

УДК 621.391.15

© 1997 г. М. Ю. Розенблом, М. А. Цфасман

КОДЫ ДЛЯ m -МЕТРИКИ¹

Вводится новая серия метрик на пространствах \mathbb{F}_q^n , обобщающих метрику Хэмминга. Изучаются верхние и нижние границы для параметров кодов в этих метриках. Приводятся простейшие конструкции, включая алгебро-геометрическую.

§ 1. Определение метрики

Пусть $V \simeq \mathbb{F}_q^n$ – n -мерное координатное линейное пространство над конечным полем из q элементов. Кодом мы будем называть любое его подмножество, а линейным кодом – \mathbb{F}_q -линейное подпространство. Пусть $n = ms$, где m и s – целые положительные числа. В этом случае элементы V можно отождествить с матрицами $\|v_{ij}\|$, $1 \leq i \leq m$, $1 \leq j \leq s$, с элементами из поля \mathbb{F}_q . Определим вес матрицы формулой

$$\text{wt}(\|v_{ij}\|) = \sum_{1 \leq j \leq s} (m - \max(i \mid v_{kj} = 0 \text{ при всех } k \leq i)). \quad (1)$$

Вес изменяется в диапазоне $0 \leq \text{wt}(v) \leq n$ и определяет метрику на пространстве V по формуле $d(v, v') = \text{wt}(v - v')$. Назовем ее m -метрикой. При $m = 1$ это обычная метрика Хэмминга. Целью настоящей работы является вычисление некоторых верхних и нижних границ для параметров кодов, отвечающих вышеуказанной метрике.

Приведем модель канала передачи информации, при использовании которого рассматриваемое нами минимальное расстояние служит естественной характеристикой качества кода. Пусть отправитель передает сообщения, состоящие из s наборов по m q -ичных символов, которые передаются параллельно по m каналам. Процесс передачи нарушается помехами, имеющими следующую структуру: в некоторые моменты времени часть каналов, идущих подряд, начиная с m -го, используется некоторым приоритетным пользователем. Каналы освобождаются приоритетным пользователем по мере того, как нужда в них отпадает, в порядке, обратном тому, в котором они занимались. Характеристикой степени вмешательства приоритетного пользователя служит суммарное количество q -ичных символов, содержащееся в переданных им “поверх” основного отправителя сообщениях. Легко видеть, что минимальное расстояние кода в смысле m -метрики характеризует его устойчивость относительно такого рода вмешательств.

Всюду далее, говоря о расстоянии, мы имеем в виду m -метрику.

¹Работа выполнена при частичной финансовой поддержке Международного научного фонда (грант MPN300) и Российского фонда фундаментальных исследований (номера проектов 93-012-458; 96-01-01378).

§ 2. Верхние оценки

Теорема 1 (граница Синглтона). Пусть $C \subset V$ - произвольный код мощности K с минимальным расстоянием $d = \min_{\substack{v, v' \in C \\ v \neq v'}} \text{wt}(v - v')$. Тогда

$$K \leq q^{n-d+1}.$$

Доказательство. Отметим в матрице $\|v_{ij}\|$ первые $d-1$ позиций в лексикографическом порядке. Никакие два элемента кода C не могут совпадать во всех оставшихся позициях из-за условия на минимальное расстояние. Следовательно, их число не превышает q^{n-d+1} . \blacktriangle

Теорема 2 (граница Плоткина). Пусть $C \subset V$ - произвольный код мощности K с минимальным кодовым расстоянием d ; $\delta = \frac{d}{n}$ - относительное минимальное расстояние. Тогда

$$\delta(K-1) \leq \delta_{\text{crit}} K,$$

$$\text{где } \delta_{\text{crit}} = 1 - \frac{1}{m} \sum_{1 \leq i \leq m} q^{-i}.$$

Доказательство. С одной стороны,

$$\sum_{\substack{v, v' \in C \\ v \neq v'}} d(v, v') = \sum_{\substack{v, v' \in C \\ v \neq v'}} d(v, v') \geq dK(K-1), \quad (2)$$

с другой стороны, положим

$$d(v_j, v'_j) = (m - \max(i \mid v_{kj} = v'_{kj} \text{ при всех } k \leq i)),$$

тогда

$$\sum_{v, v' \in C} d(v, v') = \sum_{v, v' \in C} \sum_{1 \leq j \leq s} d(v_j, v'_j) = \sum_{1 \leq j \leq s} \sum_{X, Y} d(X, Y) t_j(X) t_j(Y).$$

Здесь X и Y пробегают всевозможные столбцы длины m в \mathbb{F}_q -алфавите, а $t_j(X)$ - количество кодовых слов, j -й столбец которых совпадает с X . Последняя сумма не превосходит $s \max_{X, Y} \sum_{X, Y} d(X, Y) t_X t_Y$, где максимум берется по наборам $(t_X, X \in \mathbb{F}_q^m)$ с условиями $t_X \geq 0$, $\sum_X t_X = K$, и теорема следует из приводимой ниже оценки.

Лемма. Квадратичная форма $F = \sum_{X, Y} d(X, Y) t_X t_Y$ на гиперплоскости $\sum_X t_X = K$ достигает абсолютного максимума в точке $T_0 : \{t_X = Kq^{-m} \text{ для всех } X\}$.

Вывод теоремы из леммы. Действительно, в этом случае последняя сумма не превосходит

$$s K^2 q^{-2m} \sum_{X, Y} d(X, Y) = s K^2 q^{-2m} q^m \sum_Y d(0, Y) = s K^2 q^{-m} \left(m q^m - \sum_{1 \leq i \leq m} q^{i-1} \right).$$

Отсюда и из формулы (2) после деления на $n = ms$ следует теорема. \blacktriangle

Доказательство леммы. Легко видеть, что точка T_0 является точкой экстремума формы F на гиперплоскости $\sum_X t_X = K$, поэтому достаточно проверить, что матрица $\|d(X, Y)\|$ на гиперплоскости $\sum_X t_X = 0$ отрицательно определена. Положим $q = p^r$, и выберем \mathbb{F}_p -базис в $\mathbb{F}_q = \mathbb{F}_{p^r}$. Абелева группа G столбцов длины m в \mathbb{F}_q -алфавите примет вид

$$G = \mathbb{F}_q^m = \bigoplus_{1 \leq i \leq m} \bigoplus_{1 \leq \ell \leq r} \mathbb{Z}/p\mathbb{Z},$$

а ее групповая алгебра

$$\mathbb{C}[G] = \bigotimes_{1 \leq i \leq m} \bigotimes_{1 \leq \ell \leq r} \mathbb{C}[t]/(t^p - 1).$$

Так как расстояние $d(X, Y)$ инвариантно относительно сдвига на элементы G , то матрица $\|d(X, Y)\|$ есть матрица умножения на элемент $h = \sum_Y \text{wt}(Y) t_Y$ в групповой алгебре $\mathbb{C}[G]$ в базисе из одночленов t^a , где $a \in \mathbb{F}_q^m$, а $t^a = \prod_{\substack{1 \leq i \leq m \\ 1 \leq \ell \leq r}} t_{i\ell}^{a_{i\ell}}$, $0 \leq a_{i\ell} \leq p-1$.

По определению функции wt

$$\begin{aligned} h &= \sum_Y \text{wt}(Y) t_Y = \sum_{1 \leq i \leq m} i \left(\prod_{1 \leq \ell \leq r} \sum_{0 \leq k \leq p-1} t_{m-i+1, \ell}^k - 1 \right) \prod_{m-i+2 \leq i' \leq m} \prod_{1 \leq \ell \leq r} \\ &\sum_{0 \leq k \leq p-1} t_{i'\ell}^k = -1 - \sum_{2 \leq i \leq m} \prod_{i \leq i' \leq m} \prod_{1 \leq \ell \leq r} \sum_{0 \leq k \leq p-1} t_{i'\ell}^k + \prod_{1 \leq i \leq m} \prod_{1 \leq \ell \leq r} \sum_{0 \leq k \leq p-1} t_{i\ell}^k. \end{aligned}$$

С другой стороны, алгебра $\mathbb{C}[G]$ есть сумма экземпляров \mathbb{C} , причем проекция на каждый экземпляр задается путем присвоения переменным $t_{i\ell}$ значений, равных некоторым корням p -й степени из 1 (в том числе и 1). Отметим, что $\sum_k t_{i\ell}^k$ равна нулю при $t_{i\ell} \neq 1$ и p при $t_{i\ell} = 1$.

Условие $0 = \sum_X t_X = \prod_{\substack{1 \leq i \leq m \\ 1 \leq \ell \leq r}} \sum_{0 \leq k \leq p-1} t_{i\ell}^k$ задает подпространство, натянутое на

все экземпляры \mathbb{C} , кроме отвечающего значениям $t_{i\ell} = 1$ при всех i, ℓ . Так как последний член в формуле для h обращается в нуль при проекции на любой такой экземпляр, то при $\lambda \geq 0$ оператор $h - \lambda$ обратим на этом подпространстве, что и доказывает лемму. \blacktriangle

Т е о р е м а 3 (граница Хэмминга). Пусть $C \subset V$ - произвольный код мощности K с минимальным кодовым расстоянием d . Тогда

$$K \text{ vol} \left(S_{\lfloor \frac{d-1}{2} \rfloor} \right) \leq q^n.$$

Формула для объема $\text{vol}(S_d)$ шара радиуса d в пространстве $V \simeq \mathbb{F}_q^{ms}$ может быть получена при посредстве несложных комбинаторных вычислений.

П р е д л о ж е н и е 1. Имеет место равенство

$$\text{vol}(S_d) = \sum_{\substack{k_1, \dots, k_m \geq 0 \\ \sum_{1 \leq i \leq m} k_i \leq s \\ \sum_{1 \leq i \leq m} i k_i \leq d}} \frac{s!}{\prod_{1 \leq i \leq m} k_i! (s - \sum_{1 \leq i \leq m} k_i)!} \left(\frac{q-1}{q} \right)^{\sum_{1 \leq i \leq m} k_i} \prod_{1 \leq i \leq m} q^{i k_i}. \quad (3)$$

§ 3. Нижние оценки и примеры

Т е о р е м а 4 (граница Гилберта). В пространстве V размерности $\dim V = n = ms$ для любого $d, 0 < d < n$, существует линейный код с минимальным расстоянием d , размерность которого удовлетворяет неравенству

$$k + \log_q \text{vol}(S_{d-1}) \geq n.$$

Д о к а з а т е л ь с т в о. Так как расстояние $d(v, v')$ не меняется при одновременном умножении v и v' на ненулевой элемент \mathbb{F}_q , то требуемый код может быть построен с помощью стандартной процедуры поочередного выбора элементов его базиса. \blacktriangle

m -код Рида–Соломона. Пусть C – пространство полиномов над \mathbb{F}_q степени не выше a . Определим линейное отображение $C \xrightarrow{\text{Ev}} V = \mathbb{F}_q^{mq}$, ставя в соответствие полиному матрицу, составленную из значений его производных от нулевого до $(m-1)$ -го порядка включительно во всех точках аффинной прямой над полем \mathbb{F}_q . Так как общее число нулей ненулевого полинома, считая с кратностями, не превосходит a (в частности, отображение Ev инъективно при $a < mq$), то в m -метрике при $0 \leq a \leq mq$ код $\text{Ev}(C)$ имеет параметры

$$[mq, a + 1, mq - a]_q,$$

которые, очевидно, лежат на границе Синглтона, в то время как длина кода $\text{Ev}(C)$ в m раз превосходит длину обычного кода Рида–Соломона.

Легко видеть, что, добавляя к матрице $\text{Ev}(P)$ столбец из m старших коэффициентов полинома P , мы получим код с параметрами

$$[m(q+1), a+1, m(q+1) - a]_q,$$

невырожденный при $a \geq m-1$.

Заметим также, что, отождествляя \mathbb{F}_q -столбцы длины m с элементами \mathbb{F}_{q^m} , можно рассмотреть обычный код Рида–Соломона над \mathbb{F}_{q^m} как \mathbb{F}_q -код в m -метрике. Полученный код будет иметь параметры $[mq^m, a+1, q^m - a]_q$, не достигающие границы Синглтона.

m -код Рида–Маллера 1-го порядка. Выберем в \mathbb{F}_q^k по одному ненулевому вектору x_i на каждой проходящей через нуль прямой.

Пусть C – пространство линейных форм от k переменных над \mathbb{F}_q . Выберем m линейных операторов

$$A_1 = \text{Id}, \dots, A_m; \quad A_i \in \text{Aut}_{\mathbb{F}_q} C$$

так, чтобы все их ненулевые линейные комбинации с коэффициентами из \mathbb{F}_q были обратимы. Положим $V \simeq \mathbb{F}_q^{m \frac{q^k-1}{q-1}}$. Зададим отображение $C \xrightarrow{\text{Ev}} V$ формулой $\ell \mapsto (A_i \ell(x_j))$. Оно, очевидно, является вложением и задает код, аналогичный коду Рида–Маллера 1-го порядка.

Т е о р е м а 5. Параметры кода $\text{Ev}(C)$ в m -метрике суть

$$\left[m \frac{q^k-1}{q-1}, \quad k, \quad \frac{mq^k}{q-1} \delta_{\text{crit}} \right]_q$$

и, в частности, лежат на границе Плоткина.

Доказательство. Проверки требует только формула для минимального расстояния. Вес любого кодового слова равен, по определению,

$$\text{wt}(\ell) = \sum_{1 \leq i \leq m} (m - i + 1) \#\{x \mid A_i x = 0 \text{ при } i < i', \text{ но } A_i x \neq 0\}.$$

Так как в соответствии с выбором A_i формы $(A_i \ell, 1 \leq i \leq m)$ – линейно-независимы, какова бы ни была форма ℓ , то последняя сумма равна

$$\sum_{1 \leq i \leq m} (m - i + 1) q^{k-i} = q^{k-m} \sum_{1 \leq i \leq m} i q^{i-1} = \frac{mq^k}{q-1} \left(1 - \frac{1}{m} \sum_{1 \leq i \leq m} q^{-i} \right). \quad \blacktriangle$$

Осталось заметить, что требуемые операторы $A_1 \dots A_m$ можно выбрать при любом $m \leq k$. Достаточно отождествить C с расширением \mathbb{F}_{q^k} поля \mathbb{F}_q , и в качестве A_i выбрать операторы умножения на элементы некоторого, содержащего единицу, базиса этого расширения.

Алгебро-геометрические коды. Пусть X/\mathbb{F}_q – гладкая проективная абсолютно неприводимая алгебраическая кривая рода g , D – дивизор степени a на X , определенный над \mathbb{F}_q . Положим $C = L(D)$. Пусть $P_1 \dots P_s$ – набор различных \mathbb{F}_q -точек кривой X , причем $P_j \notin \text{Supp} D$ при всех j . Фиксируем определенные над \mathbb{F}_q локальные параметры t_j в точках P_j . Пусть $V = \bigoplus_{1 \leq j \leq s} \mathcal{O}_{P_j}/(t_j)^m \simeq \mathbb{F}_q^{ms}$, где \mathcal{O}_{P_j} –

локальное кольцо точки P_j . Имеется стандартное линейное отображение $C \xrightarrow{\text{Ev}} V$, невырожденное при $a < ms$, которое функции из $L(D)$ ставит в соответствие набор отрезков ее ряда Тэйлора в точках P_j по отношению к параметрам t_j .

Теорема 6. *В m -метрике параметры кода $\text{Ev}(C)$ при $a < ms$ удовлетворяют неравенствам*

$$[ms, \geq a - g + 1, \geq ms - a]_q.$$

В частности,

$$k + d \geq n - g + 1.$$

Доказательство легко выводится из теоремы Римана–Роха. \blacktriangle

Заметим, что, как и в случае кодов Рида–Соломона, являющихся частным случаем АГ-кодов, условие $P_j \notin \text{Supp} D$ на самом деле избыточно.

§ 4. Асимптотические границы

Под асимптотической задачей мы понимаем вопрос о возможных предельных значениях скорости передачи $R = \frac{1}{n} \log_q \#C$ и относительного минимального расстояния $\delta = \frac{1}{n} d_{\min}(C)$ для семейств кодов, длина которых n неограниченно возрастает. Прежде всего, отметим, что при неограниченном росте сомножителя m в разложении $n = ms$ ничего интересного не происходит.

Предложение 2. *Фиксируем $\delta, 0 \leq \delta \leq 1$. В пространствах $V_\ell = \mathbb{F}_q^{m_\ell s_\ell}$ рассмотрим шары радиусов d_ℓ . Пусть $\lim_{\ell \rightarrow \infty} m_\ell = \infty, \lim_{\ell \rightarrow \infty} \frac{d_\ell}{m_\ell s_\ell} = \delta$. Тогда*

$$\lim_{\ell \rightarrow \infty} \frac{1}{m_\ell s_\ell} \log_q \text{vol}(S_{d_\ell}) = \delta.$$

Д о к а з а т е л ь с т в о. Число возможных вариантов номера последней нулевой позиции в столбце матрицы $m \times s$ равно $m + 1$, а число возможных значений матричного элемента не превосходит q . Следовательно, для числа матриц веса, не превосходящего d_ℓ , справедлива оценка

$$\text{vol}(S_{d_\ell}) \leq (m + 1)^{s_\ell} q^{d_\ell}.$$

С другой стороны, в формуле

$$\text{vol}(S_d) = \sum_{\substack{k_1 \dots k_m \geq 0 \\ \sum_{1 \leq i \leq m} k_i \leq s \\ \sum_{1 \leq i \leq m} ik_i \leq d}} \frac{s!}{\prod_{1 \leq i \leq m} k_i! \left(s - \sum_{1 \leq i \leq m} k_i \right)!} \left(\frac{q-1}{q} \right)^{\sum_{1 \leq i \leq m} k_i} \frac{\sum_{1 \leq i \leq m} ik_i}{q}$$

член, отвечающий набору $\left\{ k_{\min(m_\ell, \lfloor \frac{d_\ell}{s_\ell} \rfloor)} = s_\ell, \text{остальные } k_i = 0 \right\}$, равен $\left(\frac{q-1}{q} \right)^{s_\ell} q^{s_\ell \min(m_\ell, \lfloor \frac{d_\ell}{s_\ell} \rfloor)}$. Значит,

$$\frac{1}{m_\ell} \log_q \frac{q-1}{q} + \min \left(1, \frac{1}{m_\ell} \left\lfloor \frac{d_\ell}{s_\ell} \right\rfloor \right) \leq \frac{1}{m_\ell s_\ell} \log_q \text{vol}(S_{d_\ell}) \leq \frac{1}{m_\ell} \log_q (m_\ell + 1) + \frac{d_\ell}{m_\ell s_\ell},$$

откуда при $\ell \rightarrow \infty$ следует предложение. \blacktriangle

С л е д с т в и е. При $m \rightarrow \infty$ нижняя граница Гилберта стремится к верхней границе Синглтона. \blacktriangle

Далее в этом параграфе мы будем считать, что m фиксировано.

Т е о р е м а 7 (асимптотическая граница Плоткина). Пусть C_ℓ – последовательность кодов длины ms_ℓ , $s_\ell \rightarrow \infty$, и пусть существует предел $\lim_{\ell \rightarrow \infty} \frac{1}{ms_\ell} (k(C_\ell), d_{\min}(C_\ell)) = (R, \delta)$. Тогда

$$R + \frac{\delta}{\delta_{\text{crit}}} \leq 1. \quad (4)$$

Д о к а з а т е л ь с т в о. То, что $\delta \leq \delta_{\text{crit}}$, следует из теоремы 2. Остальное следует из варианта леммы об ухудшении ([1, лемма 1.1.34]). (При $m > 1$ конструкция ухудшенных кодов приводит к кодам, минимальное расстояние которых может быть больше, чем требуется, но это не влияет на вывод формулы (4) из условия $\delta \leq \delta_{\text{crit}}$.) \blacktriangle

Т е о р е м а 8. (i) При $0 < \delta < 1$ уравнение

$$\delta = \frac{\frac{q-1}{q} \sum_{1 \leq i \leq m} iz^i}{m \left(1 + \frac{q-1}{q} \sum_{1 \leq i \leq m} z^i \right)} \quad (5)$$

имеет единственный положительный корень z_0 .

(ii) Фиксируем δ , $0 < \delta < 1$. В пространствах $V_s = \mathbb{F}_q^{ms}$ рассмотрим шары радиуса d_s . Пусть $\lim_{s \rightarrow \infty} \frac{d_s}{ms} = \delta$. Тогда

$$\lim_{s \rightarrow \infty} \frac{1}{ms} \log_q \text{vol}(S_{d_s}) = \begin{cases} 1 & \text{при } \delta \geq \delta_{\text{crit}}, \\ H_{q,m}(\delta) & \text{при } 0 \leq \delta \leq \delta_{\text{crit}}, \\ 0 & \text{при } \delta = 0, \end{cases}$$

$$\text{где } H_{q,m}(\delta) = \delta - \delta \log_q z_0 + \frac{1}{m} \log_q \left(1 + \frac{q-1}{q} \sum_{1 \leq i \leq m} z_0^i \right).$$

Замечание. Если $m = 1$, то $z_0 = \frac{q}{q-1} \frac{\delta}{1-\delta}$, $\delta_{\text{crit}} = 1 - \frac{1}{q}$ и $H_{q,1}(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta) = H_q(\delta)$, где $H_q(\delta)$ – обычная q -ичная энтропия.

Доказательство теоремы. (i) Функция в правой части (5) стремится к нулю при $z \rightarrow 0$ и к единице при $z \rightarrow \infty$, а ее производная равна

$$\frac{q-1}{qm \left(1 + \frac{q-1}{q} \sum_{1 \leq i \leq m} z^i \right)^2} \left(\sum_{1 \leq j \leq m} j^2 z^{j-1} + \frac{q-1}{q} \sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq m}} (j^2 - ij) z^{i+j-1} \right)$$

и нигде не обращается в нуль при $z > 0$, поскольку после приведения подобных членов числитель становится полиномом с положительными коэффициентами.

(ii) При $\delta > 0$ для того, чтобы определить доминирующий в асимптотике при $s \rightarrow \infty$ член суммы (3), необходимо найти максимум функции

$$\Phi(\chi) = \sum_{1 \leq i \leq m} \chi_i \ln \frac{q-1}{q} + \sum_{1 \leq i \leq m} i \chi_i \ln q - \sum_{1 \leq i \leq m} \chi_i \ln \chi_i - \left(1 - \sum_{1 \leq i \leq m} \chi_i \right) \ln \left(1 - \sum_{1 \leq i \leq m} \chi_i \right)$$

(эта функция асимптотически совпадает с $\frac{1}{s} \ln \text{vol}(S_{d_s})$, если положить $\chi_i = \frac{1}{s} k_i$ и воспользоваться формулой Стирлинга) при условиях

$$\left\{ \sum_{1 \leq i \leq m} \chi_i \leq 1; \chi_i \geq 0 \text{ при любом } i; \sum_{1 \leq i \leq m} i \chi_i \leq m\delta \right\}.$$

Обозначим область в \mathbb{R}^m , задаваемую этими условиями, через $\bar{\Delta}$, ее внутренность – через Δ , область, задаваемую первыми двумя условиями, и ее внутренность, соответственно, через $\bar{\Gamma}$ и Γ , и гиперплоскость $\sum_{1 \leq i \leq m} i \chi_i = m\delta$ через H . Функция

$\Phi(\chi)$, ограниченная в области Γ и непрерывная на ее границе, обладает в Γ единственной критической точкой X с координатами $\chi_i(X) = (q-1)q^{i-m-1}$. Нетрудно проверить, что матрица вторых производных функции $\Phi(\chi)$, равная $\|B_{ij}\| = \frac{1}{1 - \sum_{1 \leq k \leq m} \chi_k} \|A_{ij}\|$, где

$$A_{ij} = \begin{cases} -1 & \text{при } i \neq j, \\ -1 - \frac{\sum_{1 \leq k \leq m} \chi_k}{\chi_i} & \text{при } i = j, \end{cases}$$

отрицательно определена во всей области Γ .

Следовательно, критическая точка X невырождена и является точкой глобального максимума функции $\Phi(X)$ в Γ . При $\delta \geq \delta_{\text{crit}}$ она лежит в $\bar{\Delta}$, и объем шара S_{d_s} асимптотически при $s \rightarrow \infty$ равен объему всего пространства V_s . При $\delta < \delta_{\text{crit}}$ точка X находится вне области Δ . Критическая точка функции $\Phi(X)$ на гиперплоскости H

должна иметь координаты $\chi_i = \frac{q-1}{1 + \frac{q-1}{q} \sum_{1 \leq k \leq m} z_0^k} z_0^i$, где z_0 – положительный корень

уравнения (4).

Из первой части теоремы следует, что эта точка Y существует и единственна. Так как матрица вторых производных $\Phi(X)$ глобально отрицательно определена, то Y является точкой глобального максимума ограничения $\Phi(X)$ на $H \cap \bar{\Gamma}$. Так как поверхности уровня $\Phi(X)$ в области $\bar{\Gamma}$ связны, и их внутренность содержит точку X , причем при $\delta < \delta_{\text{crit}}$ точка X и область $\bar{\Delta}$ лежат по разные стороны гиперплоскости H , то точка глобального максимума функции $\Phi(X)$ в $\bar{\Delta}$ при $\delta < \delta_{\text{crit}}$ лежит на H и, следовательно, совпадает с точкой Y . Поскольку $S_{d_s} \subset S_{d'_s}$ при $d_s \leq d'_s$ и $\lim_{\delta \rightarrow 0} H_{q,m}(\delta) = 0$, то утверждение теоремы справедливо и при $\delta = 0$. \blacktriangle

Т е о р е м а 9 (асимптотическая граница Хэмминга). Пусть C_ℓ – последовательность кодов, как в теореме 7. Тогда

$$R + H_{q,m} \left(\frac{\delta}{2} \right) \leq 1.$$

Д о к а з а т е л ь с т в о следует из теорем 3 и 8. \blacktriangle

Т е о р е м а 10 (асимптотическая граница Гилберта). Для любого $\delta : 0 \leq \delta \leq 1$ существует последовательность линейных кодов C_ℓ длины ms_ℓ , $s_\ell \rightarrow \infty$, такая, что $\lim_{\ell \rightarrow \infty} \frac{1}{ms_\ell} (k(C_\ell), d_{\min}(C_\ell)) = (R, \delta)$, и при этом

$$R \geq \begin{cases} 0 & \text{при } \delta \geq \delta_{\text{crit}}, \\ 1 - H_{q,m}(\delta) & \text{при } \delta < \delta_{\text{crit}}. \end{cases}$$

Д о к а з а т е л ь с т в о следует из теорем 4 и 8. \blacktriangle

Т е о р е м а 11 (асимптотическая АГ-граница). Для любого $\delta : 0 \leq \delta \leq 1$ существует последовательность линейных кодов C_ℓ длины ms_ℓ , $s_\ell \rightarrow \infty$, такая, что $\lim_{\ell \rightarrow \infty} \frac{1}{ms_\ell} (k(C_\ell), d_{\min}(C_\ell)) = (R, \delta)$, и при этом

$$R \geq 1 - \delta - \frac{1}{mA(q)},$$

где $A(q) = \limsup (\#X(\mathbb{F}_q)/g(X))$, и максимум берется по всем гладким абсолютно неприводимым кривым X/\mathbb{F}_q .

Д о к а з а т е л ь с т в о следует из теоремы 6. \blacktriangle

Т е о р е м а 12. Асимптотическая граница Гилберта пересекает асимптотическую АГ-границу в том и только в том случае, если выполнено условие

$$\log_q \left(1 + m \frac{q-1}{q} \right) \geq \frac{1}{A(q)}.$$

Д о к а з а т е л ь с т в о. Производная функции $H_{q,m}(\delta) - \delta$ равна $-\log_q z_0$, где z_0 задается формулой (5). Поскольку $z_0(\delta)$ монотонно возрастает, то эта функция (как и сама m -энтропия) выпукла вверх и достигает максимума при условии $H'_{q,m}(\delta) = 1$.

При этом $z_0 = 1$, $\delta = \frac{(m+1)(q-1)}{2(mq+q-m)}$ и $H_{q,m}(\delta) - \delta = \frac{1}{m} \log_q \left(1 + m \frac{q-1}{q} \right)$, и теорема следует из теорем 10 и 11. ▲

С л е д с т в и е. (i) АГ-граница пересекает границу Гилберта при $m = 1$ и $q = p^{2\ell} \geq 49$ (случай метрики Хэмминга),
при $m = 2$ и $q = p^{2\ell} \geq 16$,
при $m = 3$ и $q = p^{2\ell} \geq 9$,
при $m = 4$ и $q = p^{2\ell} \geq 4$

(при $m = q = 4$ границы касаются в точке $\delta = \frac{15}{32}$).

(ii) Существует m_0 такое, что при $m \geq m_0$ АГ-граница пересекает границу Гилберта при любом q (не обязательно вида $q = p^{2\ell}$).

Д о к а з а т е л ь с т в о. (i) Если $q = p^{2\ell}$, то $A(q) = \sqrt{q} - 1$ (см. [1, теорема 2.3.24]).

(ii) Существует абсолютная константа c такая, что $A(q) \geq c \log_2 q$ при любом q (см. [1, теорема 2.3.25]). Достаточно положить $m_0 = 2^{c^{-1}+1} - 2$. ▲

Авторы благодарны Л. А. Бассалыго, Г. Л. Кацману и В. М. Сидельникову за полезные обсуждения.

СПИСОК ЛИТЕРАТУРЫ

1. Tsfasman M. A., Vlăduț S. G. Algebraic-geometric codes. Dordrecht-Boston-London: Kluwer Acad. Publ., 1991.

Поступила в редакцию
16.11.95

После переработки
16.01.96