозначают буквой $\mathcal{F}$. Очевидно, здесь $|\mathcal{F}| = 2^n$. Возникает так называемая "вероятностная тройка" $(\Omega, \mathcal{F}, P)$, именуемая также *вероятностным пространством*. Нетрудно проверить, исходя из определения, что $P : \mathcal{F} \mapsto [0,1]$ обладает некоторым набором естественных свойств типа $P(\Omega) = 1$, $P(\emptyset) = 0$, $P\left(A_1 \bigsqcup \ldots \bigsqcup A_n\right) = P(A_1) + \ldots + P(A_n)$, $P(A_1 \cup \ldots \cup A_n) \leq P(A_1) + \ldots + P(A_n)$ и т.д.

Простейшее обобщение классического определения состоит в том, чтобы считать элементарные события неравновероятными. Мы берем тройку $(\Omega, \mathcal{F}, P)$, в которой $|\Omega| = n$, $|\mathcal{F}| = 2^n$, но $P(\omega_i) = p_i$. Тем не менее, свойства вероятности мы сохраняем и, в частности, требуем, чтобы $p_1 + \ldots + p_n = 1$. Наиболее важным примером служит здесь пространство $(\Omega, \mathcal{F}, P)$ с $\Omega = \{0,1\}^n$, $P(\omega) = p^{|\{i:\, x_i = 1\}|} q^{|\{i:\, x_i = 0\}|}$, коль скоро $q = 1 - p$, $p \in [0,1]$, $\omega = (x_1, \ldots, x_n)$. Часто говорят при этом о *схеме испытаний Бернуллли*. Модель такова: n раз бросаем на стол монету со "смещенным центром тяжести" (p - вероятность решки ("успеха") из "физических" соображений), и, если при i - ом бросании (в i - ом "испытании") выпадает решка, то кладем $x_i = 1$; иначе полагаем $x_i = 0$.

Подробности см. в [22], [23], [24].

6.1.2 Геометрические вероятности и общее понятие вероятностного пространства

Иногда в роли события, вероятность которого мы хотим измерить, выступает множество точек в $\mathbb{R}^n$. Например, возможна такая задача. Два

человека договорились встретиться на остановке между двумя и тремя часами. Человек приходит, ждет 15 минут и, если не дожидается товарища, покидает остановку. Какова вероятность встречи? Разумно время прихода первого человека отмечать точкой x из отрезка $[0,1]$ на оси абсцисс, а время прихода второго человека - аналогичной точкой y на оси ординат. Тогда условием встречи будет попадание точки (x,y) в область, изображенную на рисунке 3. Довольно ясно, что здесь пространством элементарных событий следует считать $\Omega = [0,1]^2$, а наше событие A есть тогда множество с рис. 3. Основная тонкость состоит в том, что теперь Ω бесконечно и нам бы стоило полагать $P((x,y)) = 0$. Как же тогда найти $P(A)$? Это не совсем тривиальный вопрос. Грубо говоря, задают $P(A)$ равной "площади" (или, вернее, *мере*) множества A (см. [25]). В этом случае возможные события становятся подчас "невероятными": $P((x,y) \in \{(0,0),(0,1),(1,0),(1,1)\}) = 0$. Однако такое определение тоже интуитивно понятно, а главное, в нем сохраняются важнейшие свойства вероятности, часть из которых мы уже перечисляли. В общем случае рассматривают вероятностное пространство $(\Omega, \mathcal{F}, P)$, в котором $\Omega \subset \mathbb{R}^n$ - множество, имеющее конечный объем (меру μ), $\mathcal{F}$ - некоторая совокупность подмножеств Ω, обладающих естественными свойствами типа $A \in \mathcal{F}$ имеет меру или $A \cap B \in \mathcal{F}$ и $A \cup B \in \mathcal{F}$, коль скоро $A, B \in \mathcal{F}$, и $P(A) = \frac{\mu(A)}{\mu(\Omega)}$.

Общее понятие вероятностного пространства введено А.Н. Колмогоровым. Оно унифицирует все прежние разрозненные определения. В нем Ω - произвольное (сколь угодно сложное) множество объектов, $\mathcal{F}$ - совокупность подмножеств Ω, удовлетворяющих естественным аксиомам, (оно называется *сигма-алгеброй событий*) и $P : \mathcal{F} \mapsto [0,1]$ - *вероятностная мера*, также удовлетворяющая определенным аксиомам, которые повторяют основные и ранее интуитивно ясные свойства вероятности.

Подробности см. в [22], [23], [24].

6.1.3 Независимость случайных величин и событий

События A, B называются *независимыми*, если $P(A \cap B) = P(A)P(B)$. События $A_1, \ldots, A_n$ *независимы в совокупности*, если для любого набора индексов $1 \leq i_1 < \ldots < i_k \leq n$ выполнено $P(A_{i_1} \cap \ldots \cap A_{i_k}) = P(A_{i_1}) \cdot \ldots \cdot P(A_{i_k})$. *Условной вероятностью* события A относительно события B ($P(B) \neq 0$) называется величина $P(A|B) = \frac{P(A \cap B)}{P(B)}$; иначе $P(A|B) = 0$.

Событие A *не зависит от совокупности* событий $B_1, \ldots, B_n$, если при всех $1 \le i_1 < \ldots < i_k \le n$ мы имеем $P(A|B_{i_1} \cap \ldots \cap B_{i_k}) = P(A)$.

Пусть $\Omega = B_1 \bigsqcup \ldots \bigsqcup B_n$, а A - событие. Тогда

$$P(A) = \sum_{i=1}^{n} P(A|B_i)P(B_i)$$

(*формула полной вероятности*).

Функция $\xi : \Omega \mapsto \mathbb{R}$ называется *случайной величиной*, если для любого $x \in \mathbb{R}$ выполнено $\{\omega : \xi(\omega) < x\} \in \mathcal{F}$. Если Ω конечно, то случайная величина - это любая функция на Ω. Случайные величины ξ, η *независимы*, коль скоро независимы события $\{\omega : \xi(\omega) < x\}$, $\{\omega : \eta(\omega) < y\}$ при всех $x, y \in \mathbb{R}$. Аналогично определяется независимость случайных величин в совокупности и независимость случайной величины от совокупности случайных величин.

Подробности см. в [22], [23], [24].

6.1.4 Распределения случайных величин, моменты, центральная предельная теорема

Функция $F_\xi(x) = P(\xi < x) = P(\{\omega : \xi < x\})$ называется *функцией распределения* случайной величины ξ. Если ξ принимает конечное или счетное множество значений, то для задания F_ξ достаточно знать величины $P(\xi = x)$. Такая ξ называется *дискретной*. Иногда существует такая функция $p_\xi(t) \ge 0$, что $F_\xi(x) = \int\limits_{-\infty}^{x} p_\xi(t)dt$. В этом случае говорят, что ξ *абсолютно непрерывна*, а $p_\xi(t)$ - ее *плотность*. Бывают и более хитро распределенные случайные величины, но нам они не нужны.

Примером дискретной величины служит величина *биномиальная*, т.е. такая $\xi : \Omega \mapsto \{0, 1, \ldots, n\}$, что $P(\xi = k) = C_n^k p^k q^{n-k}$, коль скоро $q = 1-p$, $p \in [0, 1]$. Ее интерпретируют обычно как число решек, выпавших в схеме из n испытаний Бернулли.

Самая важная абсолютно непрерывная величина называется *нормальной*. Пишут $\xi \sim N(\mu, \sigma^2)$. У нее

$$p_\xi(t) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(t-\mu)^2}{2\sigma^2}}.$$

Математическое ожидание дискретной величины $\xi : \Omega \mapsto \{x_1, \ldots\}$ - это ее "взвешенное среднее", т.е. величина $M\xi = \sum\limits_{i=1}^{\infty} x_i P(\xi = x_i)$. В случае абсолютно непрерывной ξ полагаем $M\xi = \int\limits_{-\infty}^{\infty} x p_\xi(x) dx$. *Дисперсией* случайной величины ξ называют число $D\xi = M(\xi - M\xi)^2$ (среднее квадратичное отклонение величины от своего среднего значения). *Момент k - ого порядка* - это $M\xi^k$. Легко видеть, что $M\xi = \mu$, $D\xi = \sigma^2$, коль скоро $\xi \sim N(\mu, \sigma^2)$. Выполнена замечательная

Теорема 16 (Центральная предельная теорема). *Пусть $\xi_1, \ldots,$ $\xi_n, \ldots$ - независимые в совокупности и одинаково распределенные случайные величины. Предположим, $M\xi_i = \mu$, $D\xi_i = \sigma^2$. Тогда для любых $a, b \in \mathbb{R}$*

$$P\left(a \leq \frac{\xi_1 + \ldots + \xi_n - \mu n}{\sqrt{n}\sigma} \leq b\right) \sim \frac{1}{\sqrt{2\pi}} \int_a^b e^{-\frac{t^2}{2}} dt, \quad n \to \infty.$$

Смысл теоремы такой: если некоторое (числовое) наблюдение складывается из независимых одинаковых факторов, то асимптотически оно распределено нормально. Это, можно сказать, универсальный закон природы.

Подробности см. в [22], [23], [24].

6.2 Линейная алгебра

Полем (говоря неформально) называется некоторая совокупность объектов, на которой введены операции "сложения" и "умножения", обладающие определенным набором аксиоматических свойств типа коммутативности $x+y = y+x$, $xy = yx$, ассоциативности и дистрибутивности; кроме того, в поле есть "нулевой" и "единичный" элементы ($x + 0 = x$, $x \cdot 1 = x$), а также "обратные" элементы (подробности см. в [26]). Важнейшими для нас примерами полей являются поле действительных чисел $\mathbb{R}$, поле рациональных чисел $\mathbb{Q}$ и поле $\mathbb{Z}_p$, элементы которого суть классы вычетов по модулю p. Последнее поле конечное (см. [27]).

Над данным полем F можно определить *линейное пространство* V. Говоря опять-таки неформально, V есть множество "векторов", которые разрешается "складывать" между собой и умножать на "скаляры",

принадлежащие F; при этом снова постулируется некоторый набор естественных аксиом типа коммутативности и линейности ($\lambda(x+y) = \lambda x + \lambda y$, $\lambda \in F$, $x, y \in V$); в пространстве всегда есть "нулевой" элемент. В частности, $\mathbb{R}^n$ - это линейное пространство над полем $\mathbb{R}$, и аналогично вводятся $\mathbb{Q}^n$ или $\mathbb{Z}_p^n$ (см. [26]).

Еще над полем F определяют пространства *многочленов (полиномов)*, зависящих от некоторого числа переменных $y_1, \ldots, y_n$. Эти пространства обозначают $F[y_1, \ldots, y_n]$. Их элементы имеют вид

$$\sum c_{i_1,\ldots,i_k} y_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot y_{i_k}^{\alpha_{i_k}};$$

здесь $c_{i_1,\ldots,i_k} \in F$; выражения $y_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot y_{i_k}^{\alpha_{i_k}}$ называются *одночленами (мономами)*.

Если $x_1, \ldots, x_n$ - векторы в некотором линейном пространстве V, а $c_1, \ldots, c_n$ - скаляры из соответствующего поля, то сумма $c_1x_1 + \ldots + c_nx_n$ носит название *линейной комбинации данных векторов с данными "числовыми" коэффициентами*. Если равенство $c_1x_1 + \ldots + c_nx_n = 0$ выполняется исключительно для $c_1 = c_2 = \ldots = c_n = 0$, $c_i \in F$, то говорят, что векторы $x_1, \ldots, x_n$ *линейно независимы над полем* F. *Базис* пространства - это такой набор B линейно независимых векторов в нем, что любой другой его вектор представляется в виде линейной комбинации векторов из B. Можно показать, что во всех базисах одно и то же количество элементов. Оно же равно числу векторов в максимальной линейно независимой системе элементов из V. *Размерностью* пространства называют количество элементов в любом его базисе. Таким образом, если в пространстве дан набор линейно независимых векторов, то их число не превосходит размерности пространства (см. [26], [28]). Заметим, впрочем, что бывают и бесконечномерные пространства - скажем, таково пространство непрерывных функций на данном отрезке. Однако мы работаем лишь с конечными базисами.

Пространство *метрическое*, если в нем введено расстояние (*метрика*) $\rho(x, y)$ (см. [29]), и *гильбертово*, если расстояние можно определить с помощью *скалярного произведения*. Например, $\mathbb{R}^n$ - гильбертово пространство, и потому в нем есть стандартное скалярное произведение

$$(\mathbf{x}, \mathbf{y}) = x_1y_1 + \ldots + x_ny_n, \ \ \mathbf{x} = (x_1, \ldots, x_n), \ \mathbf{y} = (y_1, \ldots, y_n);$$

при этом (евклидово) расстояние выражается в виде

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

6.3 Теория графов

Граф - это пара $G = (V, E)$. Здесь V - некоторое (возможно, бесконечное) множество объектов, называемых *вершинами*, а E - произвольная совокупность пар объектов из V, именуемых *ребрами*. Терминология естественна, т.к. графы принято изображать на плоскости, сопоставляя вершинам точки, а ребрам отрезки, эти точки соединяющие. Обычно предполагают, что у графа нет "кратных ребер", т.е. что каждая пара (x, y) встречается в E не более одного раза. Предполагают, далее, что $(x, x) \notin E$ (нет "петель") и что $(x, y) = (y, x)$. Если от последнего свойства отказаться, то возникает *ориентированный граф (орграф)*, который изображают так, как показано на рисунке 4: порядок элементов в ребре задается стрелочкой, идущей от первой его вершины ко второй. Граф $G' = (V', E')$ называется *подграфом* в графе $G = (V, E)$, коль скоро $V' \subseteq V$, $E' \subseteq E$.

Граф называется *полным*, если в нем проведены все возможные ребра; у полного графа на n вершинах C_n^2 ребер; такой граф обозначают K_n. Полный подграф некоторого графа называется его *кликой*. Количество вершин в самой большой клике графа G обозначается $\omega(G)$. Можно, напротив, рассматривать *независимые подмножества* множества вершин графа, т.е. подмножества, элементы которых попарно не соединены ребрами. *Числом независимости* графа называется величина $\alpha(G)$, равная максимуму мощностей независимых подмножеств множества вершин графа.

Подробности см. в [30], [31], [32].

6.4 Анализ

Говорят, что функция $f(x)$ есть "о малое" от функции $g(x)$ при $x \to x_0$ и пишут $f(x) = o(g(x))$, коль скоро $\left|\frac{f(x)}{g(x)}\right| \to 0$ при $x \to x_0$. Например, $n = o(n^2)$ или $e^{\sqrt{n}} = o\left(e^n\right)$, или $\frac{1}{\ln n} = o(1)$; можно написать также $e^{\sqrt{n}} = e^{o(n)}$. Если мы записываем неравенство в виде $f(x) \leq (1 + o(1))g(x)$, то мы подразумеваем, что существует функция $h(x) = o(1)$, с которой выполнено $f(x) \leq (1 + h(x))g(x)$. Аналогичным образом мы понимаем неравенство типа $f(n) \leq (1.185 + o(1))^n$. Здесь опять-таки найдется $h(n) = o(1)$, такая, что $f(n) \leq (1.185 + h(n))^n$. Тонкость в том, что в последнем случае нельзя утверждать, будто $(1.185 + o(1))^n \sim 1.185^n$

($f(x) \sim g(x)$, если $\left|\frac{f(x)}{g(x)}\right| \to 1$). Например, $\left(2+\frac{2}{n}\right)^n \sim e2^n$; однако сама константа, стоящая в основании экспоненты $(\gamma+o(1))^n$ с ростом n только уточняется.

Подробности можно найти в [33].

Список литературы

[1] М. Холл, *Комбинаторика*, Москва, "Мир", 1970.

[2] Ф. Харари, Э. Палмер, *Перечисление графов*, Москва, "Мир", 1977.

[3] П. Эрдеш, Дж. Спенсер, *Вероятностные методы в комбинаторике*, Москва, "Мир", 1976.

[4] N. Alon and J. Spencer, *The probabilistic method*, Wiley - Interscience Series in Discrete Math. and Optimization, Second Edition, 2000.

[5] В.Ф. Колчин, *Случайные графы*, Москва, Физматлит, 2002.

[6] L. Babai and P. Frankl, *Linear algebra methods in combinatorics*, Part 1, Department of Computer Science, The University of Chicago, Preliminary version 2, September 1992.

[7] N. Alon, L. Babai, and H. Suzuki, *Multilinear polynomials and Frankl - Ray-Chaudhuri - Wilson type intersection theorems*, J. Comb. Th., Ser. A, 58 (1991), 165 - 180.

[8] А.М. Райгородский, *Проблема Борсука и хроматические числа некоторых метрических пространств*, Успехи Матем. Наук, Т. 56 (2001), Вып. 1, стр. 107 - 146.

[9] C. Godsil, *Algebraic combinatorics*, Chapman and Hall/CRC, 1993.

[10] А.М. Райгородский, *Хроматические числа*, Москва, МЦНМО, 2003.

[11] А.М. Райгородский, *Проблема Борсука*, Москва, МЦНМО, 2006.

[12] A.M. Raigorodskii, *The Borsuk partition problem: the seventieth anniversary*, Mathematical Intelligencer, V. 26 (2004), N4, 4 - 12.

[13] В.Г. Болтянский и И.Ц. Гохберг, *Теоремы и задачи комбинаторной геометрии*, Москва, "Наука", 1965.

[14] V.G. Boltyanski, H. Martini, and P.S. Soltan, *Excursions into combinatorial geometry*, Universitext, Springer - Verlag, Berlin Heidelberg, 1997.

[15] A. Soifer, *Mathematical coloring book*, Center for Excellence in Mathematical Education, 1997.

[16] А.М. Райгородский, *О числах Борсука и Эрдеша - Хадвигера*, Матем. заметки, Т. 79, N6 (2006), 913 - 924.

[17] К. Прахар, *Распределение простых чисел*, "Мир", Москва, 1967.

[18] М.Л. Гервер, *О разбиении множеств на части меньшего диаметра: теоремы и контрпримеры*, Матем. просвещение (Москва, МЦНМО), Сер. 3, 1999, N3, 168 - 183.

[19] А.Я. Хинчин, *Три жемчужины теории чисел*, Москва, "Эдиториал УРСС", 2004.

[20] Р. Грэхэм, *Начала теории Рамсея*, Москва, "Мир", 1984.

[21] B. Bollobás, *Random Graphs*, Cambridge Univ. Press, Second Edition, 2001.

[22] В. Феллер, *Введение в теорию вероятностей и ее приложения*, Москва, "Мир", 1967.

[23] Б.В. Гнеденко, *Курс теории вероятностей*, Москва, Физматлит, 1961.

[24] А.Н. Ширяев, *Вероятность*, Москва, "Наука", 1989.

[25] А.Н. Колмогоров, С.В. Фомин, *Элементы теорий функций и функционального анализа*, Москва, Физматлит, 2004.

[26] А.И. Кострикин, *Введение в алгебру*, Москва, Физматлит, 2004.

[27] Р. Лидл, Г. Нидеррейтер, *Конечные поля*, Москва, "Мир", 1988.

[28] В.В. Федорчук, *Курс аналитической геометрии и линейной алгебры*, НЦ ЭНАС, 2001.

[29] В.А. Скворцов, *Примеры метрических пространств*, Москва, МЦНМО, 2002.

[30] Ф. Харари, *Теория графов*, Москва, "Мир", 1973.

[31] О. Оре, *Графы и их применение*, Москва, "Наука", 1965.

[32] Р. Дистель, *Теория графов*, Новосибирск, Изд-во Инст. Мат., 2002.

[33] Г.М. Фихтенгольц, *Курс дифференциального и интегрального исчисления*, Москва - Ижевск, Физматлит, 2003.