

УДК 621.391.15:681

© 2006 г. А.М. Барг¹, Д.Ю. Ногин²

СПЕКТРАЛЬНЫЙ ПОДХОД К ГРАНИЦАМ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ ДЛЯ КОДОВ

Даются новые доказательства асимптотических верхних границ теории кодирования, получаемых в рамках метода линейного программирования Дельсарта. Доказательства основаны на изучении собственных векторов некоторых конечномерных операторов, связанных с ортогональными многочленами. В качестве примеров применения данного метода рассматриваются двоичные коды, двоичные равновесные коды, сферические коды и коды в проективных пространствах.

§ 1. Введение

Пусть X – компактное метрическое пространство с функцией расстояния d . Кодом C называется конечное подмножество пространства X . Минимальное расстояние кода C определяется как $d(C) = \min_{x,y \in C, x \neq y} d(x,y)$. В разнообразных приложениях возникают такие метрические пространства, как двоичные пространства Хэмминга и Джонсона, сфера в \mathbb{R}^n , действительное и комплексное проективные пространства, многообразия Грассмана и др. Оценить максимальный размер кода с данным значением d – одна из основных задач теории кодирования. Пусть M – мощность кода C . Действенным инструментом для получения верхних границ на величину M как функцию от $d(C)$ является метод линейного программирования Дельсарта [1]; этот метод применим для широкого класса метрических пространств, включая все вышеупомянутые примеры. Первыми из таких примеров явились двоичное пространство Хэмминга $H_n = \{0, 1\}^n$ и пространство Джонсона $J^{n,w} \subset H_n$, которое состоит из всех векторов пространства H_n , имеющих вес Хэмминга w , где расстоянием является метрика Хэмминга. Наилучшие известные асимптотические границы на мощность двоичных и двоичных равновесных кодов были получены Мак-Элисом, Родемичем, Рамсеем и Велчем [2] и называются “границами четырех” (или MRRW). Вскоре после этого Кабатянский и Левенштейн [3] получили аналогичную границу для кодов на единичной сфере в \mathbb{R}^n с евклидовой метрикой, а также в некоторых других связанных с ней пространствах. Там же был предложен общий подход к получению границ на мощность кода в дистанционно-транзитивных метрических пространствах, основанный на гармоническом анализе на группе изометрий пространства. Этот подход в дальнейшем был развит в [4, 5], где в том числе были исследованы границы применимости метода Дельсарта.

В настоящей статье предложен новый метод доказательства границ линейного программирования в теории кодирования. Наш подход, основанный на рассмотрении

¹ Работа выполнена при частичной финансовой поддержке NSF (Grants CCR0310961, CCF0515124) и Агентства национальной безопасности США (Grant H98230-06-1-0044).

² Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номера проектов 02-01-22005; 06-01-72550-НЦНИЛ-а) и NSF (Grant CCR0310961).

собственных векторов некоторых конечномерных операторов, связанных с ортогональными многочленами, возможно, делает некоторые шаги доказательств идейно более понятными по сравнению с известными методами. В статье также рассмотрены некоторые из основных примеров, упомянутых выше. Линейно-алгебраические идеи, которым мы следуем, были предложены в недавней работе Башок [6], где с помощью этого подхода получена асимптотическая граница для кодов в действительном многообразии Грассмана.

§ 2. Граница на мощность кода

Мы предполагаем, что X – дистанционно-транзитивное пространство, т.е. его группа изометрий G действует дважды транзитивно на упорядоченных парах точек, находящихся на заданном расстоянии. В этом случае зональные сферические ядра $K_i(\mathbf{x}, \mathbf{y})$, ассоциированные с неприводимыми регулярными представлениями группы G , зависят только от расстояния между \mathbf{x} и \mathbf{y} . Во всех вышеперечисленных примерах, за исключением многообразия Грассмана, $K_i(\mathbf{x}, \mathbf{y})$ можно представить в виде многочлена $p_i(x)$ степени i от одной переменной, где $x = \tau(d)$ – некоторая функция от расстояния $d(\mathbf{x}, \mathbf{y})$.

Пусть D – (конечное или бесконечное) множество возможных значений расстояния в X . Будем предполагать, что $\tau(d(\mathbf{x}, \mathbf{y}))$ – монотонная функция, переводящая D в некоторый отрезок $[a; b]$. Например, для пространства Хэмминга $D = \{0, 1, \dots, n\}$, а в качестве τ можно взять тождественную функцию. Для сферы $S^{n-1}(\mathbb{R})$ имеем $D = [0; 2]$. В этом случае удобно взять $\tau(d) = 1 - d^2/2$, т.е. скалярное произведение $(\mathbf{x}, \mathbf{y}) = \sum_i x_i y_i$. Инвариантная мера на G индуцирует меру $d\mu$ на $[a; b]$. Например, для $X = \{0, 1\}^n$ мера $d\mu$ соответствует биномиальному распределению вероятностей на $\{0, 1, \dots, n\}$, так что $\int_D d\mu = 1$. Мы будем предполагать, что последнее условие выполняется в общем случае (если это не так, нормируем меру μ).

Ядра $K_i(\mathbf{x}, \mathbf{y})$, $i = 0, 1, \dots$, являются положительно полуопределенными. Это означает, что $\sum_{\mathbf{x}, \mathbf{y} \in C} K_i(\mathbf{x}, \mathbf{y}) \geq 0$ для любого конечного множества $C \subset X$. Из этого свойства и того факта, что $K_i(\mathbf{x}, \mathbf{y})$ можно представить в виде многочлена от одной переменной, вытекает семейство неравенств

$$\sum_{\mathbf{x}, \mathbf{y} \in C} p_i(\tau(d(\mathbf{x}, \mathbf{y}))) \geq 0, \quad i = 0, 1, \dots, \quad (1)$$

называемых в теории кодирования неравенствами Дельсарта.

Функцию τ всегда можно выбрать таким образом, чтобы многочлены p_i , $i = 0, 1, \dots$, были ортогональны на $[a; b]$ относительно скалярного произведения $\langle f, g \rangle = \int fg d\mu$. Далее через V обозначаем пространство $L_2(d\mu)$ функций на $[a; b]$, интегрируемых с квадратом.

Будем предполагать, что многочлены p_i ортонормированы, т.е. $\|p_i\|^2 = \langle p_i, p_i \rangle = 1$. Заметим, что отсюда, в частности, следует, что $p_0 \equiv 1$. Кроме того, нам потребуется условие, что произведение $p_i p_j$ для любых $i, j \geq 0$ раскладывается по базису $\{p_k\}$ с неотрицательными коэффициентами:

$$p_i p_j = \sum_k q_{i,j}^k p_k \quad (q_{i,j}^k \geq 0). \quad (2)$$

Это свойство также вытекает из того, что зональные сферические ядра являются положительно полуопределенными (см. [3]).

Поскольку многочлены $\{p_i\}$ ортогональны, они удовлетворяют трехчленному рекуррентному соотношению [7] вида

$$xp_k = \alpha_k p_{k+1} + \beta_k p_k + \gamma_k p_{k-1} \quad (k = 0, 1, \dots, p-1 = 0). \quad (3)$$

Пусть $P_1 = \varepsilon p_1$, где $\varepsilon > 0$ – некоторая константа. Тогда справедливо и рекуррентное соотношение

$$P_1 p_k = a_k p_{k+1} + b_k p_k + c_k p_{k-1}, \quad (4)$$

которое следует из (3) с учетом того, что P_1 – линейная функция. Согласно (2) коэффициенты a_k, b_k, c_k неотрицательны.

Пусть $C \subset X$ – код мощности M с расстоянием d . Обозначим через $\Delta(C) = \{\tau(d(\mathbf{x}, \mathbf{y})), \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$ множество значений функции τ на всевозможных расстояниях между различными кодовыми точками. Положим $\tau_0 = \tau(0)$.

Основная теорема метода линейного программирования состоит в следующем утверждении.

Теорема 1 ([1, 3]). Пусть $C \subset X$ – код мощности M . Пусть $F(t) = \sum_{i=0}^m F_i p_i(x)$ – многочлен, удовлетворяющий условиям

- (i) $F_0 > 0, F_i \geq 0, i = 1, 2, \dots, m;$
- (ii) $F(x) \leq 0$ при $x \in \Delta(C)$.

Тогда $M \leq F(\tau_0)/F_0$.

Доказательство теоремы довольно очевидно, поскольку, с одной стороны, в силу (ii) выполняется

$$\sum_{\mathbf{x}, \mathbf{y} \in C} F(\tau(d(\mathbf{x}, \mathbf{y}))) \leq MF(\tau_0),$$

а с другой стороны, учитывая (1), условие (i) и тот факт, что $p_0 = 1$, получаем

$$\sum_{\mathbf{x}, \mathbf{y} \in C} F(\tau(d(\mathbf{x}, \mathbf{y}))) = \sum_i F_i \sum_{\mathbf{x}, \mathbf{y}} p_i(\tau(d(\mathbf{x}, \mathbf{y}))) \geq F_0 M^2.$$

Эта теорема эквивалентна теореме двойственности для задачи линейного программирования, в которой переменными являются коэффициенты распределения расстояний кода C , а ограничения – неравенства Дельсарта. Поэтому оценки, вытекающие из этой теоремы, называются границами линейного программирования. Цель данного параграфа – изложить новый метод получения границ на M , основанный на этой теореме.

Мы будем использовать общее обозначение $A_k(c_i, b_i, a_i)$ для трехдиагональных матриц вида

$$A_k = \begin{pmatrix} b_0 & a_0 & 0 & 0 & \dots & 0 \\ c_1 & b_1 & a_1 & 0 & \dots & 0 \\ & c_2 & b_2 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & a_{k-1} \\ 0 & 0 & \dots & \dots & c_k & b_k \end{pmatrix}.$$

Наибольшее собственное значение квадратной симметричной матрицы M будем обозначать через $\lambda_{\max}(M)$.

Всюду далее операторы, действующие на V , мы будем обозначать полужирными буквами, а матрицы этих операторов в базисе $\{p_i\}$ – соответствующими обычными латинскими буквами. Пусть V_k – подпространство в V , состоящее из многочленов

степени не выше k . Пусть E_k – оператор ортогональной проекции из V на V_k . Рассмотрим оператор

$$S_k = E_k \circ P_1 : V_k \rightarrow V_k,$$

т.е. умножение на многочлен P_1 , а затем проектирование на пространство V_k . Дальнейшие рассуждения используют тот факт, что этот оператор самосопряжен (относительно билинейной формы $\langle \cdot, \cdot \rangle$) – действительно, и умножение на функцию, и ортогональное проектирование являются самосопряженными операторами. Тем самым, матрица $S_k = A_k(c_i, b_i, a_i)$ симметрична. Иначе говоря,

$$a_i = \langle P_1 p_i, p_{i+1} \rangle = \langle p_i, P_1 p_{i+1} \rangle = c_{i+1}.$$

Матрица $A \geq 0$ (т.е. матрица с неотрицательными элементами) размера $p \times p$ называется неразложимой, если для любого разбиения множества индексов $\{1, 2, \dots, p\}$ на два непересекающихся подмножества I и J , $|I| + |J| = p$, матрица $(a_{i,j})_{i \in I, j \in J}$ ненулевая (иначе говоря, ориентированный граф G с вершинами $\{1, 2, \dots, p\}$ и ребрами (i, j) при $A_{ij} > 0$ является сильно связным). В частности, матрица S_k неотрицательна и неразложима.

В следующей лемме перечислены необходимые нам свойства неразложимых матриц.

Лемма 1. Пусть $A \geq 0$ – неразложимая симметричная $(p \times p)$ -матрица.

(а) Максимальное собственное значение $\lambda_{\max}(A)$ положительно и имеет кратность 1. При этом существует вектор $y > 0$, для которого $Ay = \lambda_{\max}(A)y$.

(б) $\lambda_{\max}(A) \leq \max_{1 \leq i \leq p} \sum_j A_{ij}$.

(в) Для любого $y \neq 0$ справедливо $\lambda_{\max}(A) \geq \frac{(Ay, y)}{(y, y)}$.

(г) Для всякой матрицы B , удовлетворяющей условию $0 \leq B \leq A$ или являющейся главным минором матрицы A , имеет место $|\lambda_{\max}(B)| \leq \lambda_{\max}(A)$.

Здесь утверждения (а), (б) и (г) составляют часть теории Перрона–Фробениуса (см., например, [8]); свойство (в), очевидно, имеет место для любой симметричной матрицы.

Предлагаемый метод получения верхних границ основан на следующей теореме.

Теорема 2. Пусть $C \subset X$ – некоторый (M, d) -код, и пусть $\rho_k = \frac{a_k p_{k+1}(\tau_0)}{p_k(\tau_0)}$.

Тогда

$$M \leq \frac{4\rho_k p_k^2(\tau_0)}{P_1(\tau_0) - \lambda_{\max}(S_k)}$$

для любого k , такого что $\lambda_{\max}(S_{k-1}) \geq P_1(x)$ при всех $x \in \Delta(C)$.

Доказательство. Пусть $g = \sum_{i=1}^k g_i p_i \in V_k$. Зафиксируем некоторое $\rho > 0$ (его значение мы выберем позже). Определим оператор $T_k : V_k \rightarrow V_k$ как

$$T_k g = S_k g - \rho g_k p_k, \tag{5}$$

и пусть θ_k – его максимальное собственное значение. Напомним, что через T_k мы обозначаем матрицу этого оператора в базе $\{p_i\}$. (Матрица T_k совпадает с матрицей S_k за исключением того, что $(T_k)_{k+1, k+1} = (S_k)_{k+1, k+1} - \rho$.) Поскольку можно “подправить” матрицу T_k на некоторую кратность единичной матрицы I так, чтобы

все ее элементы стали неотрицательными, например, рассмотреть $T_k + \rho I \geq 0$, то по лемме 1(г) получаем

$$\lambda_{\max}(S_{k-1} + \rho I) < \theta_k + \rho < \lambda_{\max}(S_k + \rho I),$$

откуда

$$\lambda_{\max}(S_{k-1}) < \theta_k < \lambda_{\max}(S_k). \quad (6)$$

Кроме того, собственное значение θ_k имеет кратность 1. Через $f = (f_0, f_1, \dots, f_k) \in V_k$ обозначим собственный вектор, соответствующий этому собственному значению. Согласно (5) имеем

$$P_1 f = \theta_k f + \rho f_k p_k + f_k a_k p_{k+1},$$

так что

$$f = \frac{\rho p_k + a_k p_{k+1}}{P_1 - \theta_k} f_k.$$

Рассмотрим многочлен $F = (\rho p_k + a_k p_{k+1}) f$. По лемме 1(а) можно выбрать f так, чтобы его координаты были положительными. Тогда согласно (2) коэффициенты разложения многочлена F по базису $\{p_i\}$ неотрицательны. Далее, если $\lambda_{\max}(S_{k-1}) \geq P_1(x)$ для $x \in \Delta(C)$, то в силу (6) справедливо $F(x) \leq 0$ для $x \in \Delta(C)$, т.е. $F(x)$ удовлетворяет условию (ii) теоремы 1. Так как умножение на f – самосопряженный оператор, получаем

$$F_0 = \langle (\rho p_k + a_k p_{k+1}) f, 1 \rangle = \langle \rho p_k + a_k p_{k+1}, f \rangle = \rho f_k > 0$$

и

$$F(\tau_0) = \frac{(\rho p_k(\tau_0) + a_k p_{k+1}(\tau_0))^2}{P_1(\tau_0) - \theta_k} f_k < \frac{(\rho p_k(\tau_0) + a_k p_{k+1}(\tau_0))^2}{P_1(\tau_0) - \lambda_{\max}(S_k)} f_k$$

при условии, что $\lambda_{\max}(S_k) < n$. Таким образом,

$$\frac{F(\tau_0)}{F_0} < \frac{(\rho p_k(\tau_0) + a_k p_{k+1}(\tau_0))^2}{\rho(P_1(\tau_0) - \lambda_{\max}(S_k))}.$$

Минимум по ρ правой части достигается при $\rho = \rho_k$. Требуемое неравенство получается применением многочлена $F = (\rho_k p_k + a_k p_{k+1}) f$ в теореме 1. \blacktriangle

Замечание 1. Согласно лемме 1(г) числа $\{\lambda_{\max}(S_k)\}$ образуют монотонно возрастающую последовательность. Поэтому последнее условие теоремы 2 выполняется для всех k , больших некоторого k_0 .

Теперь оценим максимальное собственное значение матрицы S_k .

Лемма 2. Пусть $a_{i+1} > a_i$ и $b_{i+1} > b_i$, $i = 0, 1, \dots$. Тогда для любого $s = 1, \dots, k+1$ справедливо

$$\frac{1}{s} (2(s-1)a_{k-s+1} + sb_{k-s+1}) \leq \lambda_{\max}(S_k) \leq a_{k-1} + \max(a_{k-1} + b_{k-1}, b_k).$$

Доказательство. По лемме 1(б)

$$\lambda_{\max}(S_k) \leq \max(a_{k-2} + b_{k-1} + a_{k-1}, a_{k-1} + b_k),$$

откуда следует оценка сверху. С другой стороны, возьмем $y = (0^{k-s+1}1^s)^t$ (здесь t – символ транспонирования). Тогда из леммы 1(в) получаем

$$\lambda_{\max}(S_k) \geq \frac{1}{s} \left(2 \sum_{p=1}^{s-1} a_{k-p} + \sum_{p=0}^{s-1} b_{k-p} \right).$$

С учетом предположения, что коэффициенты a_i, b_i монотонно возрастают по i , это дает оценку снизу. ▲

Замечание 2. Лемма 2 фактически дает оценку экстремальных нулей многочлена p_{k+1} . Действительно, рассмотрим оператор $X_k = E_k \circ \alpha: V_k \rightarrow V_k$. Он самосопряжен, и его матрица в базисе $\{p_i\}$ трехдиагональная, симметричная и имеет вид $X_k = A_k(\gamma_i, \beta_i, \alpha_i)$, где элементы $\alpha_i, \beta_i, \gamma_i$ – коэффициенты трехчленного соотношения (3).

Известно (см., например, [9]), что спектр оператора X_k совпадает с множеством нулей многочлена p_{k+1} . [Доказательство состоит в следующем: пусть $p_{k+1}(\lambda) = 0$. Рассмотрим действие оператора X_k на многочлен $f = p_{k+1}/(\lambda - x) \in V_k$:

$$\lambda f - X_k f = \lambda f - E_k(xf) = E_k((\lambda - x)f) = E_k p_{k+1} = 0.$$

Наоборот, если $f \in V_k, f \neq 0$, и $0 = \lambda f - X_k f = E_k((\lambda - x)f)$, то отсюда следует, что $(\lambda - x)f$ с точностью до постоянного множителя совпадает с p_{k+1} . Таким образом, $p_{k+1}(x)$ пропорционален³ многочлену $\det(xI_{k+1} - X_k)$.] Тогда максимальный нуль x_{k+1}^+ многочлена p_{k+1} может быть найден как $x_{k+1}^+ = \lambda_{\max}(X_k) = \max_{\|y\|=1} (X_k y, y)$,

или, в более явном виде,

$$x_{k+1}^+ = \max_{\|y\|=1} \left\{ \sum_{i=0}^k \beta_i y_i^2 + 2 \sum_{i=0}^{k-1} \alpha_i y_i y_{i+1} \right\}.$$

Эта формула впервые опубликована в [5, с. 580] с другим доказательством.

Отметим, что соотношение между экстремальным нулем многочлена p_{k+1} и наибольшим собственным значением $\lambda_{\max}(X_k)$ позволяет значительно снизить вычислительную сложность задачи численного нахождения экстремального нуля (по сравнению с прямыми вычислениями) благодаря наличию весьма эффективных итеративных алгоритмов нахождения собственных значений симметричных матриц. Это наблюдение оказывается полезным для вычисления границ линейного программирования (таких как границы, рассматриваемые в §3) и других подобных результатов для кодов умеренной и даже большой длины (порядка нескольких тысяч).

§ 3. Примеры

В этом параграфе рассмотрено несколько примеров, интересных для теории кодирования.

3.1. Двоичные коды. Пусть $X = \{0, 1\}^n$ – двоичное пространство Хэмминга. Известно [1, 3], что многочлены p_i являются (нормированными) многочленами Кравчука $\{\tilde{K}_k(x), k = 0, 1, \dots, n\}$. При этом $\mu(i) = 2^{-n} \binom{n}{i}$, и билинейная форма имеет

вид $(f, g) = \sum_{i=0}^n \mu(i) f(i) g(i)$. Пусть C – двоичный код длины n мощности M с расстоянием Хэмминга $d = d(C)$. Положим $\tau(k) = k$, так что $\Delta(C) \subset \{d, d+1, \dots, n\}$. Это

³ Коэффициент пропорциональности равен $\alpha_0 \alpha_1 \dots \alpha_{k-1}$ и может быть найден рекуррентно из соотношения (3) с учетом $p_0 \equiv 1$.

вложение может быть и собственным в зависимости от конкретного кода C , но мы будем игнорировать этот факт и предполагать, что $\Delta(C) = \{d, d+1, \dots, n\}$; такое предположение может лишь ослабить оценку линейного программирования на M .

Многочлены \tilde{K}_k удовлетворяют трехчленному рекуррентному соотношению [7]

$$2x\tilde{K}_k(x) = -\sqrt{(n-k)(k+1)}\tilde{K}_{k+1}(x) + n\tilde{K}_k(x) - \sqrt{(n-k+1)k}\tilde{K}_{k-1}(x); \quad (7)$$

кроме того, $\tilde{K}_0 = 1$, $\tilde{K}_i(x)\tilde{K}_j(x) = \sum_k q_{i,j}^k \tilde{K}_k(x)$ с коэффициентами $q_{i,j}^k \geq 0$ и

$$\tilde{K}_k(0) = \sqrt{\binom{n}{k}}. \quad (8)$$

В соотношении (4) возьмем $P_1 = \sqrt{n}p_1 = n - 2x$. Тогда из (7) получаем $S_k = A_k(a_{i-1}, 0, a_i)$, где $a_i = \sqrt{(i+1)(n-i)}$, $i = 0, 1, \dots$, или, в явном виде,

$$S_k = \begin{pmatrix} 0 & \sqrt{n} & 0 & \dots & \dots & 0 \\ \sqrt{n} & 0 & \sqrt{2(n-1)} & \dots & \dots & 0 \\ 0 & \sqrt{2(n-1)} & 0 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & 0 & \sqrt{(k-1)(n-k+2)} & 0 \\ \dots & \dots & \dots & \sqrt{(k-1)(n-k+2)} & 0 & \sqrt{k(n-k+1)} \\ 0 & 0 & \dots & 0 & \sqrt{k(n-k+1)} & 0 \end{pmatrix}.$$

Условие монотонности леммы 2 очевидным образом выполняется, так как $a_k > a_{k-1}$ при $k < n/2$. Таким образом, для максимального собственного значения матрицы S_k получаем оценку

$$\frac{2(s-1)}{s} \sqrt{(k-s+2)(n-k+s-1)} \leq \lambda_{\max}(S_k) \leq 2\sqrt{k(n-k+1)}.$$

Полагая $n \rightarrow \infty$, $s \rightarrow \infty$, $s = o(n)$, получаем точную асимптотику главного члена:

$$\lim_{n \rightarrow \infty, k/n \rightarrow \tau} \frac{\lambda_{\max}(S_k)}{n} = 2\sqrt{\tau(1-\tau)}. \quad (9)$$

Поскольку $\tau_0 = 0$ и $\rho_k = n - k$, оценка теоремы 2 принимает вид

$$M \leq \frac{4(n-k)}{n - \lambda_{\max}(S_k)} \binom{n}{k} \quad (10)$$

для всех k , таких что $\lambda_{\max}(S_{k-1}) \geq P_1(d) = n - 2d$. Из этой оценки с учетом (9) вытекает следующий асимптотический результат (асимптотическая "граница четырех" для двоичных кодов [2]):

$$\frac{1}{n} \log M \leq h(1/2 - \sqrt{\delta(1-\delta)})(1 + o(1)).$$

Здесь $h(x) = x \log_2 x - (1-x) \log_2(1-x)$ - двоичная энтропия. Действительно, положим $\lim \frac{d}{n} = \delta$ и предположим, что $\delta \leq 1/2$. Требуется выбрать k таким, чтобы $\frac{\lambda_{k-1}}{n} \geq (1-2\delta)(1+o(1))$ при $n \rightarrow \infty$. В пределе это означает, что τ должно быть

выбрано таким, чтобы $2\sqrt{\tau(1-\tau)} \geq 1-2\delta$, или $\tau \geq 1/2 - \sqrt{\delta(1-\delta)}$. Для завершения доказательства остается применить формулу Стирлинга.

Замечание 3. Чтобы применить замечание 2 к рассматриваемому случаю, заметим из (7), что

$$X_k = 1/2(nI_{k+1} - S_k) = 1/2A_k(-\sqrt{i(n-i+1)}, n, -\sqrt{(i+1)(n-i)}).$$

Поэтому получаем следующее выражение для максимального корня многочлена \tilde{K}_{k+1} :

$$x_{k+1}^+ = \frac{n}{2} + \max_{\|y\|=1} \sum_{i=0}^{k-1} y_i y_{i+1} \sqrt{(i+1)(n-i)}.$$

Этот результат впервые получен в [10]. С тех пор были получены более точные оценки экстремальных нулей [5, 11], тем не менее наша лемма 2 достаточна для вычисления точного значения главного члена.

Замечание 4. Оценка (10) близка к ранее известным оценкам, получаемым в рамках метода Дельсарта. В частности, Левенштейн [4, 5] построил семейство многочленов, оптимальных (при определенных условиях) для задачи Дельсарта. Из его результатов следует, что наши оценки не улучшают известные границы на M . Результаты, полученные в [2], также имеют вид, подобный (10).

Замечания 2–4 (с соответствующими поправками) относятся и к остальным примерам §3.

3.2. Равновесные коды. Пусть теперь $X \subset J^{n,w}$ – двоичное пространство Джонсона, т.е. множество векторов из $\{0, 1\}^n$ с весом Хэмминга w . В качестве d возьмем метрику Хэмминга, так что $D = \{0, 2, \dots, 2w\}$, и положим $\tau(d) = d/2$. Соответствующее семейство ортогональных многочленов – это многочлены Хана $H_k(x)$ [1]. Они ортогональны на $\tau(D) = \{0, 1, \dots, w\}$ с весами

$$\mu_j(i) = \binom{w}{i} \binom{n-w}{i} / \binom{n}{w}$$

в соответствии с

$$\int H_k H_m d\mu_j = \frac{n-2k+1}{n-k+1} \binom{n}{k} \delta_{km}$$

и удовлетворяют трехчленному соотношению

$$\begin{aligned} & (k+1)(w-k)(n-w-k)(n-2k+2)(n-2k+3)H_{k+1}(x) = \\ & = (n-2k-1)(n-2k+3) \times \\ & \times [(n+2)w(n-w) - nk(n-k+1) - (n-2k)(n-2k+2)x]H_k(x) - \\ & - (n-2k-1)(n-2k)(w-k+1)(n-w-k+1)(n-k+2)H_{k-1}(x). \end{aligned} \quad (11)$$

Отметим, что $\sum_{i=1}^w \mu_j(i) = 1$. Нормируем многочлены H_k , положив

$$\tilde{H}_k = \left(\frac{n-2k+1}{n-k+1} \binom{n}{k} \right)^{-1/2} H_k.$$

Как и ранее, имеем

$$\tilde{H}_i(x)\tilde{H}_j(x) = \sum_{k=0}^w q_{i,j}^k \tilde{H}_k(x) \quad (q_{i,j}^k \geq 0)$$

и

$$\tilde{H}_k(0) = \sqrt{\frac{n-2k+1}{n-k+1} \binom{n}{k}}.$$

Положим

$$P_1(x) = (n-1)^{-1/2} \tilde{H}_1(x) = 1 - \frac{nx}{w(n-w)}.$$

Выпишем матрицу оператора $S_k = E_k \circ P_1$ в ортонормальном базисе: $S_k = A_k(a_{i-1}, b_i, a_i)$, где элементы матрицы вычисляются из соотношения (11). Получаем

$$a_i = \frac{n(w-i)(n-w-i)}{w(n-w)(n-2i)} \sqrt{\frac{(i+1)(n-i+1)}{(n-2i+1)(n-2i-1)}},$$

$$b_i = \frac{(n-2w)^2 i(n-i+1)}{w(n-w)(n-2i)(n-2i+2)}, \quad i \geq 0.$$

Пусть $C \subset J^{n,w}$ – код мощности M с расстоянием $2d$. Применим теорему 2 для оценки M как функции от d . Имеем $\tau_0 = 0$, $\tilde{H}_0 = 1$,

$$\rho_k = a_k \frac{\tilde{H}_{k+1}(0)}{\tilde{H}_k(0)} = \frac{n(w-k)(n-w-k)(n-k+1)}{w(n-w)(n-2k)(n-2k+1)}$$

и $\Delta(C) = \{0, 1, \dots, d\}$. Таким образом, получаем следующую границу.

Теорема 3. *Справедливо неравенство*

$$M \leq \frac{4n(w-k)(n-w-k)}{(1 - \lambda_{\max}(S_k))w(n-w)(n-2k)} \binom{n}{k}$$

для всех k , таких что $\lambda_{\max}(S_{k-1}) \geq 1 - \frac{nd}{w(n-w)}$.

Найдем наименьшее k , удовлетворяющее требуемому условию. Вначале применим лемму 2 для вычисления асимптотики $\lambda_{\max}(S_k)$.

Лемма 3. *Имеет место равенство*

$$\lim_{\substack{n \rightarrow \infty \\ w/n \rightarrow \omega, k/n \rightarrow \tau}} \lambda_{\max}(S_k) = \frac{2\omega(1-\omega) + \sqrt{\tau(1-\tau)}}{\omega(1-\omega)(1 + 2\sqrt{\tau(1-\tau)})} \sqrt{\tau(1-\tau)}.$$

Доказательство. Заметим, что для верхней границы леммы 2 достаточно доказать, что значение $a_i + b_i + a_{i-1}$ возрастает по i . Полагая $\alpha = \frac{i}{n}$, вычисляем

$$a_{i-1} + b_i + a_i = \frac{2(\omega - \alpha)(1 - \omega - \alpha)\sqrt{\alpha(1-\alpha)} + (1 - 2\omega)^2 \alpha(1 - \alpha)}{\omega(1 - \omega)(1 - 2\alpha)^2} (1 + o(1)) =$$

$$= \frac{2\omega(1 - \omega)\sqrt{\alpha(1 - \alpha)} + \alpha(1 - \alpha)}{\omega(1 - \omega)(1 + 2\sqrt{\alpha(1 - \alpha)})} (1 + o(1)).$$

Главный член в правой части последнего выражения является возрастающей функцией от α . Действительно, $\sqrt{\alpha(1-\alpha)}$ возрастает по α при $\alpha < 1/2$, и остается только проверить, что функция $t(2\omega(1-\omega) + t)/(1 + 2t)$ возрастает по t при $0 \leq t \leq 1/2$,

что проверяется непосредственно. Таким образом, полагая $i = k - 1$, получаем для $\lambda_{\max}(S_k)$ верхнюю оценку требуемого вида. Лемма 2 дает и соответствующую нижнюю оценку, а именно, из ее доказательства получаем

$$\lambda_{\max}(S_k) \geq \frac{1}{s} \left(2 \sum_{p=1}^{s-1} a_{k-p} + \sum_{p=0}^{s-1} b_{k-p} \right) \quad (s = 1, \dots, k+1).$$

При больших значениях параметров можно записать

$$\lambda_{\max}(S_k) \geq (a_{k-s} + b_{k-s+1} + a_{k-s+1})(1 + o(1)).$$

Для завершения доказательства остается положить $s \rightarrow \infty$, $s = o(n)$. \blacktriangle

Применим эту лемму в теореме 3. Положим $n \rightarrow \infty$, $d = \delta n$. Условие на k в этой теореме будет выполнено для любого $k = \tau/n$, удовлетворяющего

$$\frac{2\omega(1-\omega) + \sqrt{\tau(1-\tau)}}{\omega(1-\omega)(1 + 2\sqrt{\tau(1-\tau)})} \sqrt{\tau(1-\tau)} > 1 - \frac{\delta}{\omega(1-\omega)},$$

или

$$\delta > \frac{(\omega - \tau)(1 - \omega - \tau)}{1 + 2\sqrt{\tau(1-\tau)}}.$$

Получаем, что из теоремы 3 вытекает следующая граница для $(n, M, 2\delta n)$ -кода $C \subset \mathcal{J}^{n, \omega}$ (асимптотическая "граница четырех" для равновесных кодов [2]):

$$\frac{1}{n} \log M \leq h(\tau)(1 + o(1)),$$

где $\delta = (\omega - \tau)(1 - \omega - \tau)/(1 + 2\sqrt{\tau(1-\tau)})$.

3.3. Сферические коды. Рассмотрим коды на единичной сфере S^{n-1} в \mathbb{R}^n . Многочлены p_i в этом случае относятся к классу многочленов Гегенбауэра $C_k(x)$ [7, с. 80 и далее]. Для них

$$\int_{-1}^1 C_i(x) C_j(x) (1-x^2)^{\frac{n-3}{2}} dx = \frac{\binom{n+i-3}{i}}{n+2i-2} \omega_n \delta_{i,j},$$

где $\omega_n = \frac{\pi \Gamma(n-2)}{2^{n-2} \Gamma^2(\frac{n-2}{2})}$, в частности, при $i = j = 0$ имеем $\int_{-1}^1 (1-x^2)^{\frac{n-3}{2}} dx = \omega_n/(n-2)$. Кроме того, $C_k(1) = \binom{n+k-3}{k}$.

Нормируя меру, получаем $d\mu(x) = \frac{n-2}{\omega_n} (1-x^2)^{(n-3)/2} dx$. Тогда нормированными многочленами Гегенбауэра являются

$$\tilde{C}_k = \sqrt{\frac{n+2k-2}{(n-2) \binom{n+k-3}{k}}} C_k.$$

Многочлены \tilde{C}_k удовлетворяют трехчленному соотношению вида

$$x \tilde{C}_k(x) = a_k \tilde{C}_{k+1}(x) + a_{k-1} \tilde{C}_{k-1}(x),$$

где $a_i = \sqrt{\frac{(n+i-2)(i+1)}{(n+2i)(n+2i-2)}}$, $i = 0, \dots$; здесь $\tilde{C}_{-1} = 0$, $\tilde{C}_0 = 1$. Далее, $\tilde{C}_i \tilde{C}_j = \sum_k q_{i,j}^k \tilde{C}_k$, где $q_{i,j}^k \geq 0$, и

$$\tilde{C}_k(1) = \sqrt{\frac{n+2k-2}{n-2} \binom{n+k-3}{k}}.$$

Пусть $C(n, M, t)$ обозначает код, в котором угол между различными векторами $\mathbf{x}_i, \mathbf{x}_j$ удовлетворяет условию $\cos(\widehat{\mathbf{x}_i, \mathbf{x}_j}) \leq t$. Как указано выше, мы берем $\tau(d) = 1 - d^2/2$. Тогда $D = [0; 2]$, $\tau(D) = [-1; 1]$, $\Delta(C) \subset [-1; t]$, $\tau_0 = 1$. Положим $P_1(x) = n^{-1/2} \tilde{C}_1(x) = x$, тогда матрица S_k имеет вид $A_k(a_{i-1}, 0, a_i)$, и поэтому

$$\rho_k = a_k \frac{\tilde{C}_{k+1}(1)}{\tilde{C}_k(1)} = \frac{n+k-2}{n+2k-2}.$$

Из теоремы 2 вытекает

Теорема 4. *Справедливо неравенство*

$$M \leq \frac{4}{1 - \lambda_{\max}(S_k)} \binom{n+k-2}{k} \quad (12)$$

для всех k , таких что $\lambda_{\max}(S_{k-1}) \geq t$.

Это совпадает с первоначальной границей из [3].

Лемма 4. *Для любого $s = 2, \dots, k$ справедливо*

$$\frac{2(s-1)}{s} \sqrt{\frac{(n+k-s-1)(k-s+2)}{(n+2k-2s+2)(n+2k-2s)}} \leq \lambda_{\max}(S_k) \leq 2 \sqrt{\frac{(n+k-3)k}{(n+2k-2)(n+2k-4)}}.$$

В частности,

$$\lim_{n \rightarrow \infty, \frac{k}{n} \rightarrow \rho} \frac{\lambda_{\max}(S_k)}{n} = 2 \frac{\sqrt{\rho(1+\rho)}}{1+2\rho}.$$

Доказательство. Нужно лишь проверить, что $a_i \geq a_{i+1}$. При $n \geq 5$ имеем

$$a_i^2 - a_{i-1}^2 = \frac{(n-2)(n-4)}{(n+2i)(n+2i-2)(n+2i-4)} > 0,$$

т.е. функция a_i возрастает по i . Теперь требуемые неравенства получаются непосредственно из леммы 2. Полагая $s \rightarrow \infty$, $s = o(n)$, и переходя к пределу, получаем асимптотику для $\lambda_{\max}(S_k)$. \blacktriangle

Теорема 4 и лемма 4 позволяют повторить асимптотическую границу из [3]. А именно, используя формулу Стирлинга, получаем

$$\frac{1}{n} \log M \leq ((1+\rho) \log(1+\rho) - \rho \log \rho)(1+o(1))$$

при условии $t \leq \lambda_{\max}(X_{k-1})$, которое в пределе при $n \rightarrow \infty$, $\frac{k}{n} \rightarrow \rho$ принимает вид

$$\rho \geq \frac{1 - \sqrt{1-t^2}}{2\sqrt{1-t^2}}.$$

3.4. Коды в проективных пространствах. Еще одним классом пространств, связанных с единичной сферой, являются проективные пространства $\mathbb{P}L^{n-1}$, где $L = \mathbb{R}$, \mathbb{C} или \mathbb{H} . Зональные сферические функции в этих пространствах задаются многочленами Якоби $P_k^{\alpha,\beta}(x)$ (см. [7]), где $\alpha = \sigma(n-1) - 1$, $\beta = \sigma - 1$, а $\sigma = 1/2, 1, 2$ соответственно.

Многочлены $P_k^{\alpha,\beta}(x)$ удовлетворяют соотношениям

$$\int_{-1}^1 P_i^{\alpha,\beta}(x) P_j^{\alpha,\beta}(x) (1-x)^\alpha (1+x)^\beta dx = \frac{2^{\alpha+\beta+1} (k+\alpha)! (k+\beta)!}{(2k+\alpha+\beta+1) k! (k+\alpha+\beta)!} \delta_{i,j},$$

$$P_k(1) = \binom{k+\alpha}{\alpha},$$

где по определению полагается $x! = \Gamma(x+1)$. Коэффициенты трехчленного соотношения (3) имеют вид

$$\alpha_k = \frac{2(k+1)(k+\alpha+\beta+1)}{(2k+\alpha+\beta+1)(2k+\alpha+\beta+2)}, \quad \beta_k = \frac{\beta^2 - \alpha^2}{(2k+\alpha+\beta)(2k+\alpha+\beta+2)},$$

$$\gamma_k = \frac{2(k+\alpha)(k+\beta)}{(2k+\alpha+\beta)(2k+\alpha+\beta+1)}.$$

Зададим билинейную форму на V как $\langle f, g \rangle = \int_{-1}^1 fg d\mu$, где

$$d\mu(x) = \frac{(\alpha+\beta+1) \binom{\alpha+\beta}{\alpha}}{2^{\alpha+\beta+1}} (1-x)^\alpha (1+x)^\beta dx.$$

Тогда квадрат нормы многочлена P_k равен

$$\|P_k^{\alpha,\beta}\|^2 = \frac{(\alpha+\beta+1)(\alpha+\beta)! (k+\alpha)! (k+\beta)!}{(2k+\alpha+\beta+1)\alpha! \beta! k! (k+\alpha+\beta)!}.$$

Обозначим через $\tilde{P}_k = P_k^{\alpha,\beta} / \|P_k^{\alpha,\beta}\|$ нормированные многочлены Якоби.

В соотношении (4) положим

$$P_1(x) = P_1^{\alpha,\beta}(x) = \frac{1}{2}((\alpha+\beta+2)x + \alpha - \beta),$$

тогда коэффициентами этого соотношения будут

$$a_k = \frac{\alpha+\beta+2}{2k+\alpha+\beta+2} \sqrt{\frac{(k+\alpha+1)(k+\beta+1)(k+1)(k+\alpha+\beta+1)}{(2k+\alpha+\beta+3)(2k+\alpha+\beta+1)}},$$

$$b_k = \frac{2(\alpha-\beta)k(k+\alpha+\beta+1)}{(2k+\alpha+\beta)(2k+\alpha+\beta+2)}$$

и $c_k = a_{k-1}$.

Пусть $C \subset X$ – код мощности M , в котором $|(x_i, x_j)| \leq t$ для любых двух различных векторов x_i, x_j . Тогда $D = [0; \sqrt{2}]$, и поэтому, выбирая $\tau(d) = 2(1 - d^2/2)^2 - 1$,

получаем $\tau(D) = [-1; 1]$, $\Delta(C) \subset [-1; 2t^2 - 1]$. Вычисления дают

$$\tilde{P}_k^2(1) = \frac{(2k + \alpha + \beta + 1)}{\alpha + \beta + 1} \frac{\binom{k + \alpha}{\alpha} \binom{k + \alpha + \beta}{k}}{\binom{k + \beta}{\beta}},$$

$$\rho_k = a_k \frac{\tilde{P}_{k+1}(1)}{\tilde{P}_k(1)} = \frac{(\alpha + \beta + 2)(k + \alpha + 1)(k + \alpha + \beta + 1)}{(2k + \alpha + \beta + 1)(2k + \alpha + \beta + 2)}.$$

Используя эти вычисления в теореме 2, получаем следующий результат.

Теорема 5. *Справедливо неравенство*

$$M \leq \frac{4(\alpha + \beta + 2)(k + \alpha + 1)}{(2k + \alpha + \beta + 2)(1 - \lambda_{\max}(S_k))} \frac{\binom{k + \alpha}{\alpha} \binom{k + \alpha + \beta + 1}{k}}{\binom{k + \beta}{\beta}}.$$

Применяя лемму 2 для вывода асимптотики $\lambda_{\max}(S_k)$ при $k \rightarrow \infty$, $\alpha = ak$, $\beta = bk$, $a > 0$, $b \geq 0$, получаем

$$\frac{\lambda_{\max}(S_k)}{k} \rightarrow \frac{2((a + b)\sqrt{(a + 1)(b + 1)(a + b + 1)} + (a - b)(a + b + 1))}{(a + b + 2)^2}.$$

Условием, при котором применима теорема 2, является

$$\lambda_{\max}(S_k) > P_1(2t^2 - 1) = (\alpha + \beta + 2)t^2 - \beta - 1. \quad (13)$$

В качестве примера выведем границу для случая $X = \mathbb{P}R^{n-1}$. Полагая $k = sn/2$, $\alpha = (n - 3)/2$, $\beta = -1/2$, получаем $a = 1/s$, $b = 0$,

$$\frac{\lambda_{\max}(S_k)}{k} \rightarrow \frac{4(1 + s)}{(1 + 2s)^2}.$$

Таким образом, при больших значениях параметров условие (13) принимает вид

$$\frac{4(1 + s)}{(1 + 2s)^2} = \frac{t^2}{s},$$

или $s = 1/2((1/\sqrt{1 - t^2}) - 1)$. Из теоремы 2 получаем асимптотическую границу из [3] на мощность кода:

$$\frac{1}{n} \log M \leq (1 + s) \log(1 + s) - s \log s.$$

Аналогичным образом можно повторить вывод асимптотических границ из [3] и в остальных вышеупомянутых случаях.

Представленный метод является линейно-алгебраической альтернативой аналитическому методу работ [2, 3, 5]. Он эквивалентен им в том смысле, что дает те же самые асимптотические результаты, хотя для конечных значений параметров границы, получаемые этими методами, как правило, не совпадают.

СПИСОК ЛИТЕРАТУРЫ

1. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory. Philips Res. Repts. Suppl. № 10, 1973.

2. *McEliece R.J., Rodemich E.R., Rumsey H., Welch L.R.* New Upper Bound on the Rate of a Code via the Delsarte–MacWilliams Inequalities // IEEE Trans. Inform. Theory. 1977. V. 23. № 2. P. 157–166.
3. *Кабатянский Г.А., Левенштейн В.И.* О границах для упаковок на сфере и в пространстве // Пробл. передачи информ. 1978. Т. 14. № 1. С. 3–25.
4. *Левенштейн В.И.* Границы для упаковок метрических пространств и некоторые их приложения // Проблемы кибернетики. М.: Наука, 1983. Вып. 40. С. 43–110.
5. *Levenshtein V.I.* Universal Bounds for Codes and Designs // Handbook of Coding Theory. Part 1. Amsterdam: Elsevier, 1998. P. 499–648.
6. *Vachoc C.* Linear Programming Bounds for Codes in Grassmannian Spaces: Preprint. Bordeaux: Université Bordeaux 1, 2005.
7. *Сега Г.* Ортогональные многочлены. М.: Физматлит, 1962.
8. *Гантмахер Ф.Р.* Теория матриц. М.: Наука, 1988.
9. *Ismail M.E., Li X.* Bound on the Extremal Zeros of Orthogonal Polynomials // Proc. AMS. 1992. V. 113. № 1. P. 131–140.
10. *Levenshtein V.I.* Krawtchouk Polynomials and Universal Bounds for Codes and Designs in Hamming Spaces // IEEE Trans. Inform. Theory. 1995. V. 41. № 5. P. 1303–1321.
11. *Foster W.H., Krasikov I.* Bounds for the Extreme Roots of Orthogonal Polynomials // Int. J. Math. Algorithms. 2000. V. 2. P. 121–132.

Барг Александр Михайлович
 Институт проблем передачи информации РАН
 Университет Мэриленда, Колледж Парк, США
 abarg@umd.edu
Ногин Дмитрий Юрьевич
 Институт проблем передачи информации РАН
 nogin@iitp.ru

Поступила в редакцию
 09.12.2005
 После переработки
 01.03.2006