Teorija grafov, teorija kodirovanija i blok-sxemy

П. Камерон
Дж. ван Линт

ТЕОРИЯ ГРАФОВ ТЕОРИЯ КОДИРОВАНИЯ И БЛОК-СХЕМЫ

Перевод с английского
Б. С. СТЕЧКИНА

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1980

22.18
К 18
УДК 519.6

London Mathematical Society
Lecture Note Series, 19

Graph Theory
Coding Theory and
Block Designs

P. J. CAMERON & J. H. VAN LINT

Cambridge University Press

К $\frac{20204-148}{053(02)-80}$ 41-80. 1702070000

ОГЛАВЛЕНИЕ

Предисловие переводчика 4
Введение 5
1. Краткое введение в теорию схем 6
2. Сильно регулярные графы 17
3. Квазисимметричные схемы 24
4. Сильно регулярные графы без треугольников 29
5. Полярности схем 37
6. Расширение графов 41
7. Коды 47
8. Циклические коды 54
9. Пороговое декодирование 59
10. Коды Рида — Маллера 62
11. Самоортогональные коды и схемы 67
12. Квадратично-вычетные коды 73
13. Симметричные коды над $GF(3)$ 83
14. Почти совершенные бинарные коды и равномерно упакованные коды 88
15. Ассоциативные схемы 97
Литература 109
Добавления из второго издания 114
Дополнительная литература 134
Предметный указатель 137

ПРЕДИСЛОВИЕ ПЕРЕВОДЧИКА

Книга Камерона и ван Линта представляет беглый, но емкий обзор по современной теории кодирования; в ней с особенной четкостью оттенены комбинаторные аспекты. Изложение носит конспективный характер, что делает книгу удобным пособием для специалистов по теории кодирования и комбинаторному анализу.

За небольшими исключениями (например, двойственный — дуальный), терминология согласована с русским переводом [80], имеющиеся разночтения приведены в предметном указателе.

Когда книга была уже набрана, Издательство Кембриджского университета сообщило Главной редакции о выходе нового издания книги: Graphs, Codes and Designs. — L., 1980. — LMS, LNS 43. К сожалению, эта информация оказалась слишком запоздалой. Однако редакция пошла навстречу просьбе Издательства учесть переработку в русском издании. В корректуру были внесены почти все изменения — незначительная часть непосредственно в текст, а основная часть — в виде Добавлений из второго издания; к ним делаются отсылки по тексту (курсивом); в Добавлениях делаются отсылки на соответствующие страницы. Все изменения набраны петитом.

Выражаю признательность В. А. Зиновьеву, прочитавшему рукопись перевода и сделавшему ряд полезных замечаний.

ВВЕДЕНИЕ

В 1973 году профессор ван Линт и доктор Камерон прибыли в Вестфилдский колледж каждый для чтения своей лекции на нашем семинаре по комбинаторной алгебре и геометрии. Как оказалось, содержание их лекций совпадало в наиболее интересном направлении, в связи с чем возникла идея переработать уже подготовленные заметки каждого из них в единое целое. Результат этого — настоящая книга.

Целью лекции являлось ознакомление аудитории (уже знакомой с теорией схем) с некоторыми связями этой теории и ее приложениями в других областях математики — в основном, теории графов и кодов. При этом на цель изложения повлияла связь теории схем с теорией графов и кодов; однако, последовательного изложения этих областей не дано, хотя каждой из этих теорий предшествует вводная глава.

Внимательный читатель может заметить различие стилей разных глав, демонстрирующее индивидуальность подходов обоих авторов. Мы верим, что общее математическое единство лекций и книги будет очевидным и полезным для студентов и исследователей этих разделов математики.

Новый материал включает в себя овалы в симметричных схемах, неравенства Рай-Чаудхури и Вильсона, частичные геометрии, с теоремами Хофмана — Чанга и Холла—Коннора, 1-факторизации K_6, эквидистантные коды, плоскости и биплоскости, обобщения квадратично-вычетного кода и обратимые плоскости, двухвесовые проективные коды, границу Крейна.

1. КРАТКОЕ ВВЕДЕНИЕ В ТЕОРИЮ СХЕМ

Настоящие лекции читались для специалистов, знакомых с теорией схем; для не входящих в их число эта вводная глава описывает основные понятия теории схем и некоторые конкретные примеры.

Под *t-схемой* с параметрами (v, k, λ) (или t-(v, k, λ)-*схемой*) понимается совокупность $\mathscr{D}$ подмножеств (называемых *блоками*) множества S, состоящего из v точек, такая, что каждое подмножество из $\mathscr{D}$ содержит k точек, а всякое множество из t точек содержится ровно в λ подмножествах из $\mathscr{D}$. Это определение, для исключения вырожденных случаев, обычно пополняется различными условиями; так, мы предполагаем, что S и $\mathscr{D}$ не пусты и что $v \geqslant k \geqslant t$ $(\lambda > 0)$. t-схема с параметром $\lambda = 1$ называется *штейнеровой системой.*

Иначе t-схему можно задать множеством точек, множеством блоков и бинарным отношением инцидентности между точками и блоками, удовлетворяющим соответствующим условиям.

Иногда в t-схемах допускаются «повторяющиеся» блоки, так что $\mathscr{D}$ — скорее семейство, чем множество — одно и то же подмножество S может и неоднократно фигурировать как блок. (Это естественнее согласуется с определением отношения: просто отсутствует условие, что всякие k точек инцидентны не более чем одному блоку.) В этой книге, как правило, не допускаются повторяющиеся блоки; случаи их появления оговариваются особо. Для всякого t существуют нетривиальные t-схемы с повторяющимися блоками; но известны только те примеры схем без повторяющихся блоков с $t > 5$, в которых каждые k точек образуют блок. Существование нетривиальных

t-схем при $t > 5$ есть наиболее важная нерешенная задача в этой области; даже 5-схемы настолько редки, что новые конструкции представили бы несомненный интерес. Конечно, для штейнеровых систем вопрос повторяющихся блоков не возникает. Лишь две штейнеровы системы с $t = 5$ и две с $t = 4$ известны; они будут описаны ниже *).

Замечание. 0-схема есть просто совокупность k-элементных подмножеств некоторого множества.

Пусть в t-схеме λ_i обозначает число блоков, содержащих заданное множество из i точек ($0 \leqslant i \leqslant t$). Независимо, подсчитывая число различных выборок остальных $t - i$ точек и число блоков, содержащих все t выделенных точек, находим:

$$\lambda_i \binom{k-i}{t-i} = \binom{v-i}{t-i} \lambda. \qquad (1.1)$$

Отсюда следует, что λ_i не зависит от начального выбора i точек, значит, t-схема, в то же время, является и i-схемой для $0 \leqslant i \leqslant t$. Параметры λ_0 (полное число блоков) и λ_1 (число блоков, содержащих данную точку) обычно обозначают через b и r соответственно. При $t = 1$, $i = 0$ формула (1.1) показывает, что во всякой 1-схеме

$$bk = vr. \qquad (1.2)$$

2-схема часто называется *блок-схемой* или просто схемой; в литературе термин «уравновешенная неполная блок-схема» используется, когда не каждое k-подмножество является блоком. В 2-схеме имеем равенство

$$r(k-1) = (v-1)\lambda. \qquad (1.3)$$

Матрица инцидентности схемы есть матрица M, строки и столбцы которой сопоставлены блокам и точкам схемы соответственно, а элемент в пересечении строки B и столбца p равен 1, если $p \in B$, и равен 0, если $p \notin B$. (Заметим, что часто используется и иное определение, например, в книгах Дембовского [24] и Холла [33]; разница в том, что наша матрица является транспонированной по отношению к приведен-

*) Несколько новых таких систем было недавно получено Деннистоном.

ным в этих книгах. Такое соглашение здесь принято потому, что мы хотим представлять характеристические функции блоков, или строки M, как вектор-строки, и рассматривать их линейную оболочку.)

Условия, что всякий блок содержит k точек, всякая точка лежит в r блоках, а всякая пара точек — в λ блоках, могут быть выражены в терминах матрицы M:

$$MJ = kJ,$$
$$JM = rJ,$$
$$M^TM = (r-\lambda)I + \lambda J. \tag{1.4}$$

(Здесь и далее — I — единичная матрица, а J — матрица, сплошь состоящая из единиц.) Нетрудно показать, что

$$\det((r-\lambda)I + \lambda J) = rk(r-\lambda)^{v-1},$$

так что если $r > \lambda$, то матрица M^TM несингулярна, из чего следует *неравенство Фишера*:

Теорема 1.5. *Во всякой 2-схеме при* $k \leqslant v-1$ *выполняется неравенство*

$$b \geqslant v.$$

Кроме того, если $b = v$, то $MJ = JM$; таким образом, M коммутирует с $(r-\lambda)I + \lambda J$, а значит, и с $((r-\lambda)I + \lambda J)M^{-1} = M^T$. Следовательно, $MM^T = (r-\lambda)I + \lambda J$, из чего заключаем, что всякие два блока имеют λ общих точек.

Теорема 1.6. *Во всякой 2-схеме при* $k \leqslant v-1$ *следующие утверждения эквивалентны*:

1) $b = v$;
2) $r = k$;
3) *всякие два блока имеют* λ *общих точек.*

2-схема, удовлетворяющая условиям теоремы 1.6, называется *симметричной. Двойственная* ей схема получается переменой ролей точек и блоков, посредством отождествления точки с множеством блоков, ее содержащих; эта двойственная схема есть симметричная 2-схема с теми же параметрами и матрицей инцидентности M^T. *Полярность* симметричной схемы $\mathscr{D}$ есть самообратимый изоморфизм между схемой $\mathscr{D}$ и ей двойственной, т. е. взаимно однозначное соответствие σ между точками и блоками схемы $\mathscr{D}$, такое,

Теорема Брука — Райзера — Човла дает необходимые условия существования симметричных схем с данными параметрами (v, k, λ), удовлетворяющими условию $(v-1)\lambda = k(k-1)$.

Теорема 1.8. *Предположим, что имеется симметричная* 2-(v, k, λ)-*схема и пусть* $n = k - \lambda$. *Тогда*

1) *если* v *четно, то* n — *квадрат*;

2) *если* v *нечетно, то уравнение*

$$z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2$$

резрешимо в целых x, y, z, *из которых не все равны нулю.*

Инцидентностное уравнение $M^TM = nI + \lambda J$ показывает, что матрицы I и $nI + \lambda J$ рационально кограциентны; стало быть, теорема 1.8 может быть получена применением теоремы Хассе — Минковского, хотя возможны и более элементарные доказательства. Теорема Хассе — Минковского гарантирует существование рациональной матрицы M, удовлетворяющей инцидентностному равенству в случае выполнимости условий теоремы 1.8, но это не означает, что схема существует, и неизвестно, являются ли эти условия достаточными для ее существования. Позже, в главе 11, будет подробнее обсуждаться случай $(v, k, \lambda) = (111, 11, 1)$.

Матрица Адамара — $n \times n$-матрица H с элементами ± 1, удовлетворяющая условию $HH^T = H^TH = nI$. (Она называется так потому, что ее детерминант достигает границы, принадлежащей Адамару.) Изменение знаков элементов строк и столбцов оставляет определяемое свойство неизменным, поэтому можно предполагать, что все элементы в первой строке и первом столбце равны $+1$. Если вычеркнуть эту строку и этот столбец, а в оставшихся заменить -1 на 0, то получится матрица M, которая (при $n > 4$) является матрицей инцидентности симметричной $2\text{-}\left(n-1, \frac{n}{2}-1, \frac{n}{4}-1\right)$-схемы. Такая схема называется *адамаровой* 2-*схемой*. Из схемы с такими параметрами можно восстановить матрицу Адамара обращением приведенной процедуры. Однако, матрица Адамара может быть видоизменена перестановками строк и столбцов, поэтому из «эквивалентных»

что для всякой точки p и блока B включение $p \in B$ выполняется тогда и только тогда, когда $B^\sigma \in p^\sigma$. Точка p (соотв. блок B) является абсолютной относительно полярности σ, если $p \in p^\sigma$ (соотв. $B^\sigma \in B$).

Теоремы 1.5 и 1.6 следуют из более общего результата, который приводится в главе 4.

Теорема 1.7. *Во всякой 2-схеме число блоков, не пересекающихся с данным блоком B, не меньше чем*

$$\frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}.$$

Равенство достигается тогда и только тогда, когда всякий блок, пересекающийся с B, имеет с ним постоянное число общих точек; если это условие выполнено, то постоянное число общих точек равно

$$1+\frac{(k-1)(\lambda-1)}{r-1}.$$

Доказательство. Пусть d — число блоков, отличных от B и пересекающихся с ним, и n_i из них пересекаются с B в i точках. Независимо, подсчитывая число выборов j точек в B и в другом блоке, инцидентном с этими j точками, получаем для $j = 0, 1, 2$ соответственно (суммируется от 1 до k):

$$\sum n_i = d,$$

$$\sum i n_i = k(r-1),$$

$$\sum i(i-1) n_i = k(k-1)(\lambda-1).$$

Значит,

$$\sum (i-x)^2 n_i = dx^2 - 2k(r-1)x + k((k-1)(\lambda-1)+(r-1)).$$

Эта квадратичная форма от x должна быть положительно полуопределенной и обращается в нуль, только если $d = k(r-1)^2/((k-1)(\lambda-1)+(r-1))$ и $n_i = 0$ для всех $i \neq 1+(k-1)(\lambda-1)/(r-1)$.

Замечание. Теперь теорема 1.5 следует из неравенства

$$b-1 \geqslant \frac{k(r-1)^2}{(k-1)(\lambda-1)+(r-1)}$$

с применением формул (1.2) и (1.3); точно так же, если $b = v$, то $r = k$ и

$$1+\frac{(k-1)(\lambda-1)}{r-1} = \lambda.$$

матриц Адамара можно получать различные 2-схемы Адамара.

Примеры адамаровых 2-схем включают в себя схемы Пэли, где $n-1=q$ — степень простого ($q \equiv 3 \pmod 4$). Точками такой схемы служат элементы поля $GF(q)$, а блоками — множества $Q+a$ ($a \in GF(q)$), где Q — множество ненулевых квадратов в $GF(q)$.

Пусть H — матрица Адамара порядка $n>4$, в которой каждый элемент первой строки равен $+1$. Всякая строка, отличная от первой, имеет $n/2$ единиц и $n/2$ минус единиц, определяя таким образом два множества столбцов, по $n/2$ в каждом. (Это разбиение не зависит от перемены знаков всех элементов строки.) Если рассматривать столбцы как точки, а множества, определяемые таким способом, — как блоки, то получается $3\text{-}\left(n, \frac{n}{2}, \frac{n}{4}-1\right)$-схема, именуемая *адамаровой 3-схемой*. Всякая схема с этими параметрами выводима из матрицы Адамара таким способом.

Необходимо отметить, что множество адамаровых матриц весьма велико. Примеры их известны для многих порядков n, кратных 4 (наименьший невыясненный случай: $n=188$*)), а для умеренно малых n имеется много неэквивалентных матриц.

Проективная геометрия над полем F есть, грубо говоря, совокупность подпространств векторного пространства конечного ранга над F. *Точками* геометрии являются подпространства ранга 1. Проективная геометрия часто рассматривается как решетка, в которой всякая точка является атомом и каждый элемент смежен атомам. Будем отождествлять подпространство с множеством точек, его составляющих, понимаемым как подмножество точечного множества. Размерность подпространства на единицу меньше его векторно-пространственного ранга (так, точки имеют размерность 0); размерность геометрии — та же, что и всего пространства. Прямые и плоскости — это подпространства размерности 1 и 2 соответственно; гиперплоскости — подпространства коразмерности 1. Таким образом, здесь имеют место обычные геометрические утверждения: две точки лежат на одной прямой, точка и не смежная ей прямая лежат в единственной плоскости и т. д.

*) $n=268$ (1980 г., см. [80]. — *Прим. перев.*

Для данной t-схемы $\mathscr{D}$ *производная схема* $\mathscr{D}_p$ относительно точки p есть $(t-1)$-схема, точки которой — точки схемы $\mathscr{D}$, отличные от p, а блоки — множества $B-\{p\}$ для каждого блока $B \in \mathscr{D}$, который содержит p. *Остаточная схема* $\mathscr{D}^p$ относительно точки p имеет то же точечное множество, что и $\mathscr{D}$, но ее блоки — блоки схемы $\mathscr{D}$, не содержащие точки p; она также является $(t-1)$-схемой.

Здесь, как для схем, так и для групп перестановок, весьма важен обратный вопрос, именуемый *проблемой расширений*:

Изоморфна ли данная t-схема производной $\mathscr{D}_p$ для некоторой $(t+1)$-схемы $\mathscr{D}$? Схема $\mathscr{D}$ в этом случае называется *расширением* данной схемы. Расширение может быть произведено не единожды, а может и не существовать вовсе. (Для построения расширения нужно найти подходящую схему $\mathscr{D}^p$.) Применяя формулу (1.2) к расширению, получаем простое необходимое условие расширяемости:

Предложение 1.10. *Если* t-(v, k, λ)*-схема с* b *блоками расширяема, то* $k+1$ *делит* $b(v+1)$.

Так, 2-схема $PG(2, q)$ имеет параметры $v = q^2 + q + 1 = b$, $k = q + 1$; применяя предложение 1.10, получаем результат Хьюза [39].

Теорема 1.11. *Если* $PG(2, q)$ *расширяема, то* $q = 2, 4, 10$.

Много изысканий было посвящено этим проективным плоскостям и их расширениям. Более тонкое применение предложения 1.10 показывает, что $PG(2, 2)$ и $PG(2, 10)$ могут быть расширены не более чем единожды, а $PG(2, n)$ — не более чем трижды. В действительности $PG(2, 2)$ единственна и имеет единственное расширение, именно $AG(3, 2)$. Единственна также схема $PG(2, 4)$ и может быть расширена трижды; каждое последующее расширение единственно (с точностью до изоморфизма). Существование $PG(2, 10)$ до сих пор не доказано (это будет обсуждаться в главе 11) и ее расширяемость выявится, по-видимому, не скоро.

Позднее, Хьюз показал, что имеется лишь конечное число расширений симметричных 2-(v, k, λ)-схем при всяком λ. Наиболее сильный результат в этом направлении принадлежит Камерону [17]. Он будет использован и доказан в главе 4.

Теорема 1.12. *Если симметричная* 2-(v, k, λ)-*схема* $\mathcal{D}$ *расширяема, то выполняется одно из следующих условий.*

1) $\mathcal{D}$ — *адамарова 2-схема*;
2) $v = (\lambda + 2)(\lambda^2 + 4\lambda + 2)$, $k = \lambda^2 + 3\lambda + 1$;
3) $v = 111$, $k = 11$, $\lambda = 1$;
4) $v = 495$, $k = 39$, $\lambda = 3$.

Далее см. Добавление 2.

Согласно случаю 1) этого результата, адамарова 2-схема допускает единственное расширение. Для этого нетрудно показать, что в адамаровой 3-схеме дополнение блока есть блок; тогда единственное расширение адамаровой 2-схемы $\mathcal{D}$ получается добавлением одной новой точки к каждому блоку $\mathcal{D}$, и тогда дополнение каждого такого блока будет блоком и в расширении. Помимо адамаровых схем, известной расширяемой симметричной схемой является $PG(2, 4)$ (случай 2) при $\lambda = 1$); она тоже допускает единственное расширение симметричной 2-схемой.

Для аффинных плоскостей ситуация немного иная, поскольку необходимое условие (предложение 1.10) всегда выполнено. Расширение аффинной плоскости (т. е. 3-$(q^2 + 1, q + 1, 1)$-схема) называется *обращенной плоскостью* или *Мёбиус-плоскостью*. Известно много примеров: аффинные плоскости над конечными полями все расширяемы, иногда более чем одним способом. Однако, Дембовским [22, 23] показано, что обращенная плоскость при четном q допускает естественное вложение в $PG(3, q)$ (q — степень двойки). Используя это в соединении с предложением 1.10, Кантор [42] показал, что, если $AG(2, q)$ дважды расширяема ($q > 2$), то $q = 3$, 13. В действительности, $AG(2, 3)$ трижды расширяема; эти расширения являются «погружениями» в соответствующие расширения $PG(2, 4)$, так же как в проективных геометриях над $GF(3)$. Неизвестно, верно ли, что всякая $AG(2, 13)$ дважды расширяема.

Расширения схем $PG(2, 4)$ и $AG(2, 3)$ столь важны, что мы приводим краткое описание их конструкций. См. также Витт [73, 74], Лунберг [46], Тодд [68], Джонсон [41] и т. д.

5-$(24, 8, 1)$-схема получается из $PG(2, 4)$ добавлением трех точек p, q, r; блоки, содержащие все эти три точки, суть множества $\{p, q, r\} \cup L$, где L — пря-

мая в $PG(2, 4)$. Мы должны точно определить блоки, которые не содержат все эти три точки, как подмножества $PG(2, 4)$. Они оказываются естественными геометрическими объектами: гиперовалами подплоскостями $PG(2, 2)$ и симметрическими разностями пар прямых. Действительно, это единственно возможные кандидаты; таким путем можно показать единственность схем. (При этом важно, что блоки 5-$(24, 8, 1)$-схемы могут иметь 0,2 или 4 общих элемента; это доказывается простым вычислением.)

Если U — множество абсолютных точек полярности унитарного типа (унитарная поляра) в $PG(2, 4)$, то $\{p, q, r\} \cup U$ есть точечное множество 5-$(12, 6, 1)$-схемы. Иначе, последняя схема может быть получена троекратным расширением $AG(2, 3)$ и, как и ранее, идентифицированием пополненных блоков с геометрическими объектами в плоскости.

Иное построение 5-$(12, 6, 1)$-схемы основано на том, что симметрическая группа S_6 обладает внешним автоморфизмом. Взяв два множества из шести элементов, на которых S_6 действует двумя возможными способами, блоки 5-$(12, 6, 1)$-схемы можно описать при помощи перестановок. Этот метод также позволяет доказать единственность. Этот процесс может быть продолжен: группа автоморфизмов M_{12} схемы на себя имеет один внешний автоморфизм и аналогичное построение дает 5-$(24, 8, 1)$-схему.

Можно непосредственно строить 5-кратные транзитивные группы Матье M_{12} и M_{24} и выводить свойства схем из них.

Для построения схем чисто алгебраическим путем, можно использовать приемы теории кодирования. Об этом будет сказано в главах 11 и 12.

В случае более высоких размерностей ситуация проще. Схема $PG(m, 2)$ (при $m > 2$) имеет расширение лишь если $q = 2$, когда адамарова 3-схема $AG(m + 1, 2)$ является единственно расширяемой; схема $AG(m, q)$ не расширяема при $m > 2$.

Подробнее см. Дембовский [24]: схемы — в главе 2; проективные и аффинные геометрии — в разделе 1.4; проективные плоскости — в главах 3—5 и обращенные плоскости — в главе 6. Блок-схемы также рассматриваются в книгах Холла [33] и Райзера [56]. *Далее см. Добавление* 3.

Например, пусть n — натуральное число, а V — множество всех $n \times n$-латинских квадратов с элементами $\{1, \ldots, n\}$. Образуем граф Γ_n на множестве вершин V, говоря, что два латинских квадрата смежны тогда и только тогда, когда они ортогональны. Хорошо известно, что проективная (или аффинная) плоскость порядка n существует тогда и только тогда, когда Γ_n содержит в качестве подграфа полный граф на $n-1$ вершинах. Теория графов дает нам некоторые нижние оценки для объема полных подграфов в графе, и неудивительно, что они недостаточно сильны для демонстрации существования плоскости данного порядка, за исключением тривиальных случаев. В этом свете представляется малообнадеживающей полезность применения теории графов для конечных плоскостей.

Если p — вершина графа Γ, то *валентность* p есть число ребер, содержащих p (или $|\Gamma(p)|$, т. е. число вершин, смежных с p). Если все вершины имеют одну и ту же валентность, то граф называется *регулярным*, и в таком случае эта общая для всех вершин валентность есть *валентность графа*. (Таким образом, граф является 0-схемой при $k = 2$; регулярный граф есть 1-схема, и лишь полный граф является 2-схемой, иногда называемой *парной схемой* (*схемой пар*).

Как и теории схем, можно определить *матрицу инцидентности* $M(\Gamma)$ графа Γ, как матрицу инцидентностного отношения (строки — ребра, столбцы — вершины, и элемент матрицы $a_{e,p}$ равен 1, если $p \in e$, и 0 в противном случае). Более полезна *матрица смежности* $A(\Gamma)$ — матрица отношения смежности (строки и столбцы — вершины и $a_{p_1, p_2} = 1$, если $\{p_1, p_2\}$ — ребро, и 0 в противном случае). Отметим, что $M(\Gamma)\,{}^tM(\Gamma)$ есть сумма симметричной матрицы $A(\Gamma)$ и диагональной матрицы, элементы которой с индексом (p, p) равны валентности вершины p; так что $M(\Gamma)\,{}^tM(\Gamma) = A(\Gamma) + aI$, если Γ — регулярный граф валентности a. Заметим также, что $A(\overline{\Gamma}) = J - I - A(\Gamma)$, где (как всегда) J — матрица, сплошь состоящая из единиц. Граф Γ регулярен тогда и только тогда, когда $A(\Gamma)J = aJ$ для некоторого числа a (которое тогда и будет валентностью J).

Сильно регулярный граф есть регулярный граф (не полный и не пустой), который обладает тем свой-

2. СИЛЬНО РЕГУЛЯРНЫЕ ГРАФЫ

В теории схем исследуются системы подмножеств (или отношений между двумя множествами) с высокой степенью симметрии. В противоположность этому, в большой и, на наш взгляд аморфной, области, называемой «теория графов», исследуются вопросы об «общих» отношениях на множестве. Такая общность обычно означает, что либо задаваемые вопросы слишком частны, либо получаемые результаты недостаточно мощны для вывода полезных следствий в теории схем. И все-таки есть несколько мест, в которых эти две теории взаимополезны; некоторые из них будут описаны в следующих пяти главах. Необходимая унификация здесь обеспечивается классом «сильно регулярных графов», введенных Боузом [11], определение которых отражает симметрию, присущую t-схемам. Но прежде всего, без обсуждения, укажем пример такой ситуации.

Граф состоит из конечного множества вершин и множества ребер, где каждое ребро есть подмножество множества вершин мощности 2. (Иными словами, наши графы неориентированны, не имеют петель и кратных ребер.) Как и в схемах, есть иное определение: граф состоит из множества вершин, множества ребер и «инцидентного» отношения между вершинами и ребрами, такого, что всякое ребро инцидентно двум вершинам, а любые две вершины инцидентны не более чем одному ребру. Несколько иное определение: граф состоит из конечного множества вершин и симметричного иррефлексивного бинарного отношения (называемого *смежностью*) на этом множестве вершин. Граф является *полным*, если любая пара вершин смежна, и пустым, если он не имеет ребер. *Дополнением* графа Γ является граф $\overline{\Gamma}$, множество ребер которого есть дополнение множества ребер графа Γ (относительно множества всех 2-элементных подмножеств этого вершинного множества). Во всяком графе Γ через $\Gamma(p)$ обозначаем множество вершин, смежных вершине p. Для данного множества вершин S через Γ/S обозначаем граф на множестве вершин S, ребра которого — ребра графа Γ на множестве вершин S.

ством, что число вершин, смежных вершинам p_1 и $p_2 (p_1 \neq p_2)$, зависит лишь от того, смежны эти вершины или нет. Его *параметры* суть (n, a, c, d), где n — число вершин, a — валентность, c — число вершин, смежных p_1 и p_2, если $\{p_1, p_2\} \in \Gamma$, и d — число вершин, смежных p_1 и p_2, если $\{p_1, p_2\} \notin \Gamma$. (Эти обозначения нестандартны. Мы их используем, поскольку стандартных не существует; из двух основных претендентов один здесь невозможен, так как он использует символы k и λ, а другой есть специальный случай обозначения ассоциативных схем и очень громоздкий. Так что обозначение, используемое здесь, лишь

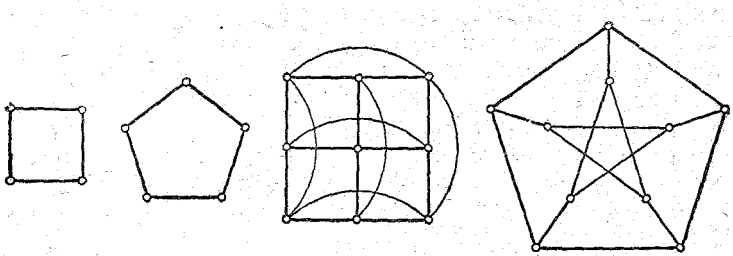

Рис. 2.1.

временное, обусловленное его применением в теории схем.)

Если Γ — сильно регулярный граф, p_1 и p_2 — пара его смежных вершин, то $a - c - 1$ вершин смежны p_1 и не смежны p_2 и $(n - a - 1) - (a - c - 1)$ вершин не смежны ни p_1, ни p_2. Аналогично проводится расчет, если p_1 и p_2 не смежны. Стало быть, дополнительный граф $\overline{\Gamma}$ тоже сильно регулярен.

Лишь несколько графов достаточно малы для их явного изображения. На рис. 2.1 маленькие окружности представляют вершины, а дуги — ребра, но две дуги могут пересекаться и не по вершине. Четыре сильно регулярных графа изображены на рис. 2.1.

Большие графы требуют уже словесного описания. Например, *треугольный граф* $T(m)$ $(m \geqslant 4)$ имеет своими вершинами двуэлементные подмножества множества мощности m: две вершины в нем смежны тогда и только тогда, когда отвечающие им подмно-

жества пересекаются. Граф $T(m)$ сильно регулярен с параметрами $n = m(m-1)/2$, $a = 2(m-2)$, $c = m-2$, $d = 4$. Четвертый граф на рис. 2.1, называемый *графом Петерсена*, есть граф, дополнительный к $T(5)$. *Решетчатый граф* $L_2(m)$ $(m \geqslant 2)$ имеет своими вершинами множество $S \times S$, где S — множество мощности m; две вершины этого графа смежны тогда и только тогда, когда они имеют общую координату. Граф $L_2(m)$ сильно регулярен с параметрами $n = m^2$, $a = 2(m-1)$, $c = m-2$, $d = 2$. Первый и третий графы на рис. 2.1 суть $L_2(2)$ и $L_2(3)$. Объединение k непересекающихся полных графов на m вершинах каждый $(k, m > 1)$ также образует сильно регулярный граф $\Gamma(k, m)$ с параметрами $n = mk$, $a = m-1$, $c = m-2$, $d = 0$, причем всякий сильно регулярный граф с $d = 0$ имеет такую форму. Граф $\Gamma(k, 2)$ называется *лестничным графом*. Дополнение графа $\Gamma(k, m)$ называется *полным k-дольным графом*. Первый граф на рис. 2.1 есть полный двудольный граф $\Gamma(2, 2)$. Если q — степень простого и $q \equiv 1 \pmod 4$, то граф Пэли $P(q)$ имеет в качестве вершин элементы поля $GF(q)$, и две его вершины смежны тогда и только тогда, когда их разность есть ненулевой квадрат. Это сильно регулярный граф с параметрами $n = q$, $a = (q-1)/2$, $c = (q-5)/4$, $d = (q-1)/4$, изоморфный своему дополнению. Второй и третий графы на рис. 2.1 суть $P(5)$ и $P(9)$. *Далее см. Добавление* 4.

Если G — группа перестановок на множестве V, то G обладает естественным покомпонентным действием на $V \times V$. Будем говорить, что группа G имеет *ранг* 3, если она транзитивна на V и имеет точно три орбиты на $V \times V$: диагональ $\{(p, p) \mid p \in V\}$ и еще две других орбиты O, O'. Если группа G ранга 3 имеет четный порядок, она содержит инволюционно заменяемые точки, скажем, p и q; таким образом, орбита, содержащая (p, q), симметрична, так же как и другая. Образуем граф Γ с множеством вершин V, ребра которого — неупорядоченные пары, соответствующие упорядоченным парам в O. Группа G является группой автоморфизмов графа Γ. Поскольку G транзитивна на вершинах, граф Γ регулярен; поскольку G транзитивна на смежных и несмежных парах вершин, Γ сильно регулярен. Много известных групп ранга 3 четного порядка дает большое число сильно регуляр-

ных графов, включая все уже приведенные; такие графы иногда называют *графами ранга* 3.

Пусть A — матрица смежности сильно регулярного графа Γ с параметрами (n, a, c, d). Элемент (p_1, p_2) матрицы A^2 равен числу вершин, смежных p_1 и p_2; это число есть a, c или d в зависимости от того, равны, смежны или не смежны p_1 и p_2, так что

$$A^2 = aI + cA + d(J - I - A), \tag{2.1}$$

а также

$$AJ = JA = aJ. \tag{2.2}$$

Таким образом, матрицы I, J, A образуют действительную алгебру размерности 3, которая коммутативна и состоит из симметричных матриц. Сильно регулярные графы можно было бы определить как графы, матрицы смежности которых удовлетворяют (2.1) и (2.2). Существует ортогональная матрица, которая одновременно диагонализирует I, J и A. Матрица A имеет собственное значение с кратностью 1, соответствующее собственному значению n матрицы J; таким образом,

$$a(a - c - 1) = (n - a - 1)d. \tag{2.3}$$

Это уравнение можно также установить, выбирая вершину p_1 и подсчитывая число ребер $\{p_2, p_3\}$ с p_2, смежным, и p_3, не смежным p_1. Любое другое собственное значение матрицы J есть нуль; значит, другие собственные значения ρ_1, ρ_2 матрицы A удовлетворяют уравнению

$$\rho^2 = (a - d) + (c - d)\rho,$$

откуда

$$\rho_1, \rho_2 = \frac{1}{2}\left[c - d \pm \sqrt{(c - d)^2 + 4(a - d)}\right].$$

Если ρ_1 и ρ_2 имеют кратности f_1 и f_2 соответственно, то

$$n = f_1 + f_2 + 1,$$
$$0 = \mathrm{Tr}(A) = a + f_1\rho_1 + f_2\rho_2.$$

Эти уравнения определяют f_1 и f_2 (так как $c = d = a$ невозможно). Без труда находим, что

$$f_1, f_2 = \frac{1}{2}\left[n - 1 \pm \frac{(n - 1)(d - c) - 2a}{\sqrt{(d - c)^2 + 4(a - d)}}\right]. \tag{2.4}$$

Очевидно, f_1 и f_2 — неотрицательные целые. Это замечание налагает весьма строгие условия на параметры — так называемые «условия рациональности» (рациональные условия). Они включают в себя наиболее известный критерий несуществования для сильно регулярных графов. Известны и иные условия; некоторые из них будут указаны ниже.

Если граф Γ имеет ранг 3, то алгебра, порожденная матрицами I, J и $A(\Gamma)$, есть в точности центральная алгебра множества матриц в перестановочном представлении группы $G = A \cup I$, а кратности собственных значений $A(\Gamma)$ суть степени неприводимых элементов перестановочного характера G.

Можно выделить два типа параметрических множеств, для которых f_1 и f_2 — целые.

Тип I. $(n-1)(d-c) = 2a$; здесь $n = 1 + 2a/(d-c) > 1 + a$, $0 < d - c < 2$. Таким образом, $d - c = 1$, и находим $c = d - 1$, $a = 2d$, $n = 4d + 1$. Можно показать, что выполнены условия, как в теореме Брука — Райзера: n должно быть суммой квадратов двух целых чисел. Графы Пали принадлежат типу I.

Тип II. Здесь $(d-c)^2 - 4(a-d)$ есть квадрат целого n, n делит $(n-1)(d-c) - 2a$ и частное от этого деления сравнимо с $n - 1 \pmod 2$. Ясно, что графы принадлежат типу II тогда и только тогда, когда n — квадрат; например, $L_2(3) \cong P(9)$.

Граф Γ с матрицей смежности A регулярен тогда и только тогда, когда единичный, т. е. сплошь состоящий из единиц вектор j является собственным вектором матрицы A; соответствующее собственное значение есть валентность. Так как A симметрична, то j есть инвариант относительно A. Так что Γ сильно регулярен тогда и только тогда, когда $A/j^{\perp}$ имеет ровно два различных собственных значения. (Необходимость этого мы уже установили. Обратно, если $(A - \rho_1 I)(A - \rho_2 I)/j^{\perp} = 0$, то $(A - \rho_1 I)(A - \rho_2 I) = \alpha J$ для некоторого α, откуда $A^2 \in \langle I, J, A \rangle$ и Γ сильно регулярен.)

Мы уже видели, что параметры сильно регулярного графа Γ определяют собственные значения матрицы A и их кратности. Имеет место и обратное — собственные значения A и их кратности определяют параметры Γ: n является суммой кратностей, a —

ных графов, включая все уже приведенные; такие графы иногда называют *графами ранга* 3.

Пусть A — матрица смежности сильно регулярного графа Γ с параметрами (n, a, c, d). Элемент (p_1, p_2) матрицы A^2 равен числу вершин, смежных p_1 и p_2; это число есть a, c или d в зависимости от того, равны, смежны или не смежны p_1 и p_2, так что

$$A^2 = aI + cA + d(J - I - A), \tag{2.1}$$

а также

$$AJ = JA = aJ. \tag{2.2}$$

Таким образом, матрицы I, J, A образуют действительную алгебру размерности 3, которая коммутативна и состоит из симметричных матриц. Сильно регулярные графы можно было бы определить как графы, матрицы смежности которых удовлетворяют (2.1) и (2.2). Существует ортогональная матрица, которая одновременно диагонализирует I, J и A. Матрица A имеет собственное значение с кратностью 1, соответствующее собственному значению n матрицы J; таким образом,

$$a(a - c - 1) = (n - a - 1)d. \tag{2.3}$$

Это уравнение можно также установить, выбирая вершину p_1 и подсчитывая число ребер $\{p_2, p_3\}$ с p_2, смежным, и p_3, не смежным p_1. Любое другое собственное значение матрицы J есть нуль; значит, другие собственные значения ρ_1, ρ_2 матрицы A удовлетворяют уравнению

$$\rho^2 = (a - d) + (c - d)\rho,$$

откуда

$$\rho_1,\ \rho_2 = \frac{1}{2}\left[c - d \pm \sqrt{(c - d)^2 + 4(a - d)}\right].$$

Если ρ_1 и ρ_2 имеют кратности f_1 и f_2 соответственно, то

$$n = f_1 + f_2 + 1,$$
$$0 = \mathrm{Tr}\,(A) = a + f_1\rho_1 + f_2\rho_2.$$

Эти уравнения определяют f_1 и f_2 (так как $c = d = a$ невозможно). Без труда находим, что

$$f_1,\ f_2 = \frac{1}{2}\left[n - 1 \pm \frac{(n-1)(d-c) - 2a}{\sqrt{(d-c)^2 + 4(a-d)}}\right]. \tag{2.4}$$

наибольшим собственным значением

$$nac = \mathrm{Tr}\,(A^3) = a^3 + f_1\rho_1^3 + f_2\rho_2^3.$$

Система

$$n = \mathrm{Tr}\,(I) = 1 + f_1 + f_2,$$
$$0 = \mathrm{Tr}\,(A) = a + f_1\rho_1 + f_2\rho_2,$$
$$na = \mathrm{Tr}\,(A^2) = a^2 + f_1\rho_1^2 + f_2\rho_2^2$$

показывает, что собственные значения определяют их кратности, если они все различны. (Но если два собственных значения равны, то граф является графом $\Gamma(k, m)$.) Однако, значение кратностей не всегда определяет собственные значения однозначно. Иногда это дает лишь частичную информацию, как показывает, например, следующий результат Виландта [71].

Теорема 2.5. *Предположим, что* Γ *— сильно регулярный граф на* $n = 2m$ *вершинах, чьи собственные значения имеют кратности* $1, m-1, m$. *Тогда*

1) *либо* Γ *или его дополнение является лестничным графом;*

2) *либо* Γ *или его дополнение имеет параметры* $n = 4s^2 + 4s + 2$, $a = s(2s+1)$, $c = s^2 - 1$, $d = s^2$ *для некоторого положительного целого* s.

Замечание. Для 2) известно много примеров. Замена недиагональных нулей на -1, дает так называемые «регулярные симметричные конференс-матрицы» [29]. Имеется единственный пример с $s = 1$ — граф Петерсена.

Доказательство. Можно предполагать, что $a < m$ (заменить, если необходимо, на граф, дополнительный к нему). Имеем

$$a + (m-1)\rho_1 + m\rho_2 = 0,$$
$$a^2 + (m-1)\rho_1^2 + m\rho_2^2 = 2ma,$$
$$a^3 + (m-1)\rho_1^3 + m\rho_2^3 = 2mac$$

и $|\rho_1| \leqslant a$ согласно теореме Перрона — Фробениуса.

Первое уравнение показывает, что $a \equiv \rho_1 \pmod m$; значит, либо $\rho_1 = a$, либо $\rho_1 = a - m$. В первом случае $\rho_2 = -a$, $2ma^2 = 2ma$, $a = 1$ и выполнено 1). Во втором случае положим $\rho_2 = s$. Находим $a = m - 1 - s$, $\rho_1 = -1 - s$; тогда из второго уравнения вытекает, что $m = 2s^2 + 2s + 1$; значение c следует из третьего уравнения. *Далее см. Добавление* 5.

связывающие эти неизвестные нам параметры; подчас этих соотношений оказывается достаточно для определения параметров. Так, в частности, имеет место

Предложение 3.3. 1) *Если* Γ *— лестничный граф, то* $\mathcal{D}$ *получается из симметричной схемы удвоением каждого блока (т. е. подсчетом каждого блока* $\mathcal{D}$ *дважды).*

2) *Если* Γ *— дополнение лестничного графа, то* $\mathcal{D}$ *является адамаровой 3-схемой.*

3) Γ *никогда не бывает решетчатым графом или его дополнением.*

Мы докажем 2) позже, используя лишь знание b и v. Результатом, тесно связанным с теоремой 3.2, является

Предложение 3.4. *В квазисимметричной схеме (без кратных блоков) выполняется неравенство*

$$b \leqslant v(v-1)/2.$$

Доказательство. Пусть $M(\varepsilon_0, \varepsilon_1, \varepsilon_2)$ — матрица со строками, индексированными парами точек, и столбцами, индексированными блоками, по правилу: элемент $(\{p_1, p_2\}, B)$ равен ε_i, если $|\{p_1, p_2\} \cap B| = i$, $i = 0, 1, 2$. Находим, что

$$M^T(0,0,1)M(\varepsilon_0, \varepsilon_1, 0) =$$

$$= \left(y(k-y)\varepsilon_1 + \binom{k-y}{2}\varepsilon_0\right)A +$$

$$+ \left(x(k-x)\varepsilon_1 + \binom{k-x}{2}\varepsilon_0\right)(J - I - A).$$

Предположим, что $b > v(v-1)/2$. Тогда это матричное произведение сингулярно при любом выборе ε_0 и ε_1. Собственный вектор с нулевым значением является собственным вектором для J и A и не есть j. Так что, если α — соответствующее собственное значение A, то для $(\varepsilon_0, \varepsilon_1) = (0, 1)$, $(1, 0)$ имеем соответственно

$$y(k-y)\alpha + x(k-x)(-1-\alpha) = 0,$$

$$\binom{k-y}{2}\alpha + \binom{k-x}{2}(-1-\alpha) = 0.$$

Поскольку случаи $\alpha = 0 = -1 - \alpha$ исключаются, детерминант этих уравнений должен быть равен нулю. Но он равен $(k-x)(k-y)(k-1)(x-y)/2$; следовательно, либо $k = x$, либо $k = y$, либо $k = 1$,

либо $x = y$. Из первых двух равенств следует, что схема имеет кратные блоки; оставшиеся два равенства невозможны.

Замечание. В этом доказательстве довольно слабо использована теорема 3.2. Более общий результат приведен в главе 15.

В специальных случаях имеют место более сильные результаты. Так:

Предложение 3.5. *В квазисимметричной схеме $\mathcal{D}$ с пересечениями мощности x и y*

1) *из* $x = 0$ следует $b \leqslant v(v-1)/k$;

2) *из* $x=0$, $y=1$ *следует* $b=v(v-1)/(k(k-1))$.

Доказательство. С утверждением 2) мы уже встречались. Для доказательства 1) предположим, что $x = 0$, и рассмотрим инцидентностную структуру, «точки» которой суть блоки $\mathcal{D}$, содержащие p, а «блоки» — точки $\mathcal{D}$, отличные от p, с инцидентностью, двойственной той, что есть в $\mathcal{D}$. Всякие две «точки» лежат в $y-1$ «блоках» и всякий «блок» имеет λ «точек», т. е. эта структура образует 2-схему. Применяя для нее неравенство Фишера $v-1 \geqslant r$, получаем результат. Кроме того, если в этом неравенстве выполнено равенство, то эта инцидентностная структура является симметричной 2-схемой, следовательно, двойственная ей схема есть также 2-схема и $\mathcal{D}$ есть 3-схема. С такими схемами мы вновь встретимся в следующей главе.

Петренюк [52] показал, что $b \geqslant v(v-1)/2$ в 4-схеме. Из работы Дельсарта получим характеристики схем, достигающих этой границы (см. главу 15).

Предложение 3.6. *Для 2-схемы $\mathcal{D}$ с параметрами $4 \leqslant k \leqslant v-4$ всякие два из следующих утверждений влекут третье:*

1) *$\mathcal{D}$ квазисимметрична;*

2) *$\mathcal{D}$ есть 4-схема;*

3) $b = v(v-1)/2$.

В действительности, с точностью до дополнения, известна только одна схема, удовлетворяющая всем условиям теоремы 3.6, а именно 4-(23, 7, 1)-схема.

Ито показал, что других не существует.

Эта 4-схема порождает ряд примеров квазисимметричных схем. Если $\mathcal{D}$ — t-схема, то через $\mathcal{D}_p$ (соотв. $\mathcal{D}^p$) обозначаем инцидентностную структуру,

соединима путем в этом графе. Функция d, определяемая по правилу: $d(p, q)$ равна длине кратчайшего пути, соединяющего вершины p и q, является метрикой в связном графе; *диаметр* графа есть наибольшее значение, принимаемое этой функцией. *Обхват* графа есть длина кратчайшего цикла без повторяющихся ребер, при условии, что такой цикл существует.

Для сильно регулярных графов связность, диаметр и обхват легко устанавливаются из его параметров. Граф Γ связен с диаметром 2, если $d > 0$, и несвязен при $d = 0$. Γ имеет обхват, если только $a > 1$; его обхват равен 3, если $c > 0$, 4, если $c = 0$ и $d > 1$, 5, если $c = 0$, $d = 1$.

Легко видеть, что граф с диаметром 2 и максимальной валентностью a имеет не более $a^2 + 1$ вершин, а граф с диаметром 5 и максимальной валентностью a — по крайней мере $a^2 + 1$ вершин. Равенство имеет место в обоих случаях тогда и только тогда, когда граф сильно регулярен с параметрами $c = 0$, $d = 1$. Такой граф называется *графом Мура* с диаметром 2. Следует отметить, что аналогичные границы существуют и для больших значений диаметра и обхвата, но, как было показано Банней, Ито [7] и Дэймрелом [20], они достигаются лишь графами, содержащими единственный цикл. В случае диаметра 2 существуют, однако, и нетривиальные примеры.

Условие $c = 0$, $d = 1$ настолько сильно, что рациональное условие может дать полезную информацию. Действительно, это показывает, что $\frac{1}{2}\left[a^2 \pm \frac{a(a-2)}{\sqrt{4a-3}}\right]$ — целые. Тип I реализуется, только если $a = 2$; здесь пентагон является единственным графом. Для типа II имеем $a = (u^2 + 3)/4$ при некотором целом, делящем $(u^2 + 3)(u^2 - 5)/16$, т. е. u делитель 15. Случай $u = 1$ невозможен, значит, $u = 3$, 5 или 15, $a = 3, 7$ или 57, $n = 10, 50$ или 3250.

Впервые это было доказано Хофманом и Синглтоном [38], которые проанализировали первые два случая. Если $n = 10$, $a = 3$, то легко видеть, что граф Петерсена есть единственный пример. Они также показали существование и единственность графа с $n = 50$, $a = 7$. Последний случай пока еще слишком обширен для полного анализа.

Поскольку этот случай довольно плотно насыщен, мы исключим его и рассмотрим сильно регулярные графы обхвата 4. Они включают полные двудольные графы (с $c=0$, $d=a$), которые не интересны — исключим и их из рассмотрения, предполагая, что $c=0$, $1<d<a$.

Теорема 4.1. *Пусть* Γ *— сильно регулярный граф с* $c=0$, $1<d<a$. *Пусть* p *— некоторая его вершина и* $\mathscr{D}(\Gamma, p)$ *обозначает инцидентностную структуру с точечным множеством* $\Gamma(p)$ *и множеством блоков* $\overline{\Gamma}(p)$, *с инцидентностью точки блоку тогда и только тогда, когда они смежны в* Γ. *Тогда* $\mathscr{D}(\Gamma, p)$ *является 2-схемой с параметрами* $v=a$, $k=d$, $\lambda=k-1$, $r=v-1$, $b=v(v-1)/k$, *возможно обладающей кратными блоками.*

Доказательство. Очевидно, всякий блок инцидентен d точкам. Возьмем две точки $\mathscr{D}(\Gamma, p)$. Обе они смежны p и не смежны между собой, и $d-1$ вершин смежны обеим, и все эти вершины должны лежать в $\overline{\Gamma}(p)$. Отсюда следуют значения и для остальных параметров.

В оставшейся части этой главы в схемах допускаются кратные блоки и используются параметры схем v и k вместо a и d. Сейчас нас интересует следующее: какие 2-схемы с $\lambda=k-1$ представимы как $\mathscr{D}(\Gamma, p)$ для некоторого сильно регулярного графа обхвата 4?

Условия рациональности дают некоторую информацию, хотя и не столь эффектную, как в случае графа Мура, именно, они показывают, что числа

$$\frac{1}{2}\left[n-1\pm\frac{v(v+k-3)}{\sqrt{k^2-4k+4v}}\right]$$

— целые. Тип I не может встречаться ($d\neq c+1$), поэтому $k^2-4k+4v$ есть полный квадрат, скажем

$$k^2-4k+4v=(k+2s)^2,$$

где s — целое, $s>0$ (поскольку $k^2-4k+4v\equiv k^2 \pmod 2$). Тогда имеет место

Предложение 4.2. *Числа* $v=(s+1)k+s^2$ *и*

$$\frac{1}{2}\left[\frac{((s+1)k+s^2)((s+2)k+s^2-1)}{k}\pm\right.$$
$$\left.\pm\frac{((s+1)k+s^2)\ ((s+2)k+s^2-3}{k+2s}\right]$$

— целые.

Что можно сказать о случае равенства? Во-первых, нам потребуется следующая простая лемма о схемах, которую полезно сравнить с предложением 3.6.

Лемма 4.4. *Рассмотрим три следующие утверждения о схеме* $\mathscr{D}$, *где* $2 < k < v - 1$:

1) $\mathscr{D}$ — *3-схема*;

2) $\mathscr{D}$ — *квазисимметричная 2-схема с* $x = 0$;

3) $b = v(v-1)/k$.

любые два из этих условий влекут третье, а также то, что $\mathscr{D}$ *является расширением симметричной 2-схемы* (*т. е., что теорема* 1.12 *справедлива для* $\mathscr{D}_p$).

Доказательство. Три этих утверждения, очевидно, эквивалентны следующим трем утверждениям о $\mathscr{D}_p$:

1) $\mathscr{D}_p$ — 2-схема;

2) двойственная к $\mathscr{D}_p$ схема есть 2-схема;

3) $\mathscr{D}_p$ имеет одинаково много точек и блоков.

Теорема 4.5. *В условиях теоремы* 4.3 *предположим, что* $k > 2$. *Тогда следующие утверждения эквивалентны*:

1) $\mathscr{D}(\Gamma, p)$ — *3-схема*;

2) $\mathscr{D}(\Gamma, p)$ *квазисимметрична*;

3) $\Gamma|\overline{\Gamma}(p)$ *сильно регулярен*;

4) $v = \lfloor 3k + 1 + (k-1)\sqrt{4k+1} \rfloor/2$.

Из всякого из этих утверждений следует, что

$$v = s(s^2 + 3s + 1), \quad k = s(s+1)$$

и что $\Gamma|\overline{\Gamma}(p)$ *является дополнением блок-графа схемы* $\mathscr{D}(\Gamma, p)$.

Замечание. Как показывает пример графа на 56 вершинах, условие $k \neq 2$ существенно.

Доказательство. Согласно 4.4 утверждения 1) и 2) эквивалентны (поскольку $b = v(v-1)/k$). Если тот или другой пункт выполнен, то теорема 1.12 дает весьма ограниченные возможности для параметров схемы $\mathscr{D}(\Gamma, p)$:

1) $v = 4y$, $k = 2y$;

2) $v = y(y^2 + 3y + 1)$, $k = y(y+1)$;

3) $v = 112$, $k = 12$, $y = 2$;

4) $v = 496$, $k = 40$, $y = 4$.

Первое из равенств исключается согласно 4.3, а

третье и четвертое не удовлетворяют рациональному условию 4.2. Так что приходим к единственной возможности:

$$v = y(y^2 + 3y + 1), \quad k = y(y + 1),$$

для которой 4) легко проверяется.

Если 4) выполнено, то имеем равенство в 4.3 и, значит, блоки смежны тогда и только тогда, когда они не пересекаются, в то время как пересекающиеся пары блоков имеют одинаково много общих точек. Значит, 2) и 3) выполнены.

Предположим, наконец, что 3) выполнено. Тогда всякие два пересекающихся блока оба смежны t другим блокам и смежны $k - t$ точкам (т. е. содержат их) для некоторого целого t; смежные блоки не пересекаются. Таким образом, $\mathscr{D}(\Gamma, p)$ квазисимметрична и $\Gamma|\overline{\Gamma}(p)$ есть дополнение к ее блоку-графу.

Замечание. Большая часть доказательства (1.12) посвящена установлению того, что, за исключением адамарова случая, число блоков, не пересекающихся с данным блоком, равно по крайней мере $v - k$. В ситуации (4.5) это выполнено автоматически, и тем самым доказательство (1.12) может быть значительно укорочено. Специальный случай (1.12), необходимый для (4.5), был доказан в первую очередь.

Если Γ удовлетворяет условиям теоремы 4.5, то $\mathscr{D}(\Gamma, p)$ является квазисимметричной 3-схемой, и значит, для всякой точки q $\mathscr{D}(\Gamma, p)^q$ есть квази-симметричная 2-схема. Таким образом, если p и q — смежные вершины, то $\Gamma|\overline{\Gamma}(p)$ и $\Gamma|(\overline{\Gamma}(p) \cap \overline{\Gamma}(q))$ являются сильно регулярными графами без треугольников. Параметры соответствующих схем таковы:

$$2 - (s^2(s + 2), \quad s^2, \quad s^2 - 1)$$

и

$$2 - (s(s^2 + s - 1), \quad s(s - 1), \quad s^2 - s - 1).$$

Заметим только, что если p и r несмежны, то $(\Gamma(p) \cap \overline{\Gamma}(r), \overline{\Gamma}(p) \cap \Gamma(r))$ есть симметричная 2-схема с параметрами $(s^2(s + 2), s(s + 1), s)$ с инцидентностью, равной смежности в Γ.

Укажем одно следствие теоремы 4.5, относящееся к расширению схем. Теорема 1.12 показывает, что параметры расширенной симметричной схемы могут иметь один из следующих видов:

1) $(4\lambda+3, 2\lambda+1, \lambda)$ (адамарова 2-схема);
2) $((\lambda+2)(\lambda^2+4\lambda+2), \lambda^2+3\lambda+1, \lambda)$;
3) $(111, 11, 1)$;
4) $(495, 39, 3)$;

Известно, что всякая адамарова схема единственно расширяема. Это неверно для других параметрических множеств. Рассмотрим случай 2). При $\lambda=1$ имеется единственная схема, именно, $PG(2,4)$, и она допускает три различных (хотя и изоморфных) расширения. При $\lambda=2$ имеется четыре известных 2-$(56, 11, 2)$-схемы (см. [26, 34] и Деннистон (частное сообщение), но Баумерт и Холл показали ее нерасширяемость (частное сообщение Холла мл.). Однако, имеет место более слабый результат:

Теорема 4.6. *Если симметричная* 2-$((\lambda+2)(\lambda^2+4\lambda+2, \lambda^2+3\lambda+1, \lambda)$-*схема расширяема, то таковой является и двойственная ей.*

Доказательство. Пусть $\mathscr{D}$ — 3-схема, а q — точка $\mathscr{D}$, для которой $\mathscr{D}$ изоморфна данной симметричной схеме. В $\mathscr{D}$ ровно $v-k$ блоков не пересекаются с данным блоком и имеется сильно регулярный граф Γ обхвата 4 с вершиной p, такой, что $\mathscr{D}(\Gamma, p)\cong\mathscr{D}$. Поскольку 4) из теоремы 4.5 не зависит от вершины p, то $\mathscr{D}(\Gamma, q)$ тоже является 3-схемой; легко видеть, что $\mathscr{D}(\Gamma, q)_p$ является двойственной к данной симметричной схеме.

Нода [51] доказал некоторые результаты этого раздела, исходя из иных соображений. Он показал, что если сильно регулярный граф с $c=0$ и $1<d<a$ обладает тем свойством, что ровно s вершин смежны каждой из трех попарно несмежных вершин, то $a=s(s^2+3s+1)$, $d=s(s+1)$. Из теоремы 4.5 можно вывести это заключение, исходя из более слабого предположения, именно, что ровно 0 или s вершин смежны каждой из всяких трех вершин при $d>2$. (Граф на 56 вершинах представляет собой контрпример для $d=1$.) На самом деле нам нужно лишь условие для троек, содержащих данную вершину. Позднее Нода показал, что если, кроме того, группа автоморфизмов графа Γ транзитивна на тройках попарно несмежных вершин и если s есть степень простого, то $s=1$ или 2 (и граф известен). Это условие на s было ослаблено в диссертации Камерона, но избавиться от него совсем не удалось.

Далее см. Добавление 7.

Если Γ — произвольный сильно регулярный граф, то $\mathscr{D}(\Gamma, p)$ есть 1-схема ($d > 0$) и, вообще говоря, не 2-схема (параметры: $v = a$, $b = n - a - 1$, $k = d$, $r = a - c - 1$). Предположим теперь, что $c > 0$ и $\mathscr{D}(\Gamma, p)$ — это 2-схема. Тогда две точки из $\Gamma(p)$ смежны λ точкам из $\overline{\Gamma}(p)$ независимо от того, смежны они между собой или нет; в то же время они смежны $c - \lambda - 1$ или $d - \lambda - 1$ точкам из $\Gamma(p)$ в зависимости от того, смежны ли они друг другу. Таким образом, граф $\Gamma|\Gamma(p)$ сильно регулярен.

Применяя «$a(a - c - 1) = (n - a - 1)d$» к нему, имеем с $\lambda = (a - c - 1)(d - \lambda - 1)$, откуда

$$\lambda = \frac{(a - c - 1)(d - 1)}{a - 1}.$$

Таким образом, получена

Теорема 4.7. *Пусть* Γ *— сильно регулярный граф с параметрами* (n, a, c, d), *где* $c > 0$ *и* $d > 0$. *Тогда* $\mathscr{D}(\Gamma, p)$ *образует 2-схему тогда и только тогда, когда* $\Gamma|\Gamma(p)$ *является сильно регулярным графом с параметрами*

$$\left(a,\ c,\ c - d + \frac{c(d-1)}{d-1},\ \frac{c(d-1)}{d-1}\right).$$

Пример такого графа найден Паулюсом и Зейделем. Γ имеет параметры $(26, 10, 3, 4)$; $\Gamma|\Gamma(p)$ — граф Петерсена с параметрами $(10, 3, 0, 1)$ и $\mathscr{D}(\Gamma, p)$ — это 2-$(10, 4, 2)$-схема. В действительности Паулюс нашел шесть неизоморфных графов с такими свойствами и параметрами.

5. ПОЛЯРНОСТИ СХЕМ

Пусть Γ — сильно регулярный граф, в котором $n = v$, $a = k$, $c = d = \lambda$. Тогда в нем всякие две вершины смежны в точности λ другим вершинам. Такой граф называется (v, k, λ)-графом. Симметричная 2-(v, k, λ)-схема может быть построена из такого графа следующим образом: и точки, и блоки этой схемы индексируются вершинами Γ. При этом блок и точка инцидентны тогда и только тогда, когда их индексы смежны. Такая схема обладает следующим замечательным свойством: соответствие между точками и блоками, индексированными одними и теми же вершинами,

является полярностью без абсолютных точек. Не удивительно, что существование такой полярности есть очень сильное ограничение на схему. Рациональное условие показывает, что числа

$$\frac{1}{2}\left[(v-1)\pm\frac{k}{\sqrt{k-\lambda}}\right]$$

— целые. Полагая $k-\lambda=u^2$, видим, что u делит $k=\lambda+u^2$ и, значит, u делит λ. Таким образом, существует лишь конечное число (v, k, λ)-графов с данным λ. В экстремальном случае $\lambda=u$ имеем $k=\lambda(\lambda+1)$, $v=\lambda^2(\lambda+2)$. Аренс и Секереш [1] показали существование графа с этими параметрами для всякого λ, являющегося степенью простого; их графы являются линейными графами обобщенных четырехугольников.

Наименьшими примерами являются: треугольник ($\lambda=1$), $L_2(4)$ и другой граф с теми же параметрами, охарактеризованный Шриханде [61] ($\lambda=2$), а также граф, вершинами которого служат 45 точек пересечения 27 прямых на общей кубической поверхности, смежных, если они коллинеарны ($\lambda=3$). То, что треугольник является единственным $(v, k, 1)$-графом, показывалось многократно, например, в форме теоремы Эрдеша, Реньи и Шош [25], для которой ряд элементарных доказательств (без использования рациональных условий) был получен недавно. Кроме того, Баером было показано, что полярность конечной проективной плоскости имеет абсолютные точки ([24], с. 152).

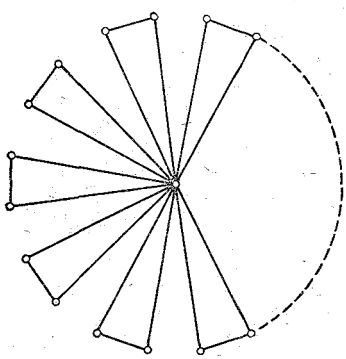

Рис. 5.1.

Граф, в котором всякие две вершины смежны λ вершинам, является либо (v, k, λ)-графом, либо одним из «ветряков» с $\lambda=1$, как на рис. 5.1.

Если симметричная 2-(v, k, λ)-схема имеет полярность σ без абсолютных точек, то можно восстановить (v, k, λ)-граф следующим образом: вершинами яв-

ляются точки этой схемы, при этом p и q смежны, если $q \in p^\sigma$ (это отношение симметрично, так как σ — инволюция и p рефлексивно, поскольку σ не имеет абсолютных точек; остальные условия следуют из свойств схемы). Итак, эти два понятия эквивалентны.

Пусть теперь Γ — сильно регулярный граф, в котором $n = v$, $a = k - 1$, $c = \lambda - 2$, $d = \lambda$. Построим некоторую инцидентностную структуру следующим образом: точки и блоки индексируются вершинами, при этом точка и блок смежны тогда и только тогда, когда их индексы либо равны, либо смежны. Такая инцидентностная структура является симметричной 2-(v, k, λ)-схемой и соответствие между точками и блоками с одинаковой пометкой есть снова полярность, но здесь уже каждая точка является абсолютной. (Такая полярность именуется нулевой.) Этот граф опять-таки может быть восстановлен из этой же схемы $\mathscr{D}$ и полярности σ. (Вершинами служат точки $\mathscr{D}$; а p и q смежны, если $q \in p^\sigma$, но $q \neq p$.) В то же время рациональное условие показывает, что числа

$$\frac{1}{2}\left[v - 1 \pm \frac{v-k}{\sqrt{k-\lambda}}\right]$$

— целые. Это не даст оценки для v в терминах λ.

Случай $\lambda = 1$ исключается, поскольку $d = \lambda - 2$ неотрицательно. Этот факт, очевидно, не характерный для конечного случая вследствие того, что абсолютная прямая в проективной плоскости имеет единственную абсолютную точку. Нулевая полярность схемы индуцирует полярность дополнительной схемы без абсолютной точки; так что в действительности оба этих случая суть одно и то же. Однако часто их удобно разделять. Ненулевые полярности привлекают меньше внимания, чем полярности без абсолютных точек. Интересным является случай с $\lambda = 2$. Здесь $d = \lambda - 2 = 0$, а графы — те же, что рассматривались в предыдущей главе, где мы видели, что $k = u^2 + 2$ для некоторого целого u, не кратного 4. Эти графы однозначно определяются их параметрами. (Для $u = 2$ это очевидно, для $u = 3$ это показал Гейвертц [26].) Таким образом, 2-(16, 6, 2)- и 2-(56, 11, 2)-схемы с нулевыми полярностями существуют и единственны. Первая из них является той самой схемой,

которая также имеет полярности без абсолютных точек! Легко проверить следующее:

Теорема 5.1. *Пусть $\mathcal{D}$ — симметричная 2-схема с $\lambda = 2$ и σ — нулевая полярность $\mathcal{D}$. Тогда*

1) *всякий блок B и всякие две точки p, $q \in B$ — $\{B^\sigma\}$, p, q и B^σ «порождают» тривиальную 2-$(4, 3, 2)$-схему;*

2) *σ однозначно определяется образом любой точки или блока;*

3) *две различные нулевые полярности коммутируют и их произведение есть свободная инволюция с фиксированной точкой;*

4) *если σ_1, σ_2, σ_3 — различные нулевые полярности, то $\sigma_1\sigma_2\sigma_3$ — полярность без абсолютных точек.*

Эта теорема следует из предыдущего замечания, что единственной нетривиальной 2-схемой с $\lambda = 2$, допускающей три различные нулевые полярности, является 2-$(16, 6, 2)$-схема, которая имеет 6 таких полярностей.

Теперь приведем несколько примеров графов со свойствами, указанными ранее.

Пусть H — матрица Адамара. Можно интерпретировать H как матрицу инцидентности (например, -1 для инцидентности и $+1$ для неинцидентности). Если H — симметричная матрица и имеет постоянную диагональ, то можно переменой знаков сделать так, чтобы первая строка и первый столбец состояли сплошь из -1; удалив их, получим матрицу инцидентности адамаровой 2-схемы с параметрами $2-(4u^2-1, 2u^2-1, u^2-1)$ и с нулевой полярностью. Если к тому же исходная матрица H имеет постоянные построчные суммы, то она (или негативная к ней, т. е. $-H$) является матрицей инцидентности 2-схемы с параметрами $2-(4u^2, 2u^2 \pm u, u^2 \pm u)$ и с нулевой полярностью; знак $+$ или $-$ выбирается в зависимости от совпадения или несовпадения знаков диагональной и построчной сумм. Такие адамаровы матрицы встречаются достаточно часто. Таким образом, эти схемы существуют при каждой возможной комбинации знаков, если существуют адамаровы матрицы порядка $2u$. Существуют они и для других порядков, таких как 36 (см. [29] и [16]).

Иные примеры нулевых полярностей дают симплектические полярности проективного $(2m-1)$-про-

странства над полем $GF(q)$ при $m \geqslant 2$. Так, если σ — ортогональная полярность проективного $2m$-пространства над $GF(q)$ при $m \geqslant 2$ и нечетном q, то абсолютные точки и гиперплоскости образуют симметричную схему, а σ индуцирует нулевую полярность этой схемы. Эта схема имеет те же параметры, что и $PG(2m-1, q)$, но не изоморфна ей.

Примеры с $q = 3$ получаются следующим образом. Пусть θ — квадратичная форма, связанная с σ. Поскольку $\theta(x) = \theta(-x)$, θ индуцирует функцию из множества проективных точек в $GF(3)$; обозначим эту функцию также через θ. Если p_i — множество тех точек, на которых θ принимает значение i ($i = \pm 1$), то (p_i, p_i^{σ}) образует симметричную схему, а σ индуцирует ее полярность без абсолютных точек. Параметры этой схемы суть

$$2 - \left(\tfrac{1}{2}3^m(3^m + i),\ \tfrac{1}{2}3^{m-1}(3^m - i),\ \tfrac{1}{2}3^{m-1}(3^{m-1} - i)\right),$$
$$i = \pm 1,$$

при условии, что знак θ выбран корректно.

Так же, как существуют «свободные» симметричные схемы с произвольным значением λ (и даже много более общие инцидентностные структуры), существуют и «свободные» графы, в которых число вершин, смежных p и q, равно c или d, в зависимости от того, смежны вершины p и q или нет (c и d — предписанные неотрицательные целые с $d > 1$). В действительности эта конструкция даже еще проще; вершины и ребра добавляются при каждом шаге. В частности, имеются свободные симметричные схемы с полярностями без абсолютных точек, произвольным λ и свободные симметричные схемы с нулевыми полярностями и произвольным $\lambda > 1$. При рассмотрении случая нулевой полярности с $\lambda = 2$ (т. е. $c = 0, d = 2$) имеем схему, в которой выполняется бесконечно много примеров «инцидентностной теоремы» (см. теорему 5.1, 1)).

6. РАСШИРЕНИЕ ГРАФОВ

В этой главе графы рассматриваются с несколько иной точки зрения — как инцидентностные структуры (см. главу 2). В частности, регулярный граф есть 1-схема с $k = 2$, и обратно (при условии, что кратные

блоки запрещены). Интересно следующее: когда такие 1-схемы обладают расширениями? Поскольку 2-схемы с $k = 3$ встречаются часто, то эта проблема достаточно широка и мы будем обычно налагать дополнительные условия на расширение. Расширения схем были первоначально использованы Виттом, Хьюзом и Дембовским при изучении транзитивных расширений групп перестановок и можно было ожидать, что расширения регулярных графов могли бы быть полезны в изучении дважды транзитивных групп.

Если мы расширяем схему добавлением новой точки p, то мы знаем все блоки расширения, содержащие p, — они получаются добавлением p к старым блокам, но для блоков, не содержащих p, возникает неоднозначность. Предположим тогда, как первую возможность, что имеется множество троек Δ, называемых блоками, в которой блоки, не содержащие точки p, однозначно определяются естественным образом из блоков, содержащих p; в частности, предположим, что когда известно, какие из троек $\{p, q, r\}$, $\{p, q, s\}$ и $\{p, r, s\}$ являются блоками, то можно легко определить, является ли $\{q, r, s\}$ блоком. Легко видеть, что это правило должно состоять в том, что для данного 4-множества $\{p, q, r, s\}$ число его 3-подмножеств, являющихся блоками, принадлежит подмножеству S из $\{0, 1, 2, 3, 4\}$ с тем свойством, что $i, j \in S$, $i \neq j \Rightarrow |i - j| \geqslant 2$. Дальнейший анализ показывает, что S есть подмножество одного из множеств $\{0, 2, 4\}$, $\{1, 4\}$ или $\{0, 3\}$ и что во втором или в третьем случаях либо Δ, либо его дополнение есть множество всех троек, содержащих данную точку, что неинтересно.

Множество троек Δ с тем свойством, что четное число 3-подмножеств всякого 4-множества принадлежит Δ, мы называем *два-графом* Хигмана, который первый изучал такие множества. Два-графа оказываются примечательными объектами, тесно связанными с теорией графов, конечной геометрией, обычной геометрией (множествами равноугольных прямых в евклидовом пространстве) и т. д. К тому же большое число известных конечных дважды транзитивных групп действует на два-графах. (Включая $PSL(2, q)$ для $q \equiv 1 \pmod 4$, $PSU(3, q)$ для нечетного q, ${}^2G_2(q)$, $\mathrm{Sp}(2n, 2)$ в обоих дважды транзитивных представлениях $V_{2^{2n}}\,\mathrm{Sp}(2n, 2)$, HS и 3). Два-графы интенсивно

изучались Тейлором, Зейделем и многими другими. Зейдель [59] представил обзор по ним на недавней конференции в Риме, так что здесь мы опишем их весьма бегло.

Очевидно два-граф можно рассматривать как отображение троек на множестве в $\mathbf{Z}_2$ с исчезающей кограницей, т. е. с 2-коциклом. Поскольку полностью подходящая когомология тривиальна, то это, таким образом, есть кограница 1-коцепи, а последнее, будучи функцией пар в $\mathbf{Z}_2$, являет собой граф; тройки два-графа являются носителями нечетного числа ребер этого графа. Две 1-коцепи имеют одну и ту же кограницу тогда и только тогда, когда они отличаются на 1-коцикл, то есть кограницу 0-коцепи (функцию из точечного множества в $\mathbf{Z}_2$); это означает существование разбиения точечного множества $X \cup Y$ и двух графов, согласованных внутри X и внутри Y и являющихся дополнительными между этими множествами. В терминологии Зейделя эти графы являются связанными по *переключению* относительно разбиения $X \cup Y$. Таким образом, два-граф эквивалентен «переключательному классу» графов. Зейдель использует $(0, -, +)$-матрицу смежности для графов (0 на диагонали, -1 — смежность, $+1$ — несмежность). Матрицы смежности A, A' переключательно эквивалентных графов связаны равенством $A' = DAD$, где D — диагональная матрица с диагональными элементами ± 1. Пустой два-граф соответствует переключательному классу полных двудольных графов, а полный два-граф — двум полным графам. Эти случаи исключаются из дальнейшего рассмотрения.

Если Δ есть некоторое множество троек на P, а p — точка из P, то через $\Delta(p)$ обозначаем граф с вершинами $P - \{p\}$ и ребрами $\{\{q, r\} \mid \{p, q, r\} \in \Delta\}$. Легко видеть, что если Δ является два-графом, то переключательный класс, соответствующий Δ, содержит непересекающееся объединение изолированной вершины p и $\Delta(p)$. (Возьмем любой граф в этом классе и переключим относительно соседей p.) Предположим, что $\Delta(p)$ регулярен. Граф $\Delta(p)$ определяет Δ однозначно; когда Δ является расширением $\Delta(p)$ в смысле схемы, т. е. когда Δ является 2-схемой? Два-граф, являющийся также и 2-схемой, называется *регулярным два-графом*. Ответ дает

Как кажется, если предположить, что только Δ (но не его дополнение) удовлетворят (*), то методы, используемые для два-графов, перестают работать; но структура Δ достаточно ограничена, чтобы некоторый прогресс был возможен. Полезной является

Лемма 6.4. *Пусть* Γ *— граф на* $v-1$ *вершинах, в котором наибольшие полные подграфы (клики) имеют объем* $k-1$ *всякая вершина находится в* λ *из них, и всякое ребро лежит, по крайней мере, в одном из них. Предположим, что* Δ *есть множество троек, удовлетворяющих* (*), *с* $\Delta(p) \cong \Gamma$ *для любой точки* p. *Тогда существует* 2-(v, k, λ)-*схема* D *такая, что* Δ *есть множество троек из некоторого блока схемы* D.

Блоки являются множествами S с $|S| = k$, тройки которых принадлежат Δ; это есть множества S, для которых $|S| - \{p\}$ есть $(k-1)$-клика в $\Delta(p)$ для некоторого (и следовательно, каждого) $p \in S$. Очевидно, что две точки лежат в λ таких блоков, и тройка находится в блоке тогда и только тогда, когда она есть в Δ. Будем говорить, что эта схема представляет множество троек. Заметим, что Γ удовлетворяет предположению из леммы 6.4, если он допускает вершинно- и реберно-транзитивную группу автоморфизмов. Для некоторых приложений полезна следующая

Теорема 6.5. *Предположим, что* Γ *— граф и* Δ *— множество троек, удовлетворяющее* (*) *с* $\Delta(p) \cong \Gamma$ *для любой точки* p.

1) *Если* Γ *есть непересекающееся объединение полных графов на* $k-1$ *вершинах, то* 2-$(v, k, 1)$-*схема представляет* Δ *и наоборот.*

2) *Если* Γ *есть трангуляционный граф* $T(k)$, *то* Δ *представляется симметричной* 2-$(v, k, 2)$-*схемой, удовлетворяющей следующей аксиоме: если* B *— блок и* $p, q, r \in B$, *то «вторичные блоки»* pq, qr *и* rp *— совпадают. (Таким образом,* p, q, r *порождают* 2-$(4, 3, 2)$-*схему.) Верно и обратное.*

3) *Если* Γ *— решетчатый граф* $L_2(m)$, *то* $m = 3$ *и* Δ *есть единственный регулярный 2-граф на 10 точках.*

Доказательство. Доказать 1) очень просто. В случае 2) заметим, что при $k > 4$ трангуляционный граф $T(k)$ имеет два вида клик, а именно: $\{\{12\}, \{13\}, \ldots, \{1k\}\}$ и $\{\{12\}, \{13\}, \{23\}\}$. Первое расширяется до блоков, второе указывает множество 2-$(4, 3, 2)$-схем. (Случай $k = 4$ можно рассмотреть

вручную. В случае 3) имеем $v = m^2 + 1$, $k = m + 1$, $\lambda = 2$; так что $r = 2m$, $b = \frac{2m(m^2+1)}{m+1}$, где $m = 3$, а однозначность устанавливается легко.

Единственная известная схема с $k > 3$, удовлетворяющая аксиоме (2) из теоремы 6.5, — это 2-(16, 6, 2)-схема, которую мы уже встречали в предыдущем разделе; для этой схемы Δ является регулярным двуграфом. Полная характеризация этой схемы посредством этой аксиомы представляется трудной задачей; отметим более слабую характеризацию. Обозначим на время эту схему через $\mathscr{D}_{16}$.

Теорема 6.6. *Если $\mathscr{D}$ — симметричная 2-$(v, k, 2)$-схема, а блок B из $\mathscr{D}$ таков, что всякие четыре точки из B порождают $\mathscr{D}_{16}$, то $\mathscr{D} \cong \mathscr{D}_{16}$.*

В качестве следствия это влечет результат о транзитивных расширениях, тесно связанных с расширениями треугольных графов:

Теорема 6.7. *Пусть H — группа перестановок степени k, индуцирующая группу автоморфизмов ранга 3 графа $T(k)$, а G — транзитивное расширение этой группы ранга 3. Тогда выполняется одно из следующих утверждений:*

1) $k = 4$, $H \cong S_4$, $G \cong PSI(2, 7)$;

2) $k = 5$, $H \cong A_5$, $G \cong PSL(2, 11)$;

3) $k = 6$, $H \cong A_6$ *или* S_6, $G \cong V_{16}.A_6$ *или* $V_{16}.S_6$.

В каждом случае группа G действует на симметричной 2-$(v, k, 2)$-схеме.

Теорему 6.8 *см. в Добавлении* 8. *Далее следует глава* 8* (*см. Добавление* 9).

7. КОДЫ

В теории кодирования рассматривается множество F из q различных символов, называемых *алфавитом*. Обыкновенно, $q = 2$ и $F = \{0, 1\}$; в более общей теории $q = p^r$ (p — простое) и $F = GF(q)$.

Используя символы множества F, образуем из них все возможные n-векторы, т. е. множество F^n; будем называть эти n-векторы *словами*, а число n — *длиной слова*. Если в этом случае $F = GF(q)$, то множество всех слов будем обозначать через $\mathscr{R}^{(n)}$ и интерпретировать это множество как n-мерное векторное пространство над $GF(q)$.

В $\mathcal{R}^{(n)}$ введем функцию расстояний d, называемую *расстоянием* (*метрикой Хэмминга*), которая естественным образом характеризует число ошибок в слове, т. е. число неправильных букв.

Определение 7.1. Для $x \in \mathcal{R}^{(n)}$ и $y \in \mathcal{R}^{(n)}$ через $d(x, y)$ обозначаем число различных координат в словах x и y.

Следующие два определения непосредственно связаны с d и с языком метрических пространств.

Определение 7.2. Для $x \in \mathcal{R}^{(n)}$ определяем *вес* слова x как величину $w(x) = d(x, 0)$. (Как обычно, 0 обозначает нулевой вектор в $\mathcal{R}^{(n)}$.)

Определение 7.3. Для $\rho > 0$ и $x \in \mathcal{R}^{(n)}$ *шар* радиуса ρ с центром в x определяем как множество

$$S(x, \rho) = \{y \in \mathcal{R}^{(n)} \mid d(x, y) \leqslant \rho\}.$$

Рассмотрим подмножество C множества $\mathcal{R}^{(n)}$, обладающее тем свойством, что расстояние между любыми двумя различными словами из C не менее чем $2e + 1$. Если взять произвольное слово x из C и изменить t его координат, где $t \leqslant e$ (т. е. внести t *ошибок*), то полученное слово, тем не менее, ближе к исходному, нежели любое другое из множества C (т. е. оно имеет меньшее расстояние до x, чем другие слова из C). Стало быть, если мы знаем C, то мы можем исправить t ошибок. Цель теории кодирования и состоит в изучении таких «e-кодов, исправляющих ошибки». Мы же по преимуществу будем интересоваться связями кодов с комбинаторными схемами.

Определение 7.4. *e-код, исправляющий ошибки, есть подмножество C множества $\mathcal{R}^{(n)}$*, обладающее свойством:

$$\forall x \in C \; \forall y \in C \quad [x \neq y \Rightarrow d(x, y) \geqslant 2e + 1],$$

т.е.

$$\forall x \in C \quad \forall y \in C \quad [x \neq y \Rightarrow S(x, e) \cap S(y, e) = \varnothing].$$

Один специальный вид кода, который не столь важен практически, но весьма интересен комбинаторикам и алгебраистам, представляет собой совершенный код.

Определение 7.5. e-код, исправляющий ошибки, $C \subset \mathcal{R}^{(n)}$, называется *совершенным*, если

$$\bigcup_{x \in C} S(x, e) = \mathcal{R}^{(n)},$$

Одним из многих интересных типов кодов является линейный код.

Определение 7.6. Всякое k-мерное линейное подпространство C пространства $\mathscr{R}^{(n)}$ называется *линейным кодом*, или иначе, — *(n, k)-кодом над $GF(q)$*.

Емкость кода, т. е. способность исправлять ошибки *), определяется *наименьшим расстоянием* между парами всех различных слов. Для произвольного кода, содержащего K кодовых слов, чтобы найти это минимальное расстояние, надо выполнить $\binom{K}{2}$ сравнений. Преимущество линейных кодов состоит в том, что они позволяют сократить число сравнений.

Теорема 7.7. *В линейном коде наименьшее расстояние равно наименьшему весу среди всех ненулевых кодов слов.*

Доказательство. Если $x \in C$, $y \in C$, то $x - y \in C$ и, значит, $d(x, y) = d(x - y, 0) = w(x - y)$.

Рассмотрим теперь два способа описания линейного кода C. Первый задается *порождающей матрицей* G, строки которой — множество базисных векторов линейного подпространства C. Поскольку нас, прежде всего, интересует свойство исправления ошибок, и свойство это не изменяется, если во всех кодовых словах переставить два символа (например, первую и вторую буквы каждого кодового слова), мы будем называть два кода *эквивалентными*, если один можно получить применением фиксированной перестановки символов слов другого кода. Учитывая это, видим, что для каждого линейного кода есть эквивалентный код, обладающий порождающей матрицей вида

$$G = (I_k P), \tag{7.8}$$

где I_k есть $k \times k$-единичная матрица, а P есть $k \times (n - k)$-матрица. Мы называем матрицу (7.8) *стандартной формой* порождающей матрицы G. Код C называется *систематическим*, если существует k-подмножество координатных мест такое, что каждой возможной k-энке элементов на этих k местах соответствует ровно одно кодовое слово. Заметим, что согласно (7.8) всякий (n, k)-код является систематическим.

*) Корректирующая способность.

Перейдем к иному описанию линейного кода C.

Определение 7.9. Если C — линейный код размерности k, то множество

$$C^{\perp} = \{x \in \mathscr{R}^{(n)} \mid \forall y \in C \quad [(x, y) = 0]\},$$

где (x, y) обозначает скалярное произведение, называется *двойственным кодом* кода C.

Код $C^{\perp}$ является $(n, n-k)$-кодом. Если H — порождающая матрица для $C^{\perp}$, то H называется *проверочной матрицей* (*матрицей проверки на четность*) кода C. Вообще, проверку на четность кода C обеспечивает вектор x, который ортогонален всем кодовым словам кода C, и мы будем всякую матрицу H называть проверочной (на четность), если строки H порождают подпространство $C^{\perp}$. Следовательно, код C определяется такой проверочной матрицей H:

$$C = \{x \in \mathscr{R}^{(n)} \mid xH^T = 0\}. \tag{7.10}$$

Замечание. Часто коды C, C^* называют *двойственными*, если C^* эквивалентен $C^{\perp}$. Это подчас приводит к недоразумениям, но имеет, однако, и свои преимущества.

Опишем один важный пример линейных кодов. Рассмотрим в $AG(m, q)$ прямые, проходящие через начало координат, и вдоль каждой из них выберем вектор x_i, $i = 1, 2, \ldots, n = (q^m - 1)/(q - 1)$. Образуем матрицу H (m строк, n столбцов) из x_i как вектор-столбцов. Поскольку в H нет двух линейно зависимых столбцов, видим, что H является проверочной матрицей кода C, в котором каждое ненулевое слово x имеет все $w(x) \geqslant 3$ (см. (7.10)). Очевидно, этот код имеет размерность $n - m$. Он называется $(n, n-m)$-*кодом Хемминга* над $GF(q)$. Предыдущее замечание показывает, что это есть 1-код, исправляющий ошибки.

Теорема 7.11. *Коды Хэмминга являются совершенными.*

Доказательство. Пусть C есть $(n, n-m)$-код Хэмминга над $GF(q)$. Тогда $n = \frac{q^m - 1}{q - 1}$. Если $x \in C$, то

$$|S(x, 1)| = 1 + n(q - 1) = q^m.$$

Поскольку $|C| = q^{n-m}$ и C является 1-кодом, исправляющим ошибки, находим, что

$$\left| \bigcup_{x \in C} S(x, 1) \right| = q^n,$$

т. е. C — совершенный код.

Пусть C — некоторый (n, k)-код. К каждому слову $(c_1, c_2, \ldots, c_n)$ из C добавим новую букву c_0 (например, спереди) такую, что $c_0 + c_1 + \ldots + c_n = 0$. Этот процесс называется *общей проверкой* (*на четность*). Таким способом получаем новый линейный код $\bar{C}$, который называется *расширенным кодом*, соответствующим C. Если H — проверочная матрица C, то

$$\bar{H} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & & & & \\ 0 & & & & \\ \cdot & & & & \\ \cdot & & H & & \\ \cdot & & & & \\ 0 & & & & \end{bmatrix}$$

— проверочная матрица для $\bar{C}$. Конечно, если вектор, сплошь состоящий из единиц (обозначаемый через $\mathbf{1}$), является проверочным вектором для H, то расширение тривиально, поскольку тогда $c_0 = 0$ для всех слов из C. Однако, если C — бинарный код с нечетным минимальным расстоянием d, то максимальное расстояние $\bar{C}$ равно $d + 1$.

В качестве первого примера связи кодов и схем рассмотрим *расширенный* $(8, 4)$*-бинарный код Хэмминга*. Как мы уже знаем, матрица

$$\bar{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

является проверочной матрицей этого кода. Легко видеть, что этот код эквивалентен коду с порождающей матрицей $G = (I_4 J_4 - I_4)$. В списке из 16 слов этого кода имеются 0, 1 и 14 слов веса 4. Поскольку два слова веса 4 имеют расстояние $\geqslant 4$, они имеют не более двух общих единиц. Отсюда следует, что нет слова веса 3, являющегося «подсловом» более чем

одного кодового слова. Имеется $\binom{8}{3} = 56$ слов веса 3 и каждое кодовое слово веса 4 имеет четыре подслова веса 3. Таким образом, получена

Теорема 7.12. *14 слов веса 4 в расширенном* $(8, 4)$*-бинарном коде Хэмминга образуют 3-схему с параметрами* $v = 8$, $k = 4$, $\lambda = 1$.

Читателю в качестве упражнения предлагается проверить, что эта схема является расширением схемы $PG(2, 2)$, т. е. схемы $AG(3,2)$.

Все это, в частности, показывает, насколько полезно знать количество слов фиксированного веса в коде. Простой способ описания такой информации дает

Определение 7.13. Пусть C — код длины n и пусть A_i, $i = 0, 1, \ldots, n$, — число кодовых слов веса i. Тогда

$$A(\xi, \eta) = \sum_{i=0}^{n} A_i \xi^i \eta^{n-i}$$

называется *весовым энумератором* кода C.

Весовые энумераторы кодов C и $C^\perp$ связаны между собой; следующее описание этой связи принадлежит МакВильямс.

Теорема 7.14. *Пусть* $A(\xi, \eta)$ — *весовой энумератор некоторого* (n, k)*-кода над* $GF(q)$ *и* $A^\perp(\xi, \eta)$ — *весовой энумератор двойственного кода* $C^\perp$. *Тогда*

$$A^\perp(\xi, \eta) = q^{-k} A(\eta - \xi, \eta + (q-1)\xi).$$

Доказательство 7.14 основано на следующей лемме. (Далее пишем $\mathcal{R}$ вместо $\mathcal{R}^{(n)}$.)

Лемма 7.15. *Пусть* χ — *нетривиальный характер на группе* $(GF(q), +)$ *и для всякого* $v \in \mathcal{R}$ *определено* χ_v: $\mathcal{R} \to C^*$ *по правилу*:

$$\forall u \in \mathcal{R} \left[\chi_v(u) = \chi((u, v))\right].$$

Если A — *векторное пространство над* C, f: $\mathcal{R} \to A$ *и если* g: $\mathcal{R} \to A$ *определяется по правилу*:

$$\forall u \in \mathcal{R} \left[g(u) = \sum_{v \in \mathcal{R}} f(v) \chi_v(u)\right],$$

то для всякого линейного подпространства $V \subset \mathcal{R}$ *и двойственного подпространства* $V^\perp$ *выполняется*

равенство

$$\sum_{u \in V} g(u) = |V| \sum_{v \in V^{\perp}} f(v).$$

Доказательство.

$$\sum_{\in V} g(u) = \sum_{u \in V} \sum_{v \in \mathcal{R}} f(v) \chi_v(u) =$$

$$= \sum_{v \in \mathcal{R}} f(v) \sum_{u \in V} \chi((u, v)) =$$

$$= |V| \sum_{v \in V^{\perp}} f(v) + \sum_{v \notin V^{\perp}} f(v) \sum_{u \in V} \chi((u, v)).$$

Во внутренней сумме второго слагаемого величина (u, v) принимает каждое значение поля $GF(q)$ одинаковое число раз, поскольку

$$\sum_{\alpha \in GF(q)} \chi(\alpha) = 0$$

для каждого нетривиального характера; это и доказывает лемму.

Доказательство теоремы 7.14. Пусть в лемме 7.15 A — пространство всех полиномов от двух переменных ξ, η с коэффициентами в C и пусть $f(v) = \xi^{w(v)}\eta^{n-w(v)}$. Если $a \in GF(q)$, пишем $w(a) = 1$; если $a \neq 0$, то $w(0) = 0$. Тогда имеем

$$g(u) = \sum_{v_1 \in GF(q)} \cdots \sum_{v_n \in GF(q)} \xi^{w(v_1) + \cdots + w(v_n)} \times$$

$$\times \eta^{(1-w(v_1)) + \cdots + (1-w(v_n))} \chi(u_1 v_1 + \ldots + u_n v_n) =$$

$$= \prod_{i=1}^{n} \left\{ \sum_{v \in GF(q)} \xi^{w(v)} \eta^{1-w(v)} \chi(u_i v) \right\}.$$

Поскольку внутренняя сумма есть $\eta + (q-1)\xi$, если $u_i = 0$, и

$$\eta + \xi \left(\sum_{\alpha \in GF(q) \setminus \{0\}} \chi(\alpha) \right) = \eta - \xi,$$

если $u_i \neq 0$, то

$$g(u) = (n + (q-1)\xi)^{n-w(u)} (\eta - \xi)^{w(u)}.$$

Теперь, согласно лемме 7.15, имеем (полагая $V = C$):

$$\sum_{v \in C^\perp} f(v) = A^\perp(\xi, \eta) = q^{-k} \sum_{u \in C} g(u) =$$

$$= q^{-k} A(\eta - \xi, \eta + (q-1)\xi).$$

В главе 11 мы покажем, какую роль играет это уравнение в исследованиях по существованию проективной плоскости порядка 10.

Ради полноты отметим, что известны обобщения теоремы 7.14 и на нелинейные коды (см. [21, 47]).

Далее см. Добавление 10.

8. ЦИКЛИЧЕСКИЕ КОДЫ

Многие интересные и известные коды оказываются циклическими. Определим их следующим образом:

Определение 8.1. (n, k)-код C над $GF(q)$ называется *циклическим*, если

$$\forall (c_0, c_1, \ldots, c_{n-1}) \in C \qquad [(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C].$$

Примем ограничение $(n, q) = 1$. Пусть R — кольцо всех многочленов с коэффициентами из $GF(q)$ и пусть S — идеал, порожденный $x^n - 1$. Ясно, что кольцо классов вычетов $R \bmod S$ (рассматриваемое как аддитивная группа) изоморфно $R^{(n)}$. Изоморфизм задается соответствием

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 x + \ldots + a_{n-1} x^{n-1},$$

поскольку очевидно, что многочлены степени $< n$ образуют множество представителей для $R \bmod S$. Далее мы не делаем различия между *словами* и *многочленами* степени $< n (\bmod x^n - 1)$. Заметим, что домножение на x в $R \bmod S$ равносильно циклическому сдвигу

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto (a_{n-1}, a_0, a_1, \ldots, a_{n-2}).$$

Отсюда следует, что циклический код C соответствует *идеалу* (который мы также обозначаем через C) в $R \bmod S$. Каждый идеал в $R \bmod S$ (т. е. каждый циклический код в $R^{(n)}$) порождается многочленом $g(x)$, который делит $x^n - 1$. Будем называть $g(x)$ *порождающим* многочленом циклического кода.

Пусть $g(x) = g_0 + g_1 x + \ldots + g_{n-d}x^{n-d}$ — порождающий многочлен циклического кода C и пусть

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1 x + \ldots + h_d x^d.$$

Слова $g(x)$, $xg(x)$, ..., $x^{d-1}g(x)$ образуют базис кода C, т. е. матрица

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-d} & 0 & 0 \ldots 0 \\ 0 & g_0 & g_1 & & & g_{n-d} & 0 \ldots 0 \\ \cdot & 0 & \cdot & \cdot & & & \cdot \\ \cdot & & \cdot & \cdot & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & & & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & g_0 & g_1 \ldots g_{n-d} \end{bmatrix} \tag{8.2}$$

является порождающей матрицей для C. Поскольку $g(x)h(x) = 0$ в кольце $R \bmod S$, матрица

$$H = \begin{bmatrix} 0 & 0 \ldots 0 & h_d & h_{d-1} & \cdots & h_1 & h_0 \\ \cdot & \cdot h_d & & & & h_0 & 0 \\ \cdot & \cdot \cdot & & & & \cdot & \cdot \cdot \\ \cdot & \cdot \cdot & & & & \cdot \cdot & \cdot \\ 0 & \cdot & & & & \cdot \cdot & \cdot \\ h_d & \ldots & & h_0 & 0 & \ldots & 0 \end{bmatrix} \tag{8.3}$$

является проверочной матрицей для C. Это позволяет перейти к терминологии главы 7 и называть $h(x)$ *проверочным многочленом* циклического кода C. Заметим, что *размерность* циклического кода совпадает со степенью проверочного многочлена. Код, порожденный многочленом $h(x)$, есть код, двойственный C, *но с символами, расположенными в обратном порядке* (см. замечание после формулы (7.10)).

Весьма часто циклические коды задают не порождающим многочленом $g(x)$, а заданием некоторых корней всем кодовым словам (в расширении поля $GF(q)$). Ясно, что такое задание кода равносильно явному заданию многочленами, потому что условие, что все кодовые слова кратны $g(x)$, означает, что они являются 0 в нулях $g(x)$. Для демонстрации такого задания кодов приведем один пример.

Пусть $q = 2$, $n = 2^m - 1$ и пусть d — *примитивный элемент* поля $GF(2^m)$. Пусть $m_1(x) = (x - \alpha)(x -$

$-\alpha^2)\ \ldots\ (x-\alpha^{2^{m-1}})$ — минимальный многочлен от α. Рассмотрим циклический код, порожденный $m_1(x)$. Каждый элемент из $GF(2^m)$ может быть единственным образом представлен в виде $\sum_{i=0}^{m-1} \varepsilon_i \alpha^i$, где $\varepsilon_i \in GF(2)$. Ненулевые элементы из $GF(2^m)$ являются степенями α^j $(j=0, 1, \ldots, 2^m-2)$. Построим матрицу H, для которой j-й столбец есть $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1})^T$, если $\alpha^j = \sum_{i=0}^{m-1} \varepsilon_i \alpha^i$ $(j=0, 1, \ldots, 2^m-2)$. Если

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

то вектор $\boldsymbol{a}H^T$ соответствует элементу $a(\alpha)$ поля $GF(q)$. Следовательно, $\boldsymbol{a}H^T = 0$ означает то же, что $m_1(x) \mid a(x)$. Поскольку столбцы матрицы H являются перестановкой бинарных представлений для 1, 2, ..., 2^m-1, получена следующая

Теорема 8.4. *Бинарный циклический код длины $n=2^m-1$, для которого порождающим многочленом служит минимальный многочлен примитивного элемента поля $GF(2^m)$, эквивалентен $(n, n-m)$-бинарному коду Хэмминга.*

Пример. Положим $q=2$, $n=7$, $g(x)=1+x+x^2$. В этом случае циклический код C, порожденный $g(x)$, имеет размерность 4. Он эквивалентен $(7,4)$-коду Хэмминга, который соответствует примеру после теоремы 7.11. Отметим, что 7 циклических сдвигов первой строки матрицы (8.2) для этого примера образуют матрицу инцидентности схемы $PG(2,2)$. Этот код состоит из этих 7 слов, 0 и 8 слов, получаемых переменой 0 и 1. Этот пример имеет отношение к одному интересному вопросу, связывающему теорию схем с теорией кодирования. Предположим, что задана Штейнерова система троек S (подобно, например, схеме $PG(2,2)$ в нашем примере). Существует ли линейный код C над некоторым полем $GF(q)$ такой, что в каждом кодовом слове веса 3 ненулевые позиции образуют блок из S, и все блоки из S представимы в этой форме (ср. [3])? *Далее см. Добавление* 11.

При выводе теоремы 8.4 мы показали, что условие: α — нуль для всех кодовых слов, — соответствует за-

данию проверочной матрицы $H = (1\ \alpha\ \alpha^2\ \ldots\ \alpha^{n-1})$, где α^j следует интерпретировать как $(\varepsilon_0\ \varepsilon_1\ \ldots\ \varepsilon_{m-1})$, если $\alpha^j = \sum_{i=0}^{n-1} \varepsilon_i \alpha^i$.

Второй полезный пример получается заменой $m_1(x)$ на $(x+1)m_1(x)$. Ясно, что новый код является подкодом кода Хэмминга. То, что 1 является нулем всех кодовых слов, означает, что все они имеют четный вес, т. е. получается $(n, n-m-1)$-код, состоящий из всех слов четного веса в $(n, n-m)$-коде Хэмминга. В терминах проверочных матриц можно сказать, что добавляется строка из единиц.

Введем сейчас очень важный класс кодов, известных под названием БЧХ-кодов. Коды эти были открыты Боузом, Рай-Чаудхури и Хокуенхемом. Пусть β — примитивный n-корень единицы в $GF(q^m)$.

Определение 8.5. Циклический код в $\mathscr{R}^{(n)}$, состоящий из всех слов, которые имеют $\beta, \beta^2, \ldots, \beta^{d-1}$ в качестве нулей, называется *БЧХ-кодом конструктивного расстояния d*. Если β — примитивный элемент поля $GF(q^m)$, $n = q^m - 1$, то код называется *примитивным*.

Порождающий многочлен $g(x)$ кода, введенного определением 8.5, представляет собой произведение максимальных многочленов $m_1(x)$ от β^i, где $i = 1, 2, \ldots, d-1$, с тем условием, что нет сомножителя, взятого более чем однократно.

Основанием для использования термина «конструктивное расстояние» может служить

Теорема 8.6. *Наименьшее расстояние БЧХ-кода конструктивного расстояния d есть по крайней мере d.*

Доказательство. Используя сокращения, принятые ранее, введем $m(d-1) \times n$-матрицу H над $GF(q)$ вида

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \ldots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \ldots & \beta^{2n-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \beta^{d-1} & \beta^{2(d-1)} & \ldots & \beta^{(n-1)(d-1)} \end{bmatrix}.$$

Слово c принадлежит БЧХ-коду тогда и только тогда, когда $cH^T = 0$. Если бы c имело вес $< d$, то в H нашлось бы $d-1$ столбцов, линейно зависимых над $GF(q)$. Детерминант матрицы, составленной из этих

столбцов, обозначаемых через $\xi_1 = \beta^{i_1}$, $\xi_2 = \beta^{i_2}$, ..., $\xi_{d-1} = \beta^{i_{d-1}}$, равен

$$\begin{vmatrix} \xi_1 & \xi_2 & \dots & \xi_{d-1} \\ \xi_1^2 & \xi_2^2 & \dots & \xi_{d-1}^2 \\ \dots & \dots & \dots & \dots \\ \xi_1^{d-1} & \xi_2^{d-1} & \dots & \xi_{d-1}^{d-1} \end{vmatrix} = \xi_1 \xi_2 \dots \xi_{d-1} \prod_{i>j} (\xi_i - \xi_j) \neq 0.$$

Это показывает, что все кодовые слова $c \neq 0$ действительно имеют вес $\geqslant d$.

Замечание. Если в определении 8.5 не требовать, чтобы и 1 являлась нулем всех кодовых слов, то полученный код имеет наименьшее расстояние по крайней мере $d+1$. Доказательство то же, что и ранее.

Посмотрим теперь на БЧХ-коды с точки зрения теории групп. Рассмотрим примитивный БЧХ-код длины $n = q^m - 1$ над $GF(q)$ с нулями $\alpha, \alpha^2, \dots, \alpha^{d-1}$ (где α — примитивный элемент в $GF(q^m)$). Обозначим *позиции* символов в кодовых словах через X_i, $i = 0, 1, \dots, n-1$, где $X_i = \alpha^i$. Расширим этот код добавлением полной проверки на четность. Обозначим добавочную позицию через X_∞ и примем, что

$$1^\infty = 1, \quad (\alpha^i)^\infty = 0 \text{ для } i \not\equiv 0 \pmod{n}.$$

Представим кодовые слова в виде $c_0 + c_1 x + \dots + c_{n-1} x^{n-1} + c_\infty x^\infty$. Покажем теперь, что расширенный код инвариантен относительно перестановок *аффинной группы перестановок* на $GF(q^m)$, применяемой к позициям кода. Эта группа состоит из перестановок

$$P_{u,v}(X) = uX + v$$
$$(u \in GF(q^m), \quad v \in GF(q^m), \quad u \neq 0)$$

и является дважды транзитивной группой. Прежде всего заметим, что перестановка $P_{\alpha,0}$ является циклическим сдвигом на позициях $X_0, X_1, \dots, X_{n-1}$ и что эта перестановка составляет X_∞ инвариантным. Следовательно, $P_{\alpha,0}$ переводит каждый расширенный циклический код в себя. Пусть теперь $(c_0, c_1, \dots, c_\infty)$ — некоторое кодовое слово в расширенном БЧХ-коде и пусть $P_{u,v}$ дает $(c'_0, c'_1, \dots, c'_\infty)$. Тогда для $k = 0$,

1, ..., $d-1$ имеем

$$\sum_i c_i' a^{ik} = \sum_i c_i (ua^i + v)^k = \sum_i c_i \sum_{l=0}^{k} \binom{k}{l} u^l a^{il} v^{k-l} =$$

$$= \sum_{l=0}^{k} \binom{k}{l} u^l v^{k-l} \sum_i c_i (a^l)^i = 0,$$

поскольку внутренняя сумма равна 0 для $l = 0, 1, \ldots$ ..., $d-1$; следовательно, представленное слово также лежит в расширенном слове. Тем самым получена

Теорема 8.7. *Каждый расширенный примитивный БЧХ-код длины $n+1 = q^m$ над $GF(q)$ инвариантен относительно аффинной группы перестановок на $GF(q^m)$.*

В качестве приложения рассмотрим примитивный бинарный БЧХ-код C длины n. Пусть $\sum_{i=0}^{n} a_i \xi^i \eta^{n-i}$ — весовой энумератор кода C, а $\sum_{i=0}^{n+1} A_i \xi^i \eta^{n+1-i}$ — весовой энумератор кода $\bar{C}$. Имеем $A_{2i} = a_{2i-1} + a_{2i}$ и $A_{2i-1} = 0$. В $\bar{C}$ имеется a_{2i-1} слов веса $2i$ с 1 в позиции X_∞. Полный вес кодовых слов веса $2i$ в $\bar{C}$ равен $2iA_{2i}$. Поскольку расширенный код инвариантен относительно транзитивной группы перестановок, этот вес равномерно распределен среди всех позиций, т. е. $(n+1)\, a_{2i-1} = 2iA_{2i}$. В качестве следствия получена

Теорема 8.8. *Минимальный вес примитивного бинарного БЧХ-кода нечетен.*

Замечание. Заметим, что результат теоремы 8.8 имеет место для всякого бинарного кода, для которого расширенный код инвариантен относительно транзитивной группы перестановок.

9. ПОРОГОВОЕ ДЕКОДИРОВАНИЕ

Имеется ряд кодов, допускающих очень простую процедуру декодирования; простейший пример представляет *мажоритарное декодирование.* Рассматривается линейный код C.

Определение 9.1. *Ортогональным проверочным множеством порядка r* позиции i кода C назы-

вается множество из r слов кода $C^{\perp}$, скажем, $\boldsymbol{y}^{(1)}$, $\boldsymbol{y}^{(2)}, \ldots, \boldsymbol{y}^{(r)}$, такое, что

1) $y_i^{(\nu)} = 1 \quad (\nu = 1, 2, \ldots, r)$;

2) если $j \neq i$, то $y_j^{(\nu)} \neq 0$ для не более чем одного значения ν.

Покажем процедуру декодирования. Пусть $i = 1$ и $\boldsymbol{a}$ — слово с $t \leqslant \left[\frac{1}{2} r\right]$ ошибками. Рассмотрим ортогональное проверочное множество $\boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(r)}$ позиции 1. Тогда

$$(\boldsymbol{a}, \boldsymbol{y}^{(\nu)}) \neq 0 \text{ для } \begin{cases} \leqslant t \text{ значений } \nu, \text{ если символ } a_1 \text{ правильный;} \\ \geqslant r - (t-1) \text{ значений } \nu, \text{ если } a_1 \text{ ошибочен.} \end{cases}$$

Поскольку $r - (t-1) > t$, большинство значений $(\boldsymbol{a}, \boldsymbol{y}^{(\nu)})$ определяет, является ли a_1 правильным или нет. В случае $GF(2)$ ошибку сразу можно исправить. Эта процедура применима к каждой позиции кода. Здесь видно преимущество циклических кодов, поскольку эта процедура, примененная к одной фиксированной позиции, продолжается циклическим сдвигом полученного слова.

Нетрудно обобщить определение 9.1, заменив в 2) слова «не более чем одного» на «не более чем λ». Тогда, если имеется $t \leqslant \left[\frac{r + \lambda - 1}{2\lambda}\right]$ ошибок в $\boldsymbol{a}$, мы можем использовать множество общих проверок, называемое *λ-проверочным множеством порядка r*, для исправления позиции i. Тем же способом, что и ранее, легко проверить, что если число проверок, которые не влекут 0, превосходит *порог* $r - \lambda(t-1) - 1/2$, то в позиции i имеется ошибка.

Читатель, естественно, уже увидел связь с комбинаторными схемами. Пусть A — матрица инцидентности BIB-схемы с параметрами (b, v, r, k, λ). Рассмотрим строки матрицы A как базисные векторы линейного кода $C^{\perp}$ над $GF(q)$; тогда двойственный ему код C имеет строки $C^{\perp}$ как проверки на четность и, кроме того, для каждой позиции i кода C можно найти λ-проверочное множество порядка r позиции i (по определению BIB-схемы). Здесь мы сталкиваемся с задачей теории кодирования, которая решена лишь

для некоторых случаев; именно, задача определения размерности кода C в вышеописанной ситуации. Это равносильно нахождению ранга матрицы A над $GF(q)$. Если этот ранг равен v, то C состоит лишь из 0, и этот случай едва ли интересен. Мы вернемся к этой задаче в главе 11. Рассмотрим теперь один пример с $q=2$. Пусть A — матрица инцидентности схемы $PG(2,2)$:

$$A=\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

В этом примере, следуя теореме 8.4, видим, что первые 4 строки матрицы A порождают циклический код $C^{\perp}$ над $GF(2)$, который имеет $g(x)=1+x+x^3$ в качестве порождающего многочлена. Значит, код C, выписанный в обратном порядке, порождается многочленом $(1+x)(1+x^2+x^3)$. Из второго примера главы 8 знаем, что этот код C состоит из слов четного веса в $(7,4)$-коде Хэмминга. Для каждой позиции этого (циклического) кода имеются 3 строки матрицы A, которые образуют ортогональное проверочное множество (исправляющее 1 ошибку) порядка 3 этой позиции. Конечно, есть намного более простая процедура исправления ошибок для кодов Хэмминга, однако этот пример подводит к обсуждению кодов, порождаемых проективными плоскостями.

Здесь следует упомянуть и дальнейшие обобщения. Вместо использования числа общих проверок для проверки одной позиции можно использовать ту же самую процедуру для выяснения того, содержит ли определенное подмножество позиций слова ошибку или нет. Это делает возможным использовать другие общие проверки (тем же способом) для локализации ошибки. Это называется *многошаговым мажоритарным декодированием* (см. главу 10).

Тем, кто более подробно интересуется вопросами этого направления, мы рекомендуем литературу [28] и [50]. См. также гл. «Самоортогональные коды».

10. КОДЫ РИДА — МАЛЛЕРА *)

Этот класс кодов, связанных с конечными геометриями, был впервые исследован Маллером и Ридом. Введем некоторые обозначения. Рассматривается схема $AG(m, 2)$; векторы стандартного базиса будем обозначать через $(u_1, \ldots, u_m)$ (векторы-столбцы). Можно выписать все точки $AG(m, 2)$ как столбцы матрицы E (состоящей из m строк и $n = 2^m$ столбцов). Порядок столбцов задается по правилу: столбец j есть двоичное представление целого j ($j = 0, 1, \ldots, 2^m - 1$).

Если $j = \sum_{i=1}^{m} \xi_{ij} 2^{i-1}$ (это обозначение используется на протяжении всей главы), то j-й столбец матрицы E есть $x_j = \sum_{i=1}^{m} \xi_{ij} u_i$. Нам также понадобится следующее

Определение 10.1. $A_i = \{x_j \in AG(m, 2) \mid \xi_{ij} = 1\}$.

Заметим, что A_i есть $(m-1)$-мерное аффинное подпространство ($(m-1)$-плоскость).

Определение 10.2. v_i ($i = 1, \ldots, m$) есть i-я строка матрицы E, т. е. характеристическая функция множества A_i, а $v_0 = \mathbf{1}$ — характеристическая функция схемы $AG(m, 2)$. (Здесь строки матрицы E рассматриваются как слова в $\mathscr{R}^{(n)}$.)

Определение 10.3. Пусть $a = (a_0, \ldots, a_{n-1})$ и $b = (b_0, \ldots, b_{n-1})$, тогда $ab = (a_0 b_0, a_1 b_1, \ldots, a_{n-1} b_{n-1})$.

Заметим, что, согласно определениям 10.1—10.3, произведение $v_{i_1} v_{i_2} \ldots v_{i_k}$ является характеристической функцией множества $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}$. Если все индексы $i_1, \ldots, i_k$ различны, то это есть некоторое $(m-k)$-мерное аффинное подпространство из $AG(m, 2)$.

Следовательно, имеет место

Теорема 10.4. $w(v_1 v_2 \ldots v_k) = 2^{m-k}$.

Определение 10.5. Пусть $S \subset \{1, 2, \ldots, m\}$; подмножество $C(S)$ множества $\{0, 1, \ldots, 2^m - 1\}$ оп-

*) В новом издании эта глава называется «Конечные геометрии и коды».

ределяем по правилу

$$C(S)=\left\{ j=\sum_{i=1}^{m}\xi_{ij}2^{i-1}\,|\,i\notin S\Rightarrow\xi_{ij}=0\right\}.$$

Стандартный базисный вектор $e_j=(0,0,\ldots,0,1,0,0,\ldots,0)\in\mathscr{R}^{(n)}$ (1 на j-й позиции) является характеристической функцией для $\{x_j\}$. Имеем

$$e_j=\prod_{i=1}^{m}\{v_i+(1+\xi_{ij})v_0\}. \tag{10.6}$$

Следовательно, каждый из 2^m базисных векторов в $\mathscr{R}^{(n)}$ может быть представлен как многочлен степени $\leqslant m$ от $v_1, v_2, \ldots, v_m$. Значит, $\mathscr{R}^{(n)}$ порождается множеством

$$\{v_0, v_1, \ldots, v_m, v_1v_2, \ldots, v_1v_2\ldots v_m\}.$$

Это множество содержит $1+\binom{m}{1}+\ldots+\binom{m}{m}=2^m$ векторов, т. е. является базисом в $\mathscr{R}^{(n)}$ так что доказана

Теорема 10.7. *Векторы* $v_0, v_1, \ldots, v_m, v_1v_2, \ldots, v_1v_2\ldots v_m$ *образуют базис пространства* $\mathscr{R}^{(n)}$.

Пример. Пусть $m=4$, $n=16$; тогда

$$\begin{aligned}
v_0&=1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\\
v_1&=0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\\
v_2&=0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\\
v_3&=0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\\
v_4&=0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\\
v_1v_2&=0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\\
v_1v_3&=0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,0\,1\\
v_1v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\\
v_2v_3&=0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,1\,1\\
v_2v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\\
v_3v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\\
v_1v_2v_3&=0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\\
v_1v_2v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\\
v_1v_3v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\\
v_2v_3v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\\
v_1v_2v_3v_4&=0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1
\end{aligned}$$

Определение 10.8. Линейное подпространство пространства $\mathscr{R}^{(n)}$, базисом которого являются векторы $v_0, v_1, \ldots, v_m$ и все произведения $v_{i_1} \ldots v_{i_k}$ $(k \leqslant r)$, называется *кодом Рида — Маллера* (РМ-кодом) r-го порядка длины $n = 2^m$. РМ-код нулевого порядка имеет v_0 в качестве базиса. Это есть повторяющийся код с повторением длины 2^m.

Многие авторы предпочитают следующее описание РМ-кодов. Рассмотрим все многочлены степени $\leqslant r$ от m переменных $x_1, x_2, \ldots, x_m$, которые принимают значения в $GF(2)$. Пусть имеется фиксированный порядок точек в $AG(m, 2)$. Последовательность значений многочленов в этих точках есть кодовое слово длины 2^m РМ-кода порядка r.

Пусть $\boldsymbol{a} = v_{i_1} \ldots v_{i_k}$ — базисный вектор РМ-кода порядка r и пусть $\boldsymbol{b} = v_{j_1} \ldots v_{j_l}$ — базисный вектор РМ-кода порядка $m - r - 1$. Тогда $\boldsymbol{ab}$ есть базисный вектор РМ-кода порядка $m - 1$ и, согласно теореме 10.4, он имеет четный вес. Отсюда следует, что $(\boldsymbol{a}, \boldsymbol{b}) = 0$. Размерность РМ-кода r-го порядка равна $1 + \binom{m}{1} + \ldots + \binom{m}{r}$. Поскольку размерность РМ-кода порядка $m - r - 1$ равна $1 + \binom{m}{1} + \ldots + \binom{m}{m-r-1} = \binom{m}{r+1} + \ldots + \binom{m}{m}$, имеет место

Теорема 10.9. *Двойственный код к РМ-коду порядка r длины 2^m есть РМ-код порядка $m - r - 1$ длины 2^m.*

Следствие 10.10. *РМ-код порядка $m - 2$ длины $n = 2^m$ есть расширенный $(n, n - m - 1)$-код Хэмминга.*

Следующая теорема устанавливает связь с предыдущей главой.

Теорема 10.11. *Пусть C — РМ-код порядка $m - l$ длины 2^m. Тогда характеристическая функция всякого l-мерного аффинного подпространства из $AG(m, 2)$ есть кодовое слово из C.*

Доказательство. Пусть A есть l-плоскость в $AG(m, 2)$ и пусть $f \in \mathscr{R}^n$ — характеристическая функция плоскости A. Предположим, что $f = \sum_{i=0}^{n-1} f_i e_i$;

тогда

$$f = \sum_{k=0}^{m} \sum_{(i_1, i_2, \ldots, i_k)} \left\{ \sum_{j \in C(i_1, i_2, \ldots, i_k)} f_j \right\} v_{i_1} v_{i_2} \ldots v_{i_k}, \tag{10.12}$$

поскольку, согласно формуле (10.6), произведение $v_{i_1} \ldots v_{i_k}$ содержится в представлении e_j, только если $\xi_{ij} = 0$ для всех $i \notin \{i_1, i_2, \ldots, i_k\}$. Далее $\sum_{j \in C(i_1, \ldots, i_k)} f_j$ есть число точек из A, которые лежат также и в k-мерном линейном подпространстве $L = \{x_j \in AG(m, 2) \mid j \in C(i_1, \ldots, i_k)\}$. Если $k > m - l$, то $L \cap A$ либо пусто, либо является аффинным подпространством размерности >0. В обоих случаях $L \cap A$ имеет четное число точек, т. е. $\sum_{j \in C(i_1, \ldots, i_k)} f_j = 0$, если $k > m - l$. Это доказывает, что f есть РМ-код порядка $m - l$.

Будем теперь комбинировать теоремы 10.9 и 10.11. Пусть C — это РМ-код порядка t длины 2^m. Мы уже знаем, что каждая $(t+1)$-плоскость в $AG(m, 2)$ дает нам уравнение общей проверки. Эти $(t+1)$-плоскости образуют BIB-схему с параметрами

$$v = 2^m, \quad b = 2^{m-t-1} \frac{(2^m - 1)(2^{m-1} - 1) \ldots (2^{m-t} - 1)}{(2^{t+1} - 1)(2^t - 1) \ldots (2 - 1)},$$

$$k = 2^{t+1},$$

$$r = \frac{(2^m - 1)(2^{m-1} - 1) \cdots (2^{m-t} - 1)}{(2^{t+1} - 1)(2^t - 1) \ldots (2 - 1)},$$

$$\lambda = \frac{(2^{m-1} - 1) \cdots (2^{m-t} - 1)}{(2^t - 1) \ldots (2 - 1)}.$$

Рассмотрим произвольную t-плоскость T в $AG(m, 2)$. Имеется ровно $2^{m-t} - 1$ различных $(t+1)$-плоскостей, содержащих T. Каждая точка, не принадлежащая T, располагается в точности в одной из этих $(t+1)$-плоскостей. Следуя процедуре, описанной в главе 9, можно ввести мажоритарную процедуру, обеспечивающую общую проверку в позициях T, если имеется менее чем 2^{m-t-1} ошибок. По индукции видно, что за $t+1$ шагов мажоритарного декодирования можно исправить до $2^{m-t-1} - 1$ ошибок. Исходя из того, что минимальный вес в РМ-коде порядка t четен,

и используя теорему 10.4, получаем следующую теорему.

Теорема 10.13. *Минимальный вес в РМ-коде порядка t длины 2^m равен 2^{m-t}.*

По определению каждое кодовое слово в РМ-коде порядка r длины 2^m есть сумма характеристических функций аффинных подпространств размерности $\geqslant m-r$. Согласно теореме 10.11, сумма характеристических функций аффинных подпространств размерности $\geqslant m-r$ есть кодовое слово в РМ-коде r-го порядка. Отсюда следует, что каждая перестановка $AG(m, 2)$, которая также переставляет аффинные подпространства, оставляет все РМ-коды инвариантными. Это есть группа аффинных преобразований $AG(m, 2)$ — трижды транзитивная группа порядка $2^m \prod_{i=0}^{m-1} (2^m - 2^i)$.

Теорема 10.14. *Всякий РМ-код длины 2^m инвариантен относительно всех аффинных преобразований, действующих на позициях, интерпретируемых как точки в $AG(m, 2)$.*

Поскольку первоначальное определение РМ-кодов более комбинаторно, мы избрали этот путь для представления их здесь. Для полноты следует подчеркнуть, что лишь позже было установлено, что РМ-коды являются расширенными циклическими кодами. Чтобы дать циклическое определение, введем обозначение $w(j)$ для веса двоичного представления j (интерпретируемого как вектор над $GF(2)$).

Теорема 10.15. *Пусть α — примитивный элемент в $GF(2^m)$ и пусть $g(x) = \prod^*(x - \alpha^j)$, где $\prod^*$ — произведение по всем целым j из $[0, 2^m - 2]$ с $w(j) < m - r$. Если C — циклический код длины 2^m, порожденный $g(x)$, то код $\bar{C}$ эквивалентен РМ-коду r-го порядка.*

Мы не приводим здесь доказательство этой теоремы; оно не сложно (см. [44]). Отметим лишь, что теорему 10.13 можно легко вывести из теорем 8.6 и 10.15. Одно из преимуществ теоремы 10.15 как определения РМ-кодов состоит в том, что это понятие может быть обобщено на другие поля $GF(q)$.

Все РМ-коды, приводимые в этом параграфе, являются примерами широкого класса кодов, известных

под названием *евклидово геометрических кодов* (см. [28]).

Тесно связанными с ними оказываются проективно геометрические коды. Укажем здесь лишь один пример.

Определение 10.16. Пусть p — простое, $q = p^\alpha$ и пусть A — матрица инцидентности точек и гиперплоскостей в $PG(m, q)$. Строки A порождают код $C^\perp$ над алфавитом $GF(p)$. Двойственный код C называется *проективно геометрическим.*

Показано (см., например, [28]), что $C^\perp$ имеет размерность $1 + \binom{m+p-1}{p-1}^\alpha$. Примером, связанным с тематикой следующей главы, служит случай $p = \alpha = m = 2$. В этом случае A — матрица инцидентности схемы $PG(2, 4)$ и код $C^\perp$ имеет размерность 10. Непосредственное вычисление показывает, что $C^\perp$ имеет ровно 21 слово веса 5. Следовательно, кодовое слово $C^\perp$ имеет вес 5 тогда и только тогда, когда оно является прямой в $PG(2, 4)$. Иными словами, A может быть найдена из своей линейной оболочки. Вновь мы имеем пример линейного кода, в котором векторы минимального веса ($\neq 0$) образуют 2-схему.

В заключение этого параграфа укажем пример еще одной связи РМ-кодов и комбинаторной теории.

Рассмотрим РМ-код 1-го порядка длины 2^m. Согласно теореме 10.9 и следствию 10.10, это есть двойственный код к расширенному коду Хэмминга. Кроме этого, согласно теореме 10.9, этот код является самоортогональным, т. е. $(a, b) = 0$ для каждой пары кодовых слов; и имеет размерность $m + 1$. В этом коде для каждого кодового слова a $1 + a$ также является кодовым словом. Из каждой такой пары выберем одно слово и из этих выбранных слов образуем матрицу (2^m строк, 2^m столбцов). Если в этой матрице заменить 0 на —1, то полученная матрица будет матрицей Адамара. *Далее см. Добавление* 12.

11. САМООРТОГОНАЛЬНЫЕ КОДЫ, СХЕМЫ И ПРОЕКТИВНЫЕ ПЛОСКОСТИ

Расширенный (8.4)-бинарный код Хэмминга, описанный в главе 7, совпадает с двойственным к нему кодом. Это служит примером класса РМ-кодов r-го по-

рядка длины 2^{2r+1} (см. следствие 10.10), которые являются самодвойственными по теореме 10.9. Дадим теперь пример такого кода над $GF(3)$.

Пусть S_5 — циркулянтная матрица с первой строкой $(0, 1, -1, -1, 1)$. Определим G как

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & & & & & & & & & & \\ 0 & & & & & & & & & & \\ 0 & & & I_5 & & & & & S_5 & & \\ 0 & & & & & & & & & & \\ 0 & & & & & & & & & & \end{bmatrix}, \qquad (11.1)$$

а H — как

$$H = \begin{bmatrix} 1 & & & & \\ 1 & & & & \\ 1 & & S_5 & & I_5 \\ 1 & & & & \\ 1 & & & & \end{bmatrix}.$$

Тогда $GH^T = 0$. Очевидно, что строки G независимы и поэтому G есть порождающая матрица $(11, 6)$-кода C над $GF(3)$, а H — проверочная матрица для C. Заметим, что

$$GG^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & & & & \\ 0 & & -J_5 & & \\ 0 & & & & \\ 0 & & & & \end{bmatrix}. \qquad (11.2)$$

Следовательно, если $a = (a_1, a_2, a_3, a_4, a_5, a_6)$, то

$$aGG^Ta^T = -\left(\sum_{i=2}^{6} a_i\right)^2 \neq 1,$$

т. е. все слова в C имеют вес $\not\equiv 1 \pmod 3$. Очевидно, нет кодового слова веса 2; отсюда сразу следует, что линейная комбинация двух строк G образует слово веса 5 или 6, а также, что линейная комбинация трех строк имеет вес >3, но поскольку этот вес не равен 4, то он должен быть по крайней мере 5. Линейная комбинация более чем трех строк G имеет вес $\geqslant 4$ и, следовательно, $\geqslant 5$. Значит, минимальный вес и минимальное расстояние равно 5, т. е. этот код является 2-кодом, исправляющим ошибки. Поскольку числов слов равно 3^6, а объем сферы $S(x, 2)$ равен

$1+2\binom{11}{1}+4\binom{11}{2}=3^5$, видим, что этот код является *совершенным*. Код этот известен как *тернарный код Галея*. Его весовой энумератор имеет вид

$$\eta^{11}+132\xi^5\eta^6+132\xi^6\eta^5+330\xi^8\eta^3+110\xi^9\eta^2+24\xi^{11}. \quad (11.3)$$

Рассмотрим теперь расширенный $(12, 6)$-код $\bar{C}$ над $GF(3)$. Он имеет порождающую матрицу $\bar{G}$, получаемую из G в (11.1) добавлением к ней столбца $(0, -1, -1, -1, -1, -1)$. Тогда согласно (11.2) имеем, что $\bar{G}\bar{G}^T=0$, т. е. этот код C самодвойствен. Из (11.3) находим, что его энумератор имеет вид

$$\eta^{12}+264\xi^6\eta^6+440\xi^9\eta^3+24\xi^{12}. \quad (11.4)$$

Замечание. Если бы мы начали с $\bar{C}$ вместо C, то доказательство даже упростилось бы (см. главу 13).

Рассмотрим два кодовых слова $\boldsymbol{a}$ и $\boldsymbol{b}$ из $\bar{C}$, оба веса 6. Пусть будет k позиций, где $\boldsymbol{a}$ и $\boldsymbol{b}$ оба имеют ненулевые координаты. Тогда либо $\boldsymbol{a}+\boldsymbol{b}$, либо $\boldsymbol{a}-\boldsymbol{b}$ имеет вес $\leqslant 12-k-\left[\frac{k+1}{2}\right]$. Значит, либо $\boldsymbol{a}=\pm\boldsymbol{b}$, либо $k\leqslant 4$. Будем говорить, что подмножество D множества $\{1, 2, \ldots, 12\}$ поддерживает кодовое слово $\boldsymbol{a}$ из C, если номера его ненулевых координат есть в D (иначе — D является *опорным подмножеством*).

Теорема 11.5. *Пусть $\mathcal{D}$ — совокупность 6-подмножеств множества $S:=\{1, 2, \ldots, 12\}$, которые поддерживают кодовые слова веса 6 в C. Тогда $\mathcal{D}$ образует 5-схему с параметрами $(12, 6, 1)$, т. е. является системой Штейнера.*

Доказательство. Ранее уже показано, что два кодовых слова $\boldsymbol{a}$ и $\boldsymbol{b}$ поддерживаются множествами, которые пересекаются не более чем в 4 точках, только если $\boldsymbol{a}\neq\pm\boldsymbol{b}$. Поэтому, согласно (11.4), есть $\frac{1}{2}\times 264\times 6=792$ различных 5-подмножеств множества S, содержащихся в множествах совокупности $\mathcal{D}$. Поскольку S имеет $\binom{12}{5}=792$ 5-подмножеств, доказательство закончено.

Конечно, это хорошая известная 5-схема (см. главу 1). Мы привели ее здесь, чтобы обосновать поиск 5-схем такого типа. В главе 13 мы вернемся к этому

вопросу. Результат теоремы 11.5 есть специальный случай теоремы 13.13. *Далее см. Добавление* 13.

Теперь покажем, как проективная плоскость порождает самодвойственный код. Первый пример кода, порожденного плоскостью, был приведен в главе 9. Пусть A — матрица инцидентности схемы $PG(2, n)$. Рассмотрим подпространство C пространства $\mathscr{R}^{(n^2+n+1)}$ над полем $GF(2)$, которое порождается строками этой матрицы A. Если n — нечетно, то легко видеть, что C есть код. Если взять сумму строк A, которые имеют 1 в фиксированной позиции, то результатом будет строка с нулем на этой позиции и единицами — на остальных. Эти векторы порождают подпространство пространства $\mathscr{R}^{(n^2+n+1)}$, состоящее из всех слов четного веса и подпространство это есть C (поскольку C, очевидно, не содержит слов нечетного веса). Случай четного n сложнее.

Теорема 11.6. *Если* $n \equiv 2 \pmod 4$, *то строки матрицы инцидентности* A *схемы* $PG(2, n)$ *порождают код* C *размерности* $(n^2+n+2)/2$.

Доказательство. 1) Так как n — четно, то код $\bar{C}$ самоортогонален, т. е. $\bar{C} \subset (\bar{C})^{\perp}$. Следовательно,

$$\dim C \leqslant (n^2+n+2)/2.$$

2) Пусть $\dim C = r$ и $k = n^2+n+1-r = \dim C^{\perp}$ и пусть H — проверочная матрица ранга k для C. Предположим, что координатные места переставлены так, что H имеет форму $(I_k P)$.

Определим $N = \begin{pmatrix} I_k & P \\ 0 & I_r \end{pmatrix}$. Интерпретируем A и N как рациональные матрицы. Тогда $\det AN^T = \det A = (n+1)\, n^{(n^2+n)/2}$. Поскольку все элементы в первых k столбцах матрицы AN^T четны, находим, что $2^k \mid \det A$, откуда следует, что $r \geqslant (n^2+n+2)/2$.

Из 1) и 2) следует утверждение теоремы.

Из теоремы 11.6 сразу следует

Теорема 11.7. *Если* $n \equiv 2 \pmod 4$, *то строки матрицы инцидентности* A *плоскости* $PG(2, n)$ *порождают код* C, *для которого* $\bar{C}$ *самодвойствен.*

Мы продолжаем анализировать свойства плоскости $PG(2, n)$, $n \equiv 2 \pmod 4$, в терминах кодирования.

Теорема 11.8. *Код* C *из теоремы* (11.6) *имеет минимальный вес* $n+1$ *и каждый вектор минимального веса является прямой в* $PG(2, n)$.

Доказательство. Пусть $v \neq 0$ есть кодовое слово с весом $w(v) = d$. Так как для каждой прямой l есть общая проверка на четность, то

1) если d — нечетно, то v пересекает каждую прямую по крайней мере единожды, а

2) если d — четно, то каждая прямая, проходящая через фиксированную точку v, пересекает v во второй точке.

В случае 2) сразу получаем, что $d > n + 1$. В случае 1) находим, что $(n+1)d \geqslant n^2 + n + 1$, т. е. $d \geqslant n + 1$. Если $w(v) = n + 1$, то в $PG(2, n)$ найдется прямая l, которая пересекает v, по крайней мере, в 3 точках. Если на l есть точка, не принадлежащая v, то каждая прямая, отличная от l, проходящая через эту точку, пересекает v согласно (1). Отсюда $d \geqslant n + 3$.

Определение 11.9. *s-дуга* в $PG(2, n)$ есть множество из s точек, любые три из которых неколлинеарны.

Теорема 11.10. *Векторы веса $n + 2$ в коде C являются в точности $(n + 2)$-дугами в $PG(2, n)$.*

Доказательство. 1) Пусть $v \in C$ и $w(v) = n + 2$. Каждая прямая пересекает v в четном числе точек. Пусть l — прямая и предположим, что v и l имеют $2a$ общих точек. Каждая из n прямых, отличных от l, проходящих через одну из этих $2a$ точек, пересекает v по крайней мере еще один раз. Следовательно, $2a + n \leqslant n + 2$, т. е. $a = 0$ или $a = 1$.

2) Пусть v — некоторая $(n + 2)$-дуга, а S — множество из $(n + 2)(n^2 - 1)/2$ различных прямых в $PG(2, n)$, проходящих через пары точек v. Каждая прямая из S содержит $n - 1$ точек не из v. Таким образом, насчитываем $(n + 2)(n^2 - 1)/2$ точек. Имеется $n^2 - 1$ точек не из v, и каждая из них лежит на, по крайней мере, $(n + 2)/2$ прямых из S. Следовательно, каждая из них лежит в точности на $(n + 2)/2$ прямых из S. Каждая точка из v лежит на $n + 1$ прямых из S. Следовательно, v есть сумма прямых из S, т. е. $v \in C$.

(См. также [3]).

Замечание. В качестве интересного упражнения читателю предлагается проверить, что теорема 11.10 также выполняется для кода, порожденного плоскостью $PG(2, n)$, приведенного в конце главы 10.

Для самодвойственного (n, k) кода C над $GF(q)$ из теоремы 7.14 выводим следующие соотношения для весового энумератора $A(\xi, \eta)$:

$$A(\xi, \eta) = q^{-k} A(\eta - \xi, \eta + (q-1)\xi), \quad (11.11)$$

где $k = n/2$. Это означает, что полином инвариантен относительно линейного преобразования с матрицей $q^{-1/2}\begin{pmatrix} -1 & q-1 \\ 1 & 1 \end{pmatrix}$. Если $q = 2$, то все кодовые слова в C имеют четный вес, т. е. $A(\xi, \eta)$ инвариантен относительно преобразования $\xi \to -\xi$. Эти два преобразования порождают группу диэдра $\mathscr{D}_8$. Глисоном (см. [8], [27], [49]) было показано, что кольцо полиномов от ξ и η, которые инвариантны относительно этой группы, есть свободное кольцо, порождаемое посредством $\xi^2 + \eta^2$ и $\xi^2\eta^2(\xi^2 - \eta^2)^2$.

Рассмотрим теперь гипотетическую плоскость десятого порядка. Из теорем 11.6, 11.7 и 11.8 мы знаем, что матрица инцидентности такой плоскости порождает код C, для которого $\bar{C}$ является (112,56)-самодвойственным кодом, а также, что весовой энумератор $A(\xi, \eta)$ кода C имеет коэффициенты $A_0 = 1$, $A_1 = A_2 = \ldots = A_{10} = 0$, $A_{11} = 111$. Так как все генераторы $\bar{C}$ имеют вес 12, а всякие два слова из $\bar{C}$ имеют четное число общих единиц, то все веса в $\bar{C}$ кратны 4. Следовательно, $A_{13} = A_{14} = 0$. Подставляя это в (11.11) или учитывая результаты Глисона, можно видеть, что $A(\xi, \eta)$ однозначно определяется, если известны A_{12}, A_{15} и A_{16}. Недавно МакВильямс, Слоэн и Томпсон ([48]) исследовали кодовые слова веса 15 в C. Предполагалось, что матрица инцидентности этой плоскости приводит к коду, у которого $A_{15} \neq 0$. Рассуждения, аналогичные используемым при доказательстве теорем 11.8 и 11.10, несколько ограничивают эту возможность. Действительно, было обнаружено, что эта плоскость должна содержать частичную конфигурацию из 15 прямых. Поиск с помощью ЭВМ показал, что если отталкиваться от такой конфигурации, то плоскость не может быть полной. Следовательно, мы знаем, что если плоскость порядка 10 существует, то

$$A_{15} = 0. \quad (11.12)$$

Бруэном и Фишером в совсем недавней работе было отмечено (см. [14]), что такой же результат следует из результата, полученного Деннистоном с помощью ЭВМ, о 6-дугах, не содержащихся в 7-дугах (применительно к двойственной плоскости).

Идея ортогональности может быть применима и к t-схемам: t-схема называется *самоортогональной*, если каждые два блока пересекаются в четном числе точек. Рассмотрим сейчас возможные самоортогональные Штейнеровы системы. Используя хорошо известные соотношения между t, b, v, r, k (см. главу 1) и простые оценочные рассуждения, легко показать (как упражнение для читателя, см. [3], [6]), что имеется четыре возможности:

1) $t = 3$, $k = 4$, $v = 8$. Это пример теоремы 7.12, т. е. $AG(3, 2)$.

2) $t = 3$, $k = 6$, $v = 22$. Это единственное расширение $PG(2, 4)$ (см. главу 1 и пример, следующий за теоремой 10.16).

3) $t = 5$, $k = 8$, $v = 24$ (см. главу 1).

4) $t = 3$, $k = 12$, $v = 112$. Это было бы расширением проективной плоскости порядка 10 (если она существует).

Замечание. Этим путем можно вновь доказать теорему 1.11.

Результат (11.12) однозначно определяет энумератор кода $\bar{C}$, если мы предполагаем, что плоскость порядка 10 расширяема, т. е., что пример (4) возможен.

Подробнее см. [57, 2*]. *Далее см. Добавление* 14.

12. КВАДРАТИЧНО-ВЫЧЕТНЫЕ КОДЫ

Прежде чем обратиться к теме этой главы, мы должны доказать теорему о циклических кодах (см. главу 8). Мы используем символ π_j для обозначения перестановки элементов $\{0, 1, \ldots, n-1\}$, задаваемой по правилу $\pi_j(k) = jk \pmod n$, а также для обозначения автоморфизма $\mathscr{R}^{(n)}$, задаваемого по правилу $\pi_j(x^k) = x^{jk} (\mathrm{mod}\,(x^n - 1))$; здесь мы отождествляем векторы из $R^{(n)}$ и многочлены по $\mathrm{mod}\,(x^n - 1)$. Рассматриваются бинарные циклические коды длины n при нечетном n.

Теорема 12.1. *Для каждого идеала V в $\mathscr{R}^{(n)}$ существует единственный многочлен $c(x) \in V$, называе-*

мый идемпотентом этого V, со следующими свойствами:

1) $c(x) = c^2(x)$;

2) $c(x)$ *порождает* V;

3) $\forall f(x) \in V\ [c(x)f(x) = f(x)]$, *т. е.* $c(x)$ — *единица для* V;

4) *если* $(j, n) = 1$, *то* $\pi_j(c(x))$ *есть идемпотент* $\pi_j V$.

Доказательство. 1) Пусть $g(x)$ — порождающий многочлен V и $g(x)h(x) = x^n - 1$ (в $GF(2)[x]$). Так как $x^n - 1$ не имеет кратных нулей, то $(g(x), h(x)) = 1$. Следовательно, есть многочлены $p_1(x)$ и $p_2(x)$, для которых

$$p_1(x)g(x) + p_2(x)h(x) = 1 \quad (\text{в } GF(2)[x]). \quad (12.2)$$

Умножая обе части равенства на $c(x) = p_1(x)g(x)$, находим

$$c^2(x) + p_1(x)p_2(x)g(x)h(x) = c(x).$$

Так как в $\mathscr{R}^{(n)}$ выполняется равенство $g(x)h(x) = 0$, то 1) доказано.

2) Нормированный многочлен наименьшей степени в идеале, порожденном $c(x)$, есть

$$(c(x),\ x^n - 1) = (p_1(x)g(x),\ g(x)h(x)) = g(x).$$

3) Согласно 2) каждый многочлен $f(x) \in V$ кратен многочлену $c(x)$. Пусть $f(x) = c(x)f_1(x)$. Тогда

$$c(x)f(x) = c^2(x)f_1(x) = c(x)f_1(x) = f(x),$$

т. е. $c(x)$ — единица в V.

4) Поскольку π_j есть автоморфизм $\mathscr{R}^{(n)}$, то многочлен $\pi_j(c(x))$ является идемпотентом и единицей для $\pi_j V$. В силу единственности единицы 4) доказано.

Пример 12.3. Рассмотрим подробно следующий пример. Пусть $n = 2^m - 1$ и пусть $m_1(x)$ — минимальный многочлен примитивного элемента α поля $GF(2^m)$. Тогда по теореме 8.4 этот многочлен $m_1(x)$ порождает код Хэмминга, который мы обозначим сейчас через H_m. Пусть $x^n - 1 = m(x)h(x)$ в $GF(2)[x]$. Мы знаем, что $h(x)$ порождает двойственный код H_m^* к коду H_m (см. главу 8). Этот код H_m^* имеет размерность m и, стало быть, он состоит из 0 и n циклических сдвигов слова $h(x)$. Это влечет существование такого показателя s, при котором $f(x) = x^s h(x)$ есть идемпотент H_m

и, значит, (12.2) принимает вид

$$p_1(x)\,m_1(x) + x^s h(x) = 1.$$

Ясно, что многочлен $1 + f(x)$ является идемпотентом H_m. Предоставляем читателю проверить, что $f(x)$ имеет вес 2^{m-1} (см. последний пример в главе 10). Например, если $m = 4$, $n = 15$, $m_1(x) = x^4 + x + 1$, то

$$(x^8 + x^2 + 1)\,m_1(x) + \\ + x(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) = 1$$

$$xh(x) = f(x) = (x + x^2 + x^4 + x^8) + (x^3 + x^6 + x^9 + x^{12}).$$

Пример 12.3 и нижеследующее предложение 12.4 понадобятся нам в главе 14.

Согласно п. 2) теоремы 12.1 имеем

Предложение 12.4. *Для каждого многочлена $q(x)$ слово $q(x)\{1 + f(x)\}$ принадлежит коду H_m.*

При описании квадратично-вычетных кодов будем использовать следующие обозначения.

Обозначения 12.5. 1) n — нечетное простое;

2) α — примитивный n-й корень единицы в некотором расширении поля $GF(q)$ (α выбирается позже надлежащим образом);

3) R_0 — множество квадратичных вычетов по $\bmod n$, R_1 — множество ненулевых элементов из $GF(n) \setminus R_0$;

4) $g_0(x) = \prod_{r \in R_0} (x - \alpha^r)$, $g_1(x) = \prod_{r \in R_1} (x - \alpha^r)$ (заметим, что $x^n - 1 = (x - 1)\,g_0(x)\,g_1(x)$).

Предполагается, что $q^{(n-1)/2} \equiv 1 \pmod n$, т. е. q есть квадратичный вычет по $\bmod n$.

Ненулевые элементы из $GF(n)$ являются степенями примитивного элемента $a \in GF(n)$. Ясно, что a^e является квадратичным вычетом, если $e \equiv 0 \pmod 2$ и не является таковым, если $e \equiv 1 \pmod 2$. Так как q — квадратичный вычет, то множество R_0 замкнуто относительно умножения на $q \pmod n$.

Определение 12.6. Циклические коды длины n над полем $GF(q)$ с порождающими многочленами $g_0(x)$ и $(x - 1)\,g_0(x)$ оба называются *квадратично-вычетными кодами* (*КВ-кодами*). Расширенный квадратично-вычетный код длины $n + 1$ получается добавлением общей проверки на четность к коду с порождающим многочленом $g_0(x)$.

(См. замечание, следующее за теоремой 12.10.)

В бинарном случае код с порождающим многочленом $(x-1)g_0(x)$ состоит из слов четного веса в коде с порождающим многочленом $g_0(x)$. Если G — порождающая матрица для первого из этих кодов, то $\begin{pmatrix} 1 & 1 & \dots & 1 \\ & G & & \end{pmatrix}$ — порождающая матрица для второго кода, а порождающая матрица для расширенного кода имеет вид

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & & & & \\ \vdots & & G & & \\ 0 & & & & \end{bmatrix}$$

см. главу 7). Заметим, что в бинарном случае условие о том, что q — квадратичный вычет по mod n, выполнено, если $n \equiv \pm 1 \pmod 8$. Если $j \in R_1$, то перестановка π_j отображает R_0 в R_1, и обратно. Легко видеть, что если заменить R_0 на R_1 в теореме 1.6, то получим эквивалентные коды в смысле главы 7 (см. [44], теорема 3.2.2). Если $n \equiv -1 \pmod 4$, то $-1 \in R_1$, и следовательно, преобразование $x \to x^{-1}$ отображает кодовое слово кода, порождаемого многочленом $g_0(x)$, в кодовое слово кода, порождаемого $g_1(x)$.

Теорема 12.7. *Если* $c = c(x) = \sum_{i=0}^{n-1} c_i(x^i)$ *есть кодовое слово КВ-кода с порождающим многочленом* $g_0(x)$, $\sum_{i=0}^{n-1} c_i \neq 0$ *и* $w(c) = d$ *есть вес этого кодового слова, то*

1) $d^2 \geqslant n$;
2) *если* $n \equiv -1 \pmod 4$, *то* $d^2 - d + 1 \geqslant n$;
3) *если* $n \equiv -1 \pmod 8$ *и* $q = 2$, *то* $d \equiv 3 \pmod 4$.

Доказательство. 1) Поскольку $\sum_{i=0}^{n-1} c_i \neq 0$, то многочлен $c(x)$ не делится на $x-1$. Посредством подходящей перестановки π_j можно преобразовать $c(x)$ в многочлен $\hat{c}(x)$, который делится на $g_1(x)$ и не делится на $x-1$. Следовательно, $c(x)\hat{c}(x) = 1 + x + x^2 + \dots + x^{n-1}$. Число ненулевых коэффициентов левой части не больше, чем d^2. Это доказывает 1).

2) Теперь π_j можно выбрать так, что $\hat{c}(x) = c(x^{-1})$, и тогда $c(x)\hat{c}(x)$ имеет не более $d^2 - d + 1$ ненулевых коэффициентов.

3) Пусть $c(x) = \sum_{i=1}^{d} x^{e_i}$, $\hat{c}(x) = \sum_{i=1}^{d} x^{-e_i}$. Если $e_i - e_j = e_k - e_l$, то $e_j - e_i = e_l = e_k$. Поэтому, если какие-то члены взаимно сокращаются, то сразу по четыре члена, т. е. $n = d^2 - d + 1 - 4a$ для некоторого $a \geqslant 0$. Это доказывает 3).

Рассмотрим вновь бинарные КВ-коды. Положим

$$\theta(x) = \sum_{r \in R_0} x^r. \tag{12.8}$$

Ясно, что $\theta(x)$ есть идемпотент в $\mathcal{R}^{(n)}$ (2 является квадратичным вычетом по $\bmod n$). Следовательно, $\{\theta_{(\alpha)}\}^2 = \theta(\alpha)$, т. е. $\theta(\alpha) \in GF(2)$. Аналогично получаем $\theta(\alpha^i) = \theta(\alpha)$, если $i \in R_0$, и $\theta(\alpha^i) + \theta(\alpha) = 1$, если $i \in R_1$. Выберем теперь α так, чтобы $\theta(\alpha) = 0$. Тогда $\theta(\alpha^i) = 0$, если $i \in R_0$, $\theta(\alpha^i) = 1$, если $i \in R_1$, и, наконец, $\theta(\alpha^0) = (n-1)/2$. Это доказывает следующую теорему.

Теорема 12.9. *Если α из п. 2) обозначений* 12.5 *выбрано надлежащим образом, то многочлен $\theta(x)$ из* (12.8) *является идемпотентом КВ-кода с производящим многочленом $(x-1)g_0(x)$, если $n \equiv 1 \pmod 8$, и КВ-кода с производящим многочленом $g_0(x)$, если $n \equiv -1 \pmod 8$.*

Пусть C — циркулянтная матрица с кодовым словом θ в качестве первой строки. Положим

$$\boldsymbol{c} = \begin{cases} 0, & \text{если } n \equiv 1 \pmod 8, \\ 1, & \text{если } n \equiv -1 \pmod 8; \end{cases}$$

$$G = \begin{bmatrix} 1 & 1 \\ \boldsymbol{c}^T & C \end{bmatrix}.$$

Из теоремы 12.9 следует, что строки матрицы G (которые не являются независимыми) порождают расширенный бинарный КВ-код длины $n+1$.

Занумеруем координаты места кодовых слов в этом расширенном бинарном КВ-коде, используя координаты проективной прямой, т. е. $\infty, 0, 1, \ldots, n-1$. Позиция общей проверки на четность есть ∞. Мы

используем обычные соглашения при арифметических операциях: $\pm 0^{-1} = \infty$, $\pm \infty^{-1} = 0$, $\infty + a = \infty$ для $a \in GF(n)$. Рассмотрим теперь $PSL(2, n)$—группу перестановок позиций и покажем, что расширенный КВ-код остается инвариантным. Эта группа порождается преобразованиями $Sx = x + 1$, $Tx = -x^{-1}$. Так как преобразование S оставляет ∞ инвариантным и является циклическим сдвигом на других позициях, то это преобразование оставляет код инвариантным. Несложно показать, что T отображает строки G в линейные комбинации не более чем трех строк G (см. [44], стр. 83). Для большинства читателей это, вероятно, простое свойство G (сопоставить с группой автоморфизмов некоторых матриц Адамара). Итак, нами доказана

Теорема 12.10. *Группа автоморфизмов расширенного бинарного КВ-кода длины* $n + 1$ *содержит* $PSL(2, n)$.

Замечание. Глесон и Прэнг (см. [2]) слегка изменили определение расширенного кода для небинарного случая. Они потребовали, чтобы координата в расширенной позиции умножалась на множество таким образом, чтобы результирующий код был либо самоортогональным (если $n \equiv -1 \pmod 4$), либо ортогональным другому КВ-коду (если $n \equiv 1 \pmod 4$). Они показали, что теорема 12.10 верна также и для q-арных кодов.

Вновь рассмотрим расширенный бинарный КВ-код. Согласно теореме 12.10 этот код инвариантен относительно дважды транзитивной группы. Учитывая замечание, следующее за 8.8, видим, что бинарный КВ-код имеет нечетный минимальный вес. Это позволяет применить теорему 12.7. Таким образом, получена

Теорема 12.11. *Минимальный вес бинарного КВ-кода длины* n *с порождающим многочленом* $g_0(x)$ *есть нечетное число* d, *для которого*

1) $d^2 > n$, *если* $n \equiv 1 \pmod 8$,

2) $d^2 - d + 1 \geqslant n$, *если* $n \equiv -1 \pmod 8$.

Замечание. Читателю, близко знакомому с теорией разностных множеств и схем, нетрудно проверить, что из доказательства п. 2), 3) в теореме 12.7 следует, что если в п. 2) теоремы 12.11 имеет место равенство, то существует проективная плоскость порядка $d - 1$ (ср. [67]).

Более комбинаторная форма границы квадратного корня (именно под таким названием известна теорема 12.11) была недавно найдена Ассмусом, Мэттсоном и Сэчером (см. [57]). Утверждается, что если C есть $(n, (n+1)/2)$-циклический код с минимальным весом d и $C^{\perp} \subseteq C$, а также если подмножества позиций, которые поддерживают слова минимального веса, образуют 2-схему, то $d^2 - d + 1 \geqslant n$, причем равенство имеет место тогда и только тогда, когда эта схема есть проективная плоскость порядка $d-1$.

Рассмотрим важный пример КВ-кодов.

Пример 12.12. Над $GF(2)$ имеем

$$x^{23}-1 = (x-1)(x^{11}+x^9+x^7+x^6+x^5+x+1)\times$$
$$\times(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1) =$$
$$= (x-1)\,g_0(x)\,g_1(x).$$

Бинарный КВ-код C длины 23 с порождающим многочленом $g_0(x)$ является $(23, 12)$-кодом. Согласно теореме 12.11 минимальное расстояние d этого кода удовлетворяет неравенству $d(d-1) \geqslant 22$. Так как d нечетно, имеем, что $d \geqslant 7$. В этом случае объем шара $S(x, 3)$ равен 2^{11}, т. е. $\left|\bigcup_{x \in C} S(x, e)\right| = 2^{23}$, или, иными словами, этот код совершенный (ср. с определением (7.5)). Этот код известен как *бинарный код Галея*. В этом случае группа автоморфизмов кода $\bar{C}$ есть M_{24}.

Если $n \equiv -1 \pmod 4$, то расширенный бинарный КВ-код $\bar{C}$ длины $n+1$ является самодвойственным. Это следует из замечания, предшествующего теоремам 12.7 и 8.3 и формы порождающей матрицы кода $\bar{C}$, найденной нами ранее. Это также можно увидеть и из матрицы G, определенной после теоремы 12.9.

Теперь мы приступаем к одной из наиболее важных теорем нашего курса. Эта теорема, которая показывает, что многие коды могут быть использованы для построения t-схем, принадлежит Ассмусу и Мэттсону [2].

Теорема 12.13. *Пусть A — некоторый (n, k)-код над $GF(q)$ и пусть $A^{\perp}$ — это $(n, n-k)$-двойственный код. Пусть минимальные веса этих кодов суть d и e. Пусть t — целое, меньшее чем d. Пусть v_0 — наибольшее целое число, удовлетворяющее неравенству*

$v_0 - \left[\frac{v_0+q-2}{q-1}\right] < d$, *и* w — *наибольшее целое, удовлетворяющее неравенству* $w_0 - \left[\frac{w_0+q-2}{q-1}\right] < e$, *где, если* $q=2$, *то* $v_0 = w_0 = n$. *Предположим, что число ненулевых весов в* $A^\perp$, *которые меньше или равны* $n-t$, *само меньше или равно* $d-t$. *Тогда для каждого веса* v, *где* $d \leqslant v \leqslant v_0$, *подмножества множества* $S=\{1, 2, \ldots, n\}$, *которые поддерживают кодовые слова веса* d *в* A, *образуют* t*-схему. Кроме того, для каждого веса* w, *где* $e \leqslant w \leqslant \min\{n-t, w_0\}$, *подмножества множества* S, *которые поддерживают кодовые слова веса* w *в* $A^\perp$, *образуют* t*-схему.*

Доказательство. В доказательстве используются следующие обозначения. $A^\perp$ обозначим через B; если T — фиксированное t-подмножество множества S, а C есть некоторый код, то через C' обозначим код, получаемый удалением координат T из кодовых слов C. Обозначим через C_0 подкод кода C, который состоит из тех слов C, которые имеют нули на всех позициях T. Доказательство состоит из 6 шагов.

1) По определению v_0 два слова из A с весом $\leqslant v_0$, которые поддерживаются одним и тем же множеством, должны быть скалярно кратными друг другу (поскольку имеется линейная комбинация этих двух слов с весом $<d$). Аналогичное утверждение выполняется и для B.

2) Будем использовать следующее свойство t-схем. Пусть $(S, \mathscr{D})$ — это t-схема и пусть T — это t-подмножество множества S. Обозначим через α_k число блоков D из $\mathscr{D}$, для которых $|D \cap T| = k$. Тогда, согласно формуле (1.1), имеем

$$\sum_{k=0}^{t} \binom{k}{j} \alpha_k = \binom{t}{j} \lambda_j \qquad (j=0, 1, \ldots, t).$$

Решая эти уравнения, находим, что α_k не зависит от выбора множества T. Из этого утверждения при $k=0$ следует, что дополнения блоков $\mathscr{D}$ также образуют t-схему.

3) Рассмотрим любые $d-1$ столбцов порождающей матрицы кода A, и удалим их. Из определения d следует, что полученная матрица имеет ранг k.

4) Рассмотрим произвольное t-подмножество T множества S. Согласно 3) A' образует $(n-t, k)$-код. Ясно, что $(B_0)' \subset (A')^{\perp}$. Размерность B_0' есть по крайней мере $n-k-t$. Следовательно, $B_0' = (A')^{\perp}$. Пусть $0 < v_1 < v_2 < \ldots < v_r \leqslant n-t$ (где $r \leqslant d-t$) — возможные ненулевые веса, меньше или равные $n-t$ в коде B. Тогда лишь они являются возможными ненулевыми весами для B_0'. Поскольку минимальный вес A' есть по крайней мере $d-t$, то мы знаем $d-t$ коэффициентов весового энумератора для A'. Это равно числу коэффициентов весового энумератора для B_0', которого мы еще не знаем. Соотношения Мак-Вильямс, т. е. теорема 7.14, приводят к системе линейных независимых уравнений, которую мы можем, в принципе, решить. Важно, однако, что это решение, т. е. весовой энумератор для B_0', не зависит от выбора T. Так как $A' = (B_0')^{\perp}$, то то же самое верно и для A', опять-таки по теореме 7.14.

5) Вначале докажем второе утверждение теоремы. Пусть $w \leqslant \min\{n-t, w_0\}$. Пусть $\mathscr{E}$ — это совокупность w-подмножеств множества S, которые поддерживают слова веса w в B. Рассмотрим множество $\mathscr{E}'$ дополнений множеств в $\mathscr{E}$. Для всякого t-подмножества T из S из 1) находим, что число множеств из $\mathscr{E}'$, содержащих T, равно $1/(q-1)$ раз взятое число слов веса w в B_0'. Согласно 4) это число не зависит от T. Следовательно, $\mathscr{E}'$ есть t-схема. Согласно 2), $\mathscr{E}$ есть также t-схема.

6) Для доказательства первого утверждения начнем со случая $v = d$. Пусть $\mathscr{D}$ — совокупность v-подмножеств из S, которые поддерживают слова веса v в A. Тем же способом, как в 5), получаем, что число множеств в $\mathscr{D}$, содержащих данное t-подмножество T из S, есть $1/(q-1)$ раз взятое число слов веса $d-t$ в A'. Согласно 4), это число не зависит от T. Теперь применим индукцию. Пусть $d \leqslant v \leqslant v_0$ и пусть утверждение теоремы выполнено для всех v', $d \leqslant v' < v$. Пусть $\mathscr{D}$ то же, что и ранее. Число подмножеств из $\mathscr{D}$, содержащих данное t-подмножество T из S, есть $1/(q-1)$ раз взятое число слов $v-t$ в A', соответствующим словам веса v в A. Согласно 4) полное число слов веса $v-t$ в A' не зависит от T. По предположению индукции и 2) это число слов веса $v-t$

в A', соответствующих словам веса $<v$ в A также не зависит от T. Следовательно, $\mathscr{D}$ есть t-схема.

Рассмотрим несколько примеров этой теоремы.

Пример 12.14. Положим $n=8$, $k=4$, $q=2$ и пусть $A=A^{\perp}$ — это расширенный $(8, 4)$-код Хэмминга. Тогда $d=e=4$. Положим $t=3$. Условие теоремы 12.13 выполнено. Полагая $v=4$, получаем результат теоремы 7.12.

Пример 12.15. Положим $n=12$, $k=6$, $q=3$ и пусть $A=A^{\perp}$ — расширенный тернарный код Галея. Тогда $d=e=6$ (см. (11.4)). Согласно (11.4), условие теоремы 12.13 выполнено для $t=5$. Получаем результат теоремы 11.5.

Пример 12.16. Пусть A — это $(12l, 6l)$-самодвойственный код над $GF(3)$. Предположим, что $d>3l$. Положим $t=5$. Поскольку все веса в A делятся на 3, то условие нашей теоремы выполнено. Полагая $v=d$, находим, что поддержки слов минимального веса в A образуют 5-схему.

Пример 12.17. Положим $n=24$, $k=12$, $q=2$ и пусть $A=A^{\perp}$ — это расширенный бинарный код Галея $\bar{C}$ из примера 12.12. Тогда $d=e=8$. Так как C совершенен, то весовой энумератор определен. Легко проверить, что лишь 0, 8, 12, 16 и 24 наличествуют в качестве весов. Следовательно, можно вновь применить нашу теорему с $t=5$. Поддержки кодовых слов веса 8 в A образуют хорошо известную 5-$(24, 8, 1)$ штейнерову систему (см. главу 1).

Пример 12.18. Пусть $n=47$. Рассмотрим бинарный КВ-код длины 47. Согласно теореме 12.11, минимальное расстояние есть по крайней мере 9. Тогда из п. 3 теоремы 12.7 следует, что минимальное расстояние есть по крайней мере 11. Поскольку $|S(x, 6)|>2^{23}$, этот код не может быть 6-кодом, исправляющим ошибки. Поэтому минимальное расстояние равно 11. Следовательно, расширенный код $\bar{C}$ имеет минимальное расстояние $d=12$ и вновь является самодвойственным. Можно вычислить весовой энумератор этого кода, используя теорему 7.14. В нем имеются лишь веса 0, 12, 16, 20, 24, 28, 32, 36 и 48. Поэтому теорема 12.13 применима при $t=5$. Можно положить $v=12$, 16, 20 или 24. Это дает 4 различных 5-схем. Если положить $v=28$, 32, 36, получим дополнительные схемы.

Эти примеры объясняют интерес (с точки зрения специалистов по схемам) к вычислению минимального веса КВ-кодов. Весьма мало известно в этой области, обзор для $n \leqslant 59$ можно найти в [4].

Остается за рамками нашего курса вхождение в метод изучения КВ-кодов, который представляется весьма обнадеживающим. Его идея состоит в *стягивании* самоортогональных кодов. Эта идея заключается в использовании некоторого элемента группы автоморфизмов самоортогонального кода для отображения этого кода в код меньшей длины, который все же самоортогонален. Этот метод был успешно использован Ассмусом и Мэттсоном для определения минимального веса $(6, 0, 36)$-расширенного КВ-кода над $GF(3)$ (см. [5]). Этот минимальный вес оказался равным 18. Это означает, что условие теоремы 12.13 выполнено при $t = 5$. В итоге этот КВ-код приводит к 5-схемам на 30 точках.

Приведем еще один пример применения теоремы 12.13, который пригодится нам позже.

Пример 12.19. Рассмотрим примитивный $(2^{2l} - 1, 2^{2l-1} - 1 - 2l) - 2$-код C, исправляющий ошибки. Используя теорему 7.14, можно показать, что в $C^{\perp}$ могут присутствовать лишь веса 2^{2l-2}, $2^{2l-2} \pm 2^{l-1}$. Положим $n = 2^{2l-1}$, $k = 2^{2l-1} - 1 - 2l$, $q = 2$ и пусть A это будет $\bar{C}$. В $A^{\perp}$ присутствует лишь 3 веса. Поэтому, если положить $t = 3$, то условие 12.13 будет выполнено. Значит, для каждого v подмножества, которые поддерживают слова веса v, образуют 3-схему.

Дополнительно по материалу этой главы см. [49], [64], [70], [80]. О связях между квадратично-вычетными кодами и 3-$(n^2 + 1, n + 1, 1)$-схемами см. [76], [79]. *Далее см. Добавление* 15.

13. СИММЕТРИЧНЫЕ КОДЫ НАД $GF(3)$

В этом разделе мы обратимся к последовательности кодов, которые обладают целым рядом свойств общих с КВ-кодами; так например, они также приводят к 5-схемам. Эти результаты принадлежат Плесс [53, 54].

Определение 13.1. *С-матрица* порядка m есть матрица C с элементами ± 1 (вне диагонали) и 0 (на диагонали) такая, что $CC^T = (m - 1)I_m$.

Об этих матрицах известно многое. Первая конструкция представляет собой хорошо известную конструкцию Пэли:

Пусть q — степень нечетного простого и пусть χ — квадратичный характер на $GF(q)$. Занумеруем строки и столбцы матрицы порядка $q+1$, используя координаты проективной прямой порядка q, т. е. ∞ и элементы $GF(q)$. Определяем C_{q+1} по правилу

$$c_{\infty,\infty}=0, \quad c_{\infty,a}=1, \quad c_{a,\infty}=\chi(-1),$$
$$c_{a,b}=\chi(b-a) \qquad (a,\ b\in GF(q)).$$

Тогда C_{q+1} является C-матрицей порядка $q+1$ (см. [38]). Заметим, что $C_{q+1}C_{q+1}^T=-I_{q+1}$ над $GF(3)$, если $q\equiv -1 \pmod 3$, и что C_{q+1} симметрична, если $q\equiv 1 \pmod 4$ и кососимметрична, если $q\equiv -1 \pmod 4$.

Определение 13.2. Пусть $q\equiv -1 \pmod 6$. Определим *симметричный код* размерности $q+1$ как $(2q+2, q+1)$-код sym_{2q+2} над $GF(3)$ с порождающей матрицей

$$G_{2q+2}=(I_{q+1}C_{q+1}),$$

где C_{q+1} есть C-матрица порядка $q+1$. Если q — степень нечетного простого, то полагаем, что C_{q+1} — матрица Пэли, определенная выше.

Докажем ряд свойств этих кодов.

Предложение 13.3. *Код* sym_{2q+2} *самодвойствен* (*и следовательно, все веса делятся на* 3).

Доказательство. Это следует из равенства

$$C_{q+1}C_{q+1}^T=-I_{q+1} \text{ над } GF(3).$$

Предложение 13.4. *Если матрица* C_{q+1} *— матрица Пэли, то* $G_{2q+2}^*=((-1)^{(q+1)/2}C_{q+1}I_{q+1})$ *также является порождающей матрицей для* sym_{2q+2}.

Доказательство. $G_{2q+2}G_{2q+2}^{*T}=0$, код sym_{2q+2} является самодвойственным и матрица G_{2q+2}^* имеет ранг $q+1$.

Предложение 13.5. *Линейное преобразование пространства* $\mathcal{R}^{(2q+2)}$ *посредством матрицы*

$$\begin{bmatrix} 0 & I_{q+1} \\ (-1)^{(q+1)/2}I_{q+1} & 0 \end{bmatrix}$$

оставляет sym_{2q+2} *инвариантным.*

Доказательство. Это следует из теоремы 13.4.

Пример 13.6. Полагая $q = 5$, находим

$$G_{12} = \left[\begin{array}{c|cccccc} & 0 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 1 & -1 & -1 & 1 \\ & 1 & 1 & 0 & 1 & -1 & -1 \\ I_6 & 1 & -1 & 1 & 0 & 1 & -1 \\ & 1 & -1 & -1 & 1 & 0 & 1 \\ & 1 & 1 & -1 & -1 & 1 & 0 \end{array}\right],$$

т. е. sym_{12} есть расширенный тернарный код Галея (см. (11.1)).

Замечание. В случае бинарного кода Галея также можно найти порождающую матрицу в форме, указанной в определении 13.2 (см. [44] с. 101).

При описании кодовых слов симметричного кода будем обозначать через $w_l(x)$, $w_r(x)$ соответственно сужение веса слова x на первые $q+1$ и на последние $q+1$ координат.

Лемма 13.7. *Для каждого слова x симметричного кода имеем*:

1) *если* $w_l(x) = 1$, *то* $w_r(x) = q$;
2) *если* $w_l(x) = 2$, *то* $w_r(x) = (q+3)/2$;
3) *если* $w_l(x) = 3$, *то* $w_r(x) = [3(q-3)/4]$.

Доказательство. Рассмотрим три строки порождающей матрицы. Поскольку умножение столбца на -1 не изменяет весов, можно предполагать, что x в 1), 2), 3) есть сумма 1, 2 или 3 строк следующей таблицы:

$$\left[\begin{array}{c|c|c|c|c|c} & & & \overbrace{}^{a} & \overbrace{}^{b} & \overbrace{}^{c} \quad \overbrace{}^{d} \\ 1000\ldots0 & 0 \;+\; + & + + \ldots + & + + \ldots + & + + \ldots + & + + \ldots + \\ 0100\ldots0 & x_{21}\; 0\; x_{23} & + + \ldots + & + + \ldots + & + - \ldots - & - - \ldots - \\ 1010\ldots0 & x_{31}\; x_{32}\; 0 & + + \ldots + & - - \ldots - & + + \ldots + & - - \ldots - \end{array}\right]$$

Буквы a, b, c, d обозначают число столбцов четырех различных типов.

По определению C-матрицы имеем (над $\mathbb{R}$)

$$\begin{aligned} a + b + c + d &= q - 2, \\ a + b - c - d &= -x_{23}, \\ a - b + c - d &= -x_{32}, \\ a - b - c + d &= -x_{21}x_{31}. \end{aligned}$$

Теперь 1) очевидно. Для доказательства 2) сложим первую и вторую строки. Тогда находим $w_r(x) = 2 +$

$+\frac{1}{2}(1+x_{23})+a+b=\frac{1}{2}(q+3)$. Теперь сложим все три строки. Тогда $w_r(x)\geqslant b+c+d=\frac{1}{4}\{3(q-2)+$ $+x_{23}+x_{32}+x_{21}x_{31}\}\geqslant\frac{3}{4}(q-3)$.

Лемма 13.8. *Пусть w_1 и w_2 — целые. Тогда в симметричном коде*:

1) *кодовое слово x с $w_l(x)=w_1$, $w_r(x)=w_2$ существует тогда и только тогда, когда существует кодовое слово y с $w_l(y)=w_2$, $w_r(y)=w_1$;*

2) *для всех кодовых слов x имеем $w_r(x)>0$.*

Доказательство. 1) Это следует из предложения 13.4; 2) C_{q+1} несингулярна.

Пример 13.9. Пусть $q=17$; рассмотрим sym_{36}. Согласно лемме 13.7 кодовое слово x с $w_l(x)\leqslant 3$ имеет вес $\geqslant 12$. Согласно предложению 13.3 все веса делятся на 3. Согласно лемме 13.8 существование кодового слова с весом <12 влечет существование кодового слова x с $w_l(x)=4$, $w_r(x)=5$. Так как C_{18} является граничной циркулянтной матрицей, то имеется не очень много различных возможностей для такого x, и вручную легко проверить, что такого x не существует. Это получается добавлением еще одной строки к таблице в доказательстве леммы 13.7 и анализом небольшого числа возможных вариантов. С компьютером это тривиальная задача. Итак, согласно п. 2) леммы 13.7, код sym_{36} имеет минимальный вес 12. Применим теперь теорему 12.13. Здесь $n=36$, $k=18$, $q=3$, $d=e=12$, $v_0=w_0=23$. Значит, можно положить $v=12$, 15, 18 или 21. Если $t=5$, то условия теоремы выполнены и мы находим 5-схему на 36 точках с блоками объемов 12, 15, 18 или 21. Схемы эти являются новыми, как и им дополнительные (с одним возможным исключением). Неизвестно, является ли схема с блоками объема 18 самодополнительной.

В [54] приведены примеры для $q=5$, 11, 17, 23 и 29. Конечно, случай $q=5$ приводит к хорошо известной штейнеровой системе 5-(12, 6, 1), как показано в теореме 11.5. Другие схемы являются новыми. Чтобы показать это, нужно изучить преобразования, оставляющие такие коды инвариантными. Пусть $G(q)$ обозначает группу мономиальных преоб-

разований, которые оставляют sym_{2q+2} инвариантными, а $\bar{G}(q)$ — группу перестановок, индуцированную группой $G(q)$.

Лемма 13.10. *Если A и B — мономиальные преобразования порядка $q+1$ такие, что $A^{-1}C_{q+1}B = C_{q+1}$, то* $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \in G(q)$.

Доказательство. Кодовые слова в sym_{2q+2} имеют форму $\boldsymbol{a}^T(I_{q+1}C_{q+1})$. Значит,

$$\boldsymbol{a}^T(I_{q+1}C_{q+1})\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = \boldsymbol{a}^T A(I_{q+1}A^{-1}C_{q+1}B),$$

что является кодовым словом.

Пусть q — степень нечетного простого. Мы определили C_{q+1} нумерацией строк и столбцов координатами проективной прямой. Мы упорядочиваем их так же, как для циклических кодов. Определим теперь мономиальные преобразования таким же образом, как это было сделано (в главе 12) в бинарном случае для КВ-кодов. S есть перестановка $x \to x+1$. Рассмотрим C_{q+1} и S как линейные преобразования пространства $\mathscr{R}^{(q+1)}$ над $GF(3)$. Для стандартных базисных векторов e_∞, e_a $(a \in GF(q))$ имеем

$$e_\infty C_{q+1} = \sum_{a \in GF(q)} e_a,$$

$$e_a C_{q+1} = \chi(-1)e_\infty + \sum_{b \in GF(q)} \chi(b-a)e_b,$$

откуда $e_\infty C_{q+1}S = e_\infty S C_{q+1}$ и

$$e_a C_{p+1}S = \chi(-1)e_\infty + \sum_{b \in GF(q)} \chi(b-a)e_{b+1} =$$

$$= \chi(-1)e_\infty + \sum_{b \in GF(q)} \chi(b-a-1)e_b = e_a S C_{q+1},$$

т. е.

$$S^{-1}C_{q+1}S = C_{q+1}. \qquad (13.11)$$

Аналогично, для перестановки $P(b^2)$ вида $x \to b^2x$ $(b \neq 0)$ можно показать, что

$$P(b^2)^{-1}C_{q+1}P(b^2) = C_{q+1}. \qquad (13.12)$$

Перестановка $Tx = x^{-1}$, которая использовалась для КВ-кодов заменяется теперь на мономиальное преоб-

разование T^*, которое ведет себя так же, как T, когда оно рассматривается только как перестановка. Определяем это T^* по правилу $e_\infty T^* = (-1)^{(q-1)/2} e_0$, $e_0 T^* = e_\infty$, $e_a T^* = \chi(a) e_{-1/a}$ $(a \neq 0, \infty)$. И вновь нетрудно проверить, что

$$T^{*-1} C_{p+1} T^* = C_{q+1}. \tag{13.13}$$

Из (13.11)—(13.13) видно, что перестановки S, $P(b^2)$ и мономиальное преобразование T^* порождают группу R^*. Легко видеть, что группа $R^*/\{1, -1\}$ изоморфна группе $PSL(2, q)$. Комбинируя это с леммой 13.10, получаем следующую теорему.

Теорема 13.14. *Группа $\bar{G}(q)$ содержит подгруппу, изоморфную группе $PSL(2, q)$.*

Замечание. В [54] показано, что $\bar{G}(q)$ содержит подгруппу, изоморфную $PGL(2, q) \times \mathbf{Z}_2$. Известно, что $\bar{G}(5) = M_{12}$. Для других значений q вид группы $G(q)$ неизвестен.

Пример 13.15. Одно из приложений теоремы 12.13 в [2] использует (24, 12)-расширенный КВ-код над $GF(3)$. Поскольку минимальный вес этого кода равен 9, находится 5-схема с параметрами (24, 9, 6). В [2] показано, что $PSL(2, 23)$ является группой автоморфизмов этой схемы. Если мы рассмотрим простое $q = 11$ и построим соответствующий симметричный код sym_{24}, то мы вновь можем применять теорему 12.13. Это также дает 5-схему. Эти две схемы имеют одинаковые параметры. По теореме 13.14 это неэквивалентные 5-схемы, поскольку $PSL(2, 11)$ не содержится в $PSL(2, 23)$. Для более детального и дальнейшего ознакомления мы рекомендуем читателю [53] и [54]. Метод, применяемый в [54], представляет собой иной пример сужения, которое кратко описано в конце главы 12. Во многих случаях sym_{2q+2} можно сузить к тернарному коду Галея.

14. ПОЧТИ СОВЕРШЕННЫЕ БИНАРНЫЕ КОДЫ И РАВНОМЕРНО УПАКОВАННЫЕ КОДЫ

Две 5-схемы, связанные с кодами Галея, имеют очень интересные группы автоморфизмов. Легко видеть, что совокупность тех $(2e+1)$-подмножеств множества

$\{1, 2, \ldots, n\}$, которые поддерживают кодовые слова веса $2e+1$ в бинарном совершенном e-коде, исправляющем ошибки со словами длины n, образуют $(e+1)$-схему с параметрами $(n, 2e+1, 1)$, т. е. штейнерову систему (см. [44], (5.2.6)). Эта схема расширяема до $(e+2)$-схемы. Эти два факта обусловливают интерес к совершенным кодам как специалистов по теории групп, так и специалистов по теории схем. Однако показано, что для $e > 1$ коды Галея являются нетривиальными совершенными кодами, только если объем алфавита есть степень простого (см. [45, 66])*).

Рассмотрим теперь некоторые элементы теории бинарных почти совершенных кодов, принадлежащей Гётхальсу и Сноверу [31] **). Эти коды являются специальным случаем более широкого класса равномерно упакованных кодов, введенным Семаковым, Зиновьевым и Зайцевым [60]. Все эти коды также приводят к t-схемам. Необходимые условия существования таких кодов очень схожи с аналогичными условиями существования совершенных кодов. В этой главе все коды бинарны.

Далее см. Добавление 16.

Пусть $C \subset \mathscr{R}^{(n)}$ — код с минимальным расстоянием $d = 2t+1$. Для всех кодов $v \in C$ определяем:

1) $T(v) = S(v, t+1) \setminus S(v, t)$;

2) $T_\alpha(v) = \{x \in T(v) \mid \exists u \in C \quad [x \in S(u, t)]\}$;

3) $T_\beta(v) = T(v) \setminus T_\alpha(v)$.

(Заметим, что в 2) кодовое слово u однозначно определяется через x.)

Лемма 14.2. *Для каждого $v \in C$ имеем*

1) $|T_\alpha(v)| \leqslant \binom{n}{t}\left[\frac{n-t}{t+1}\right]$;

2) $|T_\beta(v)| \geqslant \binom{n}{t+1} - \binom{n}{t}\left[\frac{n-t}{t+1}\right]$.

Доказательство. Если $x \in T_\alpha(v)$ и $u \in C$ таковы, что $x \in S(u, t)$, то $d(v, u) \leqslant 2t+1$, т. е.

*) См. также [82°]. (*Прим. перев.*)

**) Большинство результатов этой теории можно найти в [60], где были введены равномерно упакованные коды и выделены коды с максимальной плотностью упаковки, т. е. почти совершенные коды. (*Прим. перев.*)

$d(v, u) = 2t + 1$. Но тогда

$$|T_\alpha(v) \cap S(u, t)| = \binom{2t+1}{t+1}.$$

Пусть $N_{2t+1}(v) = \{u \in C \mid d(v, u) = 2t+1\}$. Тогда $|T_\alpha(v)| = \binom{2t+1}{t+1} |N_{2t+1}(v)|$. Для оценки $|N_{2t+1}(v)|$ заметим, что для двух кодовых слов в $N_{2t+1}(v)$ есть не более t координатных мест, в которых оба они отличаются от v. Для каждого t-подмножества координатных мест это дает не более $\left[\frac{n-t}{t+1}\right]$ элементов множества $N_{2t+1}(v)$. Следовательно,

$$|N_{2t+1}(v)| \leqslant \frac{\left[\frac{n-t}{t+1}\right]\binom{n}{t}}{\binom{2t+1}{t+1}}.$$

Это доказывает 1), после чего 2) очевидно.

Следующая оценка есть специальный случай границы Джонсона [40].

Теорема 14.3. *Если $C \subset \mathscr{R}^{(n)}$ — код с минимальным расстоянием $d = 2t+1$, то*

$$|C|\left\{\sum_{i=0}^{t}\binom{n}{i} + \frac{1}{\left[\frac{n}{t+1}\right]}\binom{n}{t}\left(\frac{n-t}{t+1} - \left[\frac{n-t}{t+1}\right]\right)\right\} \leqslant 2^n.$$

Доказательство. По определению $T_\beta(v)$ видим, что все $S(v, t)$, где $v \in C$ и $\bigcup_{v \in C} T_\beta(v)$, являются попарно непересекающимися множествами. Так как кодовые слова имеют расстояние по крайней мере $2t+1$, то $x \in \mathscr{R}^{(n)}$ может содержаться не более чем в $\left[\frac{n}{t+1}\right]$ различных множествах $T_\beta(v)$, $v \in C$. Следовательно, согласно п. 2) леммы 14.2 имеем

$$\left|\bigcup_{v \in C} T_\beta(v)\right| \geqslant \frac{|C|}{\left[\frac{n}{t+1}\right]}\left\{\binom{n}{t+1} - \binom{n}{t}\left[\frac{n-t}{t+1}\right]\right\}.$$

Это и завершает доказательство, поскольку $|\mathscr{R}^{(n)}| = 2^n$ и $|S(v, t)| = \sum_{i=0}^{t}\binom{n}{i}$.

Определение 14.4. Бинарные коды, для которых в теореме 14.3 выполняется равенство, называются *почти совершенными.*

Замечание. Если $(t+1) \mid (n+1)$, то почти совершенный код с этими параметрами оказывается совершенным. Это условие делимости представляет собой известное необходимое условие существования бинарных совершенных кодов (см. [44], (5.2.8)).

Определение 14.5 *). Если $C \subset \mathscr{R}^{(n)}$ — код с минимальным расстоянием $d = 2t+1$ и если для каждого кодового слова из $\mathscr{R}^{(n)}$, отстоящего от кода C на расстоянии, большем чем $t-1$, имеется ровно r кодовых слов на расстоянии, меньшем чем $t+2$, то код C называется *равномерно упакованным.*

Связь этих двух подходов устанавливается следующей теоремой.

(Всюду далее C обозначает почти совершенный код в $\mathscr{R}^{(n)}$ с минимальным расстоянием $d = 2t+1$.)

Теорема 14.6. 1) *Если* $x \in \mathscr{R}^{(n)}$ *и если* $\forall v \in C$ $[d(v, x) > t]$, *то* $d(v, x) = t+1$ *ровно для* $\left[\frac{n}{t+1}\right]$ *кодовых слов* v.

2) *Если* $x \in \mathscr{R}^{(n)}$, $u \in C$ *и* $d(u, x) = t$, *то* $d(v, x) = t+1$ *ровно для* $\left[\frac{n-t}{t+1}\right]$ *кодовых слов* v.

Доказательство. Из равенства в теореме 14.3 следует равенство в лемме 14.2 и в оценках для $|N_{2t+1}(v)|$ и $\bigcup_{v \in C} T_\beta(v)$, последняя из которых влечет 1), а первая — 2).

Замечание. Эти определения и теоремы 14.3, 14.6 показывают, что равномерно упакованный код с $r = [(n+1)/(t+1)]$ является почти совершенным. Если $r = 1$ или $r = (n+1)/(t+1)$, то равномерно упакованный код совершенен. В основном, мы будем иметь дело именно с почти совершенными кодами и лишь кратко рассмотрим один пример иных равномерно упакованных кодов (см. пример 14.21).

Теорема 14.7. *Если* $v \in C$, *то совокупность* $\mathscr{D}_1$ *из d-подмножеств множества* $\{1, 2, \ldots, n\}$, *которые поддерживают слова* $u - v$, *где* $u \in N_d(v)$, *образует t-схему с параметрами* $(n, d, \lambda = [(n-t)/(t+1)])$.

*) *Параллельное определение см. в Добавлении* 17.

Доказательство. Пусть A — t-подмножество координатных мест и пусть a — слово с единицами на позициях A. По п. 2) теоремы 14.6 имеется $[(n-t)/(t+1)]$ кодовых слов u в $N_d(v)$ таких, что $d(u, v+a)=t+1$, т. е. таких, что A содержится в множестве координатных мест, где $u-v$ имеет координату 1.

Теорема 14.8. *Если $v \in C$, то совокупность $\mathscr{D}_2$ из $(t+1)$-подмножеств множества $\{1, 2, \ldots, n\}$, которые поддерживают слова $u-v$, где $u \in T_\beta(v)$, образует t-схему с $\lambda=(n-t)-(t+1)[(n-t)/(t+1)]$.*

Доказательство. $T_\beta(v)$ состоит из векторов u таких, что $d(u, v)=t+1$ и $d(u, w)>1$ для всех $w \in N_d(v)$. Следовательно, $\mathscr{D}_2$ содержит все $(t+1)$-подмножества из $\{1, 2, \ldots, n\}$, которые не содержатся в подмножестве, принадлежащем схеме $\mathscr{D}_1$. Эти $(t+1)$-подмножества блоков образуют t-схему. Очевидно, $\mathscr{D}_2$ является t-схемой, образованной всеми $(t+1)$-подмножествами множества $\{1, 2, \ldots, n\}$.

Теорема 14.9. *Схема $\mathscr{D}_1$ расширяема до $(t+1)$-схемы с параметрами $(n+1, d+1, \lambda=[(n-t)/(t+1)])$.*

Доказательство. Рассмотрим $\bar{C}$ и удалим k-ю координату каждого слова (k фиксировано). Результирующий код C_k вновь имеет слово длины n, минимальное расстояние d и $|C_k|=|C|$. Стало быть, C_k почти совершенен. Поскольку это верно при каждом k, то из теоремы 14.7 следует, что совокупность $(d+1)$-подмножеств множества $\{1, 2, \ldots, n, n+1\}$, которые поддерживают слова $u-v$, где $u \in \bar{C}$, $v \in \bar{C}$, $u \in N_{d+1}(v)$, образует $(t+1)$-схему с тем же λ, как и в теореме 14.7.

До сих пор пессимистически настроенные специалисты по теории схем задают себе вопрос, существуют ли произвольные почти совершенные коды.

Пример 14.10. Рассмотрим проверочную матрицу бинарного кода Хэмминга (см. главу 7) и удалим какой-нибудь столбец. Получаем проверочную матрицу линейного кода с $d=3$, $n=2^m-2$ и размерностью 2^m-2-m. В теореме 14.3 мы имеем равенство, т. е. этот код почти совершенен, но не совершенен.

Коды Препараты (см. [55]). Введем теперь последовательность кодов, представляющих большой

комбинаторный интерес. Необходима некоторая подготовка. Пусть $m \geqslant 3$ и H_m — циклический код Хэмминга с длиной слова $n = 2^m - 1$, такой же, как в примере 12.3. Слово 1 рассматривается как многочлен в $GF(2)[x] \pmod{(x^n - 1)}$ вида $u(x) = (x^n - 1)/(x - 1)$. Пусть B_m — циклический код с порождающим многочленом $(x - 1) m_1(x) m_3(x)$. Этот БЧХ-код является подкодом кода H_m и, согласно замечанию после теоремы 8.6, видим, что этот код имеет минимальное расстояние, равное по крайней мере 6.

Определяем код C_m по правилу:

$$C_m = \{(m(x),\ i,\ m(x) + (m(1) + i)\, u(x) + s(x)) \mid m(x) \in H_m,\ i \in \{0, 1\},\ s(x) \in B_m\}. \quad (14.11)$$

Это, очевидно, линейный код с длиной слова $2n + 1$ и размерностью, равной $H_m + 1 + \dim B_m = 2n - 3m$.

Докажем теперь следующую лемму:

Лемма 14.12. *Код C_m имеет минимальное расстояние* $\geqslant 5$.

Доказательство. Поскольку код линеен, можем рассматривать веса.

1) Пусть $m(x) = 0$, $i = 0$, $s(x) \neq 0$. Тогда $w(s(x) \geqslant 6$, потому что $s(x) \in B_m$.

2) Пусть $m(x) = 0$, $i = 1$. Тогда $u(x) + s(x) \neq 0$, $u(\alpha) + s(\alpha) = u(\alpha^3) + s(\alpha^3) = 0$, и следовательно, $w(u(x) + s(x)) \geqslant 5$ по теореме 8.6.

3) $m(x) \neq 0$. Поскольку $m(x) + (m(1) + i)\, u(x) + s(x) \in H_m$, то доказательство завершено, если только не выполняется $m(x) + (m(1) + i)\, u(x) + s(x) = 0$. В этом случае, пользуясь заменой $x = \alpha^3$, находим, что $m(\alpha^3) = 0$, т. е. $w(m(x)) \geqslant 5$.

Рассмотрим теперь $S(0, 1)$ в полиномиальной форме, т. е.

$$S(0,\ 1) = \{0,\ 1, x, x^2, \ldots, x^{n-1}\} \subset GF(2)[x] \pmod{(x^n - 1)}$$

В $\mathscr{R}^{(2n+1)}$ рассмотрим множество векторов

$$\hat{S} = \{(q(x),\ 0,\ q(x) f(x)) \mid g(x) \in S(0,\ 1)\}, \quad (14.3)$$

где $f(x)$ — идемпотент кода H_m^*, определенного в примере 12.3.

Определение 14.14. *Код Препараты K_m* есть объединение комножеств C_m вида $C_m + \hat{S}$.

Очевидно, что нет двух элементов из $\hat{S}$, входящих в одно комножество. Поэтому $|K_m| = (n+1)|C_m|$.

Теорема 14.15. *Для нечетного m код Препараты K_m является почти совершенным кодом с минимальным расстоянием* 5.

Доказательство. 1) Так как код K_m нелинеен, мы должны рассматривать пары слов из K_m и определять вес их суммы. По лемме 14.12 для этого достаточно рассматривать слова из разных комножеств. Такая сумма имеет вид

$$(m(x),\ i,\ m(x)+(m(1)+i)u(x)+s(x))+$$
$$+(q_1(x)+q_2(x),\ 0,\ (q_1(x)+q_2(x))f(x)). \quad (14.16)$$

Поскольку H_m — совершенный код, то имеется единственный элемент $x^s \in S(0,1)$ такой, что

$$m'(x) = q_1(x) + q_2(x) + x^s \in H_m.$$

Заметим, что $m'(x)=0$, если $q_1(x)=0$ или $q_2(x)=0$. Положим

$$m''(x) = x^s(1+f(x)) + m'(x) + m'(1)u(x).$$

Кроме того, $m''(x) \in H_m$ (см. пример 12.3). Поскольку все многочлены рассматриваются по $\mathrm{mod}(x^n-1)$, имеем, что $m'(x)f(x)=0$. Заменим $m(x)+m'(x)$ на $m(x)$ и перепишем (14.16) так:

$$(m(x),\ i,\ m(x)+(m(1)+i)u(x)+s(x))+$$
$$+(x^s,\ 0,\ x^s)+(0,\ 0,\ m''(x)). \quad (14.17)$$

2) Из (14.17) находим, что вес W, который мы хотим определить, есть

$$W = w(m(x)+x^s)+i+w(m(x)+$$
$$+(m(1)+i)u(x)+s(x)+x^s+m''(x)). \quad (14.18)$$

3) Если $m'(x)\neq 0$, то $m'(x)$ имеет форму $x^s + x^j + x^k$ и, по определению, $m'(\alpha)=0$. Это влечет, что $m'(\alpha^3)=\alpha^{3s}(\alpha^h+\alpha^{2h})$, где $h=j-s\neq 0$. Если же $m'(x)=0$, то $m'(\alpha^3)$ можно также записать как $\alpha^{3s}(\alpha^h+\alpha^{2h})$, где $h=0$.

4) Поскольку m нечетно, то уравнение $\alpha^{3h}=1$ имеет $h=0$ как единственное решение ($\alpha^h \in GF(2^m)$). Отсюда $1+\alpha^h+\alpha^{2h}\neq 0$ для всех h. Следовательно, $m''(\alpha^3)=\alpha^{3s}+m'(\alpha^3)=\alpha^{3s}(1+\alpha^h+\alpha^{2h})\neq 0$.

5) Пусть $\varphi(x)$ — некоторое слово с $\varphi(1)=0$, $\varphi(\alpha)=\alpha^s$, $\varphi(\alpha^3)=\alpha^{3s}(\alpha^h+\alpha^{2h})$ для некоторого h. Тогда $\varphi(x)$ имеет вес по крайней мере 4. Для доказательства этого, во-первых, заметим, что $\varphi(x)$, очевидно, не 0 и что оно имеет четный вес. Если бы $\varphi(x)$ имело вес 2, то это влекло бы наличие двух элементов x_1 и x_2 в $GF(2^m)$ таких, что $x_1+x_2=\alpha^s$ и $x_1^3+x_2^3=\alpha^{3s}(\alpha^h+\alpha^{2h})$. Из этого находим, что и $\alpha^{-s}x_1+\alpha^h$ и $\alpha^{-s}x_2+\alpha^h$ являются решениями уравнения $1+\xi+\xi^2=0$. Но мы показали выше, что это уравнение не имеет решений в $GF(2^m)$ при нечетном m.

6) Пусть $s(x)\in B_m$. Определим $s'(x)=m''(x)+x^s+s(x)$. Тогда в 5) можно положить $\varphi(x)=s'(x)$, откуда

$$w(s'(x))\geqslant 4. \tag{14.19}$$

В заключительной части нашего доказательства мы рассматриваем 5 различных возможных форм выражения (14.17).

7) Пусть $m(1)=0$, $i=1$. Согласно (14.18) имеем

$$W\geqslant 1+w(s''(x)),$$

где $s''(x)=u(x)+s(x)+m''(x)$. Поскольку $s''(1)=s''(\alpha)=0$ и $s''(\alpha^3)\neq 0$ согласно 4), то из теоремы 8.6 находим, что $w(s''(x))\geqslant 4$.

8) Пусть $m(1)=0$, $i=0$, $m(x)\neq 0$. Тогда по теореме 8.6 имеем, что $w(m(x))\geqslant 4$. Значит, (14.18) влечет:

$$W\geqslant w(m(x))+w(m(x)+m''(x)+s(x))-2\geqslant$$
$$\geqslant 4+3-2=5;$$

вновь используется теорема 8.6 и тот факт, что $m(1)+m''(1)+s(1)=1$ и $m(\alpha)+m''(\alpha)+s(\alpha)=0$.

9) Пусть $m(x)=0$, $i=0$. Тогда из (14.18) и (14.19) находим:

$$W\geqslant 1+w(s'(x))\geqslant 5.$$

10) Пусть $m(1)=1$, $i=0$. Пусть $\varphi(x)=m(x)+u(x)+s'(x)$. Тогда $\varphi(x)\neq 0$. Из (14.18) получаем:

$$W\geqslant w(m(x)+x^s)+w(\varphi(x)).$$

По теореме 8.6 $w(m(x)+x^s)\geqslant 4$, если только $m(x)$ — не трехчлен. В этом случае $\varphi(x)$ удовлетворяет усло-

виям 5) и, следовательно, $w(\varphi(x)) \geqslant 4$. Значит, в обоих случаях $W \geqslant 5$.

11) Пусть $m = 1$, $i = 1$. Из (14.18) находим:

$$W \geqslant w(m(x) + x^s) + 1 + w(m(x) + s'(x)).$$

Если $m(x)$ не трехчлен, то завершаем доказательство так же, как в 10). Если же $m(x)$ — трехчлен, скажем, $m(x) = x^s + x^c + x^d$, то в этом случае $m(1) + s'(1) = 0$, и, следовательно, из $w < 5$ следовало бы, что $s'(x) = x^s + x^c + x^d + x^e$, т. е. $m(x) + m''(x) + s(x) = x^s + x^e \notin H_{m'}$ — противоречие.

Пункты 7)—11) доказывают, что K_m имеет минимальное расстояние 5.

12) Мы уже видели, что $|K_m| = 2^m 2^{2n-3m} = 2^{2n-2m}$. Длина слова равна $2n + 1$ и $d = 2t + 1 = 5$. Если m нечетно, то

$$|K_m| \left\{ 1 + \binom{2n+1}{1} + \binom{2n+1}{2} + \right.$$
$$\left. + \frac{3}{2n+1} \binom{2n+1}{2} \binom{2n-1}{3} - \left[\frac{2n-1}{3} \right] \right\} = 2^{2n+1},$$

т. е. в теореме 14.3 имеет место равенство.

Пример 14.20. Пусть $m = 2k + 1$. Рассмотрим расширенный код Препараты $\bar{K}_m$, который имеет длину слова 4^k. По теореме 14.9 слова веса 6 в этом коде образуют 3-схему с параметрами $(4^k, 6, (4^k - 4)/3)$. В качестве упражнения читателю предлагается рассмотреть случай $k = 2$, используя пример, следующий за теоремой 8.4, и пример 12.3. В этом случае B_m состоит лишь из 0 и C_m имеет минимальное расстояние 7. В силу цикличности определения должно рассматривать комножество C_m, задаваемое порождающим многочленом $q(x) = 1$ в (14.13). Это комножество имеет 6 слов веса 5 и 10 слов веса 6. В расширенном коде эти слова порождают 16 слов веса 6, образующих 2-схему, соответствующую матрице Адамара порядка 16. Это та же самая схема, что приведена после теоремы 5.1 и еще раз в теореме 6.6. 112 блоков этой 3-схемы получаются одновременными циклическими сдвигами позиций от 0 до 6 и от 8 до 14 в предположении, что общая проверка на четность расположена на 15-й позиции. Блоки этой схемы могут быть рассмотрены как 112 слов веса 6 и длины 6 с взаимными расстояниями по крайней мере 6.

Показано, что такой код не может иметь более чем 112 слов и 112 может быть реализовано лишь блоками 3-схемы.

В [33*, 81] показано, что кодами из (14.10) и (14.15) являются только почти совершенные коды. В действительности в [81] показано, что при $e \geqslant 4$ не существует нетривиального равномерно упакованного кода. При меньших значениях e имеется много интересных примеров (таких, как G_{24}). Во-первых, дадим пример равномерно упакованного кода.

Равномерно упакованные коды также приводят к t-схемам (см. [60]). Примеры равномерно упакованных кодов и некоторые результаты несуществования см. в [45]. Все q-арные равномерно упакованные коды с $e \geqslant 4$ и все бинарные равномерно упакованные коды известны см. [81].

Пример 14.21. Пусть C — это 2-исправляющий ошибки БЧХ-код из примера 12.19. Поддержки кодовых слов веса 6 в расширенном коде $\bar{C}$ образуют 3-схему. Следовательно, что каждое слово веса 2 или 3 имеет расстояние 2 или 3 от 0 и λ кодовых слов C (где λ — параметр этой 3-схемы). Следовательно, C есть равномерно упакованный код с $\beta = \lambda + 1$, $\alpha = \lambda$.

Дополнительно см. [78]. *Далее см. Добавление* 18.

15. АССОЦИАТИВНЫЕ СХЕМЫ (СХЕМЫ ОТНОШЕНИЙ)

Помимо краткого ознакомления с теорией ассоциативных схем, эта последняя глава содержит очерк части диссертации П. Дельсарта, в которой многие понятия классической теории кодирования и теории схем обобщены на классы ассоциативных схем. За доказательствами мы отсылаем читателя к [21].

Ассоциативные схемы были введены Боузом и Шимамото [13] как обобщение сильно регулярных графов. *Ассоциативная схема* состоит из множества X вместе с разбиением множества 2-элементных подмножеств этого X на n классов $\Gamma_1, \ldots, \Gamma_n$, удовлетворяющих условиям:

1) для $p \in X$ число n_i тех $q \in X$, для которых $\{p, q\} \in \Gamma_i$, зависит только от i;

2) для данных $p, q \in X$, $\{p, q\} \in \Gamma_k$, число a_{ijk} тех $r \in X$, для которых $\{p, r\} \in \Gamma_i$, $\{q, r\} \in \Gamma_j$, зависит только от i, j, k.

Удобно взять n «цветов» $c_1, \ldots, c_n$ и красить ребро полного графа на множестве вершин X в цвет c_i, если это ребро принадлежит Γ_i; так что Γ_i — это подграф цвета c_i. Первое условие утверждает: каждый граф Γ_i регулярен; второе: число треугольников с данной раскраской на данном основании зависит лишь от раскраски, а не от основания. Взаимодополняющая пара сильно регулярных графов образует ассоциативную схему из двух классов и обратно.

Имеется два важных класса ассоциативных схем, которые Дельсарт называет схемами Хэмминга и Джонсона; они обобщают соответственно квадратную решетку и триангуляционные графы. В схеме Хэмминга $H(n, q)$ множество X есть множество упорядоченных n-строк из элементов множества мощности q (на практике это часто конечное поле, но здесь это несущественно), а Γ_i — это множество пар n-строк, которые совпадают на $n - i$ координатных местах, где $1 \leqslant i \leqslant n$. В схеме Джонсона $J(v, k)$ с $k \leqslant v/2$ множество X есть множество k-подмножеств v-множества, а Γ_i — это множество пар k-подмножеств, пересечение которых есть $(k - i)$-подмножество, где $1 \leqslant i \leqslant k = n$. Схемы Хэмминга составляют расширение теории кодов, исправляющих ошибки, а схемы Джонсона можно рассматривать как некоторое расширение теории схем. Мы увидим, что эти схемы обладают свойствами, которые не типичны для ассоциативных схем вообще. Схему $H(v, 2)$ можно отождествить с множеством всех подмножеств v-множества, значит, она «содержит» все схемы Джонсона $J(v, k)$.

Если G — транзитивная группа перестановок на множестве X с тем свойством, что всякие две точки взаимно переставляемы некоторым элементом из G, то орбиты группы G на множестве 2-подмножеств множества X образуют ассоциативную схему на X. (Это условие на G может быть ослаблено: достаточно, чтобы перестановочный характер G был «мультипликативно-свободным»; достаточны и еще более слабые условия, но их не легко формулировать.) Хигманом [35] введен и изучен более общий комбинаторный объект, названный им «когерентной конфигурацией», который тем же способом «описывает» действие произвольной группы перестановок. (Основное отличие в замене неупорядоченных пар упорядоченными.)

Ассоциативная схема называется *метрической*, если Γ_i есть множество пар точек, отстоящих друг от друга на расстоянии i в графе Γ_i для $1 \leqslant i \leqslant n$. ($\Gamma_1$ в этом случае называется *метрически регулярным*, или *совершенно регулярным графом*.) Сильно регулярный граф является метрически регулярным, но для $n > 2$ метрические схемы, по-видимому, должны быть весьма редки среди ассоциативных схем. Однако, схемы Хэмминга и Джонсона, как легко видеть, являются таковыми. (В схеме $J(2k+1, k)$ граф Γ_k метрически регулярен.) Схема является метрической тогда и только тогда, когда $a_{ijk} = 0$, исключая случаи, когда $|i-j| \leqslant k \leqslant i+j$ (это как раз и есть «неравенство треугольника») и $a_{i1i+1} \neq 0$ для $1 \leqslant i \leqslant n-1$.

Для упрощения формул расширим область определения индексов, включив 0, положив $n_0 = 1$, $a_{ij0} = \delta_{ij} n_i$, $a_{i0k} = a_{0ik} = \delta_{ik}$. (Это можно интерпретировать как то, что Γ_0 есть граф, в котором каждая вершина смежна себе и никаким другим.) Теперь эти параметры удовлетворяют ряду тождеств, например,

$$a_{ijk} = a_{jik}, \quad n_k a_{ijk} = n_i a_{kji},$$
$$\sum_{j=0}^{n} a_{ijk} = n_i, \quad \sum_{t=0}^{n} a_{lit} a_{tjm} = \sum_{k=0}^{n} a_{lkm} a_{ijk}. \tag{15.1}$$

(Последнее равенство получается, если двумя способами, как показано на рис. 15.1, подсчитывать пути

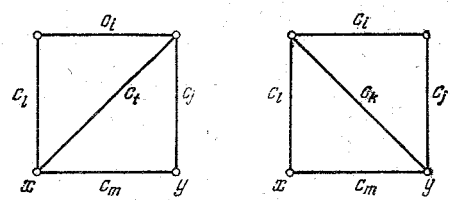

Рис. 15.1.

цветовой последовательности c_l, c_i, c_j, соединяющие x с y, где $\{x, y\} \in \Gamma_m$.)

Пусть A_i — матрица смежности графа Γ_i и $A_0 = I$. Тогда

$$A_i A_j = \sum_{k=0}^{n} a_{ijk} A_k;$$

значит, коммутирующие симметрические матрицы $A_0, \ldots, A_n$ задают $(n+1)$-мерную действительную алгебру, называемую *алгеброй Боуза — Меснера* [12], или *центральной алгеброй* [35] схемы. (Второе название вытекает из того факта, что если схема получена из группы перестановок, как это описано выше, то эта алгебра есть в точности множество матриц, коммутирующих со всеми матрицами в матричном представлении группы.) Заметим, что если схема метрическая, то A_1 порождает центральную алгебру.

Соотношения (15.1) интерпретируемы в терминах структуры этой алгебры; в частности, первое и второе означают, что $A_iA_j = A_jA_i$ и $(A_lA_i)A_j = A_l(A_iA_j)$ соответственно.

Как и для сильно регулярных графов, здесь важны собственные значения матриц A_i и их кратности. Для удобства мы говорим о (неприводимых) представлениях, или характерах, алгебры Боуза — Меснера; характер есть просто функция, ставящая в соответствие каждой матрице ее собственное значение на общем векторе собственных значений. (Заметим, что эти матрицы могут быть одновременно диагонализированы.) Неприводимые представления и их кратности определяются и определяют параметры a_{ijk}; таким образом проявляются «рациональные условия» для произвольных схем. Опишем этот процесс.

Определим «матрицы пересечений» M_i, $0 \leqslant i \leqslant n$, по правилу $(M_i)_{lm} = a_{lim}$. Тогда

$$(M_iM_j)_{lm} = \sum_{t=0}^{n} a_{lit}a_{tjm} = \sum_{k=0}^{n} a_{lkm}a_{ijk} = \left(\sum_{k=0}^{n} a_{ijk}M_k\right)_{lm}.$$

Значит, $M_iM_j = \sum_{k=0}^{n} a_{ijk}M_k$ и отображение $A_i \to M_i$ индуцирует изоморфизм этих алгебр. Значит, неприводимые представления можно находить одновременным диагонализированием M_i. (Этих матриц обычно много меньше, чем A_i, и зависят они только от параметров a_{ijk}, а не от конкретной схемы.)

Пусть $\rho_0, \ldots, \rho_n$ — неприводимые представления; можно предположить, что $\rho_0(A_i) = n_i$ для $0 \leqslant i \leqslant n$ (ρ_0 соответствует собственному вектору из одних 1).

Пусть μ_m — кратность ρ_m. Тогда $\mu_0 = 1$ и

$$|X|\delta_{t0} = \mathrm{Tr}(A_t) = \sum_{m=0}^{n} \mu_m \rho_m(A_t)$$

есть система линейных уравнений для кратностей μ_m.

Обратно, предполагаем, что ρ_m и μ_m известны. Валентности a_i определяются как $\rho_0(A_i)$, или

$$|X| n_i \delta_{ij} = \mathrm{Tr}(A_i A_j) = \sum_{m=0}^{n} \mu_m \rho_m(A_i)\rho_m(A_j).$$

Подсчитывая треугольники с реберной раскраской c_i, c_j, c_k, мы определяем a_{ijk}:

$$|X| a_k a_{ijk} = \mathrm{Tr}(A_i A_j A_k) = \sum_{m=0}^{n} \mu_m \rho_m(A_i)\rho_m(A_j)\rho_m(A_k).$$

Если схема метрическая, то процесс упрощается. Во-первых, A_1 порождает алгебру Бозуа — Мреснера; значит, мы должны лишь диагонализировать M_1. Во-вторых, эта матрица трехдиагональна, значит, она легче диагонализируется и ее собственные значения различны. Почти все приложения рациональных условий для ассоциативных схем были именно к метрическим схемам; теорема Баннаи и Ито [7] и Дамерелла [20] о графах Мура тому хороший пример.

Пусть P — $(n+1)\times(n+1)$-матрица с (i,k)-м элементом $\rho_i(A_k)$, т. е. «таблица характеров» алгебры Бозуа — Мреснера; пусть Q — матрица, определяемая соотношением $PQ = QP = |X|I$. Из главы 14 видим, что Q можно также определить, как $\Delta_{\boldsymbol{n}}^{-1} P^T \Delta_{\mu}$, где $\boldsymbol{n} = (n_0, \ldots, n_n)$, $\mu = (\mu_0, \ldots, \mu_n)$, и что для каждого $\boldsymbol{u}$ $\Delta_{\boldsymbol{u}}$ есть диагональная матрица с диагональными элементами — компонентами $\boldsymbol{u}$.

Код, исправляющий ошибки, есть просто подмножество Y — точечного множества X схемы Хэмминга; займемся расстоянием (в графе Γ_1) между двумя членами Y или между членом из Y и членом из X. Для формализации этого Дельсарт вводит для всякого подмножества Y точечного множества X любой схемы его *внутреннее распределение* $\boldsymbol{a} = (a_0, \ldots, a_n)$ по правилу

$$a_i = |Y|^{-1} |\tilde{\Gamma}_i \cap Y^2|,$$

где $\tilde{\Gamma}_0 = \{(x, x) \mid x \in X\}$ и $\tilde{\Gamma}_i = \{(x, y) \mid \{x, y\} \in \Gamma_i\}$ для $i > 0$, и *распределительную матрицу* B множества Y как $|X| \times (n+1)$-матрицу, (x, i)-й элемент которой есть $B_{x,i} = |\Gamma_i(x) \cap Y|$, $x \in X$, $0 \leqslant i \leqslant n$. Таким образом, $a_0 = 1$ и a_i есть средняя валентность графа $\Gamma_i | Y$. Говорим, что множество Y есть *регулярное подмножество*, если каждый граф $\Gamma_i | Y$ регулярен (с валентностью a_i). Если Y — регулярное подмножество, то строки B, соответствующие точкам Y, равны $\boldsymbol{a}$, и наоборот.

Какая $(n+1)$-строка может служить внутренним распределением некоторого подмножества? Ясно, что элементы строки должны быть неотрицательными рациональными числами $a_0 = 1$, а число $\sum_{i=0}^{n} a_i = |Y|$ — целым. Дельсарт нашел более серьезное необходимое условие:

$$B^T B = \frac{|Y|}{|X|} P^T \Delta_{aQ} P.$$

Это вытекает из того, что в $\boldsymbol{a}Q$ все компоненты неотрицательны.

Этот факт с использованием техники линейного программирования применен Дельсартом для нахождения границ для объемов подмножеств, внутренние распределения которых удовлетворяют различным условиям.

Ясно, что для любых различных действительных чисел $z_0, \ldots, z_n$ можно найти многочлены $\Phi_0, \ldots, \Phi_n$, каждый степени не выше n, такие, что $P_{ik} = \Phi_k(z_i)$ для $0 \leqslant i, k \leqslant n$. Дельсарт называют схему *P-полиномиальной*, если имеется такой набор чисел $z_0, \ldots, z_n$, $z_0 = 0$, для которого Φ_k имеет степень k для $0 \leqslant k \leqslant n$.

Q-полиномиальные схемы определяются аналогично, заменой P на Q в определении. Вообще говоря, полиномиальные схемы довольно редки среди ассоциативных схем; ни P-полиномиальные, ни Q-полиномиальные условия не следуют один из других, но примечательно, что важные схемы Хэмминга и Джонсона являются как P- так и Q-полиномиальными. (Для схем Хэмминга $P = Q$, $z_i = i$ для схем Джонсона, $z_i = i(v+1-i)$ для P-многочленов и $z_i = i$ для Q-многочленов. Фактически многочленами, не говоря о

тривиальных модификациях, для этих двух схем являются многочлены Кравчука и Эберлейна соответственно.) Заметим, что P-полиномиальное условие зависит от упорядочения графов Γ_i, в то время как Q-полиномиальное условие зависит от представлений ρ_i.

P-полиномиальное условие имеет простую комбинаторную трактовку:

Теорема 15.3. *Ассоциативная схема является P-полиномиальной тогда и только тогда, когда она является метрической.*

Показать это можно весьма просто, замечая, что схема является метрической тогда и только тогда, когда A_i — многочлен от A_1 степени i для $0 \leqslant i \leqslant n$. Аналогичной характеристики для Q-многочленов не обнаружено. Однако для них допустимо следующее представление: Q — это P-матрица ассоциативной схемы и определим ее «числа пересечений» b_{ijk} по вышеприведенной формуле. Это будут неотрицательные числа с $b_{ij0} = \mu_i \delta_{ij}$, удовлетворяющие соотношениям, аналогичным тем, которым удовлетворяют a_{ijk}. Тогда схема будет Q-полиномиальной тогда и только тогда, когда b_{ijk} удовлетворяют «неравенству треугольника», т. е. $\beta_{ijk} = 0$ всюду, кроме $|i-j| \leqslant k \leqslant i+j$, и $b_{i1i+1} \neq 0$ для $1 \leqslant i \leqslant n-1$.

Суммарные многочлены в P-полиномиальной схеме определяются как $\Psi_k(z) = \sum_{i=0}^{k} \Phi_i(z)$ для $0 \leqslant k \leqslant n$. Аналогично определяются суммарные многочлены и в Q-полиномиальной схеме.

Предположим, имеется P-полиномиальная (т. е. метрическая) схема на X. Для каждого $Y \subset X$ определим *минимальное расстояние* на Y как индекс первой ненулевой после a_0 компоненты его внутреннего распределения a и определим *внешнее расстояние* r как число ненулевых компонент aQ, исключая $(aQ)_0$. Минимальное расстояние, очевидно, является наименьшим расстоянием между двумя различными точками из Y. Название «внешнее расстояние» оправдано тем, что любая точка из X лежит на расстоянии не более чем r от любой точки из Y, хотя r может и не быть наименьшим.

Теорема 15.4. *Пусть Y — подмножество X с минимальным расстоянием d и внешним расстоянием r;*

положим $e = [(d-1)/2]$. *Тогда*

$$\sum_{i=0}^{e} n_i \leqslant \frac{|X|}{|Y|} \leqslant \sum_{i=0}^{r} n_i.$$

(*В частности,* $e \leqslant r$.) *Если одна из этих границ достигается, то достигается и другая.*

Доказательство. Для всякого целого c «шар радиуса c» с центром в точке x (т. е. множество точек, отстоящих от c не более чем на x) содержит $\sum_{i=0}^{c} n_i$ точек. Шары радиуса e с центрами в точках Y попарно не пересекаются, в то время как шары радиуса r покрывают X. Отсюда следует утверждение теоремы.

Можно дать и чисто алгебраическое доказательство, основывая его на P-полиномиальной концепции и методах линейного программирования, отмеченных ранее.

Подмножество, достигающее границы из теоремы 15.4, называется *совершенным* e-кодом; это просто подмножество $Y \subset X$, обладающее тем свойством, что всякая точка из X состоит не более чем на e от некоторой единственной точки из Y. Его минимальное расстояние равно $2e+1$ (лучше, чем $2e+2$). В схемах Хэмминга примерами тому могут служить коды Хэмминга и Галея. Пара непересекающихся $(2e+1)$-множеств образует совершенный e-код в схеме Джонсона $J(4e+2, 2e+1)$. Также, в схеме Джонсона $J(2k+1, k)$ с иной метрикой, определяемой графом Γ_k, нетрудно показать, что совершенный 1-код есть $(k-1)$-$(2k+1, k, 1)$-схема, и обратно. Известны примеры с $k=3$ и $k=5$. Биггсом [10] приведены иные примеры.

Наиболее сильной теоремой о классических совершенных кодах является теорема Ллойда, которая на произвольные метрические схемы обобщена независимо Дельсартом и Биггсом [10].

Теорема 15.5. *Если совершенный* e*-код* Y *существует, то нули суммарного многочлена* $\Psi_e(z)$ *содержатся в множестве* $\{z_1, \ldots, z_n\}$ *и внутреннее распределение* Y *определяется посредством* e *и параметров схемы.*

Заметим, что $\Psi_e(z)$ зависит лишь от e и параметров схемы, а множество $\{z_1, \ldots, z_n\}$ есть множество корней $\Psi_n(z)$; значит, первая часть теоремы может быть выражена так: $\Psi_e(z)$ делит $\Psi_n(z)$ в $\mathbf{R}[z]'$. Это можно сравнить с «условием сферической упаковки», которое гласит, что $\Psi_e(0)$ (объем сферы радиуса e) делит $\Psi_n(0) = |X|$ в $\mathbf{Z}$. *Далее см. Добавление* 19.

Теорема 15.5 полезна для определения параметров совершенных кодов в схемах Хэмминга $H(n, q)$, где q — степень простого. Аналогичное исследование схем Джонсона было начато Дельсартом. Заметим, однако, что для совершенных 1-кодов в $J(2k+1, k)$ с метрикой, задаваемой Γ_k, теорема 15.5 показывает лишь, что k нечетно; более сильное заключение (о том, что $k+2$ — простое) можно вывести из (1.1).

Читатель, наверное, уже подметил формальную «двойственность» между P и Q, возникающую в различных местах. Эта двойственность наводит на мысль, что можно получить результаты о Q-полиномиальных схемах, похожие на теоремы 15.4 и 15.5. Действительно, для нас это единственная возможность в поисках этих результатов, поскольку мы не обладаем достаточно хорошей геометрической интерпретацией P-полиномиальных схем; все доказательства должны быть чисто алгебраическими. Это подтверждает, что точные аналоги этих результатов существуют, но отсутствие геометрических трактовок препятствует их открытие.

В Q-полиномиальной схеме на X определяем *максимальную интенсивность* t подмножества $Y \subset X$ как на единицу меньший индекс первой ненулевой после $(\boldsymbol{a}Q)_0$ компоненты $\boldsymbol{a}Q$ и определяем *степень* s подмножества Y как число ненулевых компонент $\boldsymbol{a}$, исключая a_0, где $\boldsymbol{a}$ — внутреннее распределение Y. Таким образом, имеем двойственность $t \leftrightarrow d-1$, $s \leftrightarrow r$. Эта степень есть число красок, встречающихся в сужении схемы на подмножество Y. Смысл максимальной интенсивности не столь очевиден, и должен раскрываться в каждом конкретном случае.

Теорема 15.6. *Пусть Y — подмножество X с максимальной интенсивностью t и степенью s; положим $e = t/2$. Тогда*

$$\sum_{i=0}^{e} \mu_i \leqslant |Y| \leqslant \sum_{i=0}^{s} \mu_i.$$

(*В частности, $e \leqslant s$.*) *Если одна из этих границ достигается, то достигается и другая.*

Подмножество, достигающее эти границы, называется *плотной* $2e$*-схемой*; причины такого определения станут ясны ниже. Ее максимальная интенсивность $2e$ (а не $2e+1$).

Теорема 15.7. *Если плотная* $2e$*-схема* Y *существует, то нули суммарного многочлена* $\Psi_e(z)$ *расположены в множестве* $\{z_1, \ldots, z_n\}$ *и внутреннее распределение* Y *определяется посредством* e *и параметров этой схемы.*

Отметим иной результат, который двойствен менее известному результату для метрических схем.

Теорема 15.8 *). *В предположениях теоремы* 15.6:

1) *если* $t \geqslant s-1$, *то* Y *— регулярное подмножество*;

2) *если* $t \geqslant 2s-2$, *то сужение данной схемы на* Y *представляет собой ассоциативную схему, которая* Q*-полиномиальна с кратностями* $\mu_0, \ldots, \mu_{s-1}$, *и* $|Y| = \sum_{i=0}^{s-1} \mu_i$.

Для нас важность результатов 15.6—15.8 основывается на следующем факте.

Теорема 15.9. *Максимальная интенсивность* t *подмножества* Y *в схеме Джонсона* $J(v, k)$ *равна тому наибольшему* t, *для которого* Y *является* t*-схемой.*

Интерпретируем теперь этот результат в терминах t-схем. Для этого нам понадобится тот факт, что кратности в $J(v, k)$ задаются формулой $\mu_i = \binom{v}{i} - \binom{v}{i-1}$, $0 \leqslant i \leqslant k$. Это может быть доказано непосредственно рассуждением, использующим вложение алгебры Боуза — Меснера схемы $J(v, k-1)$ в алгебру схемы $J(v, k)$, или рассуждением, основанным на теории характеров симметрической группы. Степень схемы есть число значений, принимаемых объемом пересечения двух различных блоков. Таким образом, учитывая, что рассматриваются лишь схемы с $k \leqslant v/2$ и без кратных блоков, получаем следующую теорему.

*) В новом варианте теоремы отсутствует п. 1). (*Прим. перев.*)

Теорема 15.6′. 1) *t-схема имеет по крайней мере* $\binom{v}{e}$ *блоков, где* $e = [t/2]$; *равенство имеет место тогда и только тогда, когда это есть* $2s$*-схема.*

2) 0*-схема степени* s *имеет не более чем* $\binom{v}{s}$ *блоков; равенство имеет место тогда и только тогда, когда эта схема является* 2*-схемой.*

Таким образом, 1) обобщает неравенство Фишера (см. теорему 1.5); это было доказано в общем случае Вильсоном [72] после Петренюка [52], доказавшего первую часть при $t = 4$. Плотные 2-схемы оказываются просто симметричными 2-схемами.

2) обобщает предложение 3.4.

Теорема 15.8′. *В* $(2s-2)$*-схеме имеющей степень* s, s *отношений на блоках, определяемые мощностью пересечения, образуют ассоциативную схему.*

Это обобщает теорему 3.2; кратности, задаваемые теоремой 15.8, согласуются с найденными в теореме 3.2 для квазисимметричных схем.

Теорема 15.8 — «наилучшая возможная». Рассмотрим схему точек и плоскостей в $AG(4, 2)$. Это есть 3-(16, 4, 1)-схема; она имеет степень 3 (поскольку два блока имеют не более двух общих точек); но число блоков, не пересекающихся с данной парой непересекающихся блоков, зависит от параллельности этих заданных блоков. Примерами 4-схем со степенью 3 служат 5-(24, 8, 1), 4-(23, 8, 4) (остаточная для первой), 4-(11, 5, 1)-схемы. 4-(23, 7, 1)-схема есть единственная известная плотная 4-схема и вообще единственная известная плотная $2s$-схема при $s > 1$. Это еще не дает полной характеризации, хотя некоторый прогресс и достигнут Вильсоном, Нода и Ито. (Результат 15.7 оказывается полезным инструментом для этого.) Сравните предложение 3.6 и замечания, следующие за ним.

Максимальная интенсивность имеет хорошо известную трактовку в схемах Хэмминга. Максимальная интенсивность подмножества есть просто его максимальная интенсивность как ортогональной таблицы, как определено Рао, который доказал теорему 15.6 в этом случае. (Ортогональная таблица интенсивности t есть подмножество Y точечного множества схе-

мы $H(n, q)$, обладающее тем свойством, что для данных t координатных мест каждая t-строка одинаково часто имеет член Y на этих местах.)

Заключительное замечание о двойственности. В некоторых схемах, особенно в *аддитивных* (допускающих транзитивную абелеву группу автоморфизмов A), можно определять *двойственные схемы*, для которых P- и Q-матрицы являются соответственно Q- и P-матрицами исходной схемы. Аддитивную схему можно рассматривать как кольцо Шура на A и эта двойственность согласуется с концепцией, определенной Тамашке [65]. Точечные множества этой схемы и двойственной ей отождествляются с группой A и двойственной ей группой A' (группа характеров группы A). Подгруппе Y группы A соответствует подгруппа Y' группы A' (множество характеров, чье сужение на Y тривиально). Внутренние распределения $\boldsymbol{a}$ и $\boldsymbol{a}'$ связаны соотношениями

$$|Y|\boldsymbol{a}' = \boldsymbol{a}Q, \quad |Y'|\boldsymbol{a} = \boldsymbol{a}'P.$$

Таким образом, благодаря двойственности, параметры $d-1$ и t и параметры r и s взаимно заменяемы. Схемы Хэмминга являются аддитивными и изоморфны двойственным; для них соотношение $|Y|\boldsymbol{a}' = \boldsymbol{a}Q$ выражает тождества МакВильямс теоремы 7.14.

ЛИТЕРАТУРА

1. Ahrens R. W., Szekeres G. On a combinatorial generalization of 27 lines associated with a cubic surface. — J. Austral. Math. Soc., 1969, **10**, p. 485—492.
2. Assmus E. F., Mattson H. F. Jr. New 5-designs.—J. Combinatorial Theory; 1969, **6**, p. 122—151.
3. Assmus E. F., Jr., Mattson H. F. Jr. Algebraic theory of codes II. — Report AFCRL-0013, Appl. Research Lab. of Sylvania Electronic Systems, Bedford, 1971.
4. Assmus E. F. Jr., Mattson H. F., Jr. On weights in quadratic residue codes. — Discr. Math., 1972, **3**, p. 1—20.
5. Assmus E. F., Mattson H. F., Jr. Contractions of self-orthogonal codes. — Discr. Math., 1972, **3**, p. 21—32.
6. Assmus E. F., Jr., Mattson H. F., Jr. Marcia Guza. Self-ortogonal Steiner systems and projective planes. — Math. Z., 1974, **138**, p. 89—96.
7. Bannai E., Ito T. On finite Moore graphs. — J. Fac. Sci. Univ. Tokyo, 1973, **20**, p. 191—208.
8. Berlekamp E. R., MacWilliams F. J., Sloane N. J. A. Gleason's theorem on self-dual codes. — IEEE. Trans. Inf. Theory, 1972, **18**, p. 409—414.
9. Biggs N. L. Finite groups of automorphisms. — C. U. P., 1971 — (L. M. S. Lecture Notes; **6**).
10. Bigg N. L. Perfect codes in graphs. — J. Combinatorial Theory (B), 1973, **15**, p. 289—296.
11. Bose R. C. Strongly regular graphs, partial geometries, and partially balanced designs. — Pacific J. Math., 1963, **13**, p. 389—419.
12. Bose R. C., Mesner D. M. On linear associative algebras corresponding to association schemes of partially balanced designs. — Ann. Math. Statist. 1959, **30**, p. 21—38.
13. Bose R. C., Shimamoto T. Classification and analysis of partially balanced incomplete block design with two associate classes. — J. Amer. Statist. Assoc., 1952, **47**, p. 151—184.
14. Bruen A., Fisher J. C. Blocking sets, k-arcs and nets of order ten. — Advances in Mathematics, 1973, **10**, p. 317—320.
15. Buekenhout F. Une caracterisation des espaces affines basee sur la notion de droite. — Math. Z., 1969, **111**, p. 367—371.

16. Bussemaker F. C., Seidel J. J. Symmetric Hadamard matrices of order 36. — Ann. N. Y. Acad. Sci., 1970, **175**, p. 66—79.
17. Cameron P. J. Extending symmetric designs. — J. Combinatorial Theory (A), 1973, **14**, p. 215—220.
18. Chang Li-Chien. The uniqueness and non-uniqueness of the triangular association schemes. — Sci. Record Peking Math. (New Ser.) 1959, **3**, p. 604—613.
19. Chang Li-Chien. Association schemes of partially balanced designs with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$, and $p_{11}^2 = 4$. — Sci. Record Peking Math. (New Ser.) 1960, **4**, p. 12—18.
20. Damerell R. M. On Moore graps. — Proc. Camb. Phil. Soc., 1973, **74**, p. 227—236.
21. Delsarte P. An algebraic approach to the association schemes of coding theory. — Philips Research Reports Supplements, 1973. № 10. Русский перевод: Дельсарт Ф. Алгебраический подход к схемам отношений теорий кодирования: Пер. с англ. — М.: Мир, 1976.
22. Dembowski P. Inversive planes of even order.—Bull. Amer. Math. Soc., 1963, **69**, p. 850—854.
23. Dembowski P. Mobiusebenen Garader Ordnung. — Math. Ann. 1964, **157**, p. 175—205.
24. Dembowski P. Finite geometries. — Berlin — Heidelberg — New York, Springer Verlag, 1968.
25. Erdos P., Renyi A., Sos V. On a problem in graph theory. — Studies Math. Hungar, 1966, **1**, p. 215—235.
26. Gewirtz A. Graphs of maximal even girth. — Canad. J. Math., 1969, **21**, p. 915—934.
27. Gleason A. M. Weight polynomials of self-dual codes and the MacWilliams identities. — Actes congres Intern. Math., 1970, vol. 3, p. 211—215.
28. Goethals J. M. Some combinatorial aspects of coding theory. — In: A survey of combinatorial theory/Eds. J. N. Srivastava et al. Amsterdam: North Holland Publishing Comapny, 1973, ch. 17.
29. Goethals J. M., Seidel J. J. Orthogonal matrices with zero diagonal. — Canad. J. Math., 1967, **19**, p. 1001—1010.
30. Goethals J. M., Seidel J. J. Strongly regular graphs derived from combinatorial designs. — Canad. J. Math., 1970, **22**, p. 597—614.
31. Goethals J. M., Snover S. L. Nearly perfect binary codes. — Discr. Math., 1972, **2**, p. 65—88.
32. Hall M., Jr. Automorphisms of Steiner triple systems. — IBM J. Res. Develop., 1961, **4**, p. 460—472.
33. Hall M., Jr. Combinatorial theory. — Waltham Blaisdell, 1967. Русский перевод: Холл М. Комбинаторика: Пер. с англ./ Под ред. А. О. Гельфонда и В. Е. Тараканова. — М.: Мир, 1970.
34. Hall M., Lane R., Wales D. Designs deriver from permutation groups. — J. Combinatorial Theory, 1970, **8**, p. 12—22.
35. Higman D. G. Combinatorial considerations about permutation groups. — Oxford: Mathematical Institute, 1971.

36. Higman D. G. Partial geometries, generalized quadrangles, and strongly regular graphs. — In: Atti del convegno geometria combinatoria e sue applicazioni. Perugia, 1971.
37. Higman D. G. Remark on Shult's graph extension theorem.— In: Finite groups'72/eds. T. Gagen, M. P. Hale, Jr. and E. E. Shult). Amsterdam: North-Holland Publishing Company, 1973.
38. Hoffman A. J., Singleton R. R. On Moore graphs of diameters 2 and 3. — IBM J. Res. Develop., 1961, **4**, p. 497—504.
39. Hughes D. R. On *t*-designs and groups. Amer. J. Math., 1965, **87**, p. 761—778.
40. Johnson S. M. A new upper bound for error-correcting codes. — IEEE Trans. Inform. Theory, 1962, **8**, p. 203—207.
41. Jonsson W. On the Mathieu groups M_{22}, M_{23}, M_{24} and the associated Steiner systems. — Math. Z., 1972, **125**, p. 193—214.
42. Kantor W. M. Dimension and embedding theorems for geometric lattices. — J. Comb. Th. (A), 1974, **17**, p. 173—195.
43. Lemmens P. W., Seidel J. J. Equiangular lines. — J. Algebra, 1973, **24**, p. 494—512.
44. van Lint J. H. Coding theory. — Berlin Springer Verlag L/71. — (Lecture Notes in Math., **201**).
45. van Lint J. H. Recent results on perfect codes and related topics, in Combinatorics part 1/Ed. Mathe M. Hall and J. H. van Lint. — Mathematical Centre Tracts, 1974, **55**, p. 158—178.
46. Luneberg H. Transitive Erweiterungen endlicher Permutations-gruppen-Berlin — Heidelberg — New York: Springer Verlag, 1969. — (Lecture Notes in Mathematics, **84**).
47. MacWilliams F. J., Sloane N. J. A., Goethals J. M. The MacWilliams identities for nonlinear codes. — Bell System Tech. J., 1972, **51**, p. 803—819.
48. MacWilliams F. J., Sloane N. J. A., Thompson J. G. On the existence of a projective plane of order 10. — J. Combinatorial Theory, 1973, **14**, p. 66—78.
49. Mallows C. L., Sloane N. J. A. An upper bound for self-dual codes. — Information and Control, 1973, **22**, p. 188—200.
50. Massey J. L. Threshold decoding. Cambridge: M. I. T. Press (1963) Русский перевод: Месси Дж. Пороговое декодирование: Пер. с англ./Под ред. Ю. Л. Сагаловича. — М.: Мир, 1966.
51. Noda R. On some strongly regular graphs and rank 3 permutation groups, unpublished.
52. Петренюк А. Я. О неравенстве Фишера для тактических конфигураций. — Мат. заметки, 1968, **4**, с. 417—474.
53. Pless V. Symmetry codes over GF(3) and new 5-designs. — J. Combinatorial Theory, 1972, **12**, p. 119—142.
54. Pless V. Symmetry codes and their invariant subcodes. — J. Combinatorial Theory Ser. A, 1975, **18**, p. 116—125.
55. Preparata F. P. A class of optimum nonlinear double-error-correcting codes. — Inform. Control 1968, **13**, p. 378—400. Русский перевод: Препарата Ф. П. Класс оптимальных нелинейных кодов с исправлением двойных ошибок. — В кн.: Киб. сборник, Новая серия. М., 1970, вып. 7, с. 18—42.
56. Ryser H. J. Combinatorial mathematicss — New York: Wiley, 1965. Русский перевод: Райзер Г. Дж. Комбинаторная

ДОБАВЛЕНИЯ ИЗ ВТОРОГО ИЗДАНИЯ

1 (к стр. 13)

Аналогичным вопросом можно задаться и относительно более общих схем. Пусть $\mathscr{D}$ — симметричная 2-(V, K, λ)-схема и B — ее блок. Если удалить из $\mathscr{D}$ блок B и все его точки, то полученная структура $\mathscr{D}^B$ образует 2-$(V-K, K-\lambda, \lambda)$-схему. Если положить $v = V - K$, $k = K - \lambda$, то $v = k(k+\lambda-1)/\lambda$. Мы называем $\mathscr{D}^B$ *вычетной* (*остаточной*) *схемой* схемы $\mathscr{D}$ относительно блока B. Произвольная 2-(v, k, λ)-схема с параметрами $v = k(k+\lambda-1)/\lambda$ называется *квазиостаточной*. Естествен вопрос: какие квазиостаточные схемы являются остаточными?

Квазивычетная схема с $\lambda = 1$ есть 2-$(k^2, k, 1)$-схема, т. е. аффинная плоскость, и значит, вычетная схема. Это также верно и при $\lambda = 2$ по теореме Холла и Коннора [26*]. Мы докажем эту теорему и сформулируем теорему Боуза, Шрикханде и Сингха [6*] при рассмотрении квазивычетных схем с $\lambda < 2$ в гл. «Частичные геометрии». Имеются квазивычетные схемы, не являющиеся вычетными; см. ван Линт [35*].

2 (к стр. 15)

Теорема 1.12.* *Если* 3-(v, k, λ)-*схема* $\mathscr{D}$ *является расширением симметричной* 2-*схемы, то выполнено одно из следующих условий:* 1) $\mathscr{D}$ — *адамарова* 3-*схема*; 2) $v = (\lambda+1)(\lambda^2+5\lambda+5)$, $k = (\lambda+1)(\lambda+2)$; 3) $v = 112$, $k = 12$, $\lambda = 1$; 4) $v = 496$, $k = 40$, $\lambda = 3$.

Доказательство. Во-первых, заметим, что 3-схема $\mathscr{D}$ является расширением симметричной 2-схемы тогда и только тогда, когда всякие два блока схемы $\mathscr{D}$ пересекаются в 0 либо в $\lambda+1$ точках; в 3-(v, k, λ)-схеме с такими свойствами $r = v - 1$, $\lambda = k - 1$, $(v-2)\lambda = (k-1)(k-2)$.

Пусть $B \in \mathscr{D}$; если $p, q \in B$, то найдется $k\lambda/(\lambda+1)$ блоков, содержащих p и q и пересекающих B в $\lambda+1$ точках, и значит, $(k-\lambda-1)/(\lambda+1)$ блоков, не пересекающихся с B. Это показывает, что инцидентностная структура $\mathscr{D}_0$, чьи точки суть точки вне B, а блоки — блоки, не пересекающиеся с B, образует 2-$(v-k, k, (k-\lambda-1)/(\lambda+1))$-схему. Согласно (1.2) и (1.3) (или применяя (1.7) к $\mathscr{D}$) число блоков схемы $\mathscr{D}_0$ равно

$$(v-k)(v-k-1)(k-\lambda-1)/(k(k-1)(\lambda+1)).$$

Если схема $\mathscr{D}_0$ вырожденная (имеет, но единственный, блок), то $v = 2k$, откуда $v = 4(\lambda+1)$, $k = 2(\lambda+1)$, и значит, $\mathscr{D}$ есть адамарова 3-схема. В альтернативном случае применение нера-

венства Фишера к $\mathscr{D}_0$ влечет, что

$$(v-k-1)(k-\lambda-1) \geqslant k(k-1)(\lambda+1),$$

$$(k-1)(k-(\lambda+1)(\lambda+2)) \geqslant 0,$$

и значит, $k \geqslant (\lambda+1)(\lambda+2)$. Однако $b = v(v-1)/k = (k^2-3k+2\lambda+2)(k^2-3k+\lambda+2)/(k\lambda^2)$; значит, k делит $2(\lambda+1)(\lambda+2)$. Это же рассуждение показывает, что если $k = 2(\lambda+1)(\lambda+2)$, то $\lambda = 1$ или 3, что и влечет случаи 3) и 4) теоремы. Если $k = (\lambda+1)(\lambda+2)$, то получаем случай (2).

3 (к стр. 16)

Нашим следующим объектом в этой главе служат овалы. Пусть $\mathscr{D}$ — симметричная 2-(v, k, λ)-схема. n-дуга есть множество из n точек $\mathscr{D}$, в котором нет трех точек, лежащих в одном блоке $\mathscr{D}$. Для данной n-дуги S блок B называется *секантом*, *тангентом* или *пассантом* к S, если соответственно $|B \cap S| = 2$, 1 или 0.

Предложение 1.13. *Любая точка n-дуги в симметричной 2-(v, k, λ)-схеме лежит на $(n-1)\lambda$ секантах и $k-(n-1)\lambda$ тангентах. В частности, $n \leqslant 1 + k/\lambda$.*

Доказательство. Пусть S — n-дуга и $p \in S$. Подсчитаем пары (q, B), где B — секант, содержащий p и q, $q \in S$.

n-дуга называется *овалом типа* I, если каждая точка лежит на единственном тангенте (т. е. $n = 1 + (k-1)/\lambda$), и *овалом типа* II, если n-дуга не имеет тангентов (т. е. $n = 1 + k/\lambda$). Заметим, что овалы могут существовать только если $\lambda | k-1$ или $\lambda | k$ соответственно.

Предложение 1.14. *Если симметричная 2-(v, k, λ)-схема имеет овал типа* II, *то $k-\lambda$ четно.*

Доказательство. Пусть S — овал, а p — точка вне S. Число секантов, содержащих p, равно $n\lambda/2 = (k+\lambda)2$.

Предложение 1.15. *Пусть S — овал типа* I *в симметричной 2-(v, k, λ)-схеме с четным $k-\lambda$. Тогда каждая точка принадлежит либо одному, либо всем тангентам к овалу S.*

Доказательство. Заметим, что k, λ, n нечетны и, значит, каждая точка лежит по крайней мере на одном тангенте к овалу S. Пусть n_i — число точек, которые лежат на i тангентах. Тогда

$$\sum n_i = v, \quad \sum i n_i = nk, \quad \sum \binom{i}{2} n_i = \lambda \binom{n}{2}.$$

Следовательно, $\sum (i-1)(i-n) n_i = 0$, поэтому каждая точка лежит на одном или на всех тангентах.

Из 1.15 следует, что в проективной плоскости четного порядка все тангенты к овалу S типа I проходят через точку p — *узел* (или *ядро*, *центр*) овала S, а $\{p\} \cup S$ есть овал типа II.

Данный овал S типа II, пассанты к S и точки вне S (при обращении данного отношения инцидентности) образуют 2-$((k-2)(k-\lambda)/(2\lambda), (k-\lambda)/2, \lambda)$-схему.

Если $\mathscr{D}$ есть 3-схема, которая является расширением проективной плоскости, p — точка $\mathscr{D}$, а B — блок, не содержащий p, то B есть овал типа II в проективной плоскости $\mathscr{D}_p$.

Рассмотрим 2-(11, 5, 2)-схему Пэли $\mathcal{D}$. Каждая тройка точек, не содержащихся в блоке, образует овал типа I. Поэтому всякие две точки $\mathcal{D}$ располагаются на двух различных блоках $\mathcal{D}$ и трех овалах. Любые три точки либо лежат в одном блоке, либо образуют овал. Определим новую схему $\mathcal{D}'$ следующим образом. Точки $\mathcal{D}'$ — точки и блоки $\mathcal{D}$. Блоки $\mathcal{D}'$ — множества объема 6 следующих видов: 1) точка $\mathcal{D}$ и пять блоков $\mathcal{D}$, инцидентных с ней; 2) блок $\mathcal{D}$ и пять точек $\mathcal{D}$, инцидентных с ним; 3) овал из $\mathcal{D}$ и три его тангента.

Теперь легко проверить, что $\mathcal{D}'$ образует 3-(22, 6, 1)-схему, т. е. некоторое расширение $PG(2, 4)$ (см. [2*]). Дополнительно по овалам см. [1*].

Перейдем теперь к обобщению неравенства Фишера для схем с большими значениями t. Оно было получено в [52] для $t = 4$ и в [39*] для общего случая.

Теорема 1.16. *Пусть $\mathcal{D}$ — t-(v, k, λ)-схема с $t = 2s$ и $t \leqslant k \leqslant v - s$. Тогда $b \geqslant \binom{v}{s}$. Равенство имеет место тогда и только тогда, когда мощность пересечения двух блоков принимает в точности s различных значений.*

Доказательство. Докажем только неравенство $b \geqslant \binom{v}{s}$. Пусть M — матрица инцидентности со строками, индексированными блоками, и столбцами, индексированными s-подмножествами точечного множества схемы, в которой (B, S)-й элемент равен 1, если $S \subseteq B$, и 0 в противном случае. Достаточно показать, что строки M образуют $\mathcal{R}\binom{v}{s}$ (в смысле линейной оболочки). Поэтому пусть ρ_B — строка M с меткой B, а γ_S — вектор с 1 в столбце с меткой S и с 0 в остальных местах. Для $0 \leqslant i \leqslant s$ и фиксированного s-множества S положим

$$y_i = \sum_{|B \cap S| = i} \rho_B = \sum_{j=0}^{i} \sum_{|S' \cap S| = j} \sum_{\substack{B \supseteq S' \\ |B \cap S| = i}} \gamma_{S'} =$$

$$= \sum_{j=0}^{i} \binom{s-j}{i-j} \lambda_{s+i-j,\, s-i} \left(\sum_{|S \cap S'| = j} \gamma_{S'} \right),$$

где $\lambda_{m,n}$ обозначает число блоков, содержащих данное m-множество M и не пересекающихся с данным n-множеством N (где $M \cap N = \varnothing$); число это, как легко видеть, зависит лишь от m и n, если $m + n \leqslant t$. Полагая $x_j = \sum_{|S' \cap S| = j} \gamma_{S'}$, имеем систему из $s + 1$ линейных уравнений относительно x_j. Матрица коэффициентов треугольна с ненулевыми диагональными элементами $\lambda_{s,\, s-i}$ $(s \leqslant k \leqslant v - s)$. Значит, система имеет единственное решение. В частности, $x_s = \gamma_S$ есть линейная комбинация y-ов и, значит, располагается в пространстве строк матрицы M, что и требовалось показать.

Эта теорема будет далее обсуждаться в гл. «Квазисимметричные схемы» и «Ассоциативные схемы».

t-схема, реализующая границу из 1.16, называется *плотной*. Таким образом, из 2-схем только симметричные являются плотными (и весьма многочисленными). Однако при $t > 2$ ситуация меняется; так, в [30*, 7*, 37*] доказана

Теорема 1.17. *С точностью до дополнения единственной плотной* 4-(v, k, λ)-*схемой с* $2 < k < v - 2$ *является* 4-$(23, 7, 1)$-*схема.*

Имеются также результаты несуществования и для бо́льших значений t; в [4*] показано, что для четных $t \geqslant 10$ имеется лишь конечное число плотных t-схем.

Несколько раз в этой главе мы соприкасались с расширениями $PG(2, 4)$ и $AG(2, 3)$ — достаточно, чтобы убедить читателя в их важности для теории схем. Они также присутствуют и в теории кодирования, и в теории групп. Заканчиваем эту главу кратким обзором нескольких таких конструкций.

Простейшие конструкции используют идеи теории кодирования, поскольку эти две схемы связаны с двумя совершенными кодами Голея. Мы переносим их обсуждение в гл. «Самоортогональные коды и схемы» и «Ассоциативные схемы».

В [73] представлено непрямое конструирование этих схем; там рассмотрены две 5-кратно транзитивные группы Матье M_{24} и M_{12} как расширения известных групп перестановок и показано, что они являются группами автоморфизмов схем с подходящими свойствами. В [74] также доказана единственность этих схем.

В [46] представлена конструкция, подобная по духу (привлечением расширений известных структур), но комбинаторная по природе. Обозначим $PG(2, 4)$ через Π и рассмотрим задачу расширения Π до 5-(24, 8, 1)-схемы. Мы должны добавить три новые точки p, q, r и взять в качестве блоков все множества $\{p, q, r\} \cup L$, где L — прямая в Π. Для $i < 3$ блок, содержащий i новых точек, содержит также $8 - i$ точек из Π, образуя некоторую геометрическую конфигурацию в Π. Когда $i = 2$, эта конфигурация есть овал типа II (см. замечание после 1.15). Имеется 168 таких овалов в Π, а оценочные рассуждения показывают, что эта форма и является требуемой. Будем писать $S_1 \sim S_2$ (где S_1 и S_2 — овалы в Π), если $|S_1 \cap S_2|$ четно. Можно показать, что это отношение эквивалентности с тремя классами эквивалентности объема 56 каждый. Установим взаимно однозначное соответствие между классами эквивалентности парами новых точек и присоединим каждую пару ко всем овалам в соответствующем классе. Подобные рассуждения применимы и в случае $i = 1$ и $i = 0$, когда эти геометрические конфигурации представляют собой баеровские подплоскости и симметрические разности пар прямых соответственно. Этот способ обеспечивает как построение схемы, так и доказательство единственности.

Аналогичный метод применим и при получении 5-(12, 6, 1)-схемы из $AG(2, 3)$.

4 (к стр. 20)

Граф Клебша своими вершинами имеет все подмножества четной мощности множества $\{1, \ldots, 5\}$; две его вершины смежны всякий раз как их (как подмножеств) симметрическая разность имеет мощность 4. В этом графе множество $\bar{\Gamma}(p)$ вершин, не смежных вершине p, образует граф Петерсена.

Граф Гевиртца на 56 вершинах с $a = 10$, $c = 0$, $d = 2$ может быть определен посредством следующей конструкции, предложенной Симсом. Вершинное множество есть $\{\infty\} \cup \mathcal{P} \cup \mathcal{Q}$, где $\mathcal{P}$ — множество силовских 3-подгрупп знакопеременной группы A_6, а $\mathcal{Q}$ — множество инволюций в A_6. Соединяем ∞ со всеми вершинами в $\mathcal{P}$; соединяем $P \in \mathcal{P}$ с $q \in \mathcal{Q}$ всякий раз как $q^{-1}Pq = P$; соединяем q_1 с q_2, q_1, $q_2 \in \mathcal{Q}$, всякий раз как q_1q_2 имеет порядок 4. Комбинаторно можно отождествлять $P \in \mathcal{P}$ с парой непересекающихся 3-подмножеств множества $\{1, \ldots, 6\}$. Тогда типичные ребра второго и третьего типов соединяют $\{\{1, 2, 3\}, \{4, 5, 6\}\}$ с (12) (45), и (12) (34) с (23) (56) соответственно.

Иное описание графа Гевиртца использует в качестве вершин один класс овалов в $PG(2, 4)$ (см. замечание о конструкции Люнебурга в гл. 1), которые смежны в этом графе, если они не пересекаются. Тот факт, что этот граф сильно регулярен, будет следовать из (3.2).

Полные k-дольные графы, граф Петерсена, графы Клебша и Гевиртца — все они определяются однозначно с точностью до изоморфизма своими параметрами. (Для трех последних из этих типов графов см. [58, 26]. То же верно и для $T(n)$ при $n \neq 8$ и $L_2(n)$ при $n \neq 4$; эти результаты (см. [18, 29*, 61]) будут описаны в главе «Частичные геометрии». Графы Пэли, вообще говоря, не определяются своими параметрами; соответствующие примеры представлены в конце этой главы.

5 (к стр. 23)

Единственный граф с $s = 1$ из п. 2) теорема 2.5 есть граф Петерсена. Мы заканчиваем эту главу одним примером, принадлежащим Дельсарту, Гётхальсу и Турину, который показывает, что такие графы существуют всякий раз как $2s + 1$ есть степень простого. Связаны эти графы с так называемыми «симметрическими конференс-матрицами» [18*, 24*].

Пусть $V = V(2, q)$, где q — нечетная степень простого. Разобьем 1-мерное подпространство пространства V на два непересекающихся множества P и N равного объема $(q + 1)/2$. Образуем граф со множеством вершин V, в котором x и y смежны всякий раз как $\langle x - y \rangle \in P$. Такой граф сильно регулярен с параметрами $n = q^2$, $a = (q^2 - 1)/2$, $c = (q^2 - 5)/4$, $d = (q^2 - 1)/4$ (те же параметры, что у графа Пэли $P(q^2)$). Далее выберем элемент из множества P и отберем $(q - 1)/2$ его подмножеств; пусть X — множество из $q(q - 1)/2$ вершин, содержащихся в этих подмножествах. Удалим каждое ребро $\{x, y\}$ для $x \in X$, $y \notin X$ и добавим новые ребра $\{x, y\}$ для всех ранее не смежных пар такой формы. Добавим, наконец, новую вершину ∞, смежную каждой вершине в X. Читателю предлагается проверить, что полученный граф сильно регулярен с параметрами, отвечающими п. 2) теоремы 2.5 при $q = 2s + 1$. Эта «переключательная» конструкция будет рассматриваться далее в гл. «Расширение графов».

Заканчиваем эту главу одним неравенством о параметрах сильно регулярного графа (см. [19*]).

Теорема 2.6. *Пусть* Γ — *сильно регулярный граф на* n *вершинах, обладающий тем свойством, что* Γ *и* $\overline{\Gamma}$ *оба связны и*

что матрица смежности графа Γ *имеет собственное значение кратности* $f > 1$. *Тогда* $n \leqslant f(f+3)/2$.

Доказательство. Матрица смежности $A = A(\Gamma)$ имеет три различных собственных пространства, и любая матрица с этими собственными пространствами есть линейная комбинация матриц I, A и $J - I - A$. В частности, существует такая их линейная комбинация F, что F имеет собственные значения 0, 1 с кратностями $n - f$, f соответственно. Тогда F — положительная полуопределенная симметрическая матрица, и значит, это есть матрица Грама скалярных произведений множества S векторов в $\mathcal{R}^f$. Так как $F = \alpha I + \beta A + \gamma(J - I - A)$, то всякий вектор из S имеет длину $\alpha^{1/2}$, а два вектора из S имеют угол $\cos^{-1}(\beta/\alpha)$ или $\cos^{-1}(\gamma/\alpha)$. Нам, стало быть, надо показать, что такое множество может иметь мощность, не превосходящую $f(f+3)/2$. Можно ввести нормировку $\alpha = 1$, предполагая тем самым, что S есть подмножество единичной сферы Ω.

Для $v \in S$ пусть $f_v : \Omega \to \mathcal{R}$ — функция, определяемая по правилу $f_v(x) = ((v, x) - \beta)\,((v, x) - \gamma)/((1 - \beta(1 - \gamma))$. Ясно, что f_v есть полиномиальная функция степени 2 и все функции $f_v\,(v \in S)$ линейно независимы, поскольку $f_v(v) = 1$, $f_v(w) = 0$, $v, w \in S$, $v \neq w$. Но пространство однородных линейных и квадратичных функций на Ω имеют размерности f и $f(f+1)/2$ соответственно; и значит, можно пренебречь константами, поскольку $x_1^2 + \ldots + x_f^2 = 1$ на Ω. Таким образом, $n = |S| = f + f(f+1)/2$.

6 (к стр. 29)

4*. Частичные геометрии

Начинаем эту главу теоремой Чанга [18] и Хоффмана [29*], о которой ранее упоминалось в гл. 2. Клика в графе определяется как максимальный полный подграф.

Теорема 4*.1. *Пусть* Γ — *сильно регулярный граф с теми же параметрами, что и у графа* $T(n)$, *где* $n \geqslant 8$. *Тогда* Γ *изоморфен* $T(n)$.

Доказательство. Для любой вершины x графа Γ граф $\Gamma(x)$ содержит регулярный граф Δ степени $n-2$ на $2(n-2)$ вершинах. Пусть y, $z \in \Gamma(x)$ не смежны, и пусть m вершин $\Gamma(x)$ смежны с y и z. Поскольку $c = 4$ и x смежны с y и z, то $m \leqslant 3$. Имеется $n - 2 - m$ вершин графа $\Gamma(x)$, смежных с y, но не смежных с z, $n - 2 - m$ вершин, смежных с z и не смежных с y, и, наконец, $m - 2$ вершин, не смежных ни с y, ни с z; значит, $m \geqslant 2$. Если $m = 3$, то пусть w — вершина, не смежная ни с y, ни с z. Тогда каждая вершина графа $\Gamma(x)$, смежная с w, смежна либо с y, либо с z, откуда $n - 2 \leqslant 3 + 3$, что противоречит предположению. Значит, $m = 2$.

Рассмотрим дополнительный граф $\bar{\Delta}$. Предположим, что он содержит цикл нечетной длины; выберем такой цикл $C = (x_0, x_1, \ldots, x_k = x_0)$ с минимально возможным k. Тогда, значит, нет ребер $\{x_i, x_j\}$ в $\bar{\Delta}$ с $i - j \not\equiv \pm 1 \pmod{k}$; такое ребро делило бы цикл C на два меньших цикла, один из которых имел бы нечетную длину. Из предыдущего абзаца следует, что $k \neq 3$. Вершины x_0 и x_1 не смежны в Δ и имеют $k - 4$ общих соседей $x_3, \ldots, x_{k-2}$; значит, $k \leqslant 6$. Итак, $k = 5$. Имеется $n - 5$ вершин,

смежных с x_0 в $\bar{\Delta}$ (иных, чем x_1 и x_4); они должны быть не смежны с x_1 и x_4. Аналогично имеется $n-5$ вершин, не смежных с x_1 и x_3. Поскольку x_1 не смежна с $n-4$ с вершинами вне C, то имеется по крайней мере $n-6$ вершин вне C, не смежных с x_3 и x_4. Согласно предыдущему абзацу $n-6 \leqslant 1$, что противоречит предположению.

Итак, граф $\bar{\Delta}$ не содержит нечетных циклов; стало быть, он двудолен. Это означает, что Δ содержит две непересекающиеся клики размера $n-2$. Эквивалентно: всякая вершина в Γ лежит в двух «больших кликах» размера $n-1$, а всякое ребро — в единственной большой клике. Имеется $((n-1)n/2)\cdot(2/(n-1))=n$ больших клик и две, имеющие не более (а значит, точно) чем одну общую вершину. Таким образом, большие клики и вершины являются точками и блоками 2-$(n, 2, 1)$-схемы (парная схема на n вершинах), а Γ есть ее блок-граф; значит, $\Gamma \cong T(n)$.

Эта теорема верна и при ослабленных ограничениях: $n \neq 8$.

Случаи $n < 8$ нужно проверять отдельно. При $n = 8$ имеются три исключительных графа, описанных в [19].

Для изучения больших клик в более общих сильно регулярных графах в [11] введено следующее

Определение 4.*2. *Частичная геометрия* с параметрами (r, k, t) есть инцидентностная структура из точек и прямых, удовлетворяющая следующим условиям:

1) всякая точка инцидентна r прямым, а всякая прямая — k точкам;

2) две точки инцидентны не более чем одной прямой;

3) если точка p не инцидентна прямой L, то найдется ровно t точек, инцидентных L и коллинеарных с p.

Заметим, что двойственной к частичной геометрии с параметрами (r, k, t) оказывается частичная геометрия с параметрами (k, r, t).

Определение 4.*3. *Точечный граф* частичной геометрии имеет в качестве вершин точки геометрии, две вершины в нем смежны всякий раз как они коллинеарны (как точки геометрии.)

Предложение 4.*4. *Пусть* Γ — *точечный граф частичной геометрии с параметрами* (r, k, t). *Тогда* Γ *сильно регулярен с параметрами* $a = r(k-1)$, $c = (k-2)+(r-1)(t-1)$, $d = rt$.

Линейный граф частичной геометрии определяется двойственным образом; он также сильно регулярен.

В доказательстве теоремы 4.*1 мы просто показали, что точки и большие клики образуют частичную геометрию с параметрами $(2, n-1, 2)$. В доказательстве теоремы 4.*6 (см. [11]) используется та же самая идея.

Определение 4.*5. Сильно регулярный граф называем *псевдогеометрическим* (r, k, t)-*графом*, если $a = r(k-1)$, $c = (k-2)+(r-1)(t-1)$, $d = rt$; назовем его *геометрическим*, если он является точечным графом некоторой частичной геометрии.

Теорема 4.*6 [11]. *Псевдогеометрический* (r, k, t)-*граф является геометрическим, если* $k > (1/2)\,[r(r-1)+t(r+1)\times\times(r^2-2r+2)]$.

Поскольку частичная геометрия с параметрами $(n-1, 2, 2)$ с необходимостью является парной схемой на n точках, то 4.*1

можно рассматривать как специальный случай 4.*6. Иной важный специальный случай представляет

Теорема 4.*7 [61]. *Сильно регулярный граф с теми же параметрами, что и $L_2(n)$, при $n > 4$ изоморфен $L_2(n)$.*

Доказательство. Согласно 4.*6 такой граф является геометрическим. Но частичная геометрия $(n, 2, 1)$ есть полный двудольный граф, и значит, двойственная ей $(2, n, 1)$ с необходимостью есть $n \times n$-квадратная решетка.

Эта теорема верна при $n \neq 4$. В случае $n = 4$ Шрикханде нашел, что имеется единственное исключение. Это граф на рис. 4.*1, в котором противоположные стороны отождествляются, как это показано (т. е. это следует рассматривать как рисунок на торе).

Мы не пойдем далее в изучении частичных геометрий, отсылая читателя к [11] и [44*]. Вместо этого опишем четыре связи с теоремой схем. Во-первых, тривиальные: частичная геометрия $t = k$ есть то же самое, что и 2-$(v, k, 1)$-схема (с $(v - 1) = r(k - 1)$), а ее линейный граф есть блок-граф схемы (см. гл. 3).

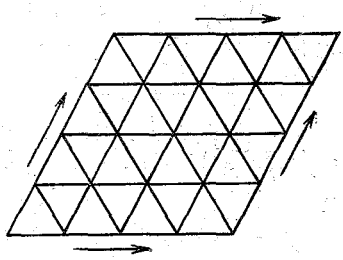

Рис. 4*.1.

Во-вторых, остановимся на двух конструкциях частичных геометрий, получаемых из овалов. Пусть Π — проективная плоскость порядка n, а O — это овал типа II в Π. Тогда точки вне O и секанты к O образуют частичную геометрию с параметрами $r = (n + 2)/2$, $k = n - 1$, $t = (n - 2)/2$. Если плоскость Π — дезаргова, то можно понимать O как совокупность одномерных подпространств векторного пространства $V = V(3, n)$, где n-степень 2. Рассматривая элементы V как точки, а множества членов овала O как прямые, получаем частичную геометрию с параметрами $r = n + 2$, $k = n$, $t = 1$. (Частичная геометрия с $t = 1$ называется *обобщенным четырехугольником.*)

В-третьих, покажем, как теорема Холла — Коннора может быть выведена из 4.*1.

Теорема 4.*8. [26*]. *Квазивычетная схема с $\lambda = 2$ является вычетной.*

Доказательство. Пусть $\mathcal{D}$ — 2-(v, k, λ)-схема с $v = k(k + 1)/2$. Предполагаем, что $k > 6$ (случаи $k < 6$ следуют тем же, но слегка усиленным, способом из 4.*1, в то время как случай $k = 6$ требует отдельного рассмотрения). Пусть B — блок $\mathcal{D}$, а n_i — число блоков, которые пересекают B в i точках $(i \geqslant 0)$. Подсчитывая как в (1.7), находим, что $\sum n_i = k(k + 3)/2$ $\sum i n_i = k(k + 1)$, $\sum i(i - 1) n_i = k(k - 1)$. Таким образом, $\sum (i - 1)(i - 2) n_i = 0$. Отсюда $n_i = 0$ при всех i за исключением $i = 1$ или 2. Значит, всякие два блока $\mathcal{D}$ пересекаются в 1 или 2 точках и $\mathcal{D}$ квазисимметрична.

Пусть Γ — блок-граф схемы $\mathcal{D}$ (где смежность соответствует пересечению мощности 1). Тогда Γ сильно регулярен и имеет те

же параметры, что и $T(k+2)$. Согласно 4.*1 $\Gamma \cong T(k+2)$, т. е. можно так пометить блоки 2-подмножествами множества $X = \{1, \ldots, k+2\}$, что два блока пересекаются в i точках тогда и только тогда, когда их метки пересекаются в $2-i$ точках для $i = 1, 2$. Присоединим теперь X к точечному множеству схемы $\mathcal{D}$; присоединим к каждому блоку его метку и будем считать X за новый блок. Получим тем самым симметричную схему с $\lambda = 2$, чей остаток относительно X есть $\mathcal{D}$.

Развивая эти идеи, Боуз, Шрикханде и Сингхи получили следующий результат.

Теорема 4.*9. [6*]. *Существует функция g, определенная на натуральных числах и обладающая тем свойством, что квазивычетная схема с $k > g(\lambda)$ является вычетной.*

В частности, они нашли, что

$$g(\lambda) = \begin{cases} 76, & \lambda = 3, \\ \frac{1}{2}(\lambda-1)(\lambda^4 - 2\lambda^2 + \lambda + 2), & 4 \leqslant \lambda \leqslant 9, \\ \frac{1}{2}(\lambda-1)(\lambda-2)\left(M + \sqrt{M^2 + 4(\lambda-1)}\right), & -(\lambda-1), \lambda \geqslant 10, \end{cases}$$

где $M = (\lambda-1)(\lambda^2 - 3\lambda + 3)$.

Наконец, связь с латинскими квадратами. Известно, что существование аффинной плоскости порядка n эквивалентно существованию системы из $n-1$ взаимно ортогональных латинских квадратов порядка n (см. [24], стр. 142). То же рассуждение указывает на более общий факт — эквивалентность существования частичной геометрии с параметрами $(r, n, r-1)$ существованию $r-2$ ортогональных латинских квадратов порядка n. Такая частичная геометрия называется *сеткой*. Например, пусть $V = V(2, n)$ — 2-мерное векторное пространство и S — некоторое множество его 1-мерных подпространств. Тогда комножества из членов S являются прямыми сетки на точечном множестве V.

Связи 4.*7 с латинскими квадратами см. в [8*].

Мы вернемся к частичным геометриям в гл. «Конечные геометрии и коды».

Смежные классы геометрий, включающие в себя обобщенные многоугольники, получастичные геометрии, геометрии Мура и частично геометрические схемы см. соответственно в [23*, 16*, 31*, 6*].

7 (к стр. 36)

Результаты этого раздела могут быть обобщены. Имеется неравенство («граница Крейна») для произвольных сильно регулярных графов, которое включает в себя (4.3); случай равенства характеризуется результатом, близким к (4.5). Все это подробнее обсуждается в главе «Ассоциативные схемы».

8 (к стр. 47)

Аналогичный результат имеет место и для решетчатых графов:

Теорема 6.8. *Пусть H — группа автоморфизмов ранга 3 $L_2(k)$, а G — транзитивное расширение группы H. Тогда $k = 3$*

и $G = PSL(2, 9)$ *или* $P\Sigma L$ (2, 9) *действует на регулярном* 2-*графе на* 10 *точках.*

См. [9*, 10*].

9 (к стр. 47)

8*. 1-факторизации графа K_6

В этой главе демонстрируется замечательное комбинаторное свойство числа 6, которое применимо для построения и доказательства единственности проективной плоскости порядка 4, графа Мура степени 7 и 5-(12, 6, 1) штейнеровой системы. Этот материал основан на лекциях Хигмана.

Пусть $A = \{a, b, c, d, e, f\}$ — множество объема 6, которое мы будем далее понимать как множество вершин полного графа K_6. 1-фактор есть множество из трех взаимно непересекающихся (иначе независимых) ребер, покрывающих все A, а 1-факторизация есть разбиение множества всех пятнадцати ребер A на пять 1-факторов. (Для краткости, вместо ребер, 1-факторов полного графа на A будем просто говорить о ребрах и 1-факторах A.)

Предложение 8.*1. *Существует шесть различных факторизаций* A, *всякие две из которых изоморфны. Два непересекающихся* 1-*фактора содержатся в единственной* 1-*факторизации.*

Доказательство. Всякие два непересекающихся 1-фактора образуют систему из непересекающихся циклов четной длины, стало быть в нашем случае — шестиугольник. Таким образом, в нашем случае шести вершин третий 1-фактор должен уже включать в себя одну или все длинные диагонали этого шестиугольника. Поскольку имеются три длинных диагонали, то каждый 1-фактор должен содержать одну из них, и значит, 1-факторизация определяется однозначно. Имеется $15 \cdot 8$ выборов двух непересекающихся 1-факторов; любая 1-факторизация содержит $5 \cdot 4$ таких пар.

Рассмотрим теперь следующую структуру $\mathcal{D}$: точками служат вершины (элементы множества A) и 1-факторы A; блоками являются ребра и 1-факторизации A. Инцидентность между вершинами и ребрами, а также между 1-факторами и 1-факторизациями устанавливается по включению, тогда как инцидентность между ребрами и 1-факторами — по обратному включению.

Предложение 8.*2. *Структура* $\mathcal{D}$ *образует проективную плоскость порядка* 4.

Доказательство. Структура $\mathcal{D}$ имеет 21 точку. Равенство $k = 5$ выполняется, поскольку ребро содержит 2 вершины и содержится в трех 1-факторах, так как 1-факторизация содержит пять 1-факторов. Равенство $\lambda = 1$ следует из рассмотрения следующих случаев:

1) две точки определяют единственное ребро;

2) для данной точки и 1-фактора единственное ребро этого 1-фактора содержит эту одну точку;

3) два 1-фактора либо имеют единственное общее ребро, либо лежат в единственной 1-факторизации согласно 8.*1.

Следствие 8.*3. *Всякие две* 1-*факторизации обладают единственным общим* 1-*фактором.*

Доказательство. Два блока в проективной плоскости пересекаются в единственной точке.

Следствие 8.*4. *Проективная плоскость порядка* 4 *единственна (с точностью до изоморфизма)*.

Доказательство. Заметим, что A является овалом типа II в плоскости $\mathcal{D}$. Можно показать, что проективная плоскость порядка 4 обязательно содержит овал A типа II. Всякое ребро определяет прямую. Для данной точки x не из A три прямые, проходящие через x и пересекающие A, определяют 1-фактор. Для данной прямой, не пересекающейся с пятью 1-факторов, определяемых ее точками, образуют 1-факторизацию. Таким образом, такая плоскость совпадает с $\mathcal{D}$.

Пусть X — множество 1-факторизаций A. Согласно 8.*3 1-факторы A можно пометить парами элементов множества X, т. е. ребрами X. Ребро A лежит в трех 1-факторах; их пометки не пересекаются, а значит, образуют 1-фактор множества X. Пять 1-факторов X, соответствующих таким образом пяти ребрам, исходящим из одной вершины множества A, образуют 1-факторизацию. Таким образом, мы имеем двойственность между A и X: вершина $\leftrightarrow$ 1-факторизация, ребро $\leftrightarrow$ 1-фактор. (Это может быть также установлено привлечением схемы, двойственной к схеме $\mathcal{D}$.)

Удобно ввести отношение между ребрами A и ребрами X: $ab \sim xy$, если ab является ребром в 1-факторе с пометкой xy. Такое определение самодвойственно, т. е. аналогичным образом определяя $xy \sim ab$, получаем, что $xy \sim ab \Leftrightarrow ab \sim xy$.

Обратимся теперь к конструкции графа Хофмана — Синглетона. Предположим, во-первых, что $\Gamma = M(n+1)$ есть граф Мура степени $n+1$ и диаметра 2. Пусть $\{\infty, 0\}$ есть произвольное ребро, A — множество вершин (отличных от 0), смежных с ∞, а X — множество вершин (отличных от ∞), смежных с 0. Тогда множества A и X не пересекаются. Всякая другая вершина смежна единственной вершине $a \in A$ и единственной вершине $x \in X$, а значит, может быть помечена упорядоченной парой $(a, x) \in A \times X$. Это приводит к описанию ребер в $A \times X$. Для любого такого ребра $\{(a, x), (b, y)\}$ мы должны иметь $a \neq b$ и $x \neq y$; кроме того, если (a, x) смежно с (b, y) и (c, z), то $b \neq c$ и $y \neq z$. Таким образом, для данных $a, b \in A$, $x \in X$ имеется единственная вершина $y \in X$ такая, что (a, x) смежно (b, y).

Отсюда сразу имеем:

1) единственность $M(3)$: если $A = \{a, b\}$ и $X = \{x, y\}$, то $\{(a, x), (b, y)\}$ и $\{(a, y), (b, x)\}$ — ребра;

2) несуществование $M(4)$: если $A = \{a, b, c\}$ и $X = \{x, y, z\}$ и если $\{(a, x), (b, y)\}$ образуют ребро, то (a, x) и (b, y) смежны с (c, z), что и влечет треугольник. Конечно, это также следует из (2.4).

Построение $M(7)$ проведем следующим образом. Отождествим множество A с нашим исходным множеством из шести вершин, а множество X — с множеством из шести 1-факторизаций A. Введем ребра $\{(a, x), (b, y)\}$, где $ab \sim xy$. Рассмотрение ряда случаев показывает, что этот граф сильно регулярен.

Доказательство единственности $M(7)$ основывается на следующей лемме, доказательство которой мы опускаем.

Лемма 8.*5. *Предположим, что множество из десяти вершин $M(7)$ содержит четырнадцать из пятнадцати ребер $M(3)$. Тогда это множество содержит также и пятнадцатое ребро.*

В наших прежних обозначениях это обеспечивает то, что $\{(a, x), (b, y)\}$ является ребром тогда же, когда и $\{(a, y), (b, x)\}$. (Рассмотрите десять вершин ∞, 0, a, b, x, y, (a, x), (a, y), (b, x), (b, y).)

Определим отношение $ab \sim xy$, если оно имеет смысл. Непосредственно проверяется, что это отношение возникает из отождествления X с множеством 1-факторизаций A, как это определялось ранее.

Обратимся теперь к 5-$(12, 6, 1)$-схеме. Выберем три элемента $x, y, z \in X$. Три 1-фактора xy, yz, zx множества A являются попарно не пересекающимися, но не содержатся в 1-факторизации; значит, оставшиеся шесть ребер должны образовывать объединение двух треугольников. Пишем, что $abc \sim xyz$, если abc — один из этих треугольников. Это отношение является также самодвойственным. Возьмем теперь инцидентностную структуру с точечным множеством $A \cup X$ и блоками следующих типов:

A, X;

$A \setminus \{a, b\} \cup \{x, y\}$, $X \setminus \{x, y\} \cup \{a, b\}$ всякий раз как $ab \sim xy$;

$\{a, b, c\} \cup \{x, y, z\}$ всякий раз как $abc \sim xyz$.

Имеется $132 = \binom{12}{5} / \binom{6}{5}$ блоков, и легко проверить, что любые пять точек лежат по крайней мере в одном блоке. Значит, мы имеем требуемую схему. Ее единственность может быть доказана аналогичным способом.

10 (к стр. 54)

Приведем один пример нелинейного кода, в конструкции которого используются схемы. Нетрудно показать, что двоичный код длины 10 с минимальным расстоянием 5 может иметь не более 12 кодовых слов. Для построения кода, реализующего эту границу, возьмем строки матрицы инцидентности 2-$(11, 5, 2)$-схемы Пэли и добавим к этому множеству слово $\bar{1}$, состоящее из единиц. Эти двенадцать двоичных слов имеют, очевидно, расстояние 6. Убирая фиксированную координату, получаем код с требуемыми свойствами.

Читателю, интересующемуся нелинейными кодами, рекомендуем обратиться к [80].

11 (к стр. 56)

Легко видеть, что двоичные коды Хэмминга, определенные как в предыдущей главе, обладают тем свойством, что слова веса 3 представляют систему троек Штейнера на $2^m - 1$ точках (как это мы уже видели для $m = 3$). В действительности, если система троек Штейнера на n точках соответствует множеству слов веса 3 двоичного линейного кода C, то $n = 2^m - 1$ и C есть код Хэмминга, а сама штейнерова система есть $PG(m-1, 2)$.

Для систем троек Штейнера на 9 и 13 точках задача решена (см. [77]). Пусть $q \equiv 1 \pmod 3$, и пусть α — примитивный кубический корень из 1 в $GF(q)$.

Положим

$$H=\begin{bmatrix} 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & -1 & -\alpha & -\alpha \\ -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Тогда H есть проверочная матрица (9.6) линейного кода над $GF(q)$ такого, что ненулевые позиции кодовых слов веса 3 образуют $AG(2, 3)$. Мы отсылаем читателя к [77] за доказательством того, что две неизоморфные системы троек Штейнера на 13 точках невыводимы из линейных кодов таким способом.

12 (к стр. 67)

Рассмотрим сейчас так называемые *эквидистантные коды*. Они представляют собой коды с тем свойством, что всякие два кодовых слова отделены друг от друга в этом коде на одинаковое расстояние d. Код, описанный в конце главы «Коды», представляет собой пример эквидистантного кода с $d = 6$. Мы исследуем лишь случай бинарных кодов. Если d — нечетно, то код, очевидно, может иметь лишь два слова. Если $d = 2k$ и код имеет m слов длины n (где n достаточно велико), то нетрудно показать, что $n \leqslant k^2 + k + 2$ или что код тривиален, т. е. если каждый столбец $m \times n$-матрицы со строками — кодовыми словами — по крайней мере $m - 1$ равных элементов (см. [21*]).

Пусть A — матрица инцидентности $PG(2, k)$. К A добавим $k - 1$ столбцов из единиц и добавим строку из нулей. Полученная матрица имеет своими строками кодовые слова эквидистантного кода с $k^2 + k + 2$ словами с общим расстоянием $d = 2k$. Гораздо более трудно показать, что верно и обратное — если эквидистантный код с $k^2 + k + 2$ словами и общим расстоянием $2k$ существует, то $PG(2, k)$ существует (см. [34*]). Заметим, что в случае $k = 6$, т. е. $d = 2$, максимальное число слов есть 32 (см. [25*]).

Отметим связь между теорией кодирования и частичными геометриями. Известна лишь одна частичная геометрия с $t = 2$ и $\min\{n, k\} > 3$. Ее параметры $-r = k = 6$. Простейший способ описать соответствующий сильно регулярный граф заключается в следующем: возьмем в качестве 81 вершины кодовые слова (5.4) линейного кода C над $GF(3)$, определяемого по правилу $c \in C \Leftrightarrow (c, 1) = 0$, и соединяем две вершины ребром тогда и только тогда, когда расстояние Хэмминга между ними (как кодовыми словами) равно 2 или 5. Нетрудно проверить, что этот граф действительно является сильно регулярным с параметрами $(81, 30, 9, 12)$, собственными значениями 3 и -6 с кратностями 50 и 30. Для построения частичной геометрии следует отобрать 6-клики и рассматривать их как прямые. Сделаем это так: положим $c_0 = 0$, $c_1 = (1, 22, 2, 2)$, $c_2 = (2, 1, 2, 2, 2)$, $c_3 = (2, 2, 1, 2, 2)$, $c_4 = (2, 2, 2, 1, 2)$, $c_5 = (2, 2, 2, 2, 1)$; шесть этих кодовых слов образуют клику в нашем графе. Возьмем теперь множество $S = \{c_0, c_1, c_2, c_3, c_4, c_5\}$ в качестве прямой, а остальные прямые зададим трансляцией, т. е. $c + S$, где $c \in C$. По существу, доказательство того, что мы теперь имеем частичную

геометрию, основывается на том факте, что $\sum_{i=1}^{5} c_i = 0$ есть единственное неотрицательное линейное соотношение, связывающее c_1 с c_5. Следовательно, все разности $c_i - c_j$ $(i \neq j)$ различны. Две точки x и y коллинеарны, если существуют c, i, j такие, что $x = c + c_i$, $y = c + c_j$, т. е. $x - y = c_i - c_j$. Это значит, что две точки лежат не более чем на одной прямой, каждая прямая имеет 6 точек и всякая точка принадлежит 6 прямым. Посредством простых подсчетов можно убедиться, что для неинцидентной «точечно-линейной» пары (x, L) среднее число прямых, проходящих через x и пересекающих L, равно 2. Достаточно взять $x \notin S$ и показать, что имеются две точки в S, коллинеарных с x. Мы видели ранее, что x коллинеарна с c_k, если $x = c_k + c_i - c_j$. Если $k \neq i$, то x также коллинеарна с c_i. Если $k = i$, то $x = -c_i - c_j$ и x коллинеарна с c_j. Имеется 15 комбинаций $c_k + c_i - c_j$ при $k = i \neq j$ и 60 таких комбинаций при попарно различных i, j, k. Согласно вышеприведенному замечанию все эти 75 комбинаций различны, а наличие 75 точек $x \notin S$ завершает доказательство.

За дальнейшей информацией о частичных геометриях и их связях с ассоциативными схемами мы отсылаем читателя к [36*].

13 (к стр. 69)

Наш следующий объект — иной замечательный совершенный код, который даст нам штейнерову систему 5-(24, 8, 1) (см. гл. 1). Рассмотрим (8, 4)-расширенный код Хэмминга $\bar{C}$, как это определялось в примере, следующем за теоремой (8.4). Пусть C' — код, полученный из C обращением порядка символов. Легко проверяется, что $\bar{C} \cap \bar{C}' = \{0, 1\}$. Построим теперь бинарный линейный код G_{24} длины 24, беря в качестве кодовых слов линейные комбинации векторов $(a, 0, a)$, $(0, b, b)$, (x, x, x), где $a \in \bar{C}$, $b \in \bar{C}$, $x \in \bar{C}'$. Следующие замечания очевидны:

1) G_{24} — линейный код размерности 12;

2) любые два базисных вектора ортогональны, т. е. G_{24} — самодвойственный код;

3) все базисные векторы имеют вес, кратный 4, и стало быть из 2) следует, что это выполняется для всех кодовых слов в G_{24};

4) если в некотором кодовом слове (p, q, r) один из символов p, q или r есть 0, то (p, q, r) есть линейная комбинация базисных векторов с $x = 0$ или 1. Следовательно, вес этого кодового слова есть сумма весов двух ненулевых слов из $\bar{C}$, т. е. 8, или один из символов p, q, r равен 1 и вес вновь равен 8.

Комбинируя 1) с 4), видим, что G_{24} имеет минимальное расстояние 8. Если укоротить G_{24} отбрасыванием одной координаты, то получатся бинарный (23, 12)-код с минимальным расстоянием 7. Тем же способом, что мы действовали ранее для тернарного кода Галея, находим, что этот код совершенен. Этот знаменитый код известен как *бинарный код Галея* (G_{24} есть соответствующий расширенный код).

Взглянем теперь на слова веса 8 в G_{24}. Поскольку код Галея совершенен, можно выписать его весовой нумератор (читатель

должен проверить это) и найти, что G_{24} имеет 759 слов веса 8. Поскольку нет двух из этих слов с 1 на одних и тех же пяти позициях, то они покрывают $759\binom{8}{5}=\binom{24}{5}$ различных пятерок. Следовательно, эти кодовые слова представляют блоки 5-(24, 8, 1)-схемы.

В [24*] показано, что код G_{24} может быть деколирован различными методами, обсуждавшимися в гл. 9.

14 (к стр, 73)

Обратимся теперь к обобщению теоремы 11.6. Заменим обычное скалярное произведение в $\mathscr{R}^{(N+1)}$, где $N=n^2+n+1$, на скалярное произведение Минковского

$$\langle x, y\rangle = x_1y_1 + x_2y_2 + \ldots + x_Ny_N - x_{N+1}y_{N+1}.$$

Теорема 11.12. *Пусть A — матрица инцидентности проективной плоскости π порядка n, а C — код, порожденный строками матрицы A над $GF(p)$ с присоединенной проверкой на четность. Тогда если $p\|n$, то C самодвойствен относительно скалярного произведения Минковского.*

Теорема 11.13 [32*]. *Пусть π — проективная плоскость порядка n с матрицей инцидентности A. Пусть $N=n^2+n+1$ и p — такое простое, что $p^s\|n$ $(s>0)$. Тогда существует последовательность*

$$\{0\}=C_{-1}\subseteq C_0\subseteq\ldots\subseteq C_s=\mathscr{R}^{(N+1)}$$

из кодов длины $N+1$ над $GF(p)$ со следующими свойствами:

1) *каждый код C_i инвариантен относительно всех автоморфизмов проективной плоскости π;*

2) *C_0 есть расширенный код, порожденный строками матрицы A;*

3) *для $-1\leqslant i\leqslant s$ $C_i^{\perp}=C_{s-1-i}$ (относительно скалярного произведения Минковского);*

4) *$\dim C_i$ равна числу инвариантных факторов A, не делящихся на p^{i+1} для $i<s$;*

5) *для $0\leqslant i\leqslant s-1$ C_i имеет минимальный вес $n+2$ и слова веса $n+2$ в C_0 соответствуют прямым или (возможно, если $p=2$) овалам в π.*

Замечания. 1. Если s нечетно, из 3) видим, что $C_{(s-1)/2}$ есть самодвойственный код, соответствующий π.

2) Ландер вычислил размерности кодов C_i в случае дезарговой плоскости π, обобщая тем самым известный результат, что в этом случае $\dim C_0=1+\binom{p+1}{2}^s$ (см. [28]).

Теорема 11.8 привела к новой попытке найти $PG(2, 10)$ (см. [2*, 3*, 45*]).

Пусть A — матрица инцидентности блок-схемы 2-(56, 11, 2) (четыре из которых известны, см. гл. 4). Тогда строки $G=(I_{56}A)$ порождают (112, 56)-бинарный самодвойственный код C. Будем обсуждать лишь тот случай, когда 2-(56, 11, 2)-схема соответствует графу Гевиртца. В этом случае A симметрична, и стало быть (AI_{56}) также является порождающей матрицей для C. Это

значит, что для демонстрации того, что C имеет минимальный вес 12, достаточно рассмотреть сумму $i \leqslant 6$ строк G. Пусть x_j $(1 \leqslant j \leqslant 56)$ — число единиц в i выбранных строках и j-м столбце матрицы A. Тогда имеем $\sum x_j = 11i$, $\sum \binom{x_j}{2} = 2\binom{i}{2}$. Стало быть $\sum x_j (x_j - 2) = 2i^2 - 13i$, т. е. по крайней мере $13i - 2i^2$ столбцов имеют ровно одну 1, что и показывает, что все суммы этих i строк — по крайней мере $2i(7 - i)$. Это равно 12, если $i = 1$ или 6. Кроме того, если сумма 6 строк G равна 12, то $x_j = 0$ для 20 значений j, $x_j = 1$ для 6 значений j, $x_j = 2$ для остальных 30 столбцов A. Значит, эти 6 строк A обладают тем свойством, что нет точки, расположенной более чем в двух из них, т. е. они соответствуют тангентам некоторого овала в 2-(56, 11, 2). В случае удачи (112, 56)-код соответствует $PG(2, 10)$. Тогда мы можем реконструировать плоскость, используя теорему 11.8, рассмотрением овалов 2-(56, 11, 2)-схемы, проходящих через фиксированную точку. Другие схемы с теми же параметрами могут быть рассмотрены аналогичным образом. Ни одна из известных схем не привела к желаемому результату.

Теорема 11.14 [1*]. *Пусть $\mathcal{D}$ — симметричная 2-(v, k, λ)-схема с $k \equiv 0 \pmod 4$, $\lambda \equiv 2 \pmod 4$, $\lambda \mid k$. Предположим, что $\mathcal{D}$ имеет овалы и что эти овалы также образуют 2-(v, K, Λ)-схему. Тогда $\mathcal{D}$ есть единственная 2-(7, 4, 2)-схема.*

15 (к стр. 83)

Рядом авторов обобщалась идея КВ-кодов (см. [14, 76, 70, 79]). Мы лишь кратко опишем здесь эти идеи и покажем связь с некоторыми хорошо известными схемами. В обобщении длина кода есть $q = p^m$ $(m > 1)$. Мы возьмем $m = 2$. В качестве алфавита мы можем использовать любое конечное поле F. Пусть G — аддитивная группа поля $GF(q)$. Мы отождествляем позиции кода с элементами G и представляем кодовое слово как выражение

$$c = \sum_{g \in G} c_g x^g \qquad (c_g \in F), \tag{12.20}$$

которое должно рассматривать как формальное. Заметим, что это соответствует представлению циклических кодов в случае $m = 1$, где $G = \{0, 1, \ldots, p - 1\}$.

Групповая алгебра FG состоит из всех выражений вида (12.20) со следующими правилами сложения и умножения:

$$\begin{aligned} \sum a_g x^g \oplus \sum b_g x^g &= \sum (a_g + b_g) x^g, \\ \sum a_g x^g * \sum b_g x^g &= \sum \Big(\sum_{g_1 + g_2 = g} a_{g_1} b_{g_2} \Big) x^g, \end{aligned} \tag{12.21}$$

где суммирование проводится по всем $g \in G$. Тогда $(FG, \oplus, *)$ образует кольцо.

Пусть ξ — примитивный p-й корень единицы в некотором расширении F поля F. Пусть α — примитивный элемент поля $GF(q)$. Каждый элемент $g \in G$ может быть представлен как $g = i_0 + i_1\alpha$

с i_0 и i_1 из $GF(p)$. Определим теперь *характер* ψ_1: $G \to F$ по правилу:

$$\psi_1(g) = \xi^{i_0} \tag{12.22}$$

и для каждого $h \in G$ определяем характер ψ_h по правилу

$$\psi_h(g) = \psi_1(gh). \tag{12.23}$$

Наконец, характеры, расширенные до FG, линейны по определению:

$$\psi_f\left(\sum_{g \in G} a_g x^g\right) = \sum_{g \in G} a_g \psi_f(g). \tag{12.24}$$

Читатель, близко знакомый с теорией характеров, увидит, что мы сейчас имеем все характеры G и что $h \leftrightarrow \psi_h$ устанавливает изоморфизм между G и группой характеров. Мы опускаем доказательство фактов, приводимых ниже (см. [79]). Обозначаем через U (соотв. V) множество ненулевых квадратов (соотв. неквадратов) в G.

Определение 12.25. *Обобщенный квадратично-вычетный код* (ОКВ-код) длины q над F состоит из всех $c = \sum c_g x^g$ таких, что $\psi_u(c) = 0$ для всех $u \in U$.

Обозначаем этот код через A^+ и обозначаем через B^+ код, получаемый заменой U на V в (12.25). Коды A и B являются подкодами, определяемыми дополнительным требованием $\psi_0(c) = 0$. Из независимости характеров видим, что A^+ имеет размерность $(q+1)/2$.

Читатель должен сейчас убедиться, что если $m = 1$, то (12.25) совпадает с (12.6).

В [79] показано, что идея идемпотента (см. (12.1)) может быть обобщена. Тем же способом, какой указан в замечании после (12.10), можно расширить A^+ и B^+ до A_∞ и B_∞ соответственно добавлением нового символа к кодовым словам, так что расширенные коды являются двойственными. Можно показать, что оба эти кода инвариантны относительно $PSL(2, q)$. Это значит, что и теорема (12.7) тоже обобщаема. Действительно, в этом случае можно показать, что если $K = GF(p)$, то слово $c = \sum_{g \in K} x^g$ лежит в A^+. Стало быть мы действительно знаем, что минимальный вес равен p. Итак, имеем полное обобщение теории КВ-кодов.

Довольно трудное доказательство показывает, что только слова минимального веса в A_∞ являются словами в орбите $\left(\sum_{g \in K} x^g, 1\right)$ относительно $PSL(2, q)$ и кратны этим словам. Это значит, что объединение поддержек (носителей) кодовых слов минимального веса в A_∞ и B_∞ являются образами $GF(p) \cup \{\infty\}$ под действием $PGL(2, p^2)$ на проективную прямую порядка p^2 (представляемую посредством $G \cup \{\infty\}$). Значит, эти слова образуют Мёбиус-плоскость $3-(p^2+1,\ p+1, 1)$ (см. гл. 1). Вновь мы нашли схему из слов минимального веса в коде (и двойственному). Коды, обсуждавшиеся здесь выше, впервые построил (для $F = GF(2)$) Дельсарт [76] исходя из схем. Дополнительно по этой главе см. [49, 64].

16 (к стр. 89)

Теория равномерно упакованных кодов развивалась Геталсом и ван Тилборгом. Обзор большинства известных результатов об этих кодах представлен в [81]. Ниже, в этой главе, будут описаны некоторые из связей между равномерно упакованными кодами, так называемыми двухвесовыми кодами и сильно регулярными графами.

17 (к стр. 91)

Определение 14.5. e-код C, исправляющий ошибки, длины n над $GF(q)$ называется *равномерно упакованным* с параметрами α и β тогда и только тогда, когда для каждого слова $x \in \mathcal{R}^{(n)}$ выполнены два условия:

1) если x имеет расстояние e до C, то x имеет расстояние $e+1$ в точности до α кодовых слов;

2) если x имеет расстояние $>e$ до C, то x имеет расстояние $e+1$ в точности до β кодовых слов, где $\alpha < (n-e)(q-1)/(e+1)$.

18 (к стр. 97)

Посредством приводимой ниже теоремы, следующей из общей теории равномерно упакованных кодов, подчас легче решить, является ли данный код равномерно упакованным, нежели пользоваться самим определением. За ее доказательством мы отсылаем читателя к [81].

Теорема 14.22. *Пусть C — линейный e-код, исправляющий ошибки. Тогда C является равномерно упакованным (соотв. совершенным) тогда и только тогда, когда число ненулевых весов в двойственном коде $C^{\perp}$ есть $e+1$ (соотв. e).*

Если в теореме 14.22 $e=1$, то $C^{\perp}$ имеет лишь два ненулевых веса. Такой код называется *двухвесовым кодом.*

Пример 14.23. Пусть H — проверочная матрица кода Хэмминга длины $(q^m-1)/(q-1)$ над $GF(q)$. Столбцы матрицы H представляют собой точки $PG(m-1, q)$. Пусть столбцы занумерованы так, что первые $(q^k-1)/(q-1)$ столбцов образуют подпространство $S = PG(k-1, q)$. Пусть $c=(c_1, \ldots, c_m)$. Уравнение $c_1x_1 + c_2x_2 + \ldots + c_mx_m = 0$ представляет гиперплоскость в $PG(m-1, q)$, которая либо содержит S, либо пересекает S в $(q^{k-1}-1)/(q-1)$ точках. Это значит, что линейная комбинация строк матрицы H имеет $(q^k-1)/(q-1)$ нулей или $(q^{k-1}-1)/(q-1)$ нулей в позициях, соответствующих S. Отбросим теперь столбцы, соответствующие S, и образуем код из строк оставшейся матрицы. Этот код имеет размерность m, а кодовая строка — веса q^{m-1} или $q^{m-1}-q^{k-1}$. По теореме 14.22 этот код двойствен равномерно упакованному коду.

Следующие две теоремы, принадлежащие Дельсарту [17*], показывают, как двухвесовые коды соотносятся с некоторыми сильно регулярными графами. Если столбцы порождающей матрицы линейного кода C попарно линейно независимы (т. е. $C^{\perp}$ имеет минимальный вес $\geqslant 3$), то код C называется *проективным.*

Теорема 14.24. *Пусть C — двухвесовой проективный код с весами W_1, W_2 $(W_1 < W_2)$. Определим граф $\Gamma(C)$, считая вер-*

шинами кодовые слова и соединяя слова x и y ребром тогда и только тогда, когда $d(x, y) = W_1$. *Тогда* $\Gamma(C)$ — *сильно регулярный граф.*

Следующая теорема есть обращение теоремы 14.24.

Теорема 14.25. *Пусть* Γ — *сильно регулярный граф на* $n = p^k$ *вершинах,* p — *простое, с целыми собственными значениями* a, ρ_1, ρ_2. *Пусть элементарная абелева* p-*группа* G_n *будет регулярной группой автоморфизмов графа* Γ. *Тогда существует двухвесовой код* C *над* $GF(p)$ *такой, что* $\Gamma = \Gamma(C)$.

За доказательством отсылаем к [17*]. В доказательстве показывается, что собственные значения для N слов из C и весов W_1, W_2 из C связаны соотношениями

$$(\rho_1 - \rho_2)(p - 1)N = -a - \rho_2(p^k - 1), \tag{14.26}$$

$$(\rho_1 - \rho_2)W_1 = \left(-\rho_2 + \frac{(-1)^i - 1}{2}\right)p^{k-1}, \quad i = 1, 2. \tag{14.27}$$

Эта теорема позволяет выявить связи между целым рядом объектов. В качестве примера рассмотрим частичную геометрию с параметрами $r = k = 6$, $t = 2$. Такая геометрия ассоциирована с сильно регулярным графом Γ с параметрами 81, 30, 9, 12 и $\rho_1 = 3$, $\rho_2 = -6$. Граф Γ был определен из (5, 4)-кода над $GF(3)$ таким образом, что трансляция над кодовым словом является, очевидно, автоморфизмом. Значит, Γ допускает элементарную абелеву группу порядка 81 в качестве группы автоморфизмов. Стало быть теорема 14.25 утверждает, что граф Γ соответствует двухвесовому коду размерности 4 над $GF(3)$, который имеет длину слов $N = 5$ и веса 15 и 18. По теореме 14.22 код, двойственный к этому коду, есть равномерно упакованный код.

19 (к стр. 105)

Другие понятия из теории кодирования (такие, например, как равномерно упакованные коды), так же как и теорема о таких кодах, тоже могут быть обобщены до метрических схем. Однако концепции теории схем более естественно возникают в Q-полиномиальных схемах. Просматривается аналогия, или «формальная двойственность», между определенными парами понятий, которая полезна в предсказывании результатов о Q-полиномиальных схемах, для которых нет простого эквивалента «метрического» условия для P-полиномиальных схем (15.3).

Для данной ассоциативной схемы пусть $E_0, \ldots, E_n$ — минимальные идемпотенты алгебры Боуза — Меснера $\mathfrak{A}$. Таким образом, E_i — матрица в $\mathfrak{A}$ с собственным значением 1 на i-м собственном пространстве и 0 на других. По определению P

$$A_k = \sum_{i=0}^{n} P_{ik}E_i,$$

откуда

$$E_i = |X|^{-1} \sum_{k=0}^{n} Q_{ki}A_k.$$

Имеем $E_iE_j = \delta_{ij}E_i$.

Имеется вторая операция, определенная на $\mathfrak{A}$; именно, адамарово (или поточечное) произведение $(a_{ij}) \circ (b_{ij}) = (a_{ij}b_{ij})$. Поскольку каждая A_i есть 0-1-матрица, то выявленные свойства обеспечивают тот факт, что $A_i \circ A_j = \delta_{ij}A_i$, откуда $A_0, \ldots, A_n$ — минимальные идемпотенты относительно этого умножения. Поскольку $\mathfrak{A}$ замкнута относительно адамарова произведения, имеем

$$E_i \circ E_j = \sum_{k \| 0}^{n} b_{ijk} E_k$$

для некоторых действительных чисел b_{ijk}, задаваемых равенством

$$|X|^2 \mu_k b_{ijk} = \sum_{m=0}^{n} n_m Q_{mi} Q_{mj} Q_{mk}.$$

Числа b_{ijk} известны как *параметры Крейна*, потому что следующий результат, доказанный Скоттом [40*], был доказан с использованием теоремы Крейна.

Теорема 15.6*. $0 \leqslant b_{ijk} \leqslant 1$.

Доказательство. Адамарово произведение $E_i \circ E_j$ есть главная подматрица кронекерова произведения $E_i \otimes E_i$, и значит ее собственные значения b_{ijk} ограничены сверху и снизу собственными значениями матрицы $E_i \otimes E_j$, которая является идемпотентом.

Для сильно регулярных графов граница Крейна принимает следующую форму:

Предложение 15.7*. *Пусть* Γ — *сильно регулярный граф, чья матрица смежности имеет собственные значения* a, ρ_1, ρ_2. *Предположим, что и* Γ, *и его дополнение связны. Тогда*

$$(\rho_1 + 1)(a + \rho_1 + 2\rho_1\rho_2) \leqslant (a + \rho_1)(\rho_2 + 1)^2,$$

$$(\rho_2 + 1)(a + \rho_2 + 2\rho_2\rho_1) \leqslant (a + \rho_2)(\rho_1 + 1)^2.$$

Замечание. (4.3) есть следствие этого результата, как это уже отмечалось в конце гл. 4.

Обращение в нуль параметров Крейна имеет и комбинаторный смысл, см. [11*, 12*]. Например, если имеет место равенство в обеих границах (15.7), то графы $\Gamma|\Gamma(p)$ и $\Gamma|\overline{\Gamma}(p)$ оба сильно регулярны для любой вершины p. Обратно, если $\Gamma|\Gamma(p)$ и $\Gamma|\overline{\Gamma}(p)$ сильно регулярны для некоторой вершины p, то в (15.7) имеют место равенства, за исключением некоторых параметрических множеств.

Параметры Крейна формально двойственны числам пересечений a_{ijk}. Например, ассоциативная схема Q-полиномиальна тогда и только тогда, когда $b_{ijk} = 0$, за исключением $|i - j| \leqslant k \leqslant i + j$, и в то же время $b_{i\,i+1} \neq 0$ для $1 \leqslant i \leqslant n - 1$. В этом же смысле теории метрических и Q-полиномиальных схем двойственны.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1*. Assmus F. F., van Lint J. H. Ovals in projective designs. — J. Combinatorial Theory (A), 1979, **27**, p. 307—324.

2*. Assmus F. F., Jr., Mezzaroba J. A., Salwach C. J. Planes and biplanes. — In: Higher Combinatorics/Ed. M. Aigner. Dordrecht, 1977, p. 205—212.

3*. Assmus F. F., Sachar H. F. Ovals from the point of view of coding theory. — In: Higher Combinatorics/Ed. M. Aigner. Dordrecht, 1977, p. 213—216.

4*. Bannai F. On tight designs. — Quart. J. Math. (Oxford), 1977, **28**, p. 433—448.

5*. Biggs N. L. Perfect codes and distance-transitive graphs. — In: Combinatorics/Ed. T. P. McDonough and V. C. Mavron. C. U. P. 1974, p. 1—8. — (L. M. S. Lecture Notes; **13**).

6*. Bose R. C., Shrikhande S. S., Singhi N. M. Edge-regular multigraphs and partial geometric designs. — In: Teorie Combinatorie, t. I. Rome: Accad. Naz. Lincei, 1977.

7*. Bremmer A. A diophantine equation arising from tight 4-designs. — Osaka J. Math., 1979, **167**, p. 353—356.

8*. Bruck R. H. Finite sets II: uniqueness and embedding. — Pacific J. Math., 1963, **13**, p. 421—457.

9*. Cameron P. J. Biplanes. — Math. Z., 1973, **131**, p. 85—101.

10*. Cameron P. J. On doubly transitive permutation groups of degree prime squared plus one. — J. Austral. Math. Soc. (A), 1978, **26**, p. 317—318.

11*. Cameron P. J., Goethals J. M., Seidel J. J. The Krein condition, spherical designs, Norton algebras and permutation groups. — Proc. Kon. Nederl. Akad. Wetensch. (A), 1978, **81** (Indag. Math., 1978, **40**), p. 196—206.

12*. Cameron P. J., Goethals J. M., Seidel J. J. Strongly regular graphs having strongly regular subconstituents. — J. Algebra, 1978, **55**, 257—280.

13*. Cameron P. J., Thas J. A., Payne S. E. Polarities of generalized hexagons and perfect codes. — Geometriae Dedicata, 1976, **5**, p. 525—528.

14*. Camion P. Global quadratic abelian codes. — In: Information Theory/Ed. G. Longo. Vienna: Springer-Verlag, 1975. — (CISM Courses and Lectures No. **219**).

15*. Cohn P. M. Algebra, v. 1. — London: Wiley, 1974.

16*. Debroey I., Thas J. A. On semipartial geometries. — J. Combinatorial Theory (A), 1978, **25**, p. 242—250.

17*. Delsarte P. Weights of linear codes and strongly regular normed spaces. — Discrete Math., 1972, 3, p. 47—64.
18*. Delsarte P., Goethals J. M., Seidel J. J. Orthogonal matrices with zero diagonal, II. — Canad. J. Math., 1971, 23, p. 816—832.
19*. Delsarte P., Goethals J. M., Seidel J. J. Spherical codes and designs. — Geometriae Dedicata, 1977, 6, p. 363—388.
20*. Denniston R. H. F. Some new 5-designs. — Bull. London Math. Soc., 1976, 8, p. 263—267.
21*. Deza M Une propriete extremale des plans projectifs finis dans une classe de codes equidistants. — Discr. Math., 1973, 6, p. 353—358.
22*. Doyen J., Hubaut X., Vandensaval M. Ranks of incidence matrices of Steiner triple systems. — Math. Z. — (В печати.)
23*. Feit W., Higman G. The nonexistence of certain generalized polygons. — J. Algebra, 1964, 1, p. 434—446.
24*. Goethals J. M. On the Golay perfect binary code. — J. Combinatorial Theory (A), 1971, 11, p. 178—186.
25*. Hall J. L., Janssen A. J. E. M., Kolen A. W. J., van Lint J. H. Equidistant codes with distance 12. — Dicrete Math., 1977, 17, p. 71—83.
26*. Hall M., Connor W. S. An embedding theorem for balanced incomplete block desings. — Canad. J. Mat., 1953, 6, p. 35—41.
27*. Hamada N. On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes. — Hiroshima Math. J., 1973, 3, p. 153—226.
28*. Higman D. G., Sims C. C. A simple group of order 44, 352, 000. — Math. Z., 1968, 105, p. 110—113.
29*. Hoffman A. J. On the uniqueness of the trinagular association scheme. — Ann. Math. Statist., 1960, 31, p. 492—497.
30*. Ito N. Tight 4-designs. — Osaka J. Math., 1975, 12, p. 493—522.
31*. Kantor W. M. Moore geometries and rank 3 groups having $\mu = 1$. — Quart. J. Math. (Oxford), 1977, 28, p. 309—328.
32*. Lander E. S. — (В печати.)
33*. Lindström K. The nonexistence of unknown nearly perfect binary codes. — Ann. Univ. Turku, ser. AI, 1975, 169.
34* van Lint J. H. Equidistant point sets. — In: Combinatoris/ Ed. T. P. McDonough and V. C. Mavron C. U. P. 1969, p. 169—176. — (L. M. S. Lecture Notes; 13).
35*. van Lint J. H. Non-embeddable quasi-residual designs. — Proc. Kon. Nederl Akad. Wetensch. (A), 1978, 81, p. 269—275.
36*. van Lint J. H., Schrijver A. Constructions of strongly regular graphs, two-weight codes and partial geometries by finite fields. Combinatorica. — (В печати.)
37*. Fnomoto H. N. Ito, Noda R. Tight 4-desings. — Osaka J. Math, 1979, 16, p. 39—43.
38*. Rao C. R. Factorial experiments derivable from combinatorial arrangements of arrays. — J. Roy. Statist. Soc., 1947, 9, p. 128—139.
39*. Ray-Chaudhuri D. K., Wilson R. M. On t-designs. — Osaka J. Math., 1975, 12, p. 737—744.

40*. Scott L. L. Some properties of character products. — J. Algebra, 1977, 45, p. 259—265.
41*. Seidel J. J. Strongly regular graphs. — Recent progress in combinatorics/Ed. W. T. Tutte. Acad. Press, 1969, p. 185—197.
42*. Seidel J. J., Taylor D. E. Two-graphs, a second survey.— In: Algebraic methods in graph theory. Szeged, 1978.
43*. Taylor D. F. Regular 2-graphs. — Proc. London Math. Soc., 1977, 35, p. 257—274.
44*. Thas J. A. Combinatorics of partial geometries and generalized quadrangles. — In: Higher Combinatoris/Ed. M. Aigner. Dordrect, 1977, p. 183—199.
45*. Salwach C. J., Mexxaroba J. A. The four known biplanes with k-11, — Internat. J. Math. and Math. Soc., 1979, 2, 251—260.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Алгебра Боуза — Меснера 100
— групповая Д15
— центральная 100
Алфавит 47
Ассоциативная схема (схема отношений) 97
— — аддитивная 108
— — двойственная дуальная 108
— — Джонсона 98
— — метрическая 99
— — P-полиномиальная 102
— — Q-полиномиальная 102
— — Хэмминга 98
Аффинная геометрия 13
— группа перестановок 58
— плоскость 13
— симплектическая геометрия 13, 32

Блок-граф 25
Блок-схема 7

Валентность 18
Вес 48
Весовой энумератор (весовая функция) 52
Внутреннее распределение 101

Геометрия аффинная 13
— — симплектическая 13, 32
— евклидова 13
— проективная 11
Граница Джонсона 88
— Крейна Д19
Граф 17
— Гевиртца Д4
— геометрический Д6
— Клебша 32
— лестничный (ступенчатый) 20
— линейный (реберный) 24
— Мура 30
— Петерсена 20
— полный 17
— — k-дольный 20
— псевдогеометрический Д6
— Пэли (Палея) 20
— ранга 321
— регулярный 18
— решетчатый 20
— связный 29
— точечный Д6
— треугольный 19
— Хигмана — Симса 32
— Хоффмана — Синглетона 30

Два-граф 42
— — регулярный 43
Диаметр 30
Длина (слова) 47
Дополнение графа 17
Дуга 71

Идеал 54
Идемпотент Д15

Код 48
— бинарный (двоичный) Галея 79

Код БЧХ 57
— двойственный дуальный 50
— двухвесовой Д18
— евклидово-геометрический 67
—, исправляющий e ошибок (e-код, исправляющий ошибки), (e-код) 48
— квадратично-вычетный (КВ) 75
— линейный 49
— обобщенный квадратично-вычетный (ОКВ) Д15
— почти совершенный 91
— Препараты 93
— проективно-геометрический 67
— проективный Д18
— равномерно упакованный 91
— расширенный 51
— Рида — Маллера РМ 64
— самодвойственный самодуальный 68
— самоортогональный 67
— симметричный 84
— систематический 49
— совершенный 48
— тернарный троичный Галея 69
— Хэмминга 51
— циклический 54
— эквидистантный Д12
e-код 48
e-код, исправляющий ошибки 48
Коды эквивалентные 49
Конечная геометрия 13
Коцикл 43
Кратность 21

Латинский квадрат Д6

Мажоритарное декодирование 61
МакВильямс соотношения 52
Максимальная интенсивность (сила) 105
Матрица Адамара 10
— инцидентности 18
— порождающая 49
Матрица проверочная (проверки на четность) 50
— распределительная 102
— смежности 18
C-матрица 83
Матье группы 16
Минимальный вес 49
Многочлен см. Полином

Неравенство Фишера 8
— — обобщенное Д3

Обобщенный четырехугольник Д6
Обхват 30
Овал Д3
Ортогональное проверочное множество 59
Ошибка 48

Пассант Д3
Переключение 43
Плоскость аффинная 13
— Мёбиуса (Мёбиус-плоскость) 15
— обращенная 15
— проективная 12
Полином (многочлен) порождающий 54
— проверочный 55
— суммарный 103
P-полином 102
Q-полином 102
Полярность (поляра) 8
Порождающая матрица 49
Проверка на четность 50
— — — общая 51
Проективная геометрия 11
Путь 29

Расстояние (метрика) внешнее 103
— минимальное 103
— Хэмминга 48
Расширение группы перестановок 45

Расширение кода 51
— симметричной схемы 14
— схемы 14
Рациональное условие (условие рациональности) 21

Секант Д3
Сетка Д6
Сила (интенсивность) 105
Система Штейнера (штейнерова система) Д11
Слово 47
Стандартная форма 49
Степень 105
Схема Адамара (адамарова) 10
— вычетная (остаточная) 14
— квазивычетная (квазиостаточная) Д1
— квазисимметричная 24
— парная (схема пар) 18
Схема плотная 106
— производная 14
— самоортогональная 73
— симметричная 8
t-схема 6

Тангенс Д3
Теорема Ассмуса — Маттсона 79
— Брука — Райзера — Човла 10
1-фактор Д9

Частичная геометрия Д6

Шар 48

П. Камерон
Дж. ван Линт

ТЕОРИЯ ГРАФОВ, ТЕОРИЯ КОДИРОВАНИЯ
И БЛОК-СХЕМЫ

М., 1980 г., 144 стр. с илл.

Редакторы *Т. И. Кузнецова, Р. Л. Смелянский*
Техн. редактор *Е. В. Морозова*
Корректор *Т. С. Вайсберг*

ИБ № 11243

Сдано в набор 08.05.80. Подписано к печати 19.11.80. Бумага 84×108$^1/_{32}$, тип. № 3. Литературная гарнитура. Высокая печать. Условн. печ. л. 7,56. Уч.-изд. л. 7,77. Тираж 10 000 экз. Заказ № 644. Цена 80 коп.

Издательство «Наука»
Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ленинградская типография № 2 головное предприятие ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 198052, г. Ленинград, Л-52, Измайловский проспект, 29.

ИЗДАТЕЛЬСТВО« НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ
ЛИТЕРАТУРЫ
117071, Москва, В-71,
Ленинский проспект, 15

Готовится к печати:

ЕМЕЛИЧЕВ В. А., КОВАЛЕВ М. М., КРАВЦОВ М. К. Многогранники, графы, оптимизация.

Книга посвящена систематическому изложению теории выпуклых многогранников с точки зрения различных задач дискретной и непрерывной оптимизации, формулируемых на геометрическом языке. Эта актуальная тема имеет широкие приложения. В книге отражен материал бурно развивающихся дисциплин, лежащих на стыке теории линейных неравенств, теории графов и целочисленного программирования. Детально изложены результаты о многогранниках, связанные с распространенной задачей линейного программирования — транспортной задачей.

Книга может быть рекомендована научным работникам, студентам и аспирантам в области прикладной математики и кибернетики.

Предварительные заказы на эту книгу принимаются без ограничения магазинами Книготорга и Академкниги.

ИЗДАТЕЛЬСТВО« НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ
ЛИТЕРАТУРЫ
117071, Москва, В-71,
Ленинский проспект, 15

Готовится к печати:

ЕМЕЛИЧЕВ В. А., КОВАЛЕВ М. М., КРАВЦОВ М. К. Многогранники, графы, оптимизация.

Книга посвящена систематическому изложению теории выпуклых многогранников с точки зрения различных задач дискретной и непрерывной оптимизации, формулируемых на геометрическом языке. Эта актуальная тема имеет широкие приложения. В книге отражен материал бурно развивающихся дисциплин, лежащих на стыке теории линейных неравенств, теории графов и целочисленного программирования. Детально изложены результаты о многогранниках, связанные с распространенной задачей линейного программирования — транспортной задачей.

Книга может быть рекомендована научным работникам, студентам и аспирантам в области прикладной математики и кибернетики.

Предварительные заказы на эту книгу принимаются без ограничения магазинами Книготорга и Академкниги.

ИЗДАТЕЛЬСТВО« НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ
ЛИТЕРАТУРЫ
117071, Москва, В-71,
Ленинский проспект, 15

Готовится к печати:

МАРКОВ А. А. Введение в теорию кодирования.

Книга содержит материал по теории кодирования, предусмотренный учебной программой курса «Математическая логика и дискретная математика» для факультетов вычислительной математики и кибернетики и факультетов прикладной математики университетов и ряда других вузов.

Книга примыкает к вышедшей в 1979 г. книге С. В. Яблонского «Введение в дискретную математику».

В книге излагаются как комбинаторно логический, так и статистический подходы к вопросам сжатия информации и помехоустойчивого кодирования. Кроме обязательного материала в объеме программы, пособие содержит дополнительные главы, и читатель подводится к современным проблемам теории информации.

Предварительные заказы на эту книгу принимаются без ограничения магазинами Книготорга и Академкниги.

ИЗДАТЕЛЬСТВО« НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ
ЛИТЕРАТУРЫ
117071, Москва, В-71,
Ленинский проспект, 15

Готовится к печати:

САЧКОВ В. Н. Введение в комбинаторные методы дискретной математики.

Книга содержит изложение основных комбинаторных методов современной дискретной математики в систематизированном виде. Предпочтение отдается тем методам, которые наиболее отработаны теоретически, и тем, которые имеют наибольшее число приложений. Наряду с общей теорией много внимания уделяется решению комбинаторных задач, в том числе прикладного характера. В конце каждой главы приводятся задачи учебного характера нарастающей трудности.

Книга предназначена в качестве учебного пособия для студентов и аспирантов по специальностям «Прикладная математика» и «Кибернетика». Она может рассматриваться как дополнение к вышедшей в 1979 году книге С. В. Яблонского «Введение в дискретную математику».

Предварительные заказы на эту книгу принимаются без ограничения магазинами Книготорга и Академкниги.

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ
ЛИТЕРАТУРЫ
117071, Москва, В-71,
Ленинский проспект, 15

Готовится к печати:

ЭНДРЮС Г. Теория разбиений, перевод с английского.

Книга вышла в США в новой серии «Энциклопедия математики и ее приложений». Предмет книги — неупорядоченные разбиения натуральных чисел на натуральные слагаемые. Автор излагает теорию и практику разбиений, не отдавая предпочтения ее теоретико-числовым или комбинаторным аспектам. За последнее время возросли приложения разбиений в вычислительной технике. В книге отражены все три типа приложений. Систематически излагается аппарат: производящие функции, геометрический и алгебраический подходы и др.

Книга будет полезна научным работникам, аспирантам и студентам в области прикладной математики, кибернетики, теории чисел.

Предварительные заказы на эту книгу принимаются без ограничения магазинами Книготорга и Академкниги.