Разностные множества, конечные геометрии, матрицы Царанкевича и экстремальные графы

С. Б. Гашков

§ 1. Введение

В статье будет рассказано о некоторых интересных понятиях и результатах современной комбинаторики. Надеемся, что они будут интересны читателю хотя бы потому, что в неявном виде появляются во многих задачах, предлагавшихся на олимпиадах для школьников. Такие задачи рассыпаны по всему следующему далее тексту [1)]. К большинству из них даны указания, а иногда и полные решения. Начнём со следующей задачи.

Задача 1 (XLIV Московская математическая олимпиада (1981), 9 кл., задача 5). У правильного 1981-угольника отмечены 64 вершины. Доказать, что существует трапеция с вершинами в отмеченных точках.

Указание. Рассмотрите все возможные прямые, продолжающие стороны и диагонали правильного n-угольника. Они разбиваются на n множеств («направлений») так, что все прямые одного направления параллельны, а прямые разных направлений — нет. Пусть в n-угольнике выделены k вершин. Если $k(k-1)/2 > n$, то согласно принципу Дирихле найдутся две параллельные прямые, пересекающие n-угольник в выделенных четырёх вершинах. Они и образуют трапецию (причём равнобокую), так как она симметрична относительно диаметра описанного вокруг n-угольника круга, перпендикулярного её основаниям; прямоугольником она быть не может, так как тогда её диагонали были бы тоже диаметрами этого круга, что невозможно в правильном нечётноугольнике.

Задача 1 равносильна следующей комбинаторной задаче. Пусть среди чисел от 0 до 1980 выбрано 64 числа. Тогда обязательно сумма по модулю 1981 каких-то двух различных выбранных чисел равна сумме по модулю

[1)] Некоторые задачи реально на олимпиадах не появлялись, но вполне могли бы быть.

1981 какой-то другой пары выбранных чисел[2]. Для того чтобы убедиться в равносильности этих задач, достаточно занумеровать все вершины многоугольника по кругу. Другая равносильная формулировка: разность по модулю 1981 каких-то двух выбранных чисел равна разности по модулю 1981 каких-то двух других выбранных чисел. Действительно, если $a+b=c+d \bmod n$, то $a-c=d-b \bmod n$ и обратно. Возникает интересная и очень трудная задача: можно ли число 64 заменить меньшим, точнее: какое наибольшее подмножество можно выбрать в множестве $\{0,\dots,1980\}$ так, чтобы в нём все попарные разности были разными. Такие множества называются *разностными* и изучаются в комбинаторике.

Если заменить 1981 произвольным числом n, то верхнюю оценку для максимальной мощности k такого разностного множества можно получить в виде

$$k \leqslant \left\lfloor \frac{\sqrt{8n+1}+1}{2} \right\rfloor,$$

где $\lfloor\cdot\rfloor$ обозначает целую часть («пол»). Действительно, рассмотрим все различные попарные суммы. Их ровно $k(k-1)/2$ штук. По условию этих сумм должно быть не больше n, т. е. должно выполняться неравенство $k(k-1) \leqslant 2n$, из которого следует, что $k \leqslant (\sqrt{8n+1}+1)/2$. Можно наложить в определении разностного множества и более сильное ограничение: разности[3] должны быть разными у любых двух упорядоченных пар чисел, даже если эти две пары содержат общее число. Таким образом, должны быть различны разности $a-b$ и $b-c$, и даже разности $a-b$ и $b-a$. Очевидно, это условие равносильно тому, что различными должны быть любые попарные суммы, например, разрешается паре состоять из равных чисел, т. е. для любых чисел a, b, c не должно выполняться равенство $a+b=2c$, а в случае чётного n не должно быть разности $a-b=n/2$. Тогда задача построения максимального разностного множества будет равносильна задаче выбора в правильном n-угольнике максимального множества вершин, среди которых не только не найдётся трапеции, но и не найдётся вершин, образующих равнобедренный треугольник (который можно рассматривать как вырожденную трапецию), а в случае чётного n ещё и не должно быть двух диаметрально противоположных вершин.

Задача 2 (вариант задачи 1). В правильном n-угольнике при нечётном n отмечено $\lceil(\sqrt{8n+1}+1)/2\rceil$ вершин. Доказать, что существует трапеция или равнобедренный треугольник с вершинами в этих точках.

[2] Операция $a+b \bmod n$ называется сложением по модулю n, если её результат равен остатку от деления обычной суммы $a+b$ на n. Аналогично определяется и вычитание по модулю n.

[3] Далее слова «по модулю n» опускаем.

Если разностное множество состоит из k чисел, то число $k(k-1)$ разностей по модулю n, образованных разными парами, должно быть не больше $n-1$, т. е. должно выполняться условие $k(k-1)+1 \leqslant n$. Вопрос, бывают ли разностные множества, у которых $k(k-1)+1=n$, представляет большой интерес. У этих множеств каждое число от 1 до $n-1$ представляется в виде разности по модулю n каких-то двух чисел из данного множества, причём единственным способом. На самом деле в комбинаторике обычно именно эти множества и называются *циклическими разностными множествами*. Ясно, что такие множества существуют только при нечётном n. Равносильная формулировка такая: если для данного множества M рассмотреть его циклические сдвиги $M+a \bmod n$, где $a=1,\ldots,n-1$, то любые два из этих сдвигов (в том числе и само $M=M+0$) имеют ровно одно общее число, и каждая пара чисел (x,y) принадлежит (ровно одному) сдвигу. Построенная система из $n=q^2+q+1$ множеств, $q=k-1$, обладает следующими свойствами. Каждое множество состоит из $q+1=k$ чисел, каждая пара различных чисел из множества $\{0,\ldots,n-1\}$ принадлежит ровно одному множеству. Указанное семейство множеств называется *конечной проективной плоскостью порядка* q. Известно, что если q есть степень простого числа, то такие плоскости действительно существуют, в частности в множестве $\{0,\ldots,1892\}$ существует[4)] циклическое разностное множество из 44 чисел, а множества большего размера не существует. Приводить пример упомянутого разностного множества здесь неуместно, так как он достаточно громоздкий и проверка его правильности затруднительна. Вместо него приведём два примера циклических разностных множеств при $n=13$: это множества $\{0,1,3,9\}$ и $\{0,1,4,6\}$.

Что будет, когда n не равно степени простого, до конца не ясно. Известно, что если q равно $4t+1$ или $4t+2$ и при этом нельзя представить q в виде суммы квадратов двух целых чисел, то такого множества не существует[5)]. Например, при $q=6$ эти условия не выполняются, т. е. в множестве $\{0,\ldots,42\}$ нет циклического разностного множества из 7 чисел. Это означает, что среди любых 7 вершин правильного 43-угольника найдётся либо трапеция, либо её вырожденный случай — равнобедренный треугольник.

Задача 3. В правильном 31-угольнике отмечены 7 вершин. Доказать, что существует трапеция или равнобедренный треугольник с вершинами в этих точках. Можно выделить 6 вершин так, что не существует ни трапеции, ни равнобедренного треугольника с вершинами в этих точках.

[4)] Согласно теореме Зингера, сформулированной далее.

[5)] Теорема Брука и Райзера, см. [13, 14].

§ 2. Разностные множества, конечные геометрии и блок-схемы

Введём понятия, о которых идёт речь в заголовке.

Блок-схемой[6] называется такое размещение v различных элементов по b блокам из k различных элементов каждый, что каждый элемент принадлежит ровно r блокам и каждая пара различных элементов появляется точно в λ блоках. Если $r = b$, то схема называется *симметричной*.

Задача 4. Докажите, что $bk = vr$, $r(k-1) = \lambda(v-1)$. Докажите, что в определении блок-схемы условие принадлежности каждого элемента равному числу блоков излишне (т. е. его можно вывести из остальных условий определения).

Множество $D = \{a_1, \dots, a_k\}$ из k различных элементов множества $\{0, \dots, v-1\}$ называется (v, k, λ)-*циклическим разностным множеством*, если для всякого $d \neq 0$ найдётся ровно λ таких упорядоченных пар (a_i, a_j), что $a_i - a_j \bmod v = d$. Связь таких множеств с блок-схемами указывает

Теорема 1. *Множество $D = \{a_1, \dots, a_k\} \subset \{0, 1, \dots, v-1\}$ является циклическим (v, k, λ)-разностным множеством тогда и только тогда, когда множества $B_i = \{a_1 + i \bmod v,\ \dots,\ a_k + i \bmod v\} \subset \{0, 1, \dots, v-1\}$, где $i = 0, \dots, v-1$, являются блоками*

Множество называется *конечной проективной плоскостью*, если выполнены следующие условия[7] (обычно называемые аксиомами).

Ах1: *для любых двух различных точек существует, причём ровно одна, прямая, через них проходящая*;

Ах2: *любые две прямые имеют ровно одну общую точку*;

Ах3: *существуют четыре точки, из которых любые три не лежат на одной прямой*.

Изучением вопросов, связанных с проективными плоскостями, московские математики заинтересовались после войны, поэтому неудивительно, что на московской олимпиаде уже в 1946 г. во всех классах с 7 по 10 предлагалась следующая задача, в которой речь шла фактически о конечных проективных плоскостях.

Задача 5 (IX Московская математическая олимпиада (1946), второй тур, 7–8 кл., задача 5). Автобусная сеть города устроена следующим образом:

1) с любой остановки на любую другую остановку можно попасть без пересадки;

[6] Сейчас более моден термин 2-дизайн.

[7] Есть и другие равносильные аксиоматизации.

2) для любой пары маршрутов найдётся, и притом единственная, остановка, на которой можно пересесть с одного из этих маршрутов на другой;

3) на каждом маршруте ровно 3 остановки.

Сколько автобусных маршрутов в городе?

Вариант задачи (второй тур, 9–10 кл., задача 4): число маршрутов равно 57, и на каждом не менее трёх остановок. Сколько остановок могут иметь маршруты?

Указание. См. теорему 2. Ответ к основной задаче см. на левой части рис. 2 (с. 154).

Ещё две задачи, связанные с конечными геометриями (хотя сразу это не очевидно).

Задача 6 (XLVIII Московская математическая олимпиада (1985), 10 кл., задача 4). Даны 1985 множеств, каждое из которых состоит из 45 элементов, причём объединение любых двух множеств содержит ровно 89 элементов. Сколько элементов содержит объединение всех этих 1985 множеств?

Задача 7. В классе ученики ходят на 10 кружков, каждый кружок посещают четверо, и для любых двух кружков есть только один ученик, который ходит на оба кружка. Сколько может быть учеников в классе?

Решим для примера последнюю задачу. Приведём сразу ответ: 31 и 13. Рассмотрим задачу в следующей формулировке: даны 10 множеств из 4 элементов каждое, причём объединение любых двух содержит ровно 7 элементов. Сколько элементов может быть в объединении всех этих множеств? Укажите все возможные значения.

Будем проводить рассуждения иногда и для более общего случая, а именно, когда в каждом из множеств k элементов, а число множеств равно n. Число элементов в объединении всех n множеств обозначим m. Из условия следует, что любые два множества имеют ровно один общий элемент. Назовём эти множества «прямыми», а их объединение — «плоскостью». Тогда полученная «конечная геометрия» удовлетворяет двум «аксиомам» — любые две разные «прямые» имеют не более одной общей «точки», и через каждую точку проходит хотя бы одна прямая (далее кавычки опускаем). Очевидно, что если все n прямых имеют общую точку, то общее число точек на них $m = 1 + n(k - 1)$. Поскольку $k = 4$, один из возможных ответов в задаче: $m = 1 + 10 \cdot 3 = 31$. А что будет, если *не все* прямые имеют общую точку? Тогда каждый *пучок прямых* (т. е. множество всех прямых, проходящих через одну точку) содержит не более чем k прямых. Действительно, есть хотя бы одна прямая l, не входящая в него. Все прямые пучка пересекают l, причём в разных точках (ведь их общая точка не лежит

на l), поэтому число прямых в пучке не больше k, а общее число точек на прямых этого пучка не больше $1 + k(k-1)$. Если в пучке k прямых, то точек на нём будет $1 + k(k-1)$. Докажем для числа прямых неравенство $n \leqslant 1 + k(k-1)$. Действительно, кроме прямой l есть не более $k(k-1)$ прямых, так как каждая прямая пересекает l в одной из k её точек, а через каждую такую точку проходит не более $k-1$ прямых, не считая самой l. Если в каждом пучке меньше k прямых, то точно так же доказывается, что $n \leqslant 1 + k(k-2)$. Так как в нашем случае $n = 10 > 1 + 4 \cdot 2$, найдётся пучок, в котором k прямых. Но тогда, как было уже доказано, $m \geqslant 1 + k(k-1)$.

Покажем, что тогда $m = 1 + k(k-1)$. Если $m > 1 + k(k-1)$, то найдётся точка A, не лежащая на прямых этого пучка. Рассмотрим проходящую через неё прямую. Она не совпадает с прямыми пучка (в силу выбора точки A) и пересекается с каждой из них, причём эти точки различны и не совпадают с A. Тогда на прямой $k+1$ точка, а это противоречит условию.

Остаётся привести пример «плоскости» с 13 точками и 10 прямыми.

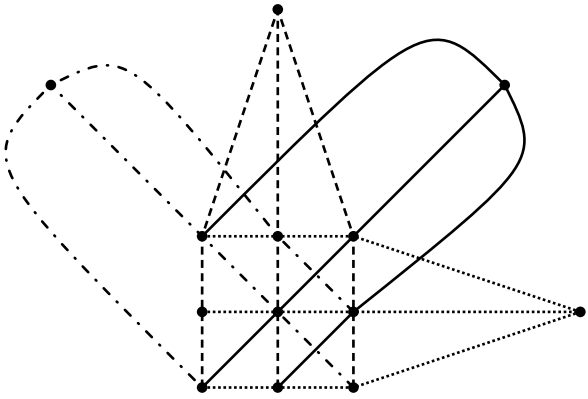


Рис. 1. «Плоскость» с 13 *точками и* 10 *прямыми*

В этом примере однотипные прямые очевидно имеют общую точку, так как образуют пучки. Прямые разного типа тоже попарно пересекаются, что менее очевидно, но легко проверяется. На самом деле даже можно нарисовать ещё 3 прямые так, чтобы любые две из 13 прямых попарно пересекались.

Равенство $n = 1 + k(k-1)$ возможно только в случае, когда в каждом пучке ровно k прямых. Докажем, что тогда через любую пару точек A, B проходит прямая (причём единственная). Действительно, проведя через A прямую l, не проходящую через B (если прямая проходит через B, то доказывать нечего, а какая-нибудь прямая через каждую точку проходит),

рассмотрим пучок из k прямых, проходящих через B. Все они пересекают прямую l, причём в разных точках. Так как точек на прямой тоже k, одна из прямых этого пучка проходит через точку A прямой l, что и требовалось. Описанная плоскость состоит из $1 + k(k-1)$ точек, содержит столько же прямых, каждая из которых содержит k точек, в каждом пучке k прямых и выполнены две аксиомы: через любые две точки проходит единственная прямая и любые две прямые имеют общую точку. Это аксиомы проективной геометрии, а описанная плоскость является *конечной проективной плоскостью.* Однако неясно, при любом ли k существует такая «плоскость» на самом деле, т. е. возможно ли такое семейство конечных множеств. Если $q = k - 1$ есть степень простого числа, то это возможно. Выше это было фактически доказано в случае $q = 3$.

Если бы в условии задачи было $n > 1 + k(k-1)$ множеств, то тривиальный ответ $1 + (k-1) \cdot n$ был бы единственным, что по существу и доказано.

В случае $k = 4$ и $10 \leqslant n \leqslant 13$ кроме тривиального ответа $1 + 3 \cdot n$ есть ещё ответ 13, что фактически и было доказано (приведённый пример для 10 прямых дополняется до 13 прямых с соблюдением условий задачи и без увеличения числа точек).

Если в условии задачи будет не 10, а 9 множеств, то кроме ответа $1 + 9 \cdot 3 = 28$ будут ещё ответы 13, 12. Для получения ответа 13 достаточно выбрать 9 прямых из указанных 10 так, чтобы какой-то пучок из 4 прямых содержался в выбранных девяти (очевидно, что этот ответ сохранится и во всех случаях $n \geqslant 4$). Для получения ответа 12 достаточно из 13 прямых, образующих плоскость с 13 точками, удалить 4 прямые, образующие пучок. Тогда оставшиеся 9 прямых содержат 12 точек (очевидно, что таким же образом получаем ответ 12 для любого n, $5 \leqslant n \leqslant 9$).

Покажем, что для $n = 8, 9$ других ответов нет. Докажем, что $m \geqslant 12$. Можно считать, что плоскость не содержит пучков с четырьмя прямыми (иначе уже на этом пучке 13 точек, а больше точек быть не может, как было доказано выше). Пусть точек, через которые проходит i прямых, имеется x_i. Подсчитывая двумя способами число пар «точка и проходящая через неё прямая», получаем уравнение $4n = 3x_3 + 2x_2 + x_1$. Подсчитывая двумя способами число пар прямых, получаем уравнение $n(n-1)/2 = 3x_3 + x_2$. В случае $n = 9$ из этих уравнений получаем $x_1 + x_2 = 0$, значит, $m = x_3 = 12$ и на плоскости 12 точек. В случае $n = 8$ имеем $x_1 + x_2 = 4$, значит,

$$m = x_3 + 4 = 4 + \frac{n(n-1)}{6} - \frac{x_2}{3} = 13 + \frac{1 - x_2}{3} \geqslant 12,$$

так как $x_2 \leqslant 4$, и очевидно $m < 14$, т. е. $m = 12, 13$.

В случае $n = 7$ аналогично получаем $x_1 + x_2 = 7$ и неравенство

$$14 \geqslant m = x_3 + 7 = 7 + 7 - \frac{x_2}{3} = 14 - \frac{x_2}{3} > 11,$$

т. е. $m = 12, 13, 14$. Возможность ответов $m = 12, 13$ уже доказана. Ответ $m = 14$ возможен только в случае $x_2 = 0, x_1 = 7$. Для построения такой «плоскости» достаточно построить плоскость с 7 точками и 7 прямыми (см. рис. 1) и добавить к каждой прямой по одной точке (разным прямым разные точки).

В случае $n = 6$ аналогично получаем $x_1 + x_2 = 9$ и неравенство

$$14 \geqslant m = x_3 + 9 = 9 + 5 - \frac{x_2}{3} = 14 - \frac{x_2}{3} \geqslant 11,$$

т. е. $m = 11, 12, 13, 14$. Ответ 11 получается, если из плоскости с 13 прямыми удалить два пучка (вместе содержащие 7 прямых). Оставшиеся 6 прямых покрывают оставшиеся 11 точек. Случай $m = 14$ невозможен, так как тогда $x_2 = 0, x_1 = 9$, значит, имеется 9 точек, через каждую проходит одна прямая, поэтому прямых не менее 9, что невозможно. Значит, при $n = 6$ ответ $m = 11, 12, 13$. В случае $n = 5$ имеем $x_1 + x_2 = 10$,

$$13 \geqslant m = x_3 + 10 = 10 + 3 + \frac{1 - x_2}{3} = 13 + \frac{1 - x_2}{3} \geqslant 10,$$

т. е. $m = 10, 11, 12, 13$. Ответы $12, 13$ возможны, как было уже показано. Ответ 10 возможен, так как тогда $x_2 = 10, x_1 = 0 = x_3$, т. е. через 5 точек проходят 10 прямых, причём через каждую точку — ровно две. Чтобы убедиться в возможности такой конфигурации, достаточно провести на обычной плоскости 5 попарно не параллельных прямых так, чтобы никакие три не пересекались в одной точке. В случае $m = 11$ очевидно $x_3 = 1, x_2 = 7, x_1 = 3$. Такой случай также возможен, достаточно провести на обычной плоскости 5 прямых, три из них через одну точку, тогда на остальных двух будет по четыре точки попарных пересечений, а всего их будет 8 (с учётом точки пересечения трёх прямых), нужно ещё на каждой из трёх прямых, проходящих через одну точку, выбрать по одной точке — и конфигурация готова.

В случае $n = 4$ имеем $x_1 + x_2 = 10$,

$$12 \geqslant m = x_3 + 10 = 10 + 2 - \frac{x_2}{3} = 12 - \frac{x_2}{3} \geqslant 10,$$

т. е. $m = 10, 11, 12$. Ответ 10 получается, если провести на обычной плоскости 4 прямые с попарными точками пересечения (таких точек, в каждой из которых пересекаются ровно две прямые, будет 6) и ещё на каждой прямой выбрать по одной точке. Ответ 11 получается, если провести

на обычной плоскости 4 попарно пересекающиеся прямые, из которых три проходят через одну точку, на них выбрать ещё по две точки, и ещё одну точку на четвёртой прямой. Случай $m = 12$ невозможен, так как тогда $x_2 = 0, x_3 = 2, x_1 = 10$, но четыре прямые не могут иметь две тройные точки пересечения (тогда прямых было бы пять).

В случае $n = 3$ имеем $x_1 + x_2 = 9$, $3 = 3x_3 + x_2$,

$$10 \geqslant m = x_3 + 9 = 9 + 1 - \frac{x_2}{3} = 10 - \frac{x_2}{3} \geqslant 9,$$

т. е. $m = 9, 10$. Ответ 9 получается, если провести на обычной плоскости 3 прямые с попарными точками пересечения (их будет 3) и ещё на каждой прямой выбрать по две точки. Ответ 10 тривиально возможен. В случае $n = 2$ очевидно возможен только тривиальный ответ.

Читатель может попробовать решить и более общую задачу: в семействе из n множеств по k элементов любые два множества имеют только один общий элемент. Сколько элементов может быть в объединении этих множеств? Получить полное решение этой задачи, по-видимому, очень трудно.

Приведённые задачи обобщает и уточняет следующая классическая

Теорема 2. *Пусть $q \geqslant 2$ — целое число. Для конечной проективной плоскости равносильны следующие шесть условий.*

(i) *Некоторая прямая содержит $q + 1$ точку.*

(ii) *Некоторая точка лежит ровно на $q + 1$ прямой.*

(iii) *Каждая прямая содержит $q + 1$ точку.*

(iv) *Каждая точка лежит ровно на $q + 1$ прямой.*

(v) *Плоскость содержит ровно $q^2 + q + 1$ точек.*

(vi) *На плоскости существует ровно $q^2 + q + 1$ прямых.*

Такая плоскость называется *конечной проективной плоскостью порядка q* и обозначается иногда $\mathrm{PG}(2, q)$. Доказательство можно найти в [13–15]. Однако несложно доказать эту теорему и самостоятельно. Связь проективных плоскостей с блок-схемами указывает следующая

Теорема 3. *Конечная проективная плоскость порядка q образует симметричную блок-схему с $v = q^2 + q + 1$ элементами, $b = v$ блоками по $k = q + 1$ элементов в каждом и $\lambda = 1$. Обратно, симметричная $(q^2 + q + 1, q + 1, 1)$-блок-схема образует плоскость* $\mathrm{PG}(2, q)$.

Доказательство её (сравнительно простое) опускается. Желающие могут найти его в [13, 14].

Примером (получающейся при $q = 2$) $(7, 3, 1)$-блок-схемы служит

$$\big\{\{1, 2, 7\}, \{3, 4, 7\}, \{2, 3, 5\}, \{1, 4, 5\}, \{1, 3, 6\}, \{2, 4, 6\}, \{5, 6, 7\}\big\}.$$

Вопрос о связи проективных плоскостей с разностными множествами рассмотрим позднее, а сейчас уместно ввести понятие конечной аффинной плоскости. Множество называется *конечной аффинной плоскостью*, если

Ax1: *для любых двух различных её точек существует, причём ровно одна, прямая, через них проходящая*;

Ax2: *через точку вне данной прямой проходит ровно одна не пересекающая её* (параллельная ей) *прямая*;

Ax3: *каждая прямая содержит не менее двух точек*;

Ax4: *существует не менее двух прямых*.

Справедлива аналогичная теореме 2

Теорема 4. *Пусть $q \geqslant 2$ — целое число. Для конечной аффинной плоскости равносильны следующие шесть условий.*

(i) *Некоторая прямая содержит q точек.*

(ii) *Некоторая точка лежит ровно на $q+1$ прямых.*

(iii) *Каждая прямая содержит q точек.*

(iv) *Каждая точка лежит ровно на $q+1$ прямых.*

(v) *Плоскость содержит ровно q^2 точек.*

(vi) *На плоскости существует ровно q^2+q прямых.*

Доказательство аналогично теореме 2 (его можно найти в [13]).

Связь аффинных плоскостей с блок-схемами указывает следующая

Теорема 5. *Конечная аффинная плоскость порядка q образует блок-схему с $v=q^2$ элементами, $b=v+q$ блоками по $k=q$ элементов в каждом и $\lambda=1$. Обратно, любая $(q^2, q, 1)$-блок-схема образует плоскость* $\mathrm{AG}(2, q)$.

Доказательство (аналогичное теореме 3) можно найти в [13].

Примером (получающейся при $q=3$) $(9, 12, 3, 1)$-блок-схемы служит $\big\{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{1,4,7\}, \{2,5,8\}, \{3,6,9\}, \{1,5,9\}, \{2,6,7\}, \{3,4,8\}, \{3,5,7\}, \{1,6,8\}, \{2,4,9\}\big\}$.

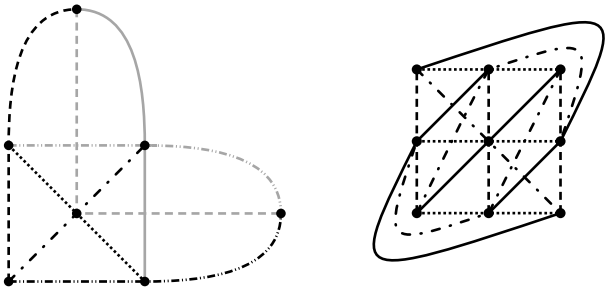


Рис. 2. Слева проективная плоскость $\mathrm{PG}(2,2)$ *— плоскость Фано, справа аффинная плоскость* $\mathrm{AG}(2,3)$.

Примеры проективной и аффинной плоскостей изображены на рис. 2.

Связь аффинных плоскостей с проективными указывает следующая

Теорема 6. *Аффинная плоскость порядка q существует тогда и только тогда, когда существует проективная плоскость порядка q.*

Доказательство (основанное на идее добавления бесконечно удалённых точек, образующих бесконечно удалённую прямую) можно найти в [13, 14].

2.1. Как можно построить конечные плоскости

Пусть $q = p^n$ — степень простого числа. Далее будет без доказательства использоваться следующий факт: существует *конечное поле* $\mathrm{GF}(q)$, состоящее из q элементов[8)]. *Простое поле* $\mathrm{GF}(p)$ можно определить как множество чисел $\{0, 1, \ldots, p-1\}$, операции сложения и умножения в котором выполняются по модулю p, т. е. для нахождения суммы или произведения нужно вычислить обычную сумму или произведение и заменить её на остаток от деления на p. Читатель может сам проверить, что эти операции удовлетворяют тем же законам, что и операции сложения и умножения рациональных чисел, а именно, переместительному: $a+b \bmod p = b+a \bmod p$, $ab \bmod p = ba \bmod p$, сочетательному: $(a+b)+c = a+(b+c) \bmod p$, $(ab)c = a(bc) \bmod p$, распределительному: $a(b+c) = ab+ac$, и удовлетворяют тождествам $a+0=a$, $a \cdot 1 = a$, а также имеют однозначно определённые обратные операции вычитания $a-b \bmod p$ и деления $a/b \bmod p$, удовлетворяющие тождествам $(a-b)+b = a \bmod p$, $(a/b)b = a \bmod p$. Указанные выше свойства арифметических операций называются *аксиомами поля*[9)]. Проверка их несложна, труднее всего доказывается возможность деления[10)].

В случае $n > 1$ поле $\mathrm{GF}(p^s)$ можно определить как множество многочленов степени, меньшей n, с коэффициентами из простого поля $\mathrm{GF}(p)$. Сложение (и вычитание) многочленов определяется стандартным образом, т. е. коэффициенты складываются или вычитаются по модулю p, а умножение выполняется *по модулю данного неприводимого многочлена* $f(x)$ степени n с коэффициентами из поля $\mathrm{GF}(p)$, т. е. результат обычного умножения многочленов заменяется на остаток от деления на $f(x)$. Многочлен называется *неприводимым* над полем $\mathrm{GF}(p)$, если его нельзя разложить в произведение многочленов меньшей степени над тем же полем. Деление

[8)] Такие поля называют полями порядка q, а обозначение напоминает о французском математике Эваристе Галуа, их открывшем.

[9)] В отличие от аксиом геометрии Евклида выполнение аксиом поля для заданных операций на множестве $\mathrm{GF}(p)$ надо доказывать. Для поля рациональных чисел справедливость этих аксиом всем известна, поэтому можно считать их очевидными.

[10)] Деление на нуль невозможно, так как из аксиом можно вывести, что $a \cdot 0 = 0$.

многочленов друг на друга с остатком определяется точно так же, как деление чисел с остатком, только вместо условия, что остаток от деления должен быть меньше делителя, используется условие, что степень остатка должна быть меньше степени делителя, т. е. многочлена $f(x)$. Доказательства того, что введённые выше арифметические операции в множестве $\mathrm{GF}(p^n)$ удовлетворяют всем аксиомам поля, и того факта, что такие поля при любом n и простом p действительно существуют, можно найти в книгах по алгебре [11)], например в [2, 7, 14].

Приведём пример построения конечного поля из 9 элементов. В нём фактически можно обойтись без использования многочленов над полем из 3 элементов, так как конструкция очень похожа на построение поля комплексных чисел. Рассмотрим множество $F_9 = \{\gamma_0, \ldots, \gamma_8\}$ из элементов вида (a, b), где $a, b = 0, \pm 1$. Определим на нём операцию сложения по формуле $(a, b) + (c, d) = (a + c, b + d)$, где $1 + 1 = -1$, $(-1) + (-1) = 1$, а всё остальное, как в обычном сложении. Операция умножения над числами $0, \pm 1$ берётся обычная, а операция умножения над парами (a, b), (c, d) определяется как $(ac - bd, ad + bc)$. Элемент $(0, 0)$ играет в этом поле роль нуля, а элемент $(1, 0)$ — роль единицы, в чём несложно убедиться. Элементы вида $(a, 0)$ образуют подполе в этом поле, состоящее из трёх элементов $(0, 0)$, $(1, 0)$, $(-1, 0)$. Для краткости их можно обозначать $0, 1, -1$. Выполнение операций в этом подполе сводится к выполнению указанных выше операций в множестве $\{0, 1, -1\}$. Элемент $(0, 1)$ при возведении в квадрат равен $(-1, 0)$, т. е. -1. Для любого (a, b) можно определить операцию вычисления обратного элемента относительно сложения (её можно назвать операцией смены знака): $-(a, b) = (-a, -b)$, где полагаем, что $-0 = 0$. Очевидно, что $(a, b) + (-(a, b)) = (0, 0) = 0$. После этого определяется операция вычитания: $(a, b) - (c, d) = (a, b) + (-c, -d)$, которая является обратной операцией к операции сложения. Для $(a, b) \neq (0, 0)$ можно ещё определить операцию вычисления обратного элемента относительно умножения: $(a, b)^{-1} = (-a, b)$, если $ab \neq 0$, а в остальных случаях $(a, 0)^{-1} = (a, 0)$, $(0, b)^{-1} = (0, -b)$. Несложно проверить, что $(a, b)^{-1} \cdot (a, b) = (1, 0)$.

Теорема 7. *Для любого q, равного степени простого числа, существует конечная проективная плоскость порядка q.*

Доказательство. Рассмотрим трёхмерное векторное пространство $\mathrm{GF}(q)^3$, т. е. множество троек (x_1, x_2, x_3), $x_i \in \mathrm{GF}(q)$, $i = 1, 2, 3$. Назовём две ненулевые тройки эквивалентными, если одна из них коллинеарна

[11)] В них также доказывается, например, что конечные поля порядка q существуют только для q, равных степени простого числа, и все поля равного порядка изоморфны, т. е. с алгебраической точки зрения одинаковы.

другой, т. е. $x_i = ay_i$, $i = 1, 2, 3$, $a \in \mathrm{GF}(q) \setminus \{0\}$. Класс эквивалентности троек назовём точкой проективной плоскости. В каждом классе эквивалентности ровно $q - 1$ ненулевых троек, поэтому число этих классов (число точек строящейся проективной плоскости) равно $(q^3 - 1)/(q - 1) = q^2 + q + 1$. Для произвольной ненулевой тройки $a = (a_1, a_2, a_3)$ рассмотрим двумерное подпространство в $\mathrm{GF}(q)^3$, состоящее из всех троек $x = (x_1, x_2, x_3) \in \mathrm{GF}(q)^3$, удовлетворяющих уравнению $(a, x) = a_1x_1 + a_2x_2 + a_3x_3 = 0$. Число таких троек равно q^2, из них одна нулевая, и все ненулевые разбиваются на $(q^2 - 1)/(q - 1) = q + 1$ классов коллинеарных троек, т. е. каждому такому двумерному подпространству можно сопоставить $q + 1$ точку строящейся проективной плоскости и назвать это множество прямой в этой плоскости. Любые два двумерных подпространства $(a, x) = 0$, $(b, x) = 0$ пересекаются по одномерному подпространству, ненулевые тройки которого определяют точку C строящейся проективной плоскости — (единственную) точку пересечения соответствующих прямых a и b. Число различных двумерных подпространств равно $(q^3 - 1)/(q - 1) = q^2 + q + 1$, так как подпространства $(a, x) = 0$, $(b, x) = 0$ совпадают тогда и только тогда, когда тройки a и b эквивалентны, следовательно, число прямых на строящейся проективной плоскости равно $q^2 + q + 1$. Через любые две точки A, C этой плоскости проходит единственная прямая a, а именно та, которая соответствует двумерному подпространству $(a, x) = 0$, натянутому на тройки из классов эквивалентности A, B. Теорема доказана. □

Теорема 8. *Для любого q, равного степени простого числа, существует конечная аффинная плоскость порядка q.*

Доказательство. Рассмотрим следующую блок-схему. Её точками являются упорядоченные пары $(x, y) \in \mathrm{GF}(q)^2$, количество которых q^2. Назовём прямой любое множество точек (пар), удовлетворяющих уравнению $ax + by = 1$, $ab \neq 0$. Число различных таких прямых равно $(q - 1)^2$. Добавим к ним ещё оси координат $(x, 0)$ и $(0, y)$ и все прямые, параллельные им, т. е. множества точек $\{(x, a) \colon x \in \mathrm{GF}(q)\}$, $\{(b, y), y \in \mathrm{GF}(q)\}$, а также все прямые, проходящие через начало координат, т. е. множества точек $\{(x, y) \colon y = kx \in \mathrm{GF}(q)\}$, $k \in \mathrm{GF}(q)\{0\}$. Число точек на каждой прямой равно q, а число всех прямых равно $(q-1)^2+q+q+(q-1) = q^2+q$. Через любую пару точек проходит ровно одна такая прямая. Для доказательства в случае точек (x_1, y_1), (x_2, y_2), не совпадающих с началом координат и не имеющих равных координат, достаточно проверить, что система двух уравнений $ax_1 + by_1 = 1$, $ax_2 + by_2 = 1$ относительно (a, b) имеет единственное решение (в остальных случаях всё очевидно). Аксиома о параллельности также может быть проверена непосредственно, но достаточно сослаться на теорему 5. □

2.2. Неожиданное явление плоскости Фано

Конечная проективная плоскость $\mathrm{PG}(2,2)$, изображённая на рис. 2, загадочным образом возникает в решении следующей задачи [12)], опубликованной в сборнике головоломок [17], но фактически относящейся к серьёзной прикладной дисциплине — публичной криптографии.

Задача 8. Два шерифа соседних городов составили список из 7 подозреваемых в качестве серийного убийцы [13)]. Потом каждый из них, проведя оперативно-разыскные действия, сократил список подозреваемых до двух человек. Эти списки различны, т. е. пересекаются только по одному подозреваемому, поэтому шерифы, обменявшись информацией, могут совместно арестовать убийцу (а в одиночку они этого сделать не могут). Но если эта информация будет перехвачена и станет известна жителям, то они поймут, кто убийца, и линчуют его, не дожидаясь ареста (список из семи подозреваемых им известен).

Как шерифам обменяться информацией, чтобы арестовать убийцу (и тем самым не допустить суда Линча)?

Задача может быть решена следующим образом (возможность придумать решение для случая 8 подозреваемых оставляется читателям).

Шерифы вначале нумеруют подозреваемых, далее подозреваемые называются точками [14)], и один из шерифов объясняет другому, как построить на множестве из семи точек плоскость Фано. Потом каждый из них мысленно проводит прямую в этой плоскости через двоих своих подозреваемых, определяет оставшуюся (третью) точку этой прямой и сообщает её коллеге, а тот в ответ делает то же самое (сообщить явно две свои точки они не могут, так как тогда те, кто за ними шпионит, сразу определят общую точку и узнают убийцу, а по информации об одной точке прямая не определяется однозначно — таких прямых три). Возможны два случая: в первом обе прямые совпадают, а во втором — нет (далее будет ясно, что шпионы не смогут понять, какой из случаев реализовался).

Очевидно, что первый случай возможен только тогда, когда каждый шериф сообщил коллеге имя одного из подозреваемых этим коллегой (если первый подозревал A и B и сообщил коллеге имя C, а у второго шерифа получилась та же самая прямая с точками A, B, C, то второй сообщил имя A или B и подозревал соответственно B, C или A, C). В этом случае

[12)] Об этой задаче и её решении мне сообщил А. В. Устинов.

[13)] В книге [17] подозреваемых было 8, но потом для случая, когда их 7, было найдено решение на форуме http://mathoverflow.net/questions/203182/the-two-sheriffs-puzzle

[14)] Как известно, Гильберт говорил, что после формулировки аксиом геометрии можно вместо точек, прямых и плоскостей говорить о столах, стульях и кружках пива.

шерифы сразу поймут, кто убийца (так как названные ими, очевидно, не являются убийцами), но шпионы об этом не узнают.

Во втором случае точка пересечения прямых очевидно указывает на убийцу. Но её нельзя найти, не зная самих прямых, — с точки зрения шпионов каждая из прямых может быть выбрана тремя способами, и пересекаться эти прямые могут в любой из пяти точек, отличных от двух, названных шерифами. Однако шерифы имеют больше информации, чем шпионы. Действительно, пусть список подозреваемых одного шерифа есть $\{A, B\}$, а назвал он точку C, тогда список второго шерифа, скажем, $\{A, D\}$ (списки должны иметь общую точку), а назвал он E. Точки C и E различны и отличаются от A, B, D (прямые $\{A, B, C\}$ и $\{A, D, E\}$ имеют только одну общую точку — точку A), шерифам (и шпионам) они известны, через них они могут провести прямую $\{C, E, F\}$ и найти ещё одну точку F, не совпадающую ни с A, B (потому, что прямые $\{A, B, C\}$ и $\{C, E, F\}$ пересекаются только в точке C), ни с D (прямые $\{A, D, E\}$ и $\{C, E, F\}$ пересекаются только в точке E). Таким образом, каждому из шерифов (и шпионов) ясно, что C, E, F выбывают из списка подозреваемых, и в нём остаются только A, B, D и ещё некий G (вне прямой лежит ровно четыре точки). Если теперь шерифы назовут двух своих подозреваемых, то в пересечении этих списков получится имя убийцы.

Но и шпионы могут сделать то же самое! Однако при этом они должны быть уверены, что реализовался именно второй случай, потому что в первом случае прямая $\{C, E, F\}$ (в обозначениях второго случая) совпала бы с прямой $\{A, B, C\}$ (в обозначениях первого случая) и предыдущий анализ потерял бы силу. Но определить, какой именно из случаев возник, шпионы очевидно не в состоянии.

В отличие от них шерифы легко замечают, что реализовался первый случай, вычисляют убийцу и для маскировки продолжают диалог так же, как и во втором случае, только называют не настоящие пары подозреваемых, а две другие пары (не лежащие на прямой $\{A, B, C\}$), и тем самым вводят шпионов в заблуждение (дезинформируя их об имени убийцы). Поэтому шпионы, понимая невозможность отличить друг от друга оба случая и соответственно верную информацию от дезинформации, вынуждены отказаться от планов линчевания.

2.3. И ещё одно появление плоскости Фано

Начнём издалека и рассмотрим простейший пример кода, исправляющего одну ошибку. Допустим, нам нужно передать двоичное слово (x_1, x_2, x_3, x_4). Добавим к нему *проверочные символы* $x_5 = x_1 + x_3 + x_4$, $x_6 = x_1 + x_2 + x_4$, $x_7 = x_1 + x_2 + x_3$ (знак $+$ здесь обозначает сложение по модулю два;

символы x_1, x_2, x_3, x_4 называются *информационными*). Процедура вычисления по информационным символам проверочных и составления из них кодового слова (закодированного сообщения) называется кодированием (так же называется и само отображение исходного сообщения в кодовое слово). На языке матриц в рассматриваемом примере кодирование сводится к умножению некоторой матрицы M на транспонированный вектор $(x_1, x_2, x_3, x_4)^T$ (т. е. вектор, расположенный в столбец):

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}.$$

Передаём закодированное сообщение $c = (x_1, \dots x_7)$ и получаем *зашумлённое сообщение* $r = c + e$, где $e = (e_1, \dots, e_7)$ — вектор ошибок. В нашем случае он имеет вес (сумму координат) 1, так как по предположению ошибка может произойти (если произойдёт) только в одной позиции. Например, возможно, $e = e_3 = (0, 0, 1, 0, 0, 0, 0)$. Тогда

$$r = c + e = (c_1, c_2, c_3 + 1, c_4, c_5, c_6, c_7) = (c_1, c_2, \bar{c}_3, c_4, c_5, c_6, c_7),$$

где $\overline{0} = 1, \overline{1} = 0$. Число 3 будет в рассматриваемом случае *позицией ошибки*. Для определения позиции ошибки (а значит, и обнаружения самой ошибки) можно вычислить *проверочные суммы*

$$S_1 = r_1 + r_3 + r_4 + r_5,$$
$$S_2 = r_1 + r_2 + r_4 + r_6,$$
$$S_3 = r_1 + r_2 + r_3 + r_7.$$

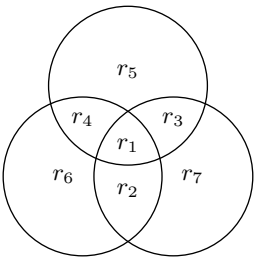


Рис. 3. Код Хэмминга с блоковой длиной 7

Построенный код является частным случаем кодов Хэмминга. Наглядно проверочные суммы изображены на рис. 3. Каждая сумма содержится в своём круге.

Обратим внимание на некоторые его свойства. Его мощность (количество кодовых слов) равна $2^4 = 16$, сумма любых двух кодовых слов по модулю два опять является кодовым словом, расстояние кода равно трём (расстояние $d(a, b)$ между кодовыми словами a, b равно числу позиций, в которых они отличаются, а расстояние кода по определению равно минимальному расстоянию между различными кодовыми словами). Так как код имеет кодовое слово веса нуль (нулевое

слово), а кодовое расстояние равно трём, кодовых слов веса 1 или 2 в нём нет. Для каждого кодового слова рассмотрим шар радиуса 1 с центром в нём. Этот шар содержит, кроме центра, ещё 7 двоичных наборов (вершин семимерного двоичного куба), получающихся, если в центральном наборе заменить ровно один из семи его символов на противоположный. Эти шары с центрами в кодовых словах не пересекаются[15], поэтому в совокупности содержат $2^4 \cdot 8 = 2^7$ различных вершин куба, т. е. все эти вершины. Такие точные покрытия многомерного куба непересекающимися шарами называются *совершенными*, а соответствующие им коды — *совершенными кодами*.

Исходя только из свойства совершенности указанного кода, можно однозначно определить число кодовых вершин на третьем слое семимерного куба[16].

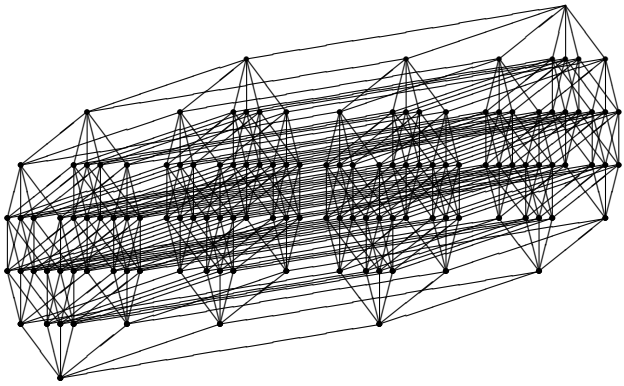


Рис. 4. Семимерный куб (*условное изображение*)

Для этого рассмотрим единичные сферы с центрами в кодовых словах веса три (сфера — это шар без центра). Заметим, что их пересечения со вторым слоем куба[17] имеют мощность 3 (так как есть только три набора веса два, лежащих на данной сфере: действительно, среди координат центра сферы только три единицы, которые можно заменять на нули). Эти сечения не пересекаются, так как расстояние между центрами сфер равно трём. Поэтому число кодовых слов веса три не больше $\binom{7}{2} : 3 = 7$. А так как вершины второго слоя покрываются только шарами с центрами в третьем слое (шары с центрами в четвёртом и более высоких слоях до второго слоя

[15] Если шары с центрами a, b имеют общую точку c, то $d(a,b) \leqslant d(a,c) + d(c,b) \leqslant 2$, что невозможно.

[16] k-й слой куба состоит из всех вершин веса k и очевидно содержит $\binom{7}{k}$ вершин.

[17] Все вершины одного слоя куба лежат на плоскости с уравнением $x_1 + \ldots + x_7 = k$, поэтому указанные пересечения можно рассматривать как сечения сфер плоскостью.

не достают), и код совершенный, то число кодовых слов веса три в точности равно 7. Вычислим, сколько вершин четвёртого слоя покрывается семью рассмотренными шарами. Каждый шар покрывает 4 вершины, эти сечения шаров плоскостью попарно не пересекаются, поэтому общее число покрытых вершин 4-го слоя равно $7 \cdot 4 = 28$. Непокрытых вершин в нём остаётся $\binom{7}{4} - 28 = 7$. В третьем слое непокрытых вершин $\binom{7}{3} - 7 = 28$, так как покрыты только центры шаров, а их семь. Непокрытые вершины третьего слоя можно покрыть только шарами с центрами в четвёртом слое, а каждый такой шар покрывает в третьем слое ровно 4 вершины. Значит, для покрытия оставшихся вершин третьего слоя нужно не менее $28/4 = 7$ шаров с центрами в четвёртом слое, а непокрытых вершин там ровно 7, значит, все их нужно использовать в качестве кодовых вершин (и центров шаров). Поэтому кодовых вершин веса 4 в точности 7. Соответствующие шары покрывают в пятом слое $7 \cdot 3 = 21$ вершину (шары попарно не пересекаются, так как их центры — кодовые слова), т. е. все его вершины. Кодовых слов на шестом слое быть не может, так как шар с центром в этом слое содержит вершины пятого слоя, а они уже покрыты. Остаётся единственная вершин седьмого слоя — единичная вершина, которая должна входить в код, чтобы её сфера покрыла шестой слой. Таким образом, предполагая существование совершенного кода с расстоянием три в семимерном кубе, можно точно установить его *весовой спектр*, а именно число его слов заданного веса. Он состоит из чисел $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 7$, $a_4 = 7$, $a_5 = 0$, $a_6 = 0$, $a_7 = 1$.

Посмотрим на кодовые слова веса три. Каждое из них определяет трёхэлементное подмножество в множестве $\{1, 2, 3, 4, 5, 6, 7\}$, состоящее из номеров позиций единиц в этом слове. Очевидно, что любые два из этих множеств имеют не более одного общего элемента (иначе расстояние между кодовыми словами было бы равно двум). Поэтому система из этих 7 троек образует *систему троек Штейнера*, т. е. каждая пара элементов (а их ровно $\binom{7}{2} = 21$) принадлежит ровно одной тройке (потому что семь троек содержат в точности 21 пару). На самом деле общий элемент у любых двух троек ровно один, так как если бы две тройки не пересекались, то остальные тройки, которые пересекаются с этими двумя не более чем по одному элементу, должны иметь один общий для всех элемент — тот, который не принадлежит двум первым тройкам. Но других общих элементов у них быть не может, значит, таких троек не более трёх, а всего троек не более пяти, в то время как их должно быть семь.

Поэтому система троек изоморфна конфигурации 7 прямых в проективной плоскости на 7 точках — плоскости Фано (см. рис. 2) А расстояние между любыми двумя кодовыми словами из третьего слоя равно 4. Из проведён-

ных рассуждений следует также, что максимальное число вершин третьего слоя семимерного куба, попарные расстояния между которыми не меньше трёх (или четырёх), равно семи. (Коды, все вершины которых лежат на одном слое куба, называются *равновесными кодами*.) Таким образом, максимальная мощность кода веса три со словами длины 7 также равна семи.

§ 3. Примеры разностных множеств и теорема Зингера

Справедлива следующая

Теорема 9 (Зингер). *В проективной геометрии* $\mathrm{PG}(2, q)$, $q = p^r$, *прямые, взятые в качестве блоков, образуют симметричную блок-схему с параметрами* $v = q^2 + q + 1$, $k = q + 1$, $\lambda = 1$. *Эта схема циклическая, а точки любой прямой определяют циклическое* (v, k, λ)*-разностное множество.*

Доказательство (непростое) можно найти в [13, 14].

Вот пример $(31, 6, 1)$-разностного множества, построенного с помощью этой теоремы: $\{0, 1, 15, 19, 21, 24\}$. Можно, вычисляя все 30 попарных разностей по модулю 31, непосредственно убедиться, что все они разные и каждое число от 1 до 30 появляется среди них ровно один раз.

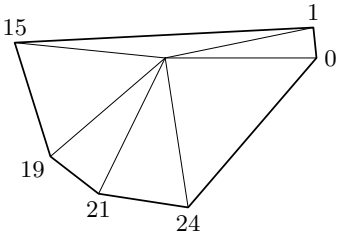


Рис. 5. Шестиугольник из вершин правильного 31*-угольника без трапеций и равнобедренных треугольников*

Применение построенного разностного множества к задаче 3 см. на рис. 5.

Вращая этот шестиугольник вокруг центра данного правильного 31-угольника, получаем 31 «вписанный» шестиугольник, любые два из которых имеют только одну общую вершину. Получим 31 множество, каждое из которых совпадает с множеством вершин соответствующего шестиугольника. Эти множества образуют модель проективной плоскости 5-го порядка.

Следующая задача подобна задаче 3, но существенно труднее.

Задача 9. В правильном 43-угольнике отмечены 7 вершин. Доказать, что существует трапеция или равнобедренный треугольник с вершинами в этих точках. Можно выделить 6 вершин так, что не существует ни трапеции, ни равнобедренного треугольника с вершинами в этих точках.

Указание. Если бы какой-то семиугольник не содержал ни трапеции, ни равнобедренного треугольника, то существовало бы $(43, 7, 1)$-разностное множество, а его не существует согласно упоминавшейся теореме Брука — Райзера.

Множество $\{0, 1, 15, 19, 21, 24\}$ превращается в разностное по модулю 43 множество $\{0, 1, 27, 31, 33, 36\}$, если «раздвинуть» интервал от 1 до 15, превратив его в интервал от 1 до 27. Непосредственно можно убедиться, что все попарные разности чисел этого множества по модулю 43 разные. Соответствующий ему шестиугольник см. на рис. 6.

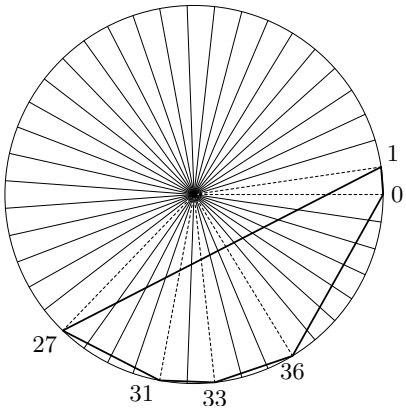


Рис. 6. Шестиугольник из вершин правильного 43-угольника без трапеций и равнобедренных треугольников

Приведём ещё примеры разностных множеств, которые нельзя получить из теоремы Зингера, но можно построить другими методами. Множество $\{2, 4, 5, 27, 31, 36\}$ является разностным по модулю 42. Можно, вычисляя все 30 попарных разностей по этому модулю, непосредственно убедиться, что все они разные. Множество $\{1, 12, 22, 29, 31, 34, 35\}$ является разностным по модулю 48. Зная эти примеры, читатель легко решит следующие задачи, подобные задаче 3.

Задача 10. В правильном 42-угольнике отмечены 7 вершин. Доказать, что существует или трапеция, или прямоугольник, или равнобедренный треугольник, или большая диагональ с вершинами в этих точках. Можно выделить 6 вершин так, что не существует ни трапеции, ни прямоугольника, ни равнобедренного треугольника, ни большой диагонали с вершинами в этих точках.

Задача 11. В правильном 48-угольнике отмечены 8 вершин. Доказать, что существует или трапеция, или прямоугольник, или равнобедренный треугольник, или большая диагональ с вершинами в этих точках. Можно выделить 7 вершин так, что не существует ни трапеции, ни прямоугольника, ни равнобедренного треугольника, ни большой диагонали с вершинами в этих точках.

Приведём пример ещё одной задачи подобного типа.

Задача 12. Можно ли в правильном 26-угольнике так отметить 8 вершин, что не будет существовать ни трапеция, ни равнобедренный треугольник с вершинами в этих точках? А можно ли это сделать так, чтобы не было ещё и прямоугольников?

Ответ на первый вопрос: можно. Пример указан на рис. 7.

Для проверки достаточно для каждой пары не диаметрально противоположных вершин (таких пар $4 \cdot 7 - 4 = 24$) найти наименьшую из двух

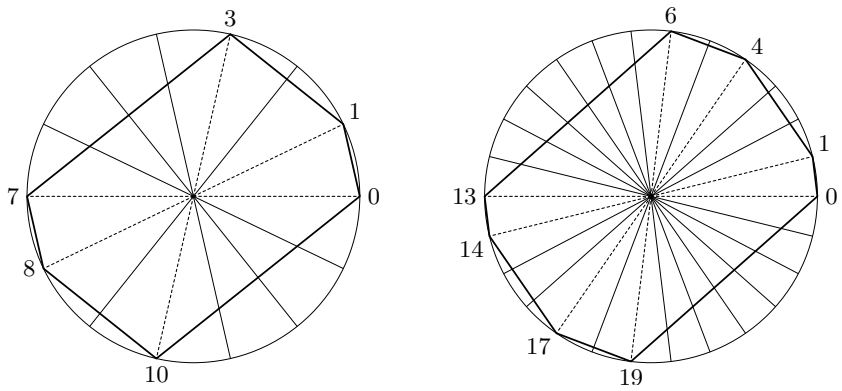


Рис. 7. Шестиугольник из вершин правильного 14*-угольника без трапеций и равнобедренных треугольников. Восьмиугольник из вершин правильного* 26*-угольника без трапеций и равнобедренных треугольников*

дуг данной окружности с концами в этих вершинах, и убедиться, что эти дуги все попарно различны по длине, за исключением пар диаметрально противоположных дуг. Так как упомянутых пар 12, достаточно вычислить длины 12 дуг. Если дуга соединяет вершины с номерами i, j, то в качестве её длины можно взять минимальное из чисел $|i-j|$, $26-|i-j|$.

На второй вопрос ответ отрицательный. Рассмотрим все $7\cdot 8/2=28$ прямых, проходящих через пары выбранных вершин. Из них две параллельны друг другу, так как стороны и диагонали правильного n-угольника образуют n классов попарно параллельных прямых. Они образуют равнобокую трапецию или прямоугольник (при нечётном n всегда получалась бы трапеция).

Указанный пример — частный случай следующего утверждения.

В правильном n-угольнике при $n=2(q^2+q+1)$, где $q=p^m$ — степень простого числа, можно так отметить $2(q+1)$ вершин, что не будет существовать ни трапеция, ни равнобедренный треугольник с вершинами в этих точках.

Его доказательство использует следующие два факта.

1. При $k=q^2+q+1$ в кольце вычетов $\mathbb{Z}_k$ по модулю k существует разностное множество из $q+1$ чисел (теорема Зингера).

2. Пусть в кольце $\mathbb{Z}_n=\{0,\dots,n-1\}$ выбрано k чисел так, что все $k(k-1)$ попарных разностей по модулю n различны. К каждому из них прибавим n и добавим полученные k чисел к выбранному множеству. Получим подмножество из $2k$ чисел в множестве $\mathbb{Z}_{2n}=\{0,\dots,2n-1\}$. Тогда равенство разностей $a-b=c-d \bmod 2n$ в этом подмножестве возможно, лишь когда $a-b=c-d=n \bmod 2n$ или $a-c=b-d \bmod 2n$. Используя эти факты, получим в кольце $\mathbb{Z}_n$ множество из $2q+2$ чисел.

Если в правильном n-угольнике выбрать $2q+2$ вершин, соответствующих этому множеству, то получим центрально-симметричный $(2q+2)$-угольник, из вершин которого нельзя образовать ни равнобедренный треугольник, ни трапецию.

Второе утверждение доказывается несложно. Действительно, если

$$\{a,b,c,d\} \subset \{0,\dots,n-1\} \quad \text{или} \quad \{a,b,c,d\} \subset \{n,\dots,2n-1\},$$

то равенство $a-b=c-d \bmod 2n$ невозможно, так как невозможно равенство $a-b=c-d \bmod n$. Если, например, $\{a,b,c\} \subset \{0,\dots,n-1\}$, $d \geqslant n$, то $d-n \in \{0,\dots,n-1\}$, и если $d-n \notin \{a,b,c\}$, то равенство $a-b=c-d \bmod 2n$ невозможно, так как иначе $a-b=c-(d-n) \bmod n$, а если $d-n \in \{a,b\}$, то $a-b=c-(d-n) \bmod n$ превращается, например, в $a-b=a-(d-n)=a-d \bmod n$, откуда $b=d$, что тоже невозможно, значит, остаётся только случай $d-n=c$, но тогда $d-c=n=b-a \bmod 2n$. Случай, когда $a,b,c \geqslant n$, а $d<n$, сводится к уже рассмотренному прибавлением n по модулю $2n$ к каждому из этих чисел.

Если $a,b<n$, а $c,d \geqslant n$, получаем или $c-n=a$, $d-n=b$, и тогда $a-c=b-d \bmod 2n$; или $c-n=b$, $d-n=a$, и тогда $a-b=(d-n)-(c-n)=$ $=d-c=c-d \bmod 2n$, т. е. $c-d=n=a-b \bmod 2n$; или $c-n \notin \{a,b\}$, или $d-n \notin \{a,b\}$, при этом в обоих случаях $a-b=(c-n)-(d-n) \mod 2n$, поэтому $a-b=(c-n)-(d-n) \mod n$, что возможно только при $a=c-n$, $b=d-n$, и тогда $a-c=n=b-d \bmod 2n$. Случай, когда $a,b \geqslant n$, а $c,d<n$, сводится к уже рассмотренному прибавлением n по модулю $2n$ к каждому из этих чисел.

Если $a,c<n$, а $b,d \geqslant n$, то $a-(b-n)=c-(d-n) \bmod 2n$, значит, $a-(b-n)=c-(d-n) \bmod n$, т. е. или $a=c$, $b-n=d-n$, поэтому $a-c=b-d \bmod 2n$, или $a=b-n$, $c=d-n$, т. е. $a-b=n=c-d \bmod 2n$.

Осталось рассмотреть случай, когда $a,d<n$, $b,c \geqslant n$. Тогда $a-(b-n)=$ $=(c-n)-d \bmod 2n$, поэтому $a-(b-n)=(c-n)-d \bmod n$, но тогда или $a=c-n$, $b-n=d$, т. е. $a-c=n=b-d \bmod 2n$, или $a=b-n$, $c-n=d$, т. е. $a-b=n=c-d \bmod 2n$.

Задача 13 (LXXIX Московская математическая олимпиада (2016), 11 кл., второй день). Можно ли отметить k вершин правильного 14-угольника так, что любой четырёхугольник с вершинами в отмеченных точках, имеющий две параллельные стороны, является прямоугольником, если: а) $k=6$; б) $k \geqslant 7$?

Задача 14. Можно ли в правильном 26-угольнике так отметить 9 вершин, что не существует ни трапеция, ни равнобедренный треугольник с вершинами в этих точках (но существуют прямоугольники)?

Следующий раздел, как это ни удивительно на первый взгляд, довольно тесно связан с предыдущими.

§ 4. Матрицы из нулей и единиц без прямоугольников

О таких матрицах фактически речь идёт в следующих олимпиадных задачах.

Задача 15 (9-я Всесоюзная математическая олимпиада (1975), 9–10 кл., 1-й день). В квадрате 13×13 нужно отметить центры k клеток, чтобы никакие четыре отмеченные точки не являлись вершинами прямоугольника со сторонами, параллельными сторонам квадрата. При каком наибольшем k это возможно?

Ответ: при $k = 13 \cdot 4$.

Задача 16 (22-я Шведская математическая олимпиада (1982 г.), задача 5). Все узлы решётки 12×12 покрашены в красный, белый или синий цвет. Покажите, что всегда найдутся четыре узла одного цвета, образующие прямоугольник со сторонами, параллельными сторонам решётки.

Их решения легко найти, прочитав доказательство следующей теоремы (найденной в 1950-е годы венгерским математиком Рейманом и с тех пор многократно переоткрывавшейся, в том числе и автором этой статьи).

Теорема 10. *Если в $(n \times n)$-матрице из нулей и единиц нет двух строк и двух столбцов, на пересечении которых стоят единицы (т. е. нет подматриц 2×2, заполненных единицами), то число единиц в матрице не больше $n(\sqrt{n - 3/4} + 1/2)$. Равносильная формулировка: если в квадратной таблице размера $n \times n$, $n > 2$, содержится более чем $n(1 + \sqrt{4n - 3})/2$ нулей, то в ней найдётся прямоугольник (четыре клетки, лежащие на пересечении двух строк и двух столбцов), состоящий из нулей.*

Чтобы доказать это, для i-й строки обозначим через M_i множество (и количество) столбцов, на пересечении которых с этой строкой стоят единицы. Число N единиц во всей таблице равно сумме чисел M_i. Можно считать, что различные множества M_i, M_j имеют не более одного общего столбца (если бы они имели пару общих столбцов, то в пересечении этих столбцов с i-й и j-й строками стояли бы одни единицы и лемма была бы уже доказана). Рассмотрим множество P_i всех различных пар столбцов из множества M_i. Число таких пар равно $M_i(M_i - 1)/2$. Из предыдущего утверждения следует, что множества P_i не пересекаются (не имеют общих пар столбцов). Поэтому число пар столбцов в объединении этих множеств

равно сумме всех чисел $M_i(M_i-1)/2$. Но число пар столбцов в указанном объединении не больше чем $n(n-1)/2$. Поэтому имеем неравенство

$$\frac{M_1(M_1-1)}{2}+\ldots+\frac{M_n(M_n-1)}{2}\leqslant\frac{n(n-1)}{2},$$

т. е.

$$\sum_{i=1}^{n}M_i^2-\sum_{i=1}^{n}M_i\leqslant n(n-1).$$

Применяя неравенство Коши $n(a_1^2+\ldots+a_n^2)\geqslant(a_1+\ldots+a_n)^2$, получаем, что

$$\left(\sum_{i=1}^{n}M_i\right)^2-n\sum_{i=1}^{n}M_i\leqslant n^2(n-1),$$

т. е. $N^2-nN\leqslant n^2(n-1)$. Значит,

$$\left(N-\frac{n}{2}\right)^2=N^2-nN+\frac{n^2}{4}\leqslant\frac{n^2}{4}+n^2(n-1),$$

откуда следует неравенство

$$N\leqslant n\Big(\sqrt{n-\frac{3}{4}}+\frac{1}{2}\Big),$$

что и требуется.

В следующей задаче найдены условия, при которых неравенство теоремы 10 превращается в равенство.

Задача 17. Если в $(n\times n)$-матрице из нулей и единиц нет прямоугольников и число единиц в матрице равно $n(\sqrt{n-3/4}+1/2)$, то $n=q^2+q+1$, в каждой строке и каждом столбце ровно $q+1$ единиц, для любых двух строк найдётся (разумеется, единственный) столбец, в пересечении которого с этими строками стоят единицы, и аналогичное утверждение верно для столбцов.

Указание. Если $n(\sqrt{n-3/4}+1/2)$ — целое число, то $\sqrt{4n-3}$ тоже, поэтому $\sqrt{4n-3}=2q+1$, тогда $n=q^2+q+1$. Согласно доказательству теоремы 10 равенство $N=\sqrt{4n-3}$ имеет место тогда и только тогда, когда справедливо равенство

$$\frac{M_1(M_1-1)}{2}+\ldots+\frac{M_n(M_n-1)}{2}=\frac{n(n-1)}{2}$$

и во всех множествах поровну элементов. Из указанного равенства следует утверждение про столбцы. Аналогично доказывается и про строки.

Остаётся построить пример экстремальной таблицы в задаче 15. Это можно сделать, построив циклическую (в другой терминологии циркулянтную) таблицу (матрицу) без прямоугольников.

Циклической называется квадратная матрица, каждая строка которой получается циклическим сдвигом предыдущей строки на одну позицию. То есть циклическая $(n \times n)$-матрица имеет вид

$$\begin{pmatrix} a_0 & a_1 & \dots & a_j & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{j+1} & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & a_{j-1} & \dots & a_0 \end{pmatrix}.$$

Для построения циклической матрицы без прямоугольников рассмотрим любое множество $S = \{s_1, \dots, s_k\} \subset \mathbb{Z}_n$, в котором все разности $s_i - s_j \mod n$, где $i \neq j$, различны. Для всех $i = 1, \dots, k$ положим $a_{s_i} = 1$, а остальные a_j положим равными нулю.

Соответствующая циклическая матрица состоит из k циклических единичных диагоналей, проходящих через s_i-е позиции первой строки. Величины $s_i - s_j$ имеют смысл расстояния между этими диагоналями. Единицы, стоящие на одинаковых позициях в некоторых двух строках, относятся к разным циклическим диагоналям. Следовательно, если бы по две единицы в некоторых двух строках были расположены на одних и тех же позициях, то для каждой из строк эти единицы относились бы к различным (упорядоченным) парам циклических диагоналей, но это противоречит построению: расстояния между диагоналями не повторяются. Поэтому построенная матрица не содержит прямоугольников.

В качестве такого множества S можно взять $(q^2+q+1, q+1, 1)$-разностное множество Зингера (при $q = 3$ получается пример таблицы с 52 клетками для задачи 15). Число единиц в этой матрице в точности равно полученной в теореме 10 верхней оценке числа единиц $n(1 + \sqrt{4n-3})/2 = nk$, где $n = q^2 + q + 1$, $k = q + 1$.

Задача 18. Докажите, что любая циклическая матрица без прямоугольников может быть получена указанным выше способом из подходящего разностного множества.

Матрица, построенная на основе множества Зингера, фактически совпадает с матрицей, строки которой являются характеристическими функциями прямых конечной проективной плоскости порядка q. Тот факт, что матрица не содержит прямоугольников, вытекает из того, что любые две прямые проективной плоскости пересекаются ровно в одной точке.

Если не требовать дополнительно свойства цикличности, то $(n \times n)$-матрицу с k единицами на каждой строке, не содержащую прямоугольников,

при $n = q^2 + q + 1$, $k = q + 1$ можно построить указанным выше способом, т. е. как *матрицу смежности точек и прямых* конечной проективной плоскости порядка q. Это несколько проще, так как не требует доказательства теоремы Зингера. Задача 17 показывает, что существование $(n \times n)$-матрицы без прямоугольников с максимально возможным числом единиц, равным $n(\sqrt{n - 3/4} + 1/2)$, равносильно существованию проективной плоскости с n точками.

Приведём более простой пример $(n \times n)$-матрицы без прямоугольников, содержащей приблизительно $n^{3/2}$ единиц. Этот пример предложил Э. И. Нечипорук в [11] для применения в теории сложности булевых функций. Через E_0 обозначим единичную матрицу размера $p \times p$, а через E_i — матрицу, получаемую из E_0 циклическим сдвигом строк на i позиций вниз.

Матрица H_p имеет вид

$$H_p = \begin{pmatrix} E_0 & E_0 & \dots & E_0 & \dots & E_0 \\ E_0 & E_1 & \dots & E_j & \dots & E_{p-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_0 & E_i & \dots & E_{ij} & \dots & E_{i(p-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_0 & E_{p-1} & \dots & E_{(p-1)j} & \dots & E_{(p-1)^2} \end{pmatrix}.$$

Проверим, что матрица H_p не содержит прямоугольников. Воспользуемся разбиением указанной матрицы на горизонтальные и вертикальные полосы ширины p, нумеруя их от 0 до $p-1$. Заметим, что на пересечении i-й горизонтальной полосы и j-й вертикальной полосы находится матрица E_{ij}.

Предположим, что некоторые две строки и некоторые два столбца матрицы H_p в пересечении образуют «единичный» прямоугольник. Пусть эти строки расположены в i_1-й и i_2-й горизонтальных полосах, а столбцы — в j_1-й и j_2-й вертикальных полосах. Очевидно, $i_1 \neq i_2$ и $j_1 \neq j_2$, так как в любой строке и любом столбце матрицы E_k содержится ровно по одной единице.

Легко видеть, что для любой строки i-й горизонтальной полосы расстояние между единицами из l_1-й и l_2-й вертикальных полос, где $l_1 < l_2$, совпадает с $i(l_1 - l_2)$ по модулю p. В частности, согласно предположению совпадают по модулю p расстояния между единицами i_1-й и i_2-й полос на пересечении с j_1-м и j_2-м столбцами. Таким образом,

$$i_1(j_1 - j_2) \equiv i_2(j_1 - j_2) \bmod p,$$

откуда следует

$$(i_1 - i_2)(j_1 - j_2) \equiv 0 \bmod p,$$

что невозможно в силу $0 < |i_1 - i_2|, |j_1 - j_2| < p$.

Матрица H_p является матрицей Нечипорука [11][18], в которой строки и столбцы нумеруются двойными индексами (a, b) и (x, y) соответственно, а единица стоит на пересечении строки (a, b) и столбца (x, y) в том и только том случае, когда $y \equiv ax + b \mod p$. Для столбцов следует принять лексикографический порядок нумерации:

$$(x, y) = (0, 0), (0, 1), \ldots, (0, p-1), (1, 0), \ldots, (1, p-1), \ldots, (p-1, p-1),$$

а для строк несколько видоизменённый:

$$(a, b) = (0, 0), (0, 1), \ldots, (0, p-1), (p-1, 0), (p-1, 1), \ldots, (p-1, p-1),$$
$$(p-2, 0), (p-2, 1) \ldots, (p-2, p-1), \ldots, (1, 0), (1, 1), \ldots, (1, p-1).$$

Проверим: i-ю горизонтальную полосу такой матрицы определяет соотношение $a = -i \mod p$, а j-ю вертикальную — соотношение $x = j$. Тогда позиции единиц матрицы в пересечении полос определяются из соотношения $y \equiv -ij + b \mod p$, где b и y нумеруют строки и соответственно столбцы данной подматрицы. Это в точности матрица E_{ij}, что и требовалось.

Очевидно, число единиц в матрице (H_p) равно p^3.

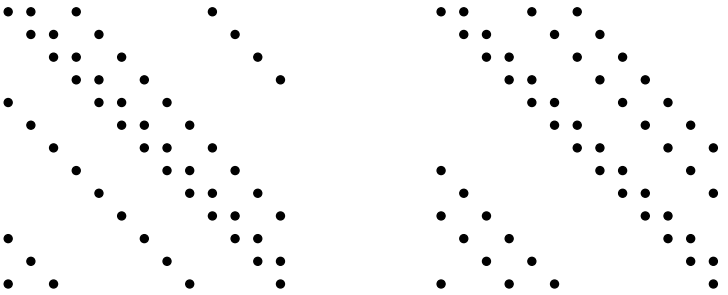
Матрица Нечипорука представляет из себя матрицу характеристических функций прямых конечной аффинной плоскости порядка p. Вместо p можно взять степень любого простого числа, если в качестве аффинной плоскости использовать координатную плоскость над конечным полем $\mathrm{GF}(q)$ (подобные вопросы рассматриваются, например, в [10]). Теперь рассмотрим семейство всех $q^2 + q$ прямых этой аффинной плоскости и заметим, что в ней через каждую точку проходит $q + 1$ прямая. Далее рассмотрим $(q^2 \times (q^2 + q))$-матрицу, в которой строки занумерованы точками плоскости $A(2, q)$, а столбцы — прямыми, причём на пересечении строки со столбцом стоит 1 тогда и только тогда, когда соответствующая точка лежит на соответствующей прямой. Эта матрица не содержит прямоугольников, имея $q + 1$ единиц в каждой строке и q единиц в каждом столбце. Из задачи 21 следует, что матрица, содержащая более $q^2(q + 1)$ единиц, обязательно содержит прямоугольник.

Задача 19. Постройте (25×25)-матрицу из нулей и единиц без прямоугольников с 5 единицами в каждой строке и в каждом столбце. Докажите, что аналогичную матрицу с 6 единицами в каждой линии построить нельзя. Дополните построенную (25×25)-матрицу до (25×30)-матрицы с 6 единицами в каждой строке и 5 единицами в каждом столбце так, чтобы в ней не появилось прямоугольников.

[18] Ранее эта матрица была построена в работе венгерских математиков Ковари, Турана и его супруги Веры Шош.

Задача 20. Постройте (13×13)-матрицу из нулей и единиц с 52 единицами без прямоугольников.

Указание. Возьмите разностное множество $\{0, 1, 3, 9\} \subset \mathbb{Z}_{13}$ и постройте циклическую матрицу, показанную слева.



Единицы в ней обозначены точками (а нули никак не обозначены). Можно взять другое разностное множество $\{0, 1, 4, 6\} \subset \mathbb{Z}_{13}$ и построить другую циклическую матрицу, показанную справа.

4.1. Проблема Царанкевича

Так называется задача, предложенная польским математиком Царанкевичем: заполнить матрицу размера $n \times m$ нулями и единицами так, чтобы единицы не образовывали прямоугольник данного размера (a, b) и единиц было максимальное число. Под прямоугольником понимается множество элементов матрицы, лежащих на пересечении a строк и b столбцов (любых, необязательно соседних). Булевы матрицы (т. е. матрицы из 0, 1) без единичных прямоугольников размера (a, b) назовём (a, b)-*редкими*. Число единиц в булевой матрице — её *вес*. В случае $a = b = 2$ эта проблема была предметом теоремы 10. Следующая теорема (Эрдёша и Царанкевича) развивает эту тему дальше.

Теорема 11. *Вес $\nu(A)$ любой $(a, 2)$-редкой булевой $(n \times m)$-матрицы A удовлетворяет неравенству*

$$\nu(A)\Big(\frac{\nu(A)}{n} - 1\Big) \leqslant m(m-1)(a-1).$$

Доказательство. Пусть $\nu(A) = k$. Для доказательства соотношения

$$k\Big(\frac{k}{n} - 1\Big) \leqslant m(m-1)(a-1)$$

оценим двумя способами число горизонтальных (т. е. лежащих в одной строке) пар единиц в матрице. Обозначим число единиц в i-й строке через x_i.

Тогда число горизонтальных пар единиц равно

$$\frac{x_1(x_1-1)+\ldots+x_n(x_n-1)}{2}.$$

С другой стороны, для каждой из $m(m-1)/2$ пар столбцов имеется не более $a-1$ горизонтальных пар единиц, накрываемых этой парой столбцов (иначе существовала бы $(a,2)$-подматрица, заполненная единицами). Поэтому

$$x_1(x_1-1)+\ldots+x_n(x_n-1)\leqslant m(m-1)(a-1).$$

Так как $x_1+\ldots+x_n=k$ — общее число единиц в матрице, применяя неравенство выпуклости к функции $f(x)=x^2-x$, имеем

$$n\frac{k}{n}\Big(\frac{k}{n}-1\Big)=nf\Big(\frac{k}{n}\Big)=nf\Big(\frac{x_1+\ldots+x_n}{n}\Big)\leqslant f(x_1)+\ldots+f(x_n)=$$
$$=x_1(x_1-1)+\ldots+x_n(x_n-1)\leqslant m(m-1)(a-1),$$

ч. т. д. □

Задача 21. Если $(q^2\times(q^2+q))$-матрица из нулей и единиц не содержит прямоугольников, то её вес не больше $q^2(q+1)$.

Указание. Примените теорему 11.

Задача 22. В клетчатом прямоугольнике 11×52 клетки раскрашены в два цвета. Доказать, что найдутся три строки и три столбца, на пересечении которых стоят клетки одного цвета.

Указание. Примените рассуждения, подобные доказательству теоремы 11.

Естественным продолжением этого раздела является раздел

§ 5. Редкие множества и редкие матрицы

В следующей задаче речь идёт по существу о матрице из нулей и единиц, в которой нет не только прямоугольников, но и параллелограммов.

Задача 23 (12-я Всесоюзная олимпиада (1978), 9 кл., 2-й день). Дано простое число $p>3$. Рассмотрим на координатной плоскости множество M, состоящее из таких точек с целыми координатами (x,y), что $0\leqslant x<p$, $0\leqslant y<p$. Докажите, что можно отметить p различных точек множества M так, чтобы никакие четыре из них не лежали в вершинах параллелограмма и никакие три из них не лежали на одной прямой.

В связи с рассмотрением этой и подобных задач обобщим введённое выше понятие разностного множества.

Пусть на множестве G определена операция $+$, удовлетворяющая сочетательному закону и тождеству $x + 0 = x$. Такие множества назовём *полугруппами*[19]. Подмножество H полугруппы $(G, +)$ назовём (k, l)-*редким*, если оно не содержит подмножеств вида $A + B = \{a + b \mid a \in A,\ b \in B\}$, где $|A| = k$ и $|B| = l$ (здесь и далее мощность конечного множества M обозначается через $|M|$).

Полугруппу назовём *группой*, если для каждого её элемента x найдётся единственный такой элемент y, что $x + y = y + x = 0$. В случае группы определение редкого множества равносильно следующему: подмножество H группы $(G, +)$ называется (k, l)-редким, если для любых различных элементов $g_1, \dots, g_k \in G$ справедливо неравенство

$$\left| \bigcap_{i=1}^{k} g_i H \right| < l, \quad \text{где} \quad g_i H = \{g_i\} + H.$$

Проверим равносильность двух определений. Действительно, пусть для некоторых $g_1, \dots, g_k \in G$ выполняется неравенство

$$\left| \bigcap_{i=1}^{k} g_i H \right| \geqslant l.$$

Поскольку

$$\{-g_1, \dots, -g_k\} + \bigcap_{i=1}^{k} g_i H \subset H,$$

H не является (k, l)-редким в смысле первого определения.

Обратно, пусть $A + B \subset H$, $A = \{g_1, \dots, g_k\}$, $|B| = l$. Поскольку

$$B \subset \bigcap_{i=1}^{k} (-g_i) H,$$

получаем

$$\left| \bigcap_{i=1}^{k} (-g_i) H \right| \geqslant l.$$

Значит, H не является (k, l)-редким в смысле второго определения.

Подмножество H группы $(G, +)$ назовём *разностным*, если для любых элементов $a, b, c, d \in H$ справедлива импликация

$$0 \neq a - b = c - d \quad \Rightarrow \quad (a = c)\ \&\ (b = d).$$

[19] Примером полугруппы служит множество векторов длины n с целыми неотрицательными координатами и покоординатной операцией сложения.

Пусть в группе $(G,+)$ операция сложения удовлетворяет тождеству $x+y=y+x$ и уравнение $x+x=0$ имеет только нулевое решение[20]. Тогда можно проверить, что в группе $(G,+)$ подмножество H является разностным тогда и только тогда, когда для любых элементов $a,b,c,d\in H$ справедливо равенство

$$a+b=c+d \quad\Rightarrow\quad ((a=c)\ \&\ (b=d))\vee((a=d)\ \&\ (b=c)).$$

Далее 2-редкое множество означает $(2,2)$-редкое. Покажем, что в группе $(G,+)$ определения разностного и 2-редкого подмножества равносильны. Пусть $H\subset G$ не является 2-редким, т. е. для некоторых элементов $a\neq b$, $c\neq d$ выполнено $a+c,a+d,b+c,b+d\in H$. Но тогда

$$0\neq(b+c)-(a+c)=(b+d)-(a+d),$$

при этом $b+c\neq b+d$, значит, H не является разностным.

Пусть теперь H не является разностным, т. е. для некоторых элементов $a,b,c,d\in H$ выполняется $a+b=c+d$, при этом $a\neq c$, $a\neq d$. Но тогда $\{a,d\}+\{c-a,0\}=\{a,b,c,d\}\subset H$, т. е. H не является 2-редким.

Обозначим через $(\mathrm{GF}(q)^n,+)$ группу, образованную упорядоченными наборами $(a_1,\dots,a_n)$ элементов конечного поля $\mathrm{GF}(q)$ порядка q, в которой операция сложения определяется как покомпонентное сложение этих наборов: $(a_1,\dots,a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n)$. Так как q^n будет степенью простого числа, если q — степень простого, существует поле $\mathrm{GF}(q^n)$ порядка q^n. По операции сложения оно образует группу, которую обозначим $(\mathrm{GF}(q^n),+)$. Известна следующая

Теорема 12. (i) *В группе* $(\mathrm{GF}(q)^2,+)$ *при нечётном* q «*парабола*» $\{(x,x^2)\mid x\in\mathrm{GF}(q)\}$ *является* 2*-редким подмножеством мощности* q.

(ii) *В группе* $(\mathrm{GF}(q)^3,+)$, *где* q *нечётно*, «*сфера*»

$$\{(x,y,z)\mid x^2+y^2+z^2=\gamma\},$$

где $-\gamma$ *не является квадратом никакого элемента поля* $\mathrm{GF}(q)$, *является* 3*-редким подмножеством мощности* q^2-q.

(iii) *В группе* $(\mathrm{GF}(q^t),+)$ *множество таких элементов* x, *что* $x^{\frac{q^t-1}{q-1}}=1$, *является* $(t,t!+1)$*-редким подмножеством мощности* $(q^t-1)/(q-1)$.

Доказательство. Докажем (i). Проверим, что из равенства для двумерных векторов над $\mathrm{GF}(q)$

$$(x,x^2)-(y,y^2)=(z,z^2)-(u,u^2)\neq(0,0)$$

[20] Примером такой группы служит множество $\{0,1,\dots,n-1\}$ с операцией сложения по модулю n при $n>2$.

следует, что $x = z$ и $y = u$. Действительно, система уравнений

$$\begin{cases} x - y = a, \\ x^2 - y^2 = b \end{cases}$$

над этим полем при $a \neq 0$ эквивалентна системе

$$\begin{cases} x - y = a, \\ x + y = \dfrac{b}{a}, \end{cases}$$

которая имеет единственное решение.

Таким образом, рассматриваемая парабола является разностным, следовательно, 2-редким подмножеством в $\mathrm{GF}(q)^2$.

Утверждение (ii) фактически доказано У. Брауном в [3]. Точнее, он доказал, что пересечение любых трёх различных сфер

$$S(a, b, c) = \{(x, y, z) \mid (x - a)^2 + (y - b)^2 + (z - c)^2 = \gamma\}$$

состоит не более чем из двух точек. Теперь, если предположить, что сфера $S(0, 0, 0)$ не является 3-редким подмножеством, т. е. $A + B \subset S(0, 0, 0)$, где $|A| = |B| = 3$, то в силу того, что произвольную сферу $S(a, b, c)$ можно представить в виде $\{(a, b, c)\} + S(0, 0, 0)$, получим, что трёхэлементное множество B содержится в каждой из сфер $S(a, b, c)$, где $(-a, -b, -c) \in A$, что противоречит доказанному.

Доказательство того, что число точек сферы $S(0, 0, 0)$ равно $q^2 - q$, опускаем, так же как и весьма сложное доказательство (iii), найденное венгерскими математиками Роньяи, Колларом и Сабо в 1996 г. □

Приведём пример 3-редкого множества в группе $\mathbb{Z}_3^3$, построенного методом Брауна. Указанная группа состоит из всех троичных наборов длины три от $(0, 0, 0)$ до $(2, 2, 2)$. Сложение в ней выполняется покомпонентно по модулю три, например $(1, 2, 0) + (2, 2, 1) = (0, 1, 1)$. К операции сложения по модулю три в группе $\mathbb{Z}_3 = \{0, 1, 2\}$ можно добавить операцию умножения по модулю три (и тогда эта группа превратится в поле $\mathrm{GF}(3)$) и рассмотреть в трёхмерном арифметическом пространстве $\mathrm{GF}(3)^3 = \{0, 1, 2\}^3$ сферу с центром в нуле $(0, 0, 0)$, определяемую уравнением $x^2 + y^2 + z^2 = 1$. Эта сфера состоит из 6 наборов (точек): $(0, 0, 1)$, $(0, 0, 2)$, $(0, 1, 0)$, $(0, 2, 0)$, $(1, 0, 0)$, $(2, 0, 0)$. Действительно, x^2 в поле $\mathrm{GF}(3)$ равен 0 или 1, а сумма трёх квадратов равна 1, только когда один из них 1, а остальные 0. Для проверки 3-редкости этого множества в группе $\mathbb{Z}_3^3$ достаточно проверить, что любая сдвинутая сфера $(x - a)^2 + (y - b)^2 + (z - c)^2$ пересекается со сферой $x^2 + y^2 + z^2 = 1$ не более чем в двух точках, в чём можно убедиться и непосредственной проверкой (в силу симметрии достаточно рассмотреть

не все 26, а меньшее число сдвигов). Тогда и любые две сдвинутые сферы пересекаются не более чем в двух точках, потому что система уравнений

$$\begin{cases} (x-a')^2+(y-b')^2+(z-c')^2=1, \\ (x-a)^2+(y-b)^2+(z-c)^2=1 \end{cases}$$

линейной заменой переменных сводится к системе

$$\begin{cases} x^2+y^2+z^2=1, \\ (x-a'')^2+(y-b'')^2+(z-c'')^2=1 \end{cases}$$

и поэтому имеет столько же решений.

Далее (k,k)-редкую матрицу называем просто k-редкой. (k,k)-редкие матрицы называем просто k-редкими. Про них известна следующая

Теорема 13. (i) *Существует k-редкая $(n\times n)$-матрица с весом не более $C_k(n^{\frac{2k}{k+1}})$, где C_k — некоторая константа, зависящая от k и не зависящая от n.*

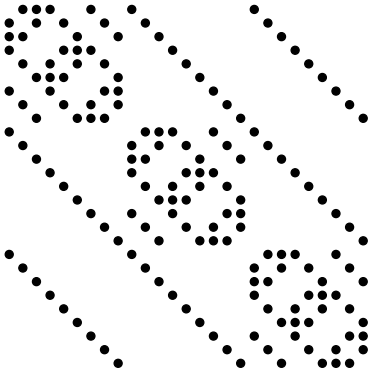
(ii) *В случае $k=2$ существует 2-редкая симметрическая $(n\times n)$-матрица с весом $(1+\varepsilon_n)n^{3/2}$, где $\varepsilon_n\to 0$ при $n\to\infty$.*

(iii) *В случае $k=3$ существует 3-редкая симметрическая $(n\times n)$-матрица с весом $(1+\varepsilon_n)n^{5/3}$, где $\varepsilon_n\to 0$ при $n\to\infty$.*

(iv) *Для $t\geqslant 2$ существует $(t,t!+1)$-редкая симметрическая $(n\times n)$-матрица с весом $(1+\varepsilon_n)n^{(2t-1)/t}$, где $\varepsilon_n\to 0$ при $n\to\infty$.*

Доказательство теоремы довольно сложное и здесь не приводится. Укажем только, что доказательство последних трёх пунктов основано на использовании теоремы 12 и асимптотического закона распределения простых чисел.

Основываясь на приведённом выше примере 3-редкого множества в группе $\mathbb{Z}_3^3$, построим 3-редкую симметричную (27×27)-матрицу, в которой в каждой строке и столбце ровно 6 единиц.



Из построения очевидна симметричность матрицы. Это её свойство даёт возможность построить по ней граф с 27 вершинами, каждая из которых соединена с 6 другими (регулярный граф степени 6). Такой граф не содержит подграфов $K_{3,3}$ — полных двудольных графов с тремя вершинами в каждой доле, содержащих всевозможные рёбра (этот граф известен как граф задачи о трёх домах и трёх колодцах). Граф по матрице строится следующим образом: вершина i соединяется ребром с вершиной j тогда и только тогда, когда элемент матрицы $a_{i,j}$, лежащий на пересечении i-й строки и j-го столбца, равен 1 (это граф, у которого матрица смежности вершин совпадает с данной матрицей A).

На рис. 8 можно увидеть, как выглядит симметричная, но не циклическая матрица порядка 125 без прямоугольников размера 3×7 с 16 единицами в каждой строке и каждом столбце, построенная методом п. (iii) теоремы 12.

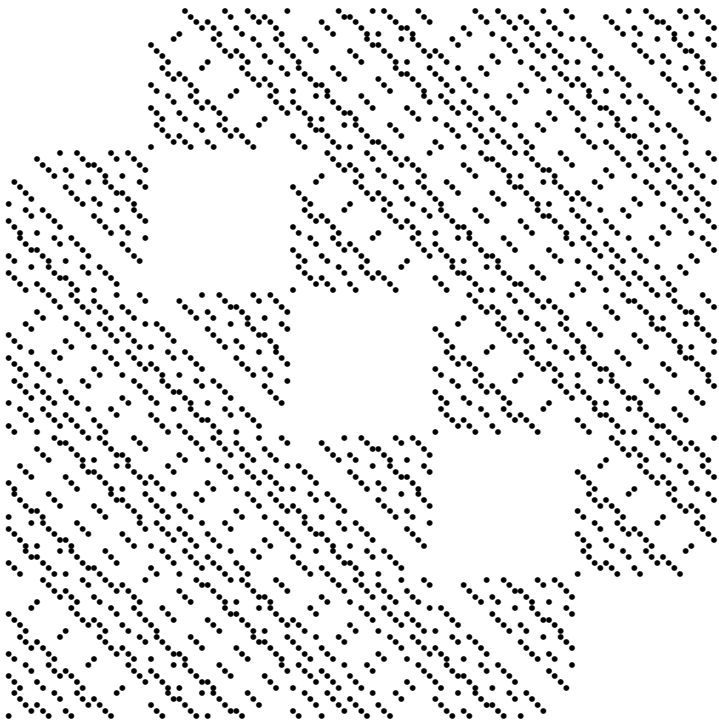


Рис. 8. Симметричная, но не циркулянтная, матрица порядка 125 *без прямоугольников* 3×7 *с* 16 *единицами на каждой линии*

Следующий параграф тесно связан с предыдущим, хотя сразу это не будет очевидно.

§ 6. Теорема Турана и экстремальные графы

На Всесоюзной олимпиаде некогда предлагалась [21)]

Задача 24 (3-я Всесоюзная математическая олимпиада (1969), 10 кл., второй день). В розыгрыше первенства страны по футболу участвуют 20 команд. Какое наименьшее число игр должно быть сыграно, чтобы среди любых трёх команд нашлись две, уже сыгравшие между собой?

На самом деле она является частным случаем следующей теоремы [16].

Теорема 14 (Мантель). *В компании из n человек среди любых трёх найдётся хотя бы одна пара незнакомых. Тогда число пар знакомых не больше $n^2/4$.*

Дальнейшим обобщением является

Теорема 15 (Туран). *Отрезки, соединяющие пары точек n-элементного множества, покрашены в белый и чёрный цвета так, что среди любых его $k+1$ точек найдётся хотя бы одна пара, соединённая белым отрезком. Тогда чёрных отрезков у этого множества не больше*

$$\frac{k-1}{2k}(n^2-r^2)+\frac{r(r-1)}{2}, \quad \text{где } n=kq+r,\ 0\leqslant r<k,\ q \text{ — целое число,}$$

причём для любых n, k эта оценка достигается.

Пять доказательств теоремы можно найти в [1].

Попытки доказать теоремы, аналогичные теореме Турана, привели к созданию *теории экстремальных графов*. В ней получены, например, следующие результаты.

Обозначим через $t(n, G)$ наибольшее число рёбер в n-вершинном графе, при котором возможно отсутствие в нём подграфа, изоморфного данному графу G [22)]. В случае $G=K_r$, где K_r — полный граф на r вершинах, число $t(n, G)=t(n, K_r)$ найдено в теореме Турана. Если $G=K_{r,s}$ — полный двудольный граф, в одной доле которого r вершин, а в другой s, то про $t(n, G)=t(n, K_{r,s})$ известно следующее.

Теорема 16 (Ковари — Шош — Туран). *При $2\leqslant r\leqslant s$ справедливо неравенство $t(n, K_{r,s})<C(s^{1/r}n^{2-1/r}+n)$, где C — некоторая константа. При $r=s$ справедливо неравенство*

$$t(n, K_{r,r})>cn^{2-2/(r+1)}.$$

[21)] Автору не довелось её решать на олимпиаде, так как он был классом младше, но задачу он с тех пор запомнил хорошо.

[22)] В теории экстремальных графов используется также обозначение $ex(n, G)$, но оно не напоминает о Туране.

Гипотеза Турана о том, что $t(n, K_{r,r}) > cn^{2-1/r}$, по-видимому, не доказана. Однако известна

Теорема 17 (Эрдёш — Реньи — Шош). *При $r = s = 2$ и $n = q^2 + q + 1$, где q — степень простого, справедливо неравенство*

$$t(n, K_{2,2}) \geqslant \frac{1}{2}q(q+1)^2;$$

при $n = q^2 - 1$, где $q = 2^m$, справедливо неравенство

$$t(n, K_{2,2}) \geqslant \frac{1}{2}q(q^2-2);$$

при любом n

$$n\frac{1+\sqrt{4n-3}}{4} \geqslant t(n, K_{2,2}) \gtrsim \frac{1}{2}n^{3/2}.$$

Доказательство. Для доказательства первого неравенства построим граф без циклов длины 4 с $n = q^2 + q + 1$ вершинами и $\frac{1}{2}q(q+1)^2$ рёбрами, где q — степень простого. Возьмём поле $\mathrm{GF}(q)$ и вспомним построение координатной проективной плоскости $\mathrm{PG}(2, q)$ над ним из п. 2.1. Её точками будут классы коллинеарности ненулевых троек (x, y, z), а прямыми — множества точек, удовлетворяющих равенству $ax + by + cz = 0$. Очевидно, коллинеарные тройки (a, b, c) и (a', b', c') определяют одну и ту же прямую, поэтому прямые тоже можно отождествить с классами коллинеарных троек. Число точек в $\mathrm{PG}(2, q)$, как и число прямых, равно $q^2 + q + 1$. Определим на множестве точек плоскости $\mathrm{PG}(2, q)$ граф, в котором пары классов ненулевых коллинеарных троек (x, y, z) и (a, b, c) соединяются ребром тогда и только тогда, когда $ax + by + cz = 0$ (это *полярное соответствие двойственности* между точками и прямыми в $\mathrm{PG}(2, q)$). Если точка не лежит на кривой $x^2 + y^2 + z^2 = 0$, то она соединяется с $q + 1$ прямой (это все прямые, через неё проходящие), т. е. степень соответствующей вершины графа равна $q + 1$. Поэтому сумма степеней таких вершин равна $(q^2 + q + 1 - (q + 1))(q + 1) = q^3 + q^2$. Если точка лежит на этой кривой, то среди проходящих через неё прямых есть и прямая, определяемая классом, содержащим тройку (x, y, z). Поэтому из соответствующей вершины графа выходит только q рёбер. Далее будет показано, что число точек на этой кривой в проективной плоскости $\mathrm{GF}(2, q)$ равно $q + 1$. Значит, сумма степеней этих вершин равна $(q + 1)q$. Следовательно, рассматриваемый граф имеет $q^2 + q + 1$ вершин и $(q^3 + q^2 + (q + 1)q)/2 = q(q + 1)^2/2$ рёбер. Любые две прямые в проективной плоскости $\mathrm{PG}(2, q)$ имеют ровно одну общую точку, поэтому в построенном графе нет циклов длины 4 (если бы вершины l, p, m, q образовывали цикл, то прямые, соответствующие вершинам l, m, проходили бы через точки, соответствующие вершинам p, q).

Покажем, что число точек на указанной кривой в проективной плоскости $\mathrm{GF}(2, q)$ равно $q+1$. Действительно, если q — степень двойки, то в поле $\mathrm{GF}(q)$ квадратные корни всегда существуют и определены однозначно, поэтому число ненулевых решений уравнения $x^2+y^2+z^2=0$ равно q^2-1. Значит, точек на кривой ровно $q+1$.

Пусть теперь $q \neq 2^m$. Число точек в пересечении данной кривой с плоскостью $z=0$ равно числу попарно неколлинеарных ненулевых решений уравнения $x^2+y^2=0$. Если из -1 не извлекается квадратный корень в поле $\mathrm{GF}(q)$ (иначе говоря, -1 — квадратичный невычет), то таких решений нет. Если же -1 есть квадратичный вычет, то неколлинеарных решений два (так как всего решений четыре: $(\pm x, \pm y)$). Число точек на кривой с $z \neq 0$ равно числу решений уравнения $x^2+y^2=-1$ в поле $\mathrm{GF}(q)$. Применяя утверждение задачи 25 (см. ниже), получаем в обоих случаях один ответ: число точек на рассматриваемой кривой в проективной плоскости $\mathrm{GF}(2, q)$ равно $q+1$.

Для доказательства второго неравенства построим граф без циклов длины 4 с $n=q^2-1$ вершинами и $\frac{1}{2}q(q^2-2)$ рёбрами. Рассмотрим поле $\mathrm{GF}(q)$, $q=2^m$, и определим граф на множестве вершин вида $(x, y) \in \mathrm{GF}(q)^2 \setminus \{(0,0)\}$, соединив пары вершин (x, y) и (a, b) ребром тогда и только тогда, когда $ax+by=1$ (т. е. точка (x, y) лежит на прямой $aX+bY=1$ в координатном представлении аффинной плоскости над полем $\mathrm{GF}(q)$, указанном в п. 2.1). Если $(a, b)=(x, y)$, ребро не проводим. Такие исключительные точки лежат на окружности $x^2+y^2=1$ в конечной плоскости $\mathrm{GF}(q)^2$ над этим полем. Так как q — степень двойки, в поле $\mathrm{GF}(q)$ квадратные корни всегда существуют и определены однозначно, поэтому число решений уравнения $x^2+y^2=1$ равно q. Из неисключительных вершин (а их ровно q^2-q-1) выходит по q рёбер, так как на каждой прямой $aX+bY=1$ лежит по q точек. Из исключительных вершин выходит по $q-1$ ребру. Удвоенное общее число рёбер равно $(q^2-q-1)q+q(q-1)=q^3-2q$. Любые две прямые имеют не более одной общей точки, поэтому в построенном графе нет циклов длины 4.

Для доказательства верхней оценки в третьем неравенстве построим по данному графу, не содержащему $K_{2,2}$, двудольный граф, удвоив каждую вершину и из дубликатов образовав вторую долю. Вершины из разных долей соединим ребром, если вершины исходного графа, из которых они были получены, соединялись ребром. Очевидно, что число рёбер в двудольном графе вдвое больше числа рёбер в исходном. Матрица смежности рёбер двудольного графа имеет число единиц, вдвое большее числа рёбер исходного графа, и не содержит прямоугольников из единиц. Действительно, эта матрица симметрична относительно главной диагонали и на диагонали

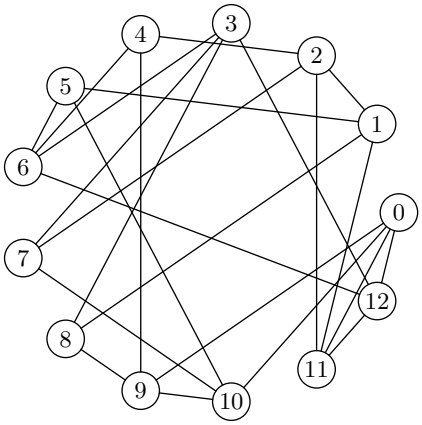
стоят нули. Если бы она содержала прямоугольник, в двудольном графе были бы вершины a, b в одной доле и вершины $c \neq a$, $c \neq b$, $d \neq a$, $d \neq b$ в другой доле, образующие подграф $K_{2,2}$. Но тогда соответствующие 4 вершины исходного графа соединялись бы рёбрами (a, c), (a, d), (b, c), (b, d), т. е. образовывали подграф $K_{2,2}$, что невозможно. Согласно теореме 10 тогда число единиц в матрице не больше $n(1 + \sqrt{4n - 3})/2$. Поэтому число рёбер в исходном графе не больше $n(1 + \sqrt{4n - 3})/4$.

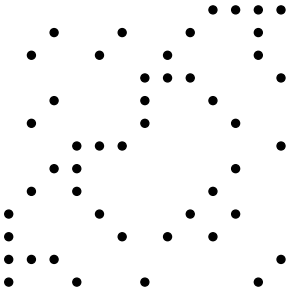
Для доказательства асимптотической нижней оценки в третьем неравенстве выберем простое $q = q_n$ так, чтобы $n \leqslant m = q^2 + q + 1$ и $q \sim \sqrt{n}$, для чего применим асимптотический закон распределения простых чисел Адамара и Валле Пуссена (из него следует, что при любом $\varepsilon > 0$ для достаточно больших n найдётся такое простое p, что $n < p < (1 + \varepsilon)n$). Очевидно, что справедливо асимптотическое равенство $n \sim m$. Возьмём построенный выше граф без циклов длины 4 с m вершинами и $e = q(q+1)^2/2 \sim n^{3/2}/2$ рёбрами. Согласно задаче 26 (см. ниже) в нём найдётся подграф с n вершинами и не менее чем

$$e\frac{n(n-1)}{m(m-1)} \sim e \sim \frac{n^{3/2}}{2}$$

рёбрами. Очевидно, в нём нет циклов длины 4, так как их не было в объемлющем графе. □

Вот пример графа с 13 вершинами и 24 рёбрами без циклов длины 4 и его матрица смежности вершин — симметричная матрица без прямоугольников.





Это симметричная относительно главной диагонали (13×13)-матрица с 48 единицами, с 9 строками по 4 единицы и 4 строками по 3 единицы, не содержащая прямоугольников.

Задача 25. Если $q \neq 2^m$ и -1 является квадратичным вычетом в поле $\mathrm{GF}(q)$, то число точек на окружности $x^2 + y^2 = -1$ в плоскости $\mathrm{GF}(q)^2$ равно $q-1$, а если -1 является квадратичным невычетом, то число точек на окружности $x^2 + y^2 = -1$ равно $q+1$.

Указание. В первом случае существует элемент $i \in \mathrm{GF}(q)$, $i^2 = -1$. Тогда число решений уравнения $x^2 + y^2 = a$, $a \neq 0$, равно общему числу решений систем $(x + iy) = u$, $(x - iy) = a/u$ при всех значениях ненулевого параметра $u \in \mathrm{GF}(q)$, т. е. равно $q-1$, так как при любом фиксированном $u \neq 0$ линейная система имеет единственное решение.

Если же -1 — невычет, то при любом y элемент $-y^2$ тоже невычет (иначе -1 — вычет). Пусть $QR \subset \mathrm{GF}(q)\setminus\{0\}$ — множество всех ненулевых вычетов (их количество, очевидно, $(q-1)/2$, так как корень из ненулевого элемента извлекается ровно двумя способами), а NR — множество всех невычетов (тогда их количество тоже $(q-1)/2$, так как количество ненулевых элементов $q-1$). Далее, пусть QR_+, NR_+ — количества квадратичных вычетов вида $a-1$, где соответственно $a \in QR$ и $a \in NR$. Число решений уравнения $x^2+1=-y^2$ вдвое больше общего числа всех решений уравнений $x^2+1=a$ с параметром $a \in NR$ (действительно, $-y^2$ при $y \neq 0$ пробегает всё множество NR, а при $y=0$ решений нет). Следовательно, оно равно $4NR_+$.

Заметим теперь, что число точек на гиперболе $x^2-y^2=-1$ вдвое больше общего числа решений уравнений $x^2 + 1 = a$ при значениях параметра $a \in QR$. Если $a=1$, то решение одно ($x=0$), а в остальных случаях решений два. Поэтому число точек на гиперболе равно $4QR_+ - 2$. Но очевидно, что уравнение $x^2-y^2=-1$ имеет столько же решений, сколько и система $x+y=u$, $x-y=-1/u$, т. е. $q-1$. Отсюда $QR_+ = ((q-1)+2)/4 = (q+1)/4$. Общее количество квадратичных вычетов, включая нулевой, равно

$$\frac{q-1}{2} + 1 = \frac{q+1}{2}.$$

С другой стороны, оно равно $QR_+ + NR_+$, поскольку $0-1=-1$ — невычет. Отсюда $NR_+ = (q+1)/2 - (q+1)/4 = (q+1)4$. Значит, число точек на окружности $x^2 + y^2 = -1$ равно $q+1$.

Задача 26. Назовём средним числом рёбер в графе с v вершинами число $e/(v(v-1))$, где e — число рёбер в нём. Докажите, что в любом графе с m вершинами при любом $n \leqslant m$ найдётся подграф с n вершинами, у которого среднее число рёбер не меньше, чем у всего графа.

Указание. Для каждого подграфа G с n вершинами определим число рёбер $e(G)$ и просуммируем эти числа по всем $\binom{m}{n}$ подграфам. Каждое ребро будет входить в эту сумму $\binom{m-2}{n-2}$ раз, потому что оно принадлежит

ровно $\binom{m-2}{n-2}$ подграфам (каждый из них определяется выбором $n-2$ вершин из числа $m-2$ вершин данного графа, отличных от концов рассматриваемого ребра). Поэтому сумма равна $e\binom{n-2}{m-2}$, где e — число рёбер в данном графе. Из принципа Дирихле следует, что один из подграфов с n вершинами имеет не менее

$$\frac{e\binom{m-2}{n-2}}{\binom{m}{n}} = \frac{en(n-1)}{m(m-1)}$$

рёбер. Деля на $n(n-1)$, получаем требуемое.

Теорема 17 была усилена в 1980-е годы молодым (тогда) венгерским математиком Золтаном Фюреди [23)].

Теорема 18 (Фюреди). *При $n = q^2+q+1$, где $q \geqslant 15$ — степень простого, $t(n, K_{2,2}) = \frac{1}{2}q(q+1)^2$. При любом $q \geqslant 13$ имеем $t(n, K_{2,2}) \leqslant \frac{1}{2}q(q+1)^2$.*

Задача 27 (Олимпиада «Студент и научно-технический прогресс», 1981 г., городской тур, II секция; [9], с. 81). В компании из 1981 человека каждый имеет не меньше 45 знакомых. Доказать, что можно выбрать четырёх человек и посадить их за круглый стол так, чтобы каждый сидел рядом со своими знакомыми.

Задача 28. На конгрессе из 1893 участников все, кроме 44, имеют по 44 знакомых, а эти 44 имеют по 43 знакомых. Доказать, что может случиться так, что никаких четырёх человек нельзя будет посадить за стол между знакомыми.

Ещё две теоремы без доказательства.

Теорема 19 (Ковари — Шош — Туран — Фюреди).

$$\frac{1}{2}\sqrt{s}n^{3/2} - cn^{4/3} \leqslant t(n, K_{2,s}) \leqslant \frac{1}{2}\sqrt{s}n^{3/2} + \frac{n}{4}\ .$$

Теорема 20. *При $r = s = 3$ справедливы неравенства*

$$cn^{5/2} \leqslant t(n, K_{3,3}) \leqslant Cn^{5/2} \quad \text{(Браун)},$$

а при $r \geqslant 4$, $s \geqslant r! + 1$ — неравенство

$$t(n, K_{r,s})) > C_r(n^{2-1/r}) \quad \text{(Коллар — Роньяи — Сабо)}.$$

Ещё кое-что на тему теоремы Турана можно прочитать в [8, 12].

[23)] Между прочим, победителем одной из международных олимпиад.

Список литературы

[1] *Айгнер М., Циглер Г.* Доказательства из книги. М.: Бином, 2015.

[2] *Артин Э.* Геометрическая алгебра. М.: Наука, 1969.

[3] *Браун У. Г.* Графы, не содержащие графа Томпсена // Кибернетический сборник. Вып. 18. М.: Мир, 1981. С. 34–38.

[4] *Васильев Н. Б., Егоров А. А.* Задачи Всесоюзных математических олимпиад. М.: Наука, 1988.

[5] *Васильев Н. Б., Гутенмахер В. Л., Раббот Ж. М., Тоом А. Л.* Заочные математические олимпиады. М.: Наука, 1987.

[6] *Гальперин Г. А., Толпыго А. К.* Московские математические олимпиады. М.: Просвещение, 1986.

[7] *Гашков С. Б.* Современная элементарная алгебра. М.: МЦНМО, 2006.

[8] *Гашков С. Б.* a-Диаметры и турановские графы // Математическое просвещение. Сер. 3. Вып. 12. М.: МЦНМО, 2008. С. 161–175.

[9] *Григорян А. А., Конягин С. В., Садовничий В. А.* Задачи студенческих математических олимпиад. М.: МГУ, 1987.

[10] *Картеси Ф.* Введение в конечные геометрии. М.: Наука, 1980.

[11] *Нечипорук Э. А.* Об одной булевской матрице // Доклады АН СССР. 1966. Т. 169(4). С. 765; Проблемы кибернетики. Вып. 21. С. 237–240. М.: Наука, 1969.

[12] *Райгородский А., Шабанов Л.* Об одной «олимпиадной» задаче про графы расстояний // Квант. 2015. №3. С. 7–10.

[13] *Таранников Ю. В.* Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011.

[14] *Холл М.* Комбинаторика. М.: Мир, 1970.

[15] *Яглом И. М., Яглом А. М.* Неэлементарные задачи в элементарном изложении. М.: Эдиториал УРСС, 2006.

[16] *Mantel W.* // Wisk Opgaven. 1907. V. 10. P. 60–61.

[17] *Winkler P.* Mathematical puzzles: a connoisseur's collection. A. K. Peters, 2004.

Сергей Борисович Гашков, мехмат МГУ
sbgashkov@gmail.com