Д. Ю. Ногин, Обобщенные веса Хэмминга для кодов на многомерных квадриках, *Пробл. передачи информ.*, 1993, том 29, выпуск 3, 21–30

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 29 1993 Вып. 3

УДК 621.391.15

© 1993 г. Д. Ю. Ногин

ОБОБЩЕННЫЕ ВЕСА ХЭММИНГА ДЛЯ КОДОВ НА МНОГОМЕРНЫХ КВАДРИКАХ

Мы изучаем проективные системы и линейные коды, соответствующие многомерным проективным квадрикам гиперболического, параболического и эллиптического типов. Вычисляется иерархия обобщенных весов Хэмминга и их распределение.

§ 1. Введение

В [1,§1.1.2] введен язык проективных систем, удобный для описания линейных кодов и исследования некоторых их свойств: каждому линейному q-ичному коду соответствует проективная $[n,k]$-система, т.е. набор из n точек в $(k-1)$-мерном проективном пространстве над $\mathbf{F}_q$, и наоборот. При этом минимальное расстояние кода, соответствующего системе, описывается через максимальное число точек, лежащих в гиперплоскости.

В [2] задан естественный с этой точки зрения вопрос о максимальном числе точек системы, лежащих в подпространстве коразмерности большей, чем 1, и показано, что этот геометрический вопрос равносилен вопросу о нахождении иерархии обобщенных весов Хэмминга, введенной Вэем [3] в связи с некоторыми задачами криптографии. Мы покажем, как возникает иерархия весов в задаче о канале с подслушиванием типа II (см.[4]) для произвольного q.

В качестве источника проективных систем можно рассматривать алгебраические многообразия. В [2] для этого применяются эрмитовы многообразия и изучаются соответствующие им коды. Мы же рассматриваем проективные системы на многомерных квадриках (т.е. многообразиях второй степени), поскольку они также имеют достаточно много точек, и их свойства хорошо изучены (см. [5, гл.22]).

Мы находим полную иерархию весов для систем и ассоциированных с ними кодов и вычисляем их обобщенные спектры.

§ 2. Обобщенные веса Хэмминга

Приведем некоторые определения и результаты из [3]. Пусть C – q-ичный линейный $[n,k]$-код, D – его линейный подкод. *Носителем* подкода D называется множество $\chi(D)$ координат, не тождественно равных нулю на D, т.е.

$$\chi(D) = \{i | \exists (x_1, \ldots, x_n) \in D,\ x_i \neq 0\}.$$

Весом подкода D (или его *эффективной длиной*) называется мощность $w(D)$ его носителя. Назовем число

$$d_r = d_r(C) = \min\{w(D) | D \subseteq C, \dim D = r\}$$

r-м минимальным весом кода C, или *r-м обобщенным весом Хэмминга* кода C. В частности, d_1 равно обычному минимальному весу Хэмминга кода C.

Нетрудно проверить, что

$$1 \leq d_1 < d_2 < \ldots < d_k \leq n$$

и

$$d_r \leq n - k + r.$$

Упорядоченное множество $\{d_1, d_2, \ldots, d_k\}$ называется *иерархией весов* кода C. Иерархия весов двойственного кода $C^\perp$ однозначно определяется иерархией весов C, а именно:

$$\{d_1^\perp, \ldots, d_{n-k}^\perp\} = \{1, \ldots, n\} \setminus \{n+1-d_k, \ldots, n+1-d_1\}.$$

Граница Грайсмера, примененная к подкодам размерности r, дает условия

$$d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d_1}{q^i} \right\rceil,$$

где через $\lceil x \rceil$ обозначено наименьшее целое число, большее или равное x.

§ 3. Иерархия весов и каналы с подслушиванием

Мы проиллюстрируем связь между обобщенными весами линейного кода и одной задачей криптографии, касающейся каналов с подслушиванием. Эта связь описана в [3, Appendix].

Каналы с подслушиванием типа II (WTC II) изучали Озаров и Вайнер [4]. Постановка задачи следующая.

Посылатель передает k информационных символов в виде слова длины n по каналу без шума (правильность декодирования обеспечена). Задано целое число $s \leq n$; подслушивающий может подслушать любые s символов из n по своему выбору. Ставится вопрос о способе кодирования, при котором подслушивающий получает как можно меньше информации.

Метод, предложенный в [4], состоит в следующем. Пусть C – линейный $[n, k]$-код. Рассматриваются смежные классы по $C^\perp$ – в соответствии с k информационными символами выбирается один из смежных классов (их всего q^k); в этом смежном классе случайным образом выбирается слово, которое и передается по каналу. Другими словами, рассматривается произвольное дополнение C' кода $C^\perp$ такое, что $C^\perp \oplus C' = \mathbf{F}_q^n$. Здесь $\dim C' = k$, и кодирование состоит в том, что к слову из C' прибавляется случайный элемент из C'. Подслушивающий имеет полную информацию о кодах $C^\perp$ и C', но не знает процедуру случайного выбора.

Пусть S – множество позиций, соответствующих подслушанным символам, $|S| = s$; $I = \{1, \ldots, n\} \setminus S$ – множество остальных позиций. Рассмотрим координатное пространство $\mathbf{F}_q^S$ и проекцию $\mathbf{F}_q^n \to \mathbf{F}_q^S$ параллельно $\mathbf{F}_q^I$; при подслушивании передаваемого слова подслушивающий знает его образ при этой проекции. Пусть $C_S^\perp$ и C_S' – образы соответственно $C^\perp$ и C' при этой проекции.

Существует всего $q^{\dim C_S'}$ образов слов, которые может получить подслушивающий; при этом каждый образ за счет выбора слова из $C^\perp$ может быть сдвинут в один из $q^{\dim(C_S' \cap C_S^\perp)}$ возможных образов. Поэтому *информацией* $\mathrm{Inf}(S)$, полученной при подслушивании символов на позициях S, естественно считать размерность факторпространства $C_S'/(C_S' \cap C_S^\perp)$; тогда

$$\mathrm{Inf}(S) = \dim C_S' / \left(C_S' \cap C_S^\perp\right) = \dim C_S' - \dim\left(C_S' \cap C_S^\perp\right).$$

Поскольку $C'_S + C_S^\perp = \mathbf{F}_q^S$ (сумма не прямая), то

$$\mathrm{Inf}(S) = \dim C'_S - \dim\left(C'_S \cap C_S^\perp\right) = s - \dim C_S^\perp,$$

т.е. информация на самом деле зависит лишь от свойств кода $C^\perp$, и не зависит от выбора дополнения C'.

Итак, $\mathrm{Inf}(S) = s - \dim C_S^\perp$. Рассмотрим сквозное отображение

$$f : \mathbf{F}_q^n \to \mathbf{F}_q^S / C_S^\perp,$$

являющееся композицией проекции $\mathbf{F}_q^n \to \mathbf{F}_q^S$ вдоль $\mathbf{F}_q^I$ и отображения факторизации $\mathbf{F}_q^S \to \mathbf{F}_q^S / C_S^\perp$. Образ f имеет размерность $\mathrm{Inf}(S)$, а его ядро $\tilde{C}$ содержит как код $C^\perp$, так и координатное пространство $\mathbf{F}_q^I$.

Тогда $\tilde{C}^\perp$ – это код размерности $\mathrm{Inf}(S)$, который, во-первых, является подкодом кода C, а во-вторых, имеет нулевую проекцию на $\mathbf{F}_q^I$. Значит,

$$d_{\mathrm{Inf}(S)}(C) \le s.$$

Назовем *неопределенностью* при подслушивании s символов величину

$$\Delta_s = \min\{k - \mathrm{Inf}(S) \,|\, |S| = s\}.$$

При $s = 0$ неопределенность равна k; при $s = n$ неопределенность равна 0. Нас интересует поведение функции $\Delta_s(s)$.

Мы показали, что $d_{k-\Delta_s}(C) \le s$. Предположим теперь, что $d_{k-\Delta_s+1}(C) \le s$. В этом случае найдется подкод C'' кода C, такой что $\dim C'' = k - \Delta_s + 1, w(C'') \le s$. Рассмотрим какое-либо множество позиций S'', содержащее носитель $\chi(C'')$, $|S''| = s$. Тогда образ проекции $(C'')^\perp \to \mathbf{F}_q^{S''}$ имеет размерность, не превосходящую

$$\dim(C'')^\perp - (n - s) = n - (k - \Delta_s) - 1,$$

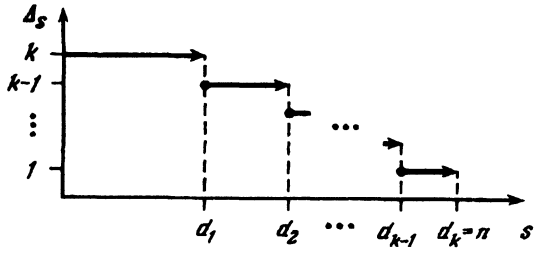
и в то же время содержит проекцию $(C'')^\perp_{S''}$, имеющую размерность $s - \mathrm{Inf}(S'')$. Значит,

$$s - \mathrm{Inf}(S'') \le s - (k - \Delta_s) - 1,$$

т.е.

$$\Delta_s \ge k - \mathrm{Inf}(S'') + 1,$$

что противоречит определению неопределенности Δ_s.



Зависимость неопределенности от s

Таким образом, мы показали, что $d_{k-\Delta_s} \leq s < d_{k-\Delta_s-1}$. Другими словами,

$$\Delta_s = k - r \quad \text{при} \quad d_r \leq s < d_{r-1}.$$

Итак, скачок неопределенности при передаче сообщений как элементов смежных классов по $C^\perp$ происходит в точности в точках $s = d_r(C)$ (см. рисунок); т.е. иерархия весов кода C определяет его поведение при использовании в каналах с подслушиванием типа II.

§ 4. Проективные системы

Здесь мы изложим подход к описанию линейных кодов и их свойств, предложенный в [1, §1.1.2] и обобщенный в [2].

Пусть $\mathbf{P}^{k-1} = \mathbf{P}(V)$ – проективное пространство размерности $k-1$, т.е. проективизации k-мерного векторного пространства V над $\mathbf{F}_q$. *Проективной* [n,k]-*системой* или просто *системой* называется множество X, состоящее из n точек (не обязательно различных) пространства $\mathbf{P}^{k-1}$. Две системы X_1 и X_2 в $\mathbf{P}^{k-1}$ *эквивалентны*, если существует проективное преобразование $\mathbf{P}^{k-1}$, при котором X_1 переходит в X_2.

Построим по произвольному линейному [n,k]-коду C некоторую проективную [n,k]-систему. Рассмотрим координатные формы $x_i : C \to \mathbf{F}_q$ такие, что

$$x_i : (v_1, \ldots, v_n) \mapsto v_i.$$

Они являются n точками пространства C^* линейных функционалов на C (двойственного линейного пространства). Если код C *невырожден*, т.е. все формы x_i не равны нулю как функции на C, то они задают n точек в $\mathbf{P}^{k-1} = \mathbf{P}(C^*)$, т.е. проективную систему.

При этом подкоду $D \subset C$ размерности r соответствует множество элементов C^*, равных нулю на D, т.е. подпространство $D^* \subset C^*$ коразмерности r; и, тем самым, плоскость коразмерности r в $\mathbf{P}^{k-1}$. Вес подкода D равен числу координатных форм, не зануляющихся на нем, т.е. числу точек системы X, не лежащих в этой плоскости коразмерности r.

Для произвольной системы X положим

$$d_r = d_r(X) = n - \max \left| \left\{ X \cap H \mid H \subset \mathbf{P}^{k-1}, \operatorname{codim} H = r \right\} \right|,$$

где кратные точки X учитываются со своей кратностью.

Проективная система называется *невырожденной*, если она не содержится ни в какой гиперплоскости, т.е. $d_1 \geq 1$. Покажем, как по произвольной невырожденной проективной системе можно построить линейный код.

Всякую систему $\{x_1, \ldots, x_n\}$ в $\mathbf{P}^{k-1} = \mathbf{P}(V)$ можно поднять произвольным образом до системы $\{y_1, \ldots, y_n\}$ векторов пространства V. Каждый из y_i задает линейное отображение $V^* \to \mathbf{F}_q$, а набор $(y_1, \ldots, y_n)$ – отображение $V^* \to \mathbf{F}_q^n$, образом которого является линейный код ($[n,k]$-код, если проективная система невырождена).

Напомним, что два кода C_1 и C_2 называются *эквивалентными*, если C_2 может быть получен из C_1 перестановкой координат и умножением их на ненулевые элементы $\mathbf{F}_q$; таким образом $C_2 = g(C_1)$ для некоторого $g \in (\mathbf{F}_q^*)^n \rtimes S_n$. Точнее утверждение о взаимосвязи проективных систем и линейных кодов следующее:

Т е о р е м а 4.1. *Существует естественное взаимно-однозначное соответствие между множеством классов эквивалентности невырожденных проективных систем и множеством классов эквивалентности невырожденных линейных кодов. При этом соответствии параметры* $n, k, d_1, d_2, \ldots, d_k$ *сохраняются.*

Это обобщение теоремы 1.1.6 из [1], полученное в [2, раздел 3]. Мы описали, как устанавливается соответствие, и проверили совпадение параметров.

§ 5. Проективные квадрики над конечным полем

Приведем необходимые результаты из [5, гл.22]. *Квадрика в* $\mathbf{P}^N$ – это гиперповерхность второй степени, т.е. множество нулей однородной квадратичной формы

$$F = \sum_{i=0}^{N} a_i x_i^2 + \sum_{i<j} a_{ij} x_i x_j.$$

Если форма *невырождена*, т.е. не приводится линейными заменами к форме, зависящей от меньшего количества переменных, то соответствующая квадрика $\mathcal{Q}_N$ является неособой. С точностью до проективного преобразования $\mathbf{P}^N$ существует либо одна, либо две неособые квадрики в зависимости от четности N, а именно:

1. Если N четно, то всякая неособая квадрика $\mathcal{Q}_N$ проективно эквивалентна квадрике $\mathcal{P}_N$, заданной уравнением

$$x_0^2 + x_1 x_2 + \ldots + x_{N-1} x_N = 0.$$

2. Если N нечетно, то всякая неособая квадрика $\mathcal{Q}_N$ проективно эквивалентна либо квадрике $\mathcal{H}_N$, заданной уравнением

$$x_0 x_1 + x_2 x_3 + \ldots + x_{N-1} x_N = 0,$$

либо квадрике $\mathcal{E}_N$, заданной уравнением

$$f(x_0, x_1) + x_2 x_3 + \ldots + x_{N-1} x_N = 0,$$

где f – неприводимый над $\boldsymbol{F}_q$ однородный многочлен второй степени.

Квадрики, эквивалентные $\mathcal{P}_N$, называются *параболическими*, эквивалентные $\mathcal{H}_N$ – *гиперболическими*, а эквивалентные $\mathcal{E}_N$ – *эллиптическими*.

Через Π_s мы обозначаем в дальнейшем подпространство размерности s в $\mathbf{P}^N$; при этом Π_0 является точкой пространства $\mathbf{P}^N$, $\Pi_{-1} = \varnothing$. Всякая особая квадрика является конусом $\Pi_s \mathcal{Q}_t$ с вершиной Π_s над неособой квадрикой $\mathcal{Q}_t$ в Π_t, где $\Pi_s \cap \Pi_t = \Pi_{-1}$, $t + s + 1 = n$; т.е. $\Pi_s \mathcal{Q}_t$ есть объединение всех прямых, проходящих через точку пространства Π_s и точку $\mathcal{Q}_t$. Здесь $s \geq -1$; при $s = -1$ квадрика является неособой.

Квадрики $\mathcal{H}_{-1}$, $\mathcal{P}_0$ и $\mathcal{E}_1$ пусты; $\mathcal{H}_1$ – пара точек на прямой; $\mathcal{P}_2$ – коника в плоскости; $\mathcal{E}_3$ состоит из $q^2 + 1$ точек в $\mathbf{P}^3$, никакие три из которых не коллинеарны.

(Проективным) *индексом* квадрики $\mathcal{Q}_N$ называется проективная размерность g наибольшего линейного подпространства, лежащего в $\mathcal{Q}_N$. Для $\mathcal{Q}_N$ индекс равен $\frac{N-1}{2}$, для $\mathcal{P}_N$ – равен $\frac{N-2}{2}$, для $\mathcal{E}_N$ – равен $\frac{N-2}{2}$. *Характером* неособой квадрики называется число $w = 2g - N + 3$, т.е. квадрики гиперболического типа имеют характер 2, параболического типа – характер 1, и эллиптического типа – характер 0. Характер особой квадрики $\Pi_s \mathcal{Q}_t$ полагают равным характеру $\mathcal{Q}_t$.

Число $\mathbf{F}_q$-точек на квадрике $\Pi_s \mathcal{Q}_t$ характера w в $\mathbf{P}^{s+t+1} = \mathbf{P}^N$ равно

$$\tau(s,t,w) = |\Pi_s \mathcal{Q}_t(\mathbf{F}_q)| = \theta_{s+t} + (w-1) q^{s+\frac{t+1}{2}}, \tag{5.1}$$

где $\theta_{s+t} = \theta_{N-1} = \left|\mathbf{P}^{N-1}(\mathbf{F}_q)\right| = \left|\mathbf{P}^{N-1}(\mathbf{F}_q)\right| = \left(q^N - 1\right)/(q-1)$ – число точек проективного пространства. В частности, число $\mathbf{F}_q$-точек неособой квадрики равно

$$|\mathcal{Q}_N(\mathbf{F}_q)| = \theta_{N-1} + (w-1) q^{\frac{N-1}{2}}. \tag{5.2}$$

Сечение неособой квадрики $\mathcal{Q}_N$ подпространством Π_m также является квадрикой, так как ограничение квадратичной формы на подпространство есть квадратичная форма (быть может, от меньшего количества переменных). Для неособой

квадрики $\mathcal{Q}_N$ характера w сечение $\mathcal{Q}_N \cap \Pi_m$ вида $\Pi_{m-t-1}\mathcal{Q}_t$ характера v существует тогда и только тогда, когда

$t - v$ нечетно

и

$$N > m \geq t \geq \max\{2m - N + \mid w - v \mid, 1 - v\} \tag{5.3}$$

Если такие сечения существуют, то число таких подпространств Π_m равно

$$\rho(m,t,v;N,w) = q^{1/2(T[t+1+vw(2-v)(2-w)]-v(2-v)(w-1)^2)} \times$$
$$\times \left[\frac{1}{2}\{T + v + w - vw + vw(2-v)(2-w)\}, \frac{1}{2}(n+1-w)\right]_+ \times$$
$$\times \left[\frac{1}{2}\{T - v - w + vw + vw(2-v)(2-w)\}, \frac{1}{2}(n-1+w)\right]_- /$$
$$/\left\{\left[v(2-v), \frac{1}{2}(t+1-v)\right]_+ \left[1, \frac{1}{2}(t-1+v)\right]_- [1, m-t]_-\right\}, \tag{5.4}$$

где $T = N - t + 2m$,

$$[a,b]_\pm = \begin{cases} (q^a \pm 1)(q^{a+1} \pm 1)\ldots(q^b \pm 1) & , a \leq b, \\ 1 & , a > b. \end{cases}$$

§ 6. Коды, ассоциированные с квадриками

Рассмотрим теперь [n,k]-систему, состоящую из $\mathbf{F}_q$-точек неособой квадрики $\mathcal{Q}_{k-1}$ в $\mathbf{P}^{k-1}$.

Т е о р е м а 6.1. *Код, ассоциированный с неособой квадрикой $\mathcal{Q}_{k-1}$ характера w, имеет размерность k и следующие параметры:*

в гиперболическом случае ($w = 2, k$ – четно):

$$n = \theta_{k-2} + q^g,$$

$$d_r = \begin{cases} q^{k-r-1}\theta_{r-1} & , r \leq k-1-g, \\ q^{k-r}\theta_{r-2} + q^g & , r \geq k-1-g, \end{cases} \tag{6.1}$$

в параболическом случае ($w = 1, k$ – нечетно):

$$n = \theta_{k-2},$$

$$d_r = \begin{cases} q^{k-r-1}\theta_{r-1} - q^g & , r \leq k-1-g, \\ q^{k-r}\theta_{r-2} & , r \geq k-1-g, \end{cases} \tag{6.2}$$

в эллиптическом случае ($w = 0, k$ – четно):

$$n = \theta_{k-2} + q^g \cdot q,$$

$$d_r = \begin{cases} q^{k-r-1}\theta_{r-1} - q^g \cdot q & , r = 1, \\ q^{k-r-1}\theta_{r-1} - q^g(q+1) & , 2 \leq r \leq k-1-g, \\ q^{k-r}\theta_{r-2} - q^g \cdot q & , r \geq k-1-g, \end{cases} \tag{6.3}$$

где g – проективный индекс квадрики, равный $\frac{k+w}{2} - 2$.

Доказательство. Это непосредственно следуют из результатов §§4 и 5. Длина n определяется из (5.2) при $N = k-1$. Далее, по определению

$$d_r = n - \max|\mathcal{Q}_{k-1} \cap \Pi_{k-1-r}|.$$

Пересечение $\mathcal{Q}_{k-1} \cap \Pi_{k-1-r}$ также является квадрикой вида $\Pi_{(k-1-r)-t-1}\mathcal{Q}_t$; обозначим ее характер через v. Тогда в силу (5.3) и (5.1) получаем

$$\begin{aligned} d_r &= n - \max_{(t,v)} |\Pi_{k-r-t-2}\mathcal{Q}_t| = \\ &= n - \max_{(t,v)} \left(\theta_{k-r-2} + (v-1)q^{k-r-t-2+\frac{t+1}{2}}\right) = \\ &= n - \theta_{k-r-2} - q^{k-r-2} \max_{(t,v)} (v-1)q^{-(t-1)/2} = \\ &= q^{k-r-1}\theta_{r-1} + (w-1)q^{\frac{k}{2}-1} - q^{k-r-2} \max_{(t,v)} (v-1)q^{-(t-1)/2}, \end{aligned} \tag{6.4}$$

где максимум берется по всем парам (t,v) таким, что

$$\begin{aligned} &k-r-1 \geq t \geq \max\{k-2r-1+\mid w-v\mid, 1-v\} \\ &2 \geq v \geq 0, \quad t+v \equiv 1 \pmod 2. \end{aligned} \tag{6.5}$$

Очевидно, что $\max(v-1)q^{-(t-1)/2}$ достигается при $v=2$, если найдется хотя бы одна пара $(t,2)$, удовлетворяющая (6.5). При этом t должно быть как можно меньшим.

Рассмотрим отдельно три случая: $\mathcal{H}_{k-1}, \mathcal{P}_{k-1}, \mathcal{E}_{k-1}$.

I. Гиперболический случай; $w=2, k$ – четно. Здесь случай $v=2$ возможен при любом r, ибо условия (6.5) при $v=2$ принимают вид

$$k-r-1 \geq t \geq \max\{k-2r-1, -1\}, \quad t \text{ – нечетно},$$

откуда

$$t = \begin{cases} k-2r-1 & , r \leq \frac{k}{2}, \\ -1 & , r \geq \frac{k}{2}. \end{cases}$$

Тогда

$$d_r = q^{k-r-1}\theta_{r-1} + q^{\frac{k}{2}-1} - q^{k-r-2} \cdot \begin{cases} q^{-(\frac{k}{2}-r-1)} & , r \leq \frac{k}{2}, \\ 1 & , r \geq \frac{k}{2} \end{cases} =$$

$$= q^{k-r-1}\theta_{r-1} + q^{\frac{k}{2}-1} - \begin{cases} q^{\frac{k}{2}-1} & , r \leq \frac{k}{2}, \\ q^{k-r-1} & , r \geq \frac{k}{2}, \end{cases}$$

откуда получаем (6.1), поскольку $g = \frac{k}{2} - 1$.

II. Параболический случай; $w=1, k$ – нечетно. Аналогично, условия (6.5) при $v=2$ имеют вид

$$k-r-1 \geq t \geq \max\{k-2r, -1\}, \quad t \text{ – нечетно},$$

что также возможно при любом r. Отсюда

$$t = \begin{cases} k-2r & , r \leq \frac{k+1}{2}, \\ -1 & , r \geq \frac{k+1}{2}. \end{cases}$$

Тогда

$$d_r = q^{k-r-1}\theta_{r-1} - q^{k-r-2}\cdot\begin{cases} q^{-\frac{k-2r-1}{2}} & ,r \le \frac{k+1}{2}, \\ q & ,r \ge \frac{k+1}{2} \end{cases} =$$

$$= q^{k-r-1}\theta_{r-1} - \begin{cases} q^{\frac{k-1}{2}-1} & ,r \le \frac{k+1}{2}, \\ q^{k-r-1} & ,r \ge \frac{k+1}{2}, \end{cases}$$

откуда получаем (6.2), поскольку $g = \frac{k-1}{2} - 1$.

III. Эллиптический случай; $w = 0, k$ – четно. Условия (6.5) при $v = 2$ имеют вид

$$k - r - 1 \ge t \ge \max\{k - 2r + 1, -1\}, \quad t \text{ – нечетно.}$$

При r=1 таких t не существует; при $r \ge 2$ получаем

$$t = \begin{cases} k - 2r + 1 & ,2 \le r \le \frac{k}{2} + 1, \\ -1 & ,r \ge \frac{k}{2} + 1. \end{cases}$$

Для r=1 возьмем $v = 1$, тогда

$$k - 2 \ge t \ge \max\{k - 2, -1\}, \quad t \text{ – четно,}$$

т.е. подходит $t = k - 2$. Итак, максимум (6.4) достигается при

$$t = \begin{cases} k - 2 & ,r = 1, \\ k - 2r + 1 & ,2 \le r \le \frac{k}{2} + 1, \\ -1 & ,r \ge \frac{k}{2} + 1. \end{cases}$$

Тогда

$$d_r = q^{k-r-1}\theta_{r-1} - q^{\frac{k}{2}-1} - q^{k-r-2}\cdot\begin{cases} 0 & ,r = 1, \\ q^{-(\frac{k}{2}-2)} & ,2 \le r \le \frac{k}{2} + 1, \\ q & ,r \ge \frac{k}{2} \end{cases} =$$

$$= q^{k-r-1}\theta_{r-1} - q^{\frac{k}{2}-1} - \begin{cases} 0 & ,r = 1, \\ q^{\frac{k}{2}-2} & ,2 \le r \le \frac{k}{2} + 1, \\ q^{k-r-1} & ,r \ge \frac{k}{2} + 1, \end{cases}$$

откуда получаем (6.3), поскольку $g = \frac{k}{2} - 2$.

Следствие 6.2. *При $r \le \frac{k}{2}$ веса d_r для гиперболической квадрики $\mathcal{H}_{k-1}$ лежат на границе Грайсмера.*

Доказательство. Из теоремы 6.1 при $r \le \frac{k}{2} = k - 1 - g$ получаем

$$d_r = q^{k-r-1}\theta_{r-1}, \quad d_1 = q^{k-2}.$$

Тогда

$$\sum_{i=0}^{r-1}\left\lceil\frac{d_1}{q^i}\right\rceil = q^{k-2} + q^{k-1} + \ldots + q^{k-r-1} = q^{k-r-1}\theta_{r-1} = d_r.$$

(Напротив, при $r > \frac{k}{2}$, т.е. при $k - r - 1 < g$, существуют подпространства Π_{k-r-1}, целиком лежащие на квадрике; поэтому соответствующие веса d_r являются в некотором смысле наихудшими.)

Следствие 6.3. Для неособой гиперболической или параболической квадрики выполняется

$$d_{r+1} - d_r = \begin{cases} q^{k-r-2} & \text{при } r < k-1-g \\ q^{k-r-1} & \text{при } r \geq k-1-g \end{cases}.$$

Это непосредственно следует из (6.1) и (6.2).

В качестве иллюстрации мы приводим таблицу разностей иерархии весов для гиперболических и параболических квадрик. Здесь четные k соответствуют гиперболическому случаю, нечетные – параболическому.

k	d_1	d_2-d_1	d_3-d_2	d_4-d_3	d_5-d_4	d_6-d_5	d_7-d_6	d_8-d_7
3	$q-1$	1	1					
4	q^2	q	q	1				
5	q^3-q	q^2	q	q	1			
6	q^4	q^3	q^2	q^2	q	1		
7	q^5-q^2	q^4	q^3	q^2	q^2	q	1	
8	q^6	q^5	q^4	q^3	q^3	q^2	q	1

Замечания. Коды, ассоциированные с неособыми квадриками, рассматривал Вольфманн [6] с точки зрения минимального расстояния и спектра; обобщение на случай особых квадрик сделано в [7].

В качестве проективной системы можно рассматривать точки особой квадрики и получить аналогичные результаты, однако параметры соответствующих кодов будут хуже.

§ 7. Обобщенные спектры

Для произвольного невырожденного $[n,k]$-кода C обозначим через $A_i^r(C)$ число r-мерных подкодов веса i; $1 \leq r \leq k-1$, $1 \leq i \leq n$. Множество $\{A_i^r\}$ назовем *обобщенным спектром* кода C (в работе [2] принято несколько отличное определение обобщенного спектра). Заметим, что если $\{A_i\}$ – обычный спектр, то

$$A_i = (q-1)A_i^1.$$

Формулы (5.1) и (5.4) позволяют вычислить обобщенный спектр кодов, ассоциированных с неособой квадрикой; функция ρ, определена в формуле (5.4), а τ – в формуле (5.1).

Теорема 7.1. *Для кода, ассоциированного с неособой квадрикой $\mathcal{Q}_{k-1}$ характера w,*

$$A_i^r = \begin{cases} \rho(k-r-1,t,v;k-1,w) & \text{при } i = n-\tau(k-r-t-2,t,v) \text{ для} \\ & \text{некоторых } t \text{ и } v, \text{ удовлетворяющим} \\ & \text{условиям (6.5)}, v \neq 1, \\ \sum_t \rho(k-r-1,t,1;k-1,w) & \text{при } i = n-\theta_{k-r-2}, \\ 0 & \text{в остальных случаях}, \end{cases}$$

где суммирование ведется по нечетным t таким, что

$$k-r-1 \geq t \geq \max\{k-2r-1+\mid w-1\mid, 0\}.$$

Доказательство. Это непосредственно следует из определений и результатов §5 с учетом того, что для различных s и t при $s+t$ =const функция $\tau(s,t,v)$ принимает одно значение θ_{s+t}, если $v=1$, и различные значения, если $v=2$ или $v=0$.

Следствие 7.2. Число различных r-весов кода, ассоциированного с неособой квадрикой $\mathcal{Q}_{k-1}$ характера w, равно

$$\min\left\{\left\lceil\frac{r+w-1}{2}\right\rceil,\left\lceil\frac{k-r+1}{2}\right\rceil\right\}+\min\left\{\left\lceil\frac{r-w+1}{2}\right\rceil,\left\lceil\frac{k-r-1}{2}\right\rceil\right\}+1.$$

Автор весьма признателен М.А.Цфасману, обратившему его внимание на эту тему.

СПИСОК ЛИТЕРАТУРЫ

1. *Tsfasman M.A., Vlăduţ S.G.* Algebraic–Geometric Codes. Dordrecht / Boston / London: Kluwer Academic Publishers, 1991.
2. *Hirschfeld J.W.P., Tsfasman M.A., Vlăduţ S.G.* The Weight Hierarchy of Higher-Dimensional Hermitian Codes // IEEE Trans. Inform. Theory (в печати).
3. *Wei V.K.* Generalized Hamming Weights for Linear Codes // IEEE Trans. Inform. Theory. 1991.V.37. P.1412-1418.
4. *Ozarow L.H., Wyner A.D.* Wire–Tap–Channel II // Bell Lab. Techn. J. 1984. V.3. P.2135-2157.
5. *Hirschfeld J.W.P., Thas J.A.* General Galois Geometries. Oxford University Press, 1991.
6. *Wolfmann J.* Codes projectifs à deux ou troi poids associés aux hyperquadriques d'une géométrie finie // Discrete Math. 1975. V.13. P.185-211.
7. *Aubry Y.* Reed–Muller codes associated to projective algebraic varieties // Lect.Notes in Math. V.1518. N.Y. :Springer–Verlag, 1992. P.4-17.

Поступила в редакцию
28.12.92