Наш семинар: математические сюжеты

Коды и олимпиады

С. Б. Гашков

§ 1. Введение

> Прикладная математика — это когда вы ищете решение задачи, а чистая — это когда вы ищете задачу для решения.
>
> *Финн, «Анна и Чёрный рыцарь»*

Пусть читатель попробует самостоятельно решить хотя бы некоторые из приведённых далее задач. Некоторые из них в том или ином виде предлагались на различных олимпиадах [1)] (в скобках указано, где именно, и эти задачи можно найти в [2, 8–11]). Что между ними общего?

Задача 1 (ММО 1954, второй тур, 10.5). Рассматриваются всевозможные десятизначные десятичные числа, записываемые при помощи цифр 1 и 2. Разбейте их на два класса так, чтобы сумма любых двух чисел из одного класса содержала в своей записи не менее двух троек.

Задача 2 (ММО 1967, второй тур, 8.3). Для зашифровки телеграфных сообщений требуется разбить всевозможные десятичные «слова» — наборы из десяти точек и тире — на две группы так, чтобы любые два слова одной группы отличались не менее чем в трёх разрядах. Укажите способ такого разбиения или докажите, что его не существует.

[1)] ММО означает Московскую, а ВМО — Всесоюзную математическую олимпиаду.

Задача 3 (олимпиада ФРГ, 1970/71 г., второй тур). В племени Мумбо-Юмбо все имена различны, состоят из букв А и Б, имеют длину n и отличаются друг от друга не менее чем тремя буквами. Докажите, что в племени не более $2^n/(n+1)$ человек. Может ли эта граница достигаться? В соседнем племени АББА имена отличаются не менее чем двумя буквами. Докажите, что в племени не более 2^{n-1} человек. Может ли эта граница достигаться?

Задача 4. Множество из всех k-значных n-разрядных упорядоченных наборов $(x_1, \ldots, x_n)$, $x_i \in \{0, \ldots, k-1\}$, назовём n-мерной k-ичной шахматной доской. Будем говорить, что ладья, находящаяся в поле с координатами $(x_1, \ldots, x_n)$, бьёт любое поле $(x_1, \ldots x_{i-1}, y, x_{i+1}, \ldots, x_n)$, $y = 0, \ldots, k-1$, $i = 1, \ldots, n$. Обозначим через $m(n, k)$ минимальное число ладей, бьющих все поля доски. Докажите, что

а) $m(2, k) = k$;

б) (ВМО 1971, 9.6, 10.6) $m(3, k) = \lfloor k^2/2 \rfloor$;

в) $m(n, k) \leqslant k^n/((k-1)n+1)$;

г) если k равно степени простого числа, то неравенство пункта (в) обращается в равенство при $n = 1 + k + \ldots + k^i$, $i = 1, 2, \ldots$

Задача 5 (волшебный веер Эдуарда Люка[2)]). Зрителю предлагается задумать число от 1 до 31. Фокусник предлагает ему сказать, в каких полосках веера он видит задуманное число, а в каких — нет.

На первой полоске написаны все нечётные числа.

На второй — числа 2, 3, 6, 7, 10, 11, 14, 15, 18, 19, 22, 23, 26, 27, 30, 31.

На третьей — числа 4, 5, 6, 7, 12, 13, 14, 15, 20, 21, 22, 23, 28, 29, 30, 31.

На четвёртой — числа 8, 9, 10, 11, 12, 13, 14, 15, 24, 25, 26, 27, 28, 29, 30, 31, и на последней — все числа от 16 до 31.

Как фокусник угадывает задуманное число?

Задача 6 (теорема Заранкевича[3)]). Пусть $k = k_{a,b}(n, m)$ — наибольшее число единиц в таблице с n строками и m столбцами, заполненной нулями и единицами и не содержащей a строк и b столбцов, на пересечении которых стояли бы сплошь единицы. Тогда k — наибольшее такое число, что[4)]

$$n\binom{k/n}{b} \leqslant (a-1)\binom{m}{b}.$$

[2)] Эта задача из книги по занимательной математике, опубликованной в XIX в. французским математиком Э. Люка (1842–1891), автором многих красивых задач и теорем.

[3)] К. Заранкевич (1902–1959) — польский математик, опубликовавший задачу на эту тему в 50-е годы. Сама теорема впервые появилась в статьях венгерского математика П. Эрдёша (1913–1996). Несколько олимпиадных задач, фактически являющихся частными случаями этой теоремы, можно найти в [4].

[4)] Далее через $\binom{x}{y}$ обозначается количество сочетаний из x по y (другое распространённое обозначение — C_x^y).

Все эти задачи относятся к интересной области современной прикладной математики — теории кодирования. Как они решаются, станет понятно при чтении соответствующих разделов этой статьи.

§ 2. Что такое коды?

> Изначально его убеждение состояло в том, что перед ним — именно шифр, ибо то, что алхимики и некроманты в старину часто пользовались тайнописью, давно стало общеизвестным фактом: видимо, эти искатели истины пытались либо уберечь секреты от соперников, либо укрыть их от ревнивых глаз церковных властей.
>
> *Джон Гласби, «Чёрное зеркало»*

Двоичным кодом C с *блоковой длиной* n можно назвать любое множество двоичных наборов длины n (называемых также *кодовыми словами*)[5]. *Расстоянием* между словами a, b называется число позиций, в которых эти слова различаются. Например, $d(a, b) = 3$ в случае $a = (11001)$, $b = (00011)$. Очевидно, что для любых $a, b, c \in B^n$ выполняется *неравенство треугольника* $d(a, b) + d(b, c) \geqslant d(a, c)$, а также ещё два условия: $d(a, b) = d(b, a)$ и $d(a, b) = 0$ только в случае $a = b$. *Минимальным расстоянием* кода C называется число $d(C) = \min_{a,b \in C} d(a, b)$, равное минимальному расстоянию между его различными словами. В задаче 3 на самом деле речь идёт о коде с минимальным расстоянием, не меньшим 3, и о коде с минимальным расстоянием, не меньшим 2. В задаче 2 также фигурируют два кода с расстоянием, не меньшим 3. Задача 1 легко решается, если увидеть её связь с кодом с минимальным расстоянием 2.

Интерес для кодирования с исправлением ошибок представляют только коды с расстоянием, большим единицы. Например, код C, состоящий из всех наборов чётного веса. *Весом* набора называется число ненулевых позиций в нём. Этот код (он даёт решение второй половины задачи 3) можно использовать для обнаружения одной ошибки. Предположим, что надо передать по ненадёжному каналу связи двоичное слово $x = (x_1, \ldots, x_{n-1})$. Известно, что в полученном слове может быть одна ошибка (замена двоичного символа 0 или 1 на противоположный). Если передавать в точности слово x, то ошибку заметить невозможно. Но если к слову x добавить

[5] Код C можно рассматривать как подмножество множества вершин двоичного n-мерного куба $B^n = \{0, 1\}^n$.

один *проверочный символ* $c_n = x_1 \oplus \ldots \oplus x_n$ (где $\oplus$ — операция *сложения по модулю два*[6]) и передать закодированное слово

$$c = (c_1, \ldots, c_n) = (x_1, \ldots, x_{n-1}, c_n),$$

то ошибку легко обнаружить, так как если её не было, то $c_1 \oplus \ldots \oplus c_n = 0$, а если ошибка была, то эта сумма равна единице. Указанный код называется *проверкой на чётность*[7].

Бинарным линейным кодом длины n называется любое такое множество двоичных векторов длины n, что покомпонентная сумма по модулю два любых двух его векторов всегда принадлежит коду. Число единиц в сумме двух векторов по модулю два очевидно равно расстоянию между этими векторами. Бинарный линейный код можно рассматривать как линейное пространство над полем $\{0, 1\}$ из двух элементов. Размерность этого пространства называется *размерностью кода*. Простейшая часть их теории является переформулировкой теорем линейной алгебры. В задачах 9, 10 как раз речь идёт о линейных кодах (и их размерностях).

Можно рассматривать не только двоичные (бинарные), но и q-ичные коды при $q > 2$. *Расстоянием* между q-ичными векторами x, y называется число $\rho(x, y)$ координат, в которых эти векторы не совпадают. Так определённое расстояние совпадает в случае $q = 2$ с введённым выше, и для него выполнено неравенство треугольника $\rho(x, y) \leqslant \rho(x, z) + \rho(y, z)$. Кодовым расстоянием называется, как и в бинарном случае, минимальное расстояние между разными кодовыми векторами.

Если код имеет кодовое расстояние $d = 2t + 1$, то он может исправлять вплоть до t ошибок. Действительно, если при передаче кодового слова x в нём произошло t ошибок, то мы получим искажённое слово x', для которого $\rho(x', x) = t$. По искажённому слову можно однозначно восстановить кодовое слово, так как если из двух разных кодовых слов x, y получено одно и то же искажённое не более чем t ошибками слово $x' = y' = z$, то согласно неравенству треугольника

$$2t + 1 = d \leqslant \rho(x, y) \leqslant \rho(x, z) + \rho(y, z) \leqslant 2t,$$

а это невозможно. Восстановление кодового слова по искажённому слову называется *декодированием*[8].

---

[6] По определению $x_1 \oplus \ldots \oplus x_n$ равно остатку от деления обычной суммы $x_1 + \ldots + x_n$ на два. Сложение по модулю два отличается от обычного только равенством $1 \oplus 1 = 0$.

[7] Его часто применяют для проверки целостности информации. Он обнаруживает наличие ошибки, но не находит и не исправляет её.

[8] Декодирование — непростой процесс, и он далее не рассматривается.

Если кодовое расстояние равно d, то код обнаруживает $d-1$ ошибку (если принятое слово является кодовым, то ошибок не было, потому что для получения другого кодового слова нужно сделать не менее d ошибок, а по предположению их не больше $d-1$; если же полученное слово не кодовое, то ошибки были).

Интересно для любых n, d найти q-ичный код максимальной мощности[9] с блоковой длиной n и расстоянием d. Обозначим его мощность $m_q(n,d)$. Для произвольного нечётного $d=2t+1$ легко получить следующую верхнюю оценку (из которой следует решение первой половины задачи 3 и п. (в) задачи 4):

Теорема 1 (граница Хэмминга — Рао[10], граница сферической упаковки). *Для любых* n, q, d

$$m_q(n,d) \leqslant \frac{q^n}{\sum\limits_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

В частности, при $q=2$

$$m_2(n,d) \leqslant \frac{2^n}{\sum\limits_{i=0}^{t} \binom{n}{i}}.$$

Доказательство. Достаточно рассмотреть *шары радиуса* t *с центрами в кодовых словах* и заметить, что они не пересекаются, а каждый из них состоит из $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i$ наборов (каждый набор в шаре однозначно определяется не более чем t позициями, в которых он отличается от центра, и значение в каждой позиции определяется $q-1$ способом). Поэтому общее число слов во всех шарах равно

$$m_q(n,d)\left(\sum_{i=0}^{t}\binom{n}{i}(q-1)^i\right),$$

но оно не может быть больше q^n — общего числа q-ичных слов, откуда следует нужное неравенство. □

Коды, для которых достигается эта граница, называются *совершенными* (или *плотно упакованными*, потому что они порождают совершенную упаковку многомерного q-ичного куба шарами).

---

[9] *Мощностью кода* называется число элементов в нём.

[10] Ричард Хэмминг (1915–1998) — американский математик, Кальямпуди Радхакришна Рао (р. 1920) — индийский специалист по математической статистике.

Нижняя граница сферической упаковки была указана Гилбертом [11].

Теорема 2. *Для любых* n, q, d

$$m_q(n,d) \geqslant \frac{q^n}{\sum\limits_{i=0}^{d-1}\binom{n}{i}(q-1)^i}.$$

В частности, при $q=2$

$$m_2(n,d) \geqslant \frac{2^n}{\sum\limits_{i=0}^{d-1}\binom{n}{i}}.$$

Доказательство. Рассмотрим максимальный код с расстоянием d (его мощность равна по определению $m_q(n,d)$) и построим шар радиуса $d-1$ с центром в каждом кодовом слове. Выше было показано, что мощность каждого такого шара равна $\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i$. Объединение этих шаров должно покрывать весь q-ичный куб (непокрытая вершина была бы удалена от центров шаров, т. е. от кодовых слов, на расстояние не меньше d, и её можно было бы добавить к коду, не уменьшая его расстояния и увеличивая мощность, что противоречит его максимальности), поэтому

$$m_q(n,d)\left(\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i\right) \geqslant q^n,$$

откуда и следует нужная нам оценка [12]. □

Идеи доказательства границ сферической упаковки давно известны в геометрии [13] и используются также в теории приближений [14]. Эти идеи давно попали и в сборники олимпиадных задач.

Задача 7. Докажите, что на стол размера 12×22 можно положить не менее 74 монет единичного радиуса.

Задача 8 (первый вопрос — ММО 1958, второй тур, 8.5, 9.4). Обозначим через a наибольшее число непересекающихся кругов диаметра 1,

[11] Эдгар Гилберт (E. Gilbert, 1923–2013) — известный американский специалист по дискретной математике. Не нужно путать Э. Гилберта со знаменитым немецким математиком Д. Гильбертом (D. Hilbert, 1862–1943).

[12] Советский математик Р. Р. Варшамов (1927–1999) чуть уточнил эту оценку для любых линейных кодов, поэтому её часто называют *границей Варшамова — Гилберта*.

[13] Неравенства Бликфельдта для плотности упаковки шаров в пространстве, см. [15].

[14] Для установления неравенств между *энтропией* и *ёмкостью метрических пространств*.

центры которых лежат внутри многоугольника M, через b — наименьшее число кругов радиуса 1, которыми можно покрыть весь многоугольник M, а через c — наибольшее число непересекающихся кругов радиуса 1, центры которых лежат внутри многоугольника M. Что больше: a или b? b или c?

Задача 9 (ММО 1980, 9.2). На пульте имеется несколько кнопок, с помощью которых осуществляется управление световым табло. После нажатия любой кнопки некоторые лампочки на табло переключаются (для каждой кнопки есть свой набор лампочек, причём наборы могут пересекаться). Докажите, что число состояний, в которых может находиться табло, равно некоторой степени числа 2. (Два состояния табло различны, если они различаются состоянием хотя бы одной лампочки).

Задача 10. Комиссия составила N списков, и оказалось, что для любых двух списков найдётся третий, который получается из этих двух сначала объединением, а затем последующим вычёркиванием тех, кто входил в оба списка. Докажите, что N на единицу меньше некоторой степени двойки.

§ 3. Границы для кодов с большими расстояниями

> Однако все его попытки отыскать ключ к шифру проваливались раз за разом, и тогда Смит понял, что придерживался изначально ложной посылки.
>
> *Джон Гласби, «Чёрное зеркало»*

Для двоичных кодов в случае больших расстояний оценка теоремы 1 становится очень грубой и её можно существенно уточнить. Справедливы следующие утверждения.

Лемма 1. *Выполнено неравенство* $m(n, d) \leqslant 2m(n-1, d)$.

Доказательство. У кода мощности $m(n, d)$ не менее половины кодовых слов имеют одинаковую n-ю компоненту (нуль или единицу). Если её отбросить, то получим код мощности не меньше $m(n, d)/2$ с расстоянием не меньшим d. □

Лемма 2. *Если d нечётно, то* $m(n, d) = m(n+1, d+1)$.

Доказательство. Добавим к каждому слову максимального кода с длиной n и расстоянием d ещё одну компоненту так, чтобы вес полученного слова был чётным (рассмотрим *расширенный код*). Мощность кода не изменится, а расстояние между любыми словами кода станет чётным.

Так как оно не уменьшилось, то оно будет не меньше $d+1$ (и равно $d+1$ там, где было равно d). Отсюда $m(n,d) \leqslant m(n+1,d+1)$.

Обратно, пусть имеем код мощности $m(n+1,d+1)$. Возьмём в нём два слова на расстоянии $d+1$ и выберем компоненту, которая в этих двух словах различна. Отбросив её во всех словах, получим код мощности $m(n+1,d+1)$ с длиной n и минимальным расстоянием $(d+1)-1=d$. Значит, $m(n,d) \geqslant m(n+1,d+1)$, отсюда следует нужное равенство. □

Теорема 3 (граница Плоткина[15)]).

1) *При* $2d > n \geqslant d$

$$m(n,d) \leqslant 2\left\lfloor \frac{d}{2d-n} \right\rfloor;$$

2) *при* $2d = n$ *справедливо неравенство* $m(n,d) \leqslant 2n$;

3) *при нечётном* d *и* $2d+1 > n \geqslant d$

$$m(n,d) \leqslant 2\left\lfloor \frac{d+1}{2d+1-n} \right\rfloor;$$

4) *при* $2d+1 = n$ *справедливо неравенство* $m(n,d) \leqslant 2n+2$.

Доказательство. Рассмотрим максимальный код мощности $m = m(n,d)$ с расстоянием d и оценим сумму R попарных расстояний между его словами. Очевидно, $R \geqslant dm(m-1)/2$, причём равенство возможно лишь для эквидистантных кодов (у которых попарные расстояния между словами равны). Если через h_i обозначить число кодовых слов, у которых i-я компонента равна 1, то $R = \sum_{i=1}^{n} h_i(m-h_i)$ (количество пар слов, различающихся в i-й компоненте, равно $h_i(m-h_i)$). Согласно неравенству между средним геометрическим и средним арифметическим $h_i(m-h_i) \leqslant m^2/4$, поэтому при целых h_i имеем $h_i(m-h_i) \leqslant \lfloor m^2/4 \rfloor$ и $R \leqslant n\lfloor m^2/4 \rfloor$. Таким образом,

$$\frac{dm(m-1)}{2} \leqslant \frac{nm^2}{4}.$$

Значит, при $2d > n$, если m чётно, имеем

$$m \leqslant \frac{2d}{2d-n} \leqslant 2\left\lfloor \frac{d}{2d-n} \right\rfloor,$$

а если m нечётно, то

$$m+1 \leqslant \frac{2d}{2d-n} \leqslant 2\left\lfloor \frac{d}{2d-n} \right\rfloor.$$

При $2d = n$ имеем согласно лемме 1

$$m = m(2d,d) \leqslant 2m(2d-1,d) \leqslant 4\left\lfloor \frac{d}{2d-(2d-1)} \right\rfloor = 4d = 2n.$$

[15)] М. Плоткин — американский специалист по теории кодирования, доказал эту теорему около 1960 г.

Если d нечётно, то при $2d+1>n$ по лемме 2

$$m(n,d)=m(n+1,d+1)\leqslant 2\left\lfloor\frac{d+1}{2d+1-n}\right\rfloor,$$

а при $2d+1=n$

$$m=m(2d+1,d)=m(2d+2,d+1)\leqslant 4(d+1)=2(n+1).\qquad\square$$

В. И. Левенштейн[16] доказал (см., например, [6, 7, 14]), что равенства в указанных оценках возможны тогда и только тогда, когда существуют матрицы Адамара любого порядка n, кратного 4. О матрицах Адамара см. раздел 3.1.

Задача 11 (на основе ММО 1993, 10.5). В ботаническом определителе растения описываются 100 бинарными признаками. Определитель считается хорошим, если любые два растения отличаются более чем по половине признаков. Докажите, что в хорошем определителе описано а) не более 50 растений, б) не более 34 растений.

Задача 12. В ботаническом определителе растения описываются 128 бинарными признаками. Определитель считается точным, если любые два растения отличаются не более чем в половине признаков. Докажите, что в точном определителе описано не более 256 растений, и покажите, что существует такой определитель, содержащий ровно 256 растений.

Задача 13. (i) (ММО 1948, второй тур, 9–10 кл., задача 4). Какое наибольшее число лучей можно провести из одной точки в трёхмерном пространстве так, чтобы все попарные углы между ними были тупыми?

(ii) Будем говорить, что два набора чисел $(a_1,\ldots,a_n)$ и $(b_1,\ldots,b_n)$ длины n образуют «тупой угол», если $a_1b_1+\ldots+a_nb_n<0$. Докажите, что если любые два из m наборов образуют тупой угол, то $m\leqslant n+1$.

Задача 14 (ВМО 1970, 9.4). Из цифр 1 и 2 составили 5 n-разрядных чисел так, что у каждых двух чисел совпали цифры ровно в m разрядах, но ни в одном разряде не совпали все пять чисел. Докажите, что $2/5\leqslant m/n\leqslant 3/5$.

Задача 15. Из цифр 0 и 1 составлены $N=2k+1$ различных n-разрядных чисел, у любых двух из которых совпадают ровно m разрядов. Докажите, что

$$\frac{m}{n}\leqslant\frac{N+1}{2N},$$

а если $N=2k$, то

$$\frac{m}{n}\leqslant\frac{N}{2(N-1)}.$$

[16] Владимир Иосифович Левенштейн (1935–2017) — известный российский специалист по теории кодирования.

Задача 16. Из цифр 0 и 1 составлены N различных n-разрядных чисел, причём нет ни одного разряда, в котором они все совпадают. Докажите, что $m/n \geqslant 2/N$.

3.1. Матрицы Адамара

> Золотая карта теперь была в круглых дырочках, словно швейцарский сыр. Все они располагались в узлах координатной сетки мсье Декарта, однако не все узлы были пробиты. Результат являл собой странное смешение упорядоченного и случайного; таким, наверное, предстаёт чётко отпечатанный, но зашифрованный текст.
>
> *Нил Стивенсон, «Система мира»*

Жак Адамар (выдающийся французский математик, 1865–1963) пришёл к этим матрицам, решая экстремальную задачу: найти среди всех матриц данного размера $n \times n$ с элементами, по модулю не превосходящими единицы, матрицу с максимальным определителем. Оказалось, что если n кратно 4 (или равно 2), то такая матрица состоит из ± 1, причём скалярное произведение любых двух (различных) строк и любых двух столбцов равно нулю. Под *скалярным произведением* двух векторов $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$ понимается число $x_1y_1 + \ldots + x_ny_n$. Векторы с нулевым скалярным произведением называются *ортогональными*. Матрицы с указанными свойствами называются *матрицами Адамара*. Легко доказать, что смена знака на противоположный в любой строке превращает матрицу Адамара в другую матрицу Адамара[17]. Аналогичное утверждение верно и для столбцов. Поэтому иногда в определение матриц Адамара добавляют условие, что верхняя строка и левый столбец должны состоять из единиц.

Из условия ортогональности любой строки верхней единичной строке следует, что во всех остальных строках поровну плюс и минус единиц, значит, n чётно. В теории кодирования используют матрицы, которые получаются из матриц Адамара заменой минус единиц на нули. Заменяя нули и единицы на мальчиков и девочек и решив задачу 18, читатель легко докажет, что если размер матрицы Адамара $n > 2$, то он кратен четырём.

Для построения матриц Адамара придуманы хитроумные методы, но гипотеза о том, что для любого n, кратного четырём, существуют такие матрицы порядка n, пока не доказана.

Приведём здесь только одну, самую простую конструкцию матриц Адамара, которая позволяет строить их для любого $n = 2^k$. Для $n = 2$, очевидно,

[17] Надо только не забыть проверить ортогональность столбцов.

матрица Адамара имеет вид

$$A_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Если матрица A_{2^k} размера $2^k \times 2^k$ уже построена, то матрицу $A_{2^{k+1}}$ можно составить из четырёх блоков размера $2^k \times 2^k$ следующим образом:

$$A_{2^{k+1}} = \begin{pmatrix} A_{2^k} & A_{2^k} \\ A_{2^k} & -A_{2^k} \end{pmatrix}.$$

Задача 17. Докажите по индукции, что построенная последовательность матриц действительно состоит из матриц Адамара [18)].

Теперь читатель легко решит последний пункт задачи 12.

Задача 18 (ВМО 1983, 9.5). Группа детского сада построилась парами друг за другом. При этом оказалось, что в каждой из двух колонн стоит поровну мальчиков и девочек, а число пар, в которых стоят девочка и мальчик, равно числу остальных пар. Докажите, что число детей в группе делится на 8.

Задача 19 (ММО 1959, второй тур, 7.5). Даны числа $x_i = \pm 1$, $i = 1, \ldots, n$. Докажите, что если $x_1x_2 + x_2x_3 + \ldots + x_{n-1}x_n + x_nx_1 = 0$, то n делится на 4.

Задача 20 (ММО 1971, второй тур, 10.1). В вершинах правильного n-угольника стоят числа 1 или -1. Если его повернуть на произвольный угол $2k\pi/n$, $k = 1, \ldots, n-1$, перемножить числа в совместившихся вершинах и все такие произведения сложить, то результат будет равен нулю. Докажите, что n есть квадрат целого числа.

В задаче [19)] 20, как теперь нетрудно догадаться, на самом деле тоже идёт речь о матрицах Адамара, а точнее, о таких матрицах с дополнительным свойством цикличности. На олимпиаде также предлагалось найти все такие матрицы. Ответ к этой задаче жюри не знало, и задача получила название «проблемы Зелевинского» [20)]. Ещё раньше она была известна как проблема Райзера о циркулянтных матрицах Адамара. Она не решена и по сей день.

3.2. Эквидистантные равновесные коды

Под этим термином скрывается довольно простое понятие, о котором фактически идёт речь в следующей задаче (рассматривавшейся в [4]).

[18)] Эту конструкцию ещё до Адамара предложил Дж. Сильвестр (1814–1897), поэтому такие матрицы можно называть матрицами Адамара — Сильвестра.

[19)] Задача 19 по существу является её упрощённым вариантом и близка к задаче 18.

[20)] На олимпиаду её предложил известный математик А. В. Зелевинский (1953–2013), в прошлом призёр международной олимпиады, а в то время студент второго курса.

Задача 21. 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.

Ответ: $1 + 3 \cdot 10 = 31$ и $1 + 3 + 3^2 = 13$.

Пусть объединение этих множеств состоит из m элементов. Сопоставив каждому из этих множеств набор из нулей и единиц с 4 единицами на позициях, соответствующих элементам данного множества, получим множество вершин двоичного m-мерного куба, лежащих в его четвёртом слое (т. е. имеющих веса, равные 4). Условие задачи означает, что попарные расстояния между этими вершинами равны 7. Коды, лежащие в одном слое, т. е. состоящие из наборов равного веса, называются равновесными, а коды, у которых расстояния между любыми двумя кодовыми словами равны, называются эквидистантными. Задача описания всех равновесных эквидистантных кодов крайне сложна.

Задача 22. Докажите, что максимальный эквидистантный код кодовой длины $n = q^2 + q + 1$ с весом $q + 1$ и расстоянием $2q + 1$ имеет мощность не более $q^2 + q + 1$. Равенство возможно тогда и только тогда, когда существует проективная плоскость порядка q.

§ 4. Простейший пример кода, исправляющего одну ошибку

Всё следует сделать настолько простым,
насколько это возможно, но не проще.

Альберт Эйнштейн

Клод Шеннон[21)] выдвинул идею *помехоустойчивого кодирования* (кодирования с исправлением ошибок). Рассмотрим пример кода, исправляющего одну ошибку (простейший нетривиальный частный случай кода Хэмминга). Пусть 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).

[21)] Клод Элвуд Шеннон (1916–2001) — американский математик и инженер, основоположник теории информации.

На языке матриц в рассматриваемом примере кодирование сводится к умножению 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 примере он имеет вес 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 нахождения самой ошибки) можно вычислить *проверочные суммы*

$$\begin{aligned} S_1 &= r_1 + r_3 + r_4 + r_5, \\ S_2 &= r_1 + r_2 + r_4 + r_6, \\ S_3 &= r_1 + r_2 + r_3 + r_7. \end{aligned}$$

Наглядно все эти суммы изображены на рис. 1. Каждая сумма содержится в своём круге. На матричном языке эта процедура равносильна умножению матрицы на вектор:

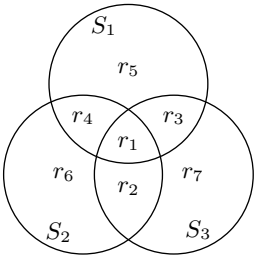

Рис. 1. Код Хэмминга с блоковой длиной 7

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_7 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \end{pmatrix}.$$

Указанная матрица H называется *проверочной матрицей* кода. В краткой нотации умножение матрицы H на вектор r^T записывается как $S = Hr^T$ (где S — вектор-столбец $(S_1, S_2, S_3)^T$).

Заметим, что матрица H выбрана так, что $Hc^T = 0$ (где 0 — нулевой вектор-столбец) для любого кодового вектора c. Это можно проверить

непосредственно (и даже не пользуясь матричным языком, просто подставив в указанные выше три суммы S_i вместо x_5, x_6, x_7 их выражения через (x_1, x_2, x_3, x_4). На матричном языке это также легко показать. Заметим, что матрица M представима в виде

$$\binom{E}{A},$$

где E — единичная матрица [22)] размера 4×4, а A — матрица размера 3×4. Матрица H составлена из той же подматрицы A и единичной подматрицы размера 3×3, поэтому

$$\begin{aligned} Hc^T &= A \cdot (x_1, x_2, x_3, x_4)^T + E \cdot (x_5, x_6, x_7)^T = \\ &= A \cdot (x_1, x_2, x_3, x_4)^T + (x_5, x_6, x_7)^T = 0^T, \end{aligned}$$

так как в силу равенства

$$M \cdot (x_1, x_2, x_3, x_4)^T = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)^T$$

имеем

$$A \cdot (x_1, x_2, x_3, x_4)^T = (x_5, x_6, x_7)^T.$$

Используя легко проверяемые свойства матричного умножения и сложения, получаем

$$S = Hr^T = H(c^T + e^T) = He^T = H_i,$$

где e — вектор с единственной единицей в i-й позиции, H_i — i-й столбец матрицы H (это равенство можно проверить и непосредственно, заменяя r_j в суммах S_i на $c_j + e_j = x_j + e_j$). Заметим теперь, что все столбцы матрицы H различны и отличны от нуля [23)]. Поэтому по столбцу H_i можно однозначно определить его номер, а значит, и позицию ошибки. Если же ошибки не было, то очевидно, что $S = Hr^T = Hc^T = 0$, и это равенство можно проверить, сравнив S с нулевым вектором-столбцом (если же S ненулевой, то ошибка, очевидно, была). Для определения позиции ошибки по вычисленному вектору S (называемому *синдромом*) можно заготовить таблицу, содержащую номера позиций ошибок, например в двоичной записи. Эта таблица состоит из восьми строк, которые занумерованы двоичными набо-

[22)] Квадратная матрица называется *единичной*, если на главной диагонали стоят единицы, а в остальных местах нули. Главная диагональ — это диагональ, идущая от левого верхнего угла матрицы к правому нижнему углу. Если умножить единичную матрицу на вектор, то в результате получится тот же вектор.

[23)] Это стало возможным благодаря тому, что всего имеется 8 различных двоичных столбцов высоты 3.

рами длины 3. Если ошибки нет, то номер можно считать равным нулю. Если проверочная матрица имеет вид

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

то эта таблица не требуется, так как синдром S совпадает в этом случае с двоичным номером позиции ошибки. Разумеется, матрицу M также придётся тогда изменить.

Построенный код является частным случаем кодов Хэмминга, которые рассматриваются далее. В случае когда длина кодовых слов равна 31, идея построения кода очень близка к задаче 5, предложенной французским математиком Люка ещё в XIX веке (это станет ясно после прочтения § 5). Да и следующие три задачи тоже к ней очень близки.

Задача 23 (из задачной базы московских олимпиад). В n-элементном множестве выбрано $5n$ различных двухэлементных подмножеств. Докажите, что, объединяя их попарно, можно получить не менее $45n$ трёхэлементных подмножеств.

Задача 24. Найдите среди 63 монет фальшивую, выполнив всего 6 взвешиваний, если известно, что она легче остальных. За одно взвешивание можно взвесить сразу несколько монет. План взвешиваний требуется составить заранее.

Задача 25 (ММО 1990, 8.5). Табло, состоящее из 64 лампочек, управляется 64 кнопками: каждая лампочка — своей кнопкой. За одно включение можно одновременно нажать любой набор кнопок и записать, какие лампочки при этом зажглись. За какое наименьшее количество включений можно узнать обо всех лампочках табло: какая лампочка какой кнопкой управляется?

Обратим внимание на некоторые свойства построенного выше кода. Его мощность равна $2^4 = 16$, сумма любых двух кодовых слов по модулю два опять является кодовым словом (т. е. этот код линейный), расстояние кода равно трём. Меньше трёх оно быть не может, иначе бы он не исправлял ошибки, но можно расстояние вычислить и явно, заметив, что $d(a, b) = d(a + b, 0)$. Поскольку код содержит кодовое слово веса нуль (нулевое слово) и кодовое расстояние равно трём, в коде нет слов веса 1 или 2. Для каждого кодового слова рассмотрим шар радиусом 1 с центром в этом слове. 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.

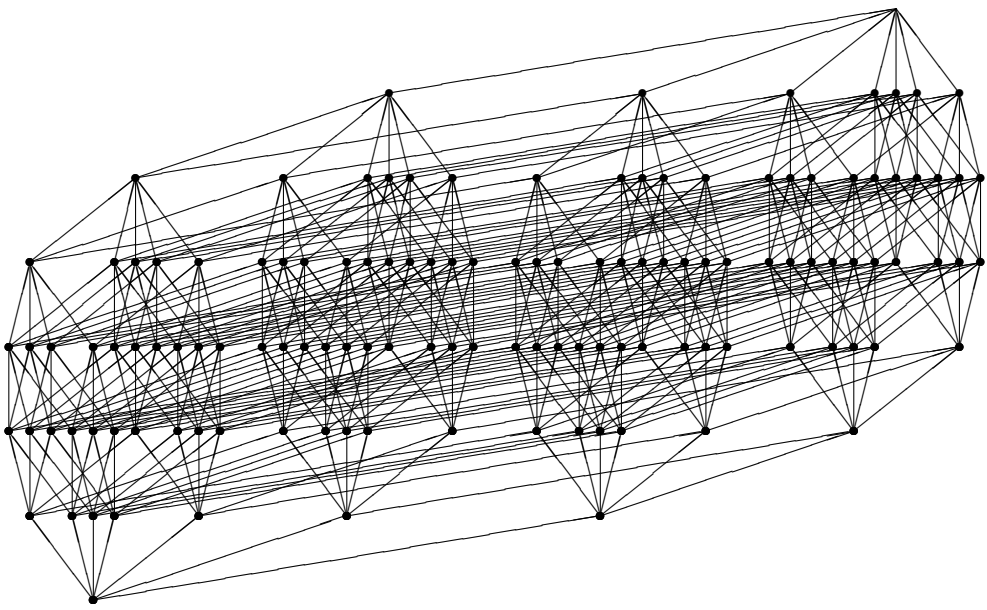

Рис. 2. Семимерный куб

Эти шары с центрами в кодовых словах не пересекаются[24] (не имеют общих вершин) и поэтому в совокупности содержат $2^4 \cdot 8 = 2^7$ различных вершин куба, т. е. все его вершины (в семимерном кубе 2^7 вершин). Такие точные покрытия многомерного куба непересекающимися шарами называются *совершенными*, а соответствующие им коды — *совершенными кодами*.

В [4] исходя только из свойства совершенности указанного кода объяснено, как можно однозначно определить число кодовых вершин на третьем слое семимерного куба[25], см. рис. 2.

Там найден его *весовой спектр*, а именно количество слов каждого заданного веса. Он имеет вид

$$a_0 = 1, \quad a_1 = 0, \quad a_2 = 0, \quad a_3 = 7,$$
$$a_4 = 7, \quad a_5 = 0, \quad a_6 = 0, \quad a_7 = 1.$$

Также там объяснено, что кодовые слова веса три определяют интересную комбинаторную конфигурацию — *систему троек Штейнера*[26], и показано, что эта система троек изоморфна конфигурации семи трёхто-

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

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

[26] Якоб Штейнер (1796–1863) — выдающийся швейцарский геометр.

чечных прямых в проективной плоскости на семи точках — так называемой плоскости Фано [27] (рис. 3).

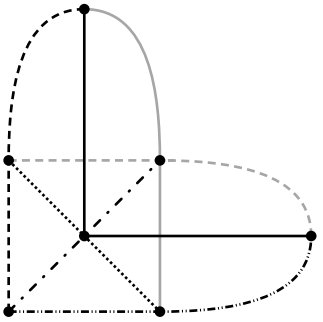

Рис. 3. Плоскость Фано

Коды, все вершины которых лежат на одном слое куба, называются *равновесными кодами*. Таким образом, максимальный код веса три с блоковой длиной семь также имеет мощность 7. Кодовые слова веса четыре также определяют интересную комбинаторную конфигурацию. Каждое из них задаёт четырёхэлементное подмножество в множестве $\{1, 2, 3, 4, 5, 6, 7\}$, состоящее из номеров позиций единиц в этом слове. Система из этих семи четвёрок образует пример *блок-схемы*, в которой каждая пара элементов принадлежит в точности двум четвёркам [28].

Указанные конфигурации (блок-схемы) третьего и четвёртого слоёв обладают ещё одним интересным свойством. Они двойственны друг к другу, а именно: четвёрки из второй блок-схемы являются дополнениями троек из первой блок-схемы до множества $\{1, \ldots, 7\}$.

§ 5. Код Хэмминга

> Два выходных подряд я приходил и обнаруживал, что все мои данные выгружены и ровным счётом ничего не сделано. Я был в ярости, потому что мне были нужны ответы, а два выходных оказались потеряны зря. Тогда я сказал себе: «Чёрт, если машина может обнаружить ошибку, то что мешает ей определить, где эта ошибка произошла, и исправить её?»
>
> *Ричард Хэмминг, по*: *Дж. Маккормик, «Девять алгоритмов, которые изменили мир»*

Начнём с двоичного кода Хэмминга. Его можно построить, например, так. Пусть $n = 2^m - 1$, $k = n - m$, и пусть $x_1, \ldots, x_k$ — информационный вектор, который нужно закодировать. Добавим к нему проверочные символы $x_{k+1}, \ldots, x_n$, для вычисления которых умножим вектор-столбец $X = (x_1, \ldots, x_k)^T$ на (m, k)-матрицу M_n (с m строками и k столбцами), столбцы которой представляют из себя все возможные наборы длины m из нулей и единиц, содержащие хотя бы две единицы (таких наборов ровно

[27] Джино Фано (1871–1951) — выдающийся итальянский математик.

[28] О блок-схемах см., например, [4, 14, 16].

$2^m - 1 - m = n - m = k$). Добавим к этой матрице ещё m столбцов, содержащих ровно одну единицу каждый (можно считать, что они образуют квадратную матрицу с единицами по диагонали), и получим (m, n)-матрицу H_n, столбцами которой являются все возможные ненулевые наборы длины m из нулей и единиц. Так же как и в § 4, можно проверить, что для любого кодового слова $x = (x_1, \ldots, x_n)$ справедливо матричное равенство

$$H_n x^T = 0.$$

Матрица H (далее индекс n опускаем) называется проверочной матрицей этого кода. Она позволяет не только проверить, является ли данное слово c кодовым, но и позволяет найти ошибку, если она была одна. Действительно, как и в § 4, имеем

$$S = Hr^T = H(c^T + e^T) = He^T = H_i,$$

где e — вектор ошибок, имеющий одну единицу в i-й позиции, а H_i — столбец матрицы H с номером i. Так как все столбцы различны и отличны от нулевого, то по синдромному вектору S можно однозначно найти ошибку.

Как и в § 4, рассмотрим некоторые свойства построенного кода. Его мощность равна 2^k, он линейный, размерность его как линейного пространства над полем из двух элементов равна k (потому что если базис пространства состоит из k векторов, то пространство состоит из всех возможных их сумм, которых ровно 2^k, включая и пустую сумму, равную по определению нулю), расстояние кода равно трём (меньше трёх оно быть не может, иначе бы он не исправлял ошибки). Так как код имеет кодовое слово веса нуль (нулевое слово) и расстояние его равно трём, то кодовых слов веса 1 или 2 в нём нет. Для каждого кодового слова рассмотрим шар радиуса 1 с центром в этом слове. Этот шар содержит, кроме центра, ещё n двоичных наборов (вершин n-мерного двоичного куба). Эти шары с центрами в кодовых словах не пересекаются, поэтому в совокупности содержат $2^k \cdot (n + 1) = 2^{k+m} = 2^n$ различных вершин куба, т. е. все эти вершины. Поэтому код Хэмминга H_n является совершенным (и плотно упакованным). Очевидно также, что он лежит на границе сферической упаковки. Обратно, любой максимальный код с расстоянием три имеет такие же параметры, что и код Хэмминга. Действительно, если граница оценки $m(n, 3) \leqslant 2^n/(n+1)$ достигается, то $n+1 = 2^m$ (иначе данная дробь не будет целым числом), откуда $m(n, 3) = 2^{n-m}$. Тем самым полностью решена задача 3, и теперь легко решить задачу 26.

Задача 26. Всегда ли можно угадать число от 1 до 2048, задав 15 вопросов с ответом «да» или «нет», если на один из них может быть дан неправильный ответ? Вопросы требуется составить заранее.

Ещё одна задача на ту же тему:

Задача 27 [19, p. 120]. У трёх мудрецов шляпы двух цветов. Ведущий надевает мудрецам шляпы так, что в результате каждый видит шляпы всех остальных мудрецов, но не видит своей шляпы и не знает её цвета. По команде ведущего они одновременно называют цвет. Каждый мудрец должен назвать цвет, исходя только из того, какие цвета он видит у остальных, но им разрешается пасовать, что означает отказ от угадывания. Мудрецы выигрывают только при условии, что хотя бы один из них угадал цвет и при этом никто не назвал цвет неправильно. Перед тестом мудрецам сообщили правила и дали возможность договориться о том, как действовать во время теста. Оптимальная стратегия — это стратегия, которая для всевозможных раскладов шляп даёт наибольшее число выигрышей.

а) Предложите стратегию мудрецов, при которой они выигрывают больше чем в половине случаев.

б) Найдите оптимальную стратегию и докажите, что она оптимальна.

5.1. q-ичные коды Хэмминга

> Я бедная девушка, у которой плохо с арифметикой! Выше двух для меня сразу начинается высшая математика!
>
> *Дмитрий Емец, «Таня Гроттер»*

В некоторых случаях существуют также совершенные q-ичные коды. Границы Хэмминга они могут достигать, например, когда $1+(q-1)n=q^m$. Тогда мощность кода будет равна q^{n-m}, где n — его блоковая длина. Такие коды можно построить в случае существования конечного поля из q элементов[29)].

Полем называется любое множество, на котором можно определить операции сложения и умножения так, что эти операции удовлетворяют тем же законам, что и операции сложения и умножения рациональных чисел, а именно, переместительному: $a+b=b+a$, $ab=ba$, сочетательному: $(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$, распределительному: $a(b+c)=ab+ac$, и удовлетворяют тождествам $a+0=a$, $a\cdot 1=a$, а также имеют однозначно определённые обратные операции вычитания $a-b$ и деления a/b, удовлетворяющие тождествам $(a-b)+b=a$, $(a/b)b=a$. Из алгебры известно, что порядок (число элементов) q любого конечного поля — степень простого

[29)] Есть гипотеза, что при q, не равном степени простого числа, таких совершенных кодов не существует.

числа p, $q=p^n$, причём для любого такого q существует единственное[30] поле порядка q, называемое полем Галуа[31] и обозначаемое $\mathrm{GF}(q)$. Например, $\mathrm{GF}(2)=(\{0,1\},\oplus,\cdot)$.

Построим над полем $\mathrm{GF}(q)$ коды, являющиеся обобщением кодов Хэмминга. Для каждого ненулевого вектора v длины m над полем $\mathrm{GF}(q)$ рассмотрим множество коллинеарных ему векторов λv, где $\lambda\in\mathrm{GF}(q)\setminus\{0\}$. Это множество образует прямую в пространстве $\mathrm{GF}(q)^n$, проходящую через начало координат. Выберем на каждой такой прямой (а их будет $n=(q^m-1)/(q-1)$, так как они имеют только одну общую точку — начало координат) любую точку, отличную от начала координат, например можно выбрать точку, у которой последняя координата равна 1. Это всегда можно сделать, за исключением случая, когда все точки прямой имеют нулевую последнюю координату. В этом случае можно выбрать точку, у которой предпоследняя координата равна единице. Если таковой не найдётся и предпоследняя координата равна нулю, можно найти точку, у которой третья с конца координата равна единице, и т. д. Указанная точка на прямой (и соответствующий радиус-вектор) определяется однозначно. Все остальные получаются теперь умножением на элементы поля (при умножении на нуль получается нулевой вектор). Очевидно, что любой ненулевой вектор из пространства $\mathrm{GF}(q)^n$ получается из одного из указанных выше векторов $v_1,\dots v_n$ умножением на ненулевой элемент поля, причём такое представление определено однозначно.

Рассмотрим (m,n)-матрицу H_n над полем $\mathrm{GF}(q)$, столбцы которой являются указанными векторами $v_1,\dots,v_m$. Определим код как множество таких векторов c, что $Hc^T=0$ (т. е. как нулевое пространство этой матрицы). Тогда матрица H_n является проверочной матрицей указанного кода. Код исправляет одну ошибку, потому что, как и в § 4, имеем

$$S=Hr^T=H(c^T+e^T)=He^T=e_iH_i,$$

где e — вектор ошибок, имеющий один ненулевой символ e_i в i-й позиции, а H_i — i-й столбец матрицы H. Так как все столбцы различны и отличны от нулевого, а результаты их умножения на ненулевые элементы поля тоже различны, по вектору S можно однозначно найти и позицию ошибки i, и её величину e_i. Поскольку матрица H_n (после подходящей перестановки столбцов) содержит единичную (m,m)-подматрицу, размерность кода (размерность нулевого подпространства) равна $n-m$, а значит, его мощность равна q^{n-m} (множество всех линейных комбинаций базисных векторов над полем

[30] С точностью до изоморфизма.

[31] Эварист Галуа (1811–1832) — великий французский математик.

$\mathrm{GF}(q)$ имеет мощность q^{n-m}), т. е. код находится точно на границе сферической упаковки и, следовательно, является совершенным кодом. Тем самым решён п. (г) задачи 4. Решение п. (б) читатель может найти в [2, с. 165–166].

§ 6. Коды Рида — Соломона

В полях Галуа, полных цветов, примитивные корни танцуют часами [32)].

С. Б. Вейнстейн (IEEE Transactions of Information Theory, 1971)

Пусть $q > 2$ — простое число. Напомним, что q-ичным линейным кодом C длины n и размерности k (сокращённо $[n, k]$-кодом) называется любое линейное k-мерное подпространство C пространства $\mathrm{GF}(q)^n$ всех n-мерных векторов над полем $\mathrm{GF}(q)$. Легко видеть, что кодовое расстояние линейного кода равно минимальному весу, который может иметь ненулевой кодовый вектор Если $[n, k]$-код имеет кодовое расстояние d, то он называется $[n, k, d]$-кодом.

Простейший вариант построения кодов Рида — Соломона [33)] над полем $\mathrm{GF}(q)$ (сокращённо RS-кодов) следующий. Пусть $k < n \leqslant q$. Сопоставим каждому вектору $a = (a_0, \ldots, a_{k-1}) \in \mathrm{GF}(q)^k$ многочлен

$$a(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}$$

степени $k - 1$ над полем $\mathrm{GF}(q)$. Пусть $x_1, \ldots, x_n \in \mathrm{GF}(q)$ — различные элементы этого поля. Рассмотрим (линейное) отображение $l\colon \mathrm{GF}(q)^k \to \mathrm{GF}(q)^n$, определяемое равенством

$$l(a) = (a(x_1), \ldots, a(x_n)) \in \mathrm{GF}(q)^n.$$

Образ $l(\mathrm{GF}(q)^k) \subset \mathrm{GF}(q)^n$ этого отображения — линейный код C, называемый RS-кодом. В силу неравенства $n > k$ многочлен $a(x)$ степени $k-1$ однозначно восстанавливается по своим значениям в n точках, поэтому отображение $l\colon \mathrm{GF}(q)^k \to C$ взаимно однозначно. Значит, мощность кода C равна q^k, поэтому его размерность равна k. Кодовое расстояние $d(C) \geqslant n - k + 1$, так как для любого ненулевого многочлена $a(x)$ вектор его значений $(a(x_1), \ldots, a(x_n)) \in C \subset \mathrm{GF}(q)^n$ имеет вес, не меньший $n - k + 1$, потому что ненулевой многочлен степени $k - 1$ имеет не более $k - 1$ корней.

[32)] In Galois Fields, full of flowers, primitive elements dance for hours.

[33)] Ирвинг Рид (1923–2012) и Густав Соломон (1930–1996) — американские специалисты по теории кодирования.

На самом деле $d(C) = n - k + 1$, потому что, согласно так называемой границе Синглтона, для любого $[n, k]$-кода $d(C) \leqslant n - k + 1$. Коды, лежащие на этой границе, называются *кодами с максимальным расстоянием* (maximim-distance separable (MDS) — кодами). Такими являются RS-коды. Бинарные коды не достигают этой границы.

Соответствующая теорема может быть сформулирована ещё и так (определение $m_q(n, d)$ см. в § 2):

Теорема 4 (граница Синглтона[34)], или проекционная граница).

$$m_q(n, d) \leqslant q^{n-d+1}.$$

Доказательство. Достаточно спроектировать все q^k кодовых слов на подпространство $\mathrm{GF}(q)^{k-1}$, для чего надо заполнить нулями последние $n - k + 1$ координат кодового вектора, не изменяя первые $k - 1$ координат. В силу принципа Дирихле какие-то два кодовых слова при этом будут иметь одинаковую проекцию, т. е. первые $k - 1$ координат у них совпадают, поэтому расстояние между ними будет не больше $n - k + 1$. Значит, $d \leqslant n - k + 1$ (причём это верно и для нелинейных кодов мощности больше q^{k-1}). □

Теперь легко решаются задачи 28 и 29.

Задача 28. На n-мерной k-ичной шахматной доске поставлена $k^m + 1$ ладья. Докажите, что найдутся две ладьи, координаты которых различаются не более чем в $n - m$ позициях. В частности, если $m = n - 1$, то найдутся две ладьи, угрожающие друг другу.

Задача 29. Если k равно степени простого числа и $n > m + 1$, то можно в задаче 28 так расставить k^{m+1} ладью, что координаты любых двух будут отличаться не менее чем в $n - m$ позициях. В частности, если $m = n - 2$, то на n-мерной k-ичной шахматной доске можно расставить k^{n-1} ладей так, чтобы они не били друг друга. При $n = 2$ это очевидно.

А к задаче 30 дадим ответ и указание.

Задача 30. Вы заходите в комнату, где лежит шахматная доска, на некоторых клетках которой стоят фигуры (или шашки). Вам сообщают координаты одной клетки доски и дают задание передать информацию об этой клетке вашему другу, который войдёт в эту комнату позже вас. Взятие фигуры или установка на пустую клетку фигуры считается ходом. У вас не будет возможности после посещения этой комнаты встретиться с другом или сообщить ему что-либо. До его прихода позиция на доске

[34)] Ричард Коллом Синглтон (1928–2007) — американский специалист по теории кодирования.

изменяться не будет. Но перед посещением этой комнаты у вас есть возможность договориться с другом о совместных действиях. За какое наименьшее количество ходов можно решить поставленную задачу?

Ответ: достаточно одного хода.

Указание. Координаты клетки можно «закодировать» двоичным набором длины 6. Расстановка фигур на доске определяется двоичным набором длины 64. Воспользуйтесь проверочной матрицей линейного $[64, 58]$-кода, т. е. кода Хэмминга, расширенного добавлением нулевой координаты. Это двоичная $(6, 64)$-матрица, все столбцы которой различны (можно удалить из неё нулевой столбец и использовать $(6, 63)$-матрицу — проверочную матрицу обычного кода Хэмминга). Если умножить двоичный набор длины 64 на эту матрицу, изменив его в одном месте, можно получить любой заданный набор. Этот набор можно выбрать так, чтобы он «кодировал» нужную клетку.

Ещё одна задача на эту тему:

Задача 31 [19, p. 121]. Шпион, засланный в чужую страну, может использовать для общения с центром только передачи местной радиостанции, ежедневно передающей в эфир одно сообщение длиной 255 бит. У шпиона есть доступ к тексту передаваемого сообщения до его выхода в эфир, но всё, что он может сделать, — это изменить в сообщении один из битов (или вообще ничего не менять). Сколько битов информации сможет ежедневно передавать шпион в Центр? (Разумеется, договариваться с центром о способе шифровки/дешифровки он может и должен заранее.)

§ 7. Теорема Заранкевича и декодирование

> Гамильтон наугад открыл страницу и убедился, что книга, судя по всему, является компендиумом самых диких идей...
>
> *Ричард Тирни, «Крик во тьме»*

Код C с блоковой длиной n называется (e, l)-*списочно-декодируемым*, если для любого слова y длины n в шаре $B(y, e)$ радиуса e с центром в y (в метрике Хэмминга) находится не более l кодовых слов, т. е. $|B(y, e) \cap C| \leqslant l$. Судан и Гурусвами[35] [18] доказали[36], что справедлива

[35] Мадлу Судан (р. 1966), Венкатесан Гурусвами (р. 1976) — индийско-американские специалисты по информатике.

[36] На самом деле они доказали существенно больше, а именно, предложили также эффективный алгоритм, перечисляющий для любого кодового слова список слов, удалённых от него на расстояние, не большее e.

Теорема 5. *Любой (n, k, d)-код $(e, n(d-e))$-списочно-декодируем при $e<n-\sqrt{(n-d)n}$. В частности, любой $RS(n,k)_q$-код $(e, n(d-e))$-списочно-декодируем при $e < n - \sqrt{(k-1)n}$.*

Доказательство. Очевидно, что

$$n-d=\sqrt{n-d}\sqrt{n-d}<\sqrt{(n-d)n} \quad \text{и} \quad n-\sqrt{(n-d)n}\geqslant\frac{d}{2},$$

так как

$$n-\frac{d}{2}=\frac{n+n-d}{2}\geqslant\sqrt{(n-d)n}$$

согласно неравенству между средним арифметическим и средним геометрическим.

Теорема 5 выводится из теоремы Заранкевича, сформулированной в виде задачи 6. Пусть $c_j \in B(y,e)\cap C$, $j\leqslant m$, — все кодовые слова, лежащие в шаре $B(y,e)$, где $y=(y_1,\ldots,y_n)$ — произвольное слово длины n в кодовом алфавите. Нужно показать, что $m\leqslant n(d-e)$.

Определим (n,m)-матрицу A из нулей и единиц так, что $a_{i,j}=1 \Leftrightarrow y_i=c_{j,i}$, где $c_{j,i}$ — i-я координата вектора c_j. Так как для любых j_1, j_2 в силу определения минимального кодового расстояния $d(c_{j_1}, c_{j_2})\geqslant d$, то число совпадающих координат у этих векторов не больше $n-d$, поэтому в j_1-м и j_2-м столбцах матрицы A имеется не более $n-d$ общих единиц. Значит, матрица не содержит $(n-d+1,2)$-матриц второго порядка, состоящих из единиц. Поэтому число k единиц в ней, согласно теореме Заранкевича, таково, что

$$n\frac{\frac{k}{n}\left(\frac{k}{n}-1\right)}{2}\leqslant\frac{m(m-1)(n-d)}{2},$$

откуда

$$k(k-n)\leqslant nm(m-1)(n-d).$$

Слова y, c_j совпадают не менее чем в $t=n-e>\sqrt{(n-d)n}$ позициях, так как по условию $d(c_j,y)\leqslant e$, поэтому в каждом столбце матрицы A не меньше t единиц, откуда следует, что $k\geqslant mt$. Можно считать, что $k>n$, иначе

$$m<\sqrt{\frac{n}{n-d}}\leqslant\sqrt{n}\leqslant n(d-e).$$

Поэтому

$$mt(mt-n)\leqslant k(k-n)\leqslant m(m-1)n(n-d),$$

откуда

$$m^2t^2-mnt\leqslant m(m-1)n(n-d).$$

Значит,

$$m^2(t^2 - n(n-d)) \leqslant mn(t-n+d),$$
$$m \leqslant \frac{n(t-n+d)}{t^2-n(n-d)} \leqslant n(t+d-n) = n(d-e) < n^2.$$

Теорема доказана. □

§ 8. Алфавитное кодирование

> Алфавиты стали более знакомыми, и теперь, кроме букв, стали попадаться и цифры — в порядках, которые я не сразу узнала.
>
> *Скарлетт Томас, «Наваждение Люмаса»*

Теория кодирования — обширная область, имеющая тесные связи с алгеброй, теорией чисел, комбинаторикой, теорией графов, теорией вероятности, теорией информации. Она не ограничивается теорией кодов, исправляющих ошибки. Важным её разделом является, например, алфавитное кодирование. Оно применяется не с целью коррекции ошибок, а, например, для сжатия текста[37)], а в старые времена применялось и для шифрования[38)]. Так называемый генетический код[39)] тоже можно рассматривать как схему алфавитного кодирования. Задачи 32, 33, 34 относятся как раз к этой области.

Задача 32 (ММО 1962, второй тур, 9.5). Даны 2^n конечных последовательностей из нулей и единиц, причём ни одна из них не является началом никакой другой. Докажите, что сумма длин этих последовательностей не меньше $n \cdot 2^n$.

Задача 33. В генеалогическом древе князя Рюрика ни у кого из его потомков не было больше k сыновей. На годовщину рождения князя собрались вместе все n княжичей и вычислили суммарную длину своих ветвей генеалогического древа. Докажите, что она оказалась не меньше $n \log_k n$.

Задача 34 (студенческая олимпиада мехмата). В списке из n слов, составленных из букв k-буквенного алфавита, ни одно из которых не является началом другого, количество слов любой данной длины l, $l = 1, 2, \ldots, m$,

[37)] Вероятно, впервые для этой цели была применена азбука Морзе, которую можно рассматривать как схему алфавитного кодирования, впрочем, не префиксную и не обладающую свойством однозначности декодирования.

[38)] Например, шифры простой замены, шифр Полибия, шифр Бэкона можно рассматривать как схемы алфавитного кодирования.

[39)] Сопоставление аминокислотам троек символов из алфавита А, Г, Ц, Т.

равно n_l. Докажите, что $n_1/k + \ldots + n_m/k^m \leqslant 1$. Неравенство может обращаться в равенство [40)].

В задаче 32 на самом деле речь идёт о средней длине элементарного кодового слова при кодировании n-буквенного алфавита двухбуквенным. Процедура кодирования слов в данном n-буквенном алфавите, например двоичными словами, заключается в замене каждой буквы этого алфавита двоичным кодовым словом. Если ни одно кодовое слово не является началом другого, то такое кодирование называется *префиксным*. Это условие на кодовые слова позволяет легко выполнять декодирование [41)]. В задаче 32 на самом деле ищется префиксный код с минимальной средней длиной элементарного кодового слова.

Эту задачу можно решить в более общей постановке — когда буквам данного алфавита сопоставляются такие числа $p_i > 0$, что $p_1 + \ldots + p_n = 1$ (p_i — это вероятности появления этих букв), а для кодирования используется k-ичный алфавит. Тогда средняя длина элементарного кодового слова будет равна $l_c = p_1 l_1 + \ldots + p_n l_n$, где l_i — длина кодового слова. Для неё Шеннон получил следующую оценку:

Теорема 6. *Справедливо неравенство* $l_c \geqslant H_k(p_1, \ldots, p_n)$, *где*

$$H_k(p_1, \ldots, p_n) = -(p_1 \log_k p_1 + \ldots + p_n \log_k p_n)$$

— *энтропия Шеннона.*

Доказательство появится чуть позже, а вначале укажем связь между префиксными кодами в k-ичном алфавите и корневыми k-арными деревьями [42)]. Так называются деревья с ориентированными рёбрами, в которых из корня (единственной вершины нулевого яруса) и любой внутренней вершины i-го яруса выходит не более k рёбер, направленных в вершины $(i+1)$-го яруса.

Индукцией по номеру яруса легко доказать, что число вершин на i-м ярусе не превосходит k^i. По определению, в каждую вершину, кроме корня, входит ровно одно ребро. Вершины, из которых не выходит ни одного ребра, назовём листьями [43)]. Для каждого листа существует единственный

[40)] Эта задача предлагалась на олимпиаде в 1980-е годы, когда ещё не было ни курса дискретной математики, ни учебника [17].

[41)] Разумеется, вместо префиксных кодов можно использовать постфиксные, т. е. такие, в которых ни одно элементарное кодовое слово не является концом другого. Менее очевидно, что существуют и не префиксные и не постфиксные коды, которые тоже обладают свойством однозначности декодирования.

[42)] О которых идёт речь в задаче 33.

[43)] Используется также термин «висячие вершины».

путь, ведущий в него из корня. Число рёбер в нём обозначим l_i, где i — номер листа (в произвольной нумерации). Если для каждой внутренней вершины сопоставить выходящим из неё рёбрам различные числа (метки) из множества (алфавита) $A_k = \{0, \ldots, k-1\}$, то пути из корня в лист i можно сопоставить слово w_i в алфавите A_k длины l_i, которое получится, если выписать все метки рёбер этого пути, начиная с ребра, выходящего из корня. Совокупность полученных слов w_i образует набор элементарных кодовых слов схемы алфавитного кодирования, определяемой по данному дереву. Очевидно, что эта схема является префиксной.

Верно и обратное, а именно, по любой префиксной схеме алфавитного кодирования можно построить корневое дерево, которому будет указанным выше образом сопоставляться как раз упомянутая префиксная схема алфавитного кодирования. Аккуратное доказательство этого утверждения проводится по индукции и оставляется читателю в качестве ещё одной задачи. В силу указанной связи между префиксными кодами и деревьями, утверждения про префиксные коды можно переформулировать как утверждения про деревья. Поэтому из теоремы 6 следуют оценки не только задачи 32, но и задачи 33 (которую можно рассматривать как обобщение задачи 32). А задачу 34 можно считать следствием теоремы 7:

Теорема 7 (неравенство Крафта[44]). *Пусть в корневом k-арном дереве длины всех путей от корня к листьям равны l_i, $i = 1, \ldots, n$. Тогда справедливо неравенство $k^{-l_1} + \ldots + k^{-l_n} \leqslant 1$.*

Доказательство. Представим, что из каждого листа i, как из корня, вырастает ветка, имеющая вид полного k-арного дерева высоты $l - l_i$, где $l = \max_i l_i$ (назовём k-арное дерево *полным высоты* h, если из каждой внутренней вершины выходит ровно k рёбер, а листья образуют h-й ярус). Тогда на этой ветке будет k^{l-l_i} листьев, и все листья «расцветшего» дерева образуют в нём l-й ярус. Всего листьев будет $k^{l-l_1} + \ldots + k^{l-l_n} \leqslant k^l$, так как в l-м ярусе не может быть больше k^l листьев. Остаётся поделить обе части неравенства на k^l. □

Теперь можно доказать теорему 6. Воспользуемся тем, что для функции $\log_k x$ при подходящем[45] значении K справедливо неравенство $\log_k x \leqslant K(x-1)$, имеющее простой геометрический смысл: график функции (за исключением точки касания) лежит ниже касательной к нему, проведённой через точку графика ($x=1$, $y=\log_k 1=0$). Подставляя в неравенство

[44] То же самое неравенство для произвольного кода с однозначным декодированием доказывается более сложно и называется неравенством Макмиллана.

[45] Точная формула для K далее не существенна.

$x = k^{-l_i}/p_i$, получаем, что

$$-l_i + \log_k\Big(\frac{1}{p_i}\Big) \leqslant K\Big(\frac{k^{-l_i}}{p_i} - 1\Big),$$

откуда

$$l_i \geqslant K\Big(1 - \frac{k^{-l_i}}{p_i}\Big) + \log_k\Big(\frac{1}{p_i}\Big).$$

Далее,

$$p_i l_i \geqslant K(p_i - k^{-l_i}) + p_i \log_k\Big(\frac{1}{p_i}\Big).$$

Складывая эти неравенства, получаем

$$\begin{aligned} &p_1 l_1 + \ldots + p_n l_n \geqslant \\ &\geqslant K(p_1 + \ldots + p_n - k^{-l_1} - \ldots - k^{-l_n}) + p_1 \log_k\Big(\frac{1}{p_1}\Big) + \ldots + p_n \log_k\Big(\frac{1}{p_n}\Big) = \\ &= K(1 - k^{-l_1} - \ldots - k^{-l_n}) + H_k(p_1, \ldots, p_n) \geqslant H_k(p_1, \ldots, p_n) \end{aligned}$$

согласно теореме 7. Таким образом, теорема 6 доказана.

Благодарности

Автор благодарен А. В. Устинову и рецензенту редколлегии за полезные советы.

Список литературы

[1] *Берлекэмп Э. Р.* Алгебраическая теория кодирования. М.: Мир, 1971.

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

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

[4] *Гашков С. Б.* Разностные множества, конечные геометрии, матрицы Заранкевича и экстремальные графы // Математическое просвещение. Сер. 3. Вып. 21. М.: МЦНМО, 2017. С. 145–185.

[5] *Гашков С. Б.* Графы-расширители и их применения в теории кодирования // Математическое просвещение. Сер. 3. Вып. 13. М.: МЦНМО, 2009. С. 104–126.

[6] *Левенштейн В. И.* Элементы теории кодирования // Дискретная математика и математическая кибернетика. Т. 1. М.: Наука, 1974.

[7] *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.

[8] *Прасолов В. В. и др.* Московские математические олимпиады 1935–1957 гг. М.: МЦНМО, 2010.

[9] *Прасолов В. В. и др.* Московские математические олимпиады 1958–1967 гг. М.: МЦНМО, 2013.

[10] *Бегунц А. В. и др.* Московские математические олимпиады 1981–1992 гг. М.: МЦНМО, 2017.

[11] *Фёдоров Р. М. и др.* Московские математические олимпиады 1993–2005 гг. / 3-е изд. М.: МЦНМО, 2017.

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

[13] *Сидельников В. М.* Теория кодирования. М.: Физматлит, 2008.

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

[15] *Фейеш Тот Л.* Расположения на плоскости, на сфере и в пространстве. М.: Физматгиз, 1958.

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

[17] *Чашкин А. В.* Дискретная математика. М.: Академия, 2012.

[18] *Guruswami V., Sudan M.* Improved decoding of Reed — Solomon and algebraic-geometric codes // IEEE Trans. Inform. Theory. 1999. Vol. 45. P. 1757–1767.

[19] *Winkler P.* Mathematical puzzles: a connoisseur's collection. Natick, USA: Taylor and Francis Inc., 2004.

Сергей Борисович Гашков, мехмат МГУ
sbgashkov@gmail.com