ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Ноябрь—декабрь 2014. Том 21, № 6. С. 3–10

УДК 519.1

ОЦЕНКИ МОЩНОСТИ МИНИМАЛЬНОГО 1-СОВЕРШЕННОГО БИТРЕЙДА В ГРАФЕ ХЭММИНГА *)

К. В. Воробьёв, Д. С. Кротов

Аннотация. Улучшены известные нижняя и верхняя оценки на минимальную мощность носителя собственной функции графа Хэмминга $H(n,q)$, где $q > 2$. В частности, оценена мощность минимального 1-совершенного битрейда в $H(n,q)$. Показано, что мощность такого битрейда ограничена снизу величиной $2^{n-\frac{n-1}{q}}(q-2)^{\frac{n-1}{q}}$ в случае $q \geqslant 4$ и $3^{\frac{n}{2}}(1-O(1/n))$ в случае $q = 3$. Кроме того, предложена конструкция, позволяющая строить битрейды мощности $q^{\frac{(q-2)(n-1)}{q}} 2^{\frac{n-1}{q}+1}$ при $n \equiv 1 \bmod q$, где q — степень простого числа.

Ключевые слова: граф Хэмминга, полином Кравчука, 1-совершенный битрейд.

1. Предварительные сведения

Обозначим через $H(n,q)$ граф, вершинами которого являются все слова длины n над алфавитом $\{0,1,\ldots,q-1\}$. *Расстоянием Хэмминга* $d(x,y)$ между вершинами $x,y \in H(n,q)$ называется число позиций, в которых x и y различны, рёбрам графа соответствуют пары вершин на расстоянии 1. Известно [1], что множество собственных чисел матрицы смежности такого графа есть $\{\lambda_m = n(q-1)-qm \mid m = 0,1,\ldots,n\}$. Соответствующие собственные подпространства будем обозначать через V_m, т. е.

$$V_m = \Big\{ f : H(n,q) \to \mathbb{C} \mid \sum_{\substack{y \in H(n,q),\\ d(x,y)=1}} f(y) = \lambda_m f(x),\ x \in H(n,q) \Big\}.$$

Известно также [1], что для произвольных $f \in V_m$ и $x \in H(n,q)$ имеет место следующее соотношение, задающее распределение значений соб-

*) Исследование выполнено при финансовой поддержке Российского научного фонда (проект № 14–11–00555).

ственной функции f относительно x:

$$\sum_{\substack{y \in H(n,q),\\ d(x,y)=r}} f(y) = K_r(m,q,n) f(x), \tag{1}$$

где $K_r(t,q,n) = \sum\limits_{j=0}^{r} (-1)^j (q-1)^{r-j} \binom{t}{j} \binom{n-t}{r-j}$ — полиномы Кравчука, производящая функция которых имеет вид

$$\sum_{k=0}^{n} K_k(t,q,n) z^k = (1+(q-1)z)^{n-t}(1-z)^t. \tag{2}$$

Множество $S(f) = \{x \in H(n,q) \mid f(x) \neq 0\}$ называется *носителем функции* f.

Окрестностью $\Omega(T)$ *множества вершин* T назовём множество вершин на расстоянии не более 1 от T. 1-*Совершенным битрейдом* называется пара (T_0, T_1) непересекающихся множеств вершин таких, что $\Omega(T_0) = \Omega(T_1)$, причём в каждом шаре радиуса 1 содержится не более одного элемента из каждого T_0 и T_1. Составляющие T_0 и T_1 1-совершенного битрейда (T_0, T_1) называются 1-*совершенными трейдами*, при этом отметим, что разность характеристических функций T_0 и T_1 является собственной функцией графа с собственным числом -1.

Примером 1-совершенного битрейда в $H(n,q)$ является пара разностей $(C_0 \backslash C_1, C_1 \backslash C_0)$ двух совершенных кодов C_0 и C_1 (1-совершенный код — множество C вершин графа такое, что любой шар радиуса 1 в этом графе содержит ровно одну вершину из C). Трейды такого вида, т. е. вложимые в 1-совершенный код, известны как «свитчинговые компоненты» 1-совершенных кодов [10]. Кроме того, широко изучаются латинские трейды в графах Хэмминга [2, 3] и трейды Штейнера в графах Джонсона [5], которые определяются аналогично 1-совершенным трейдам, если заменить шары радиуса 1 максимальными кликами соответствующего графа. Латинские битрейды и битрейды Штейнера также соответствуют собственным функциям графа.

Из результатов работы [9] следует, что мощность носителя собственной функции $f : H(n,q) \to \{-1, 0, 1\}$ с собственным значением $\lambda = q(n-m) - n$ можно оценить следующим образом:

$$|S(f)| \geqslant 2^m$$

(неравенство легко доказывается индукцией по n при фиксированном m). Если $\lambda = -1$, то оценка принимает вид

$$|S(f)| \geqslant 2^{\frac{n(q-1)+1}{q}},$$

при этом она достижима при $q = 2$ [4].

В [8] показано существование вложимых в 1-совершенный код трейдов мощности $q^{\frac{(q-2)(n-1)}{q}} p^{\frac{n-1}{q}}$ для $n = (q^k - 1)/(q-1)$, $k = 2, 3, \ldots$, где q — степень простого числа p. Нетрудно построить аналогичный трейд такой мощности для любого $n \equiv 1 \bmod q$ без условия вложимости.

Цель данной работы — улучшить указанные выше оценки мощности носителя собственных функций и мощности 1-совершенного трейда. Докажем нижнюю оценку $2^m(q-2)^{n-m}$ в случае, когда $\frac{mq^2}{2n(q-1)} > 2$, и $q^n\left(\frac{1}{q-1}\right)^{\frac{m}{2}}\left(\frac{m}{n-m}\right)^{\frac{m}{2}}\left(1-\frac{m}{n}\right)^{\frac{n}{2}}$ в случае, когда $\frac{mq^2}{2n(q-1)} \leqslant 2$, на мощность носителя собственной функции с собственным значением $\lambda_m = n(q-1) - qm$. Половина этой величины для собственного значения -1 ограничивает снизу мощность 1-совершенного трейда. Покажем существование 1-совершенного трейда мощности $q^{\frac{(q-2)(n-1)}{q}} 2^{\frac{n-1}{q}}$, где q — степень простого числа p (при $p > 2$ это меньше мощности трейда, рассмотренного в [8]), что даёт оценку вдвое больше на мощность минимального носителя собственной функции.

2. Нижняя оценка мощности минимального битрейда

В данном разделе будем рассматривать функции, заданные на вершинах $H(n,q)$ и принимающие значения из $\mathbb{R}$. Для таких функций всегда имеет место следующая оценка мощности их носителя.

Предложение 1. *Пусть $f : H(n,q) \to \mathbb{R}$, $f \in V_m$ и $f \not\equiv 0$. Тогда*

$$|S(f)| \geqslant \sum_{k=0}^{n} |K_k(m,q,n)|. \tag{3}$$

Доказательство. Рассмотрим $x \in H(n,q)$ такой, что

$$|f(x)| = \max_{y \in H(n,q)} |f(y)|.$$

Тогда $|S(f) \cap \{z \in H(n,q) \mid d(x,z) = k\}| \geqslant |K_k(m,q,n)|$, так как f принимает лишь значения, не превышающие $|f(x)|$ по модулю, и справедливо (1). Суммированием по всем целым k, $0 \leqslant k \leqslant n$, получаем требуемое. Предложение 1 доказано.

Заметим, что вопрос об асимптотическом поведении полиномов Кравчука до конца не решён, поэтому найти асимптотику суммы из (3) не представляется возможным. Далее эта сумма будет оценена снизу, и для этого понадобится следующее соотношение, которое является частным случаем неравенства Коши — Буняковского,

$$\sum_{k=0}^{n} |\alpha_k| \geqslant \sqrt{\left(\sum_{k=0}^{n} \alpha_k \cos\varphi_k\right)^2 + \left(\sum_{k=0}^{n} \alpha_k \sin\varphi_k\right)^2}, \tag{4}$$

где $\alpha_k,\ \varphi_k \in \mathbb{R},\ 0 \leqslant k \leqslant n,\ k, n \in \mathbb{N}$.

Основываясь на этом несложном наблюдении и соотношении (2), следующая теорема позволяет оценить снизу сумму из неравенства (3).

Теорема 1. *Пусть $f : H(n,q) \to \mathbb{R}$, $f \in V_m$ и $f \not\equiv 0$. Тогда*

$$|S(f)| \geqslant \begin{cases} 2^m (q-2)^{n-m}, & \text{если } \frac{mq^2}{2n(q-1)} > 2, \\ q^n \left(\frac{1}{q-1}\right)^{\frac{m}{2}} \left(\frac{m}{n-m}\right)^{\frac{m}{2}} \left(1-\frac{m}{n}\right)^{\frac{n}{2}}, & \text{если } \frac{mq^2}{2n(q-1)} \leqslant 2. \end{cases} \tag{5}$$

Доказательство. По предложению 1

$$|S(f)| \geqslant \sum_{k=0}^{n} |K_k(m,q,n)|.$$

Воспользуемся неравенством (4) при $\varphi_k = k\varphi$ и $\alpha_k = K_k(m,q,n)$:

$$|S(f)| \geqslant \sqrt{\left(\sum_{k=0}^{n} K_k(m,q,n)\cos k\varphi\right)^2 + \left(\sum_{k=0}^{n} K_k(m,q,n)\sin k\varphi\right)^2}.$$

Благодаря соотношению (2) получаем

$$\sqrt{\left(\sum_{k=0}^{n} K_k(m,q,n)\cos k\varphi\right)^2 + \left(\sum_{k=0}^{n} K_k(m,q,n)\sin k\varphi\right)^2} = \left|\big(1+(q-1)z\big)^{n-m}(1-z)^m\right|,$$

где $z = \cos\varphi + i\sin\varphi$. Таким образом, имеем

$$|S(f)| \geqslant \max_{\varphi\in\mathbb{R}} F(\varphi), \tag{6}$$

где $F(\varphi) = \left|(1+(q-1)(\cos\varphi + i\sin\varphi))^{n-m}(1-(\cos\varphi+i\sin\varphi))^m\right|$. Непосредственное вычисление функций F, F' даёт

$$F(\varphi) = (2-2\cos\varphi)^{\frac{m}{2}} \left(q^2 - 2q + 2 + 2(q-1)\cos\varphi\right)^{\frac{n-m}{2}},$$

$$F'(\varphi) = 2n(q-1)(2-2\cos\varphi)^{\frac{m}{2}-1}(q^2-2q+2+2(q-1)\cos\varphi)^{\frac{n-m}{2}-1} \times \sin\varphi\left(\cos\varphi - 1 + \frac{mq^2}{2n(q-1)}\right).$$

В результате анализа функции F' несложно определить максимум функции $F(\varphi)$ и получить следующее соотношение:

$$\max_{\varphi\in\mathbb{R}} F(\varphi) = \begin{cases} 2^m(q-2)^{n-m}, & \text{если } \frac{mq^2}{2n(q-1)} > 2, \\ q^n\left(\frac{1}{q-1}\right)^{\frac{m}{2}}\left(\frac{m}{n-m}\right)^{\frac{m}{2}}\left(1-\frac{m}{n}\right)^{\frac{n}{2}}, & \text{если } \frac{mq^2}{2n(q-1)} \leqslant 2, \end{cases}$$

при этом в первом случае максимум $F(\varphi)$ достигается при $\cos\varphi = -1$, а во втором — при $\cos\varphi = 1 - \frac{mq^2}{2n(q-1)}$. Последнее соотношение вместе с (6) даёт требуемое. Теорема 1 доказана.

Любому 1-совершенному битрейду (T_0, T_1) в $H(n,q)$ можно сопоставить функцию $f : H(n,q) \to \{-1,0,1\}$, равную разности характеристических функций множеств T_0 и T_1. Из определения битрейда видно, что для f выполняется $f \in V_{n-\frac{n-1}{q}}$. Далее, говоря об 1-совершенном битрейде, будем подразумевать соответствующую ему функцию f.

Особый интерес представляет случай $m = n - \frac{n-1}{q}$, так как тогда неравенство (5) даёт нижнюю оценку на мощность носителя 1-совершенного битрейда в $H(n,q)$.

Следствие 1. *Пусть f есть 1-совершенный битрейд в $H(n,q)$, $q \geqslant 3$, и $f \not\equiv 0$. Тогда*

$$|S(f)| \geqslant \begin{cases} 2^{n-\frac{n-1}{q}}(q-2)^{\frac{n-1}{q}}, & \text{если } q \geqslant 4, \\ 3^{\frac{n}{2}}(1-\frac{1}{n})^{\frac{n}{2}}\left(1+\frac{3}{2(n-1)}\right)^{\frac{2n+1}{6}} = 3^{\frac{n}{2}}\big(1-O(1/n)\big), & \text{если } q = 3. \end{cases}$$

Доказательство. Как замечено выше, соответствующая 1-совершенному битрейду в $H(n,q)$ функция f принадлежит $V_{n-\frac{n-1}{q}}$. Применение теоремы 1 при $m = n - \frac{n-1}{q}$ даёт

$$|S(f)| \geqslant \begin{cases} 2^{n-\frac{n-1}{q}}(q-2)^{\frac{n-1}{q}}, & \text{если } \frac{(n-\frac{n-1}{q})q^2}{2n(q-1)} > 2, \\ q^{\frac{n}{2}}\big(1-\frac{1}{n}\big)^{\frac{n}{2}}\Big(\big(1+\frac{q}{(n-1)(q-1)}\big)^{\frac{(n-1)(q-1)}{q}}\Big)^{\frac{n(q-1)+1}{2(n-1)(q-1)}} & \text{иначе.} \end{cases}$$

Упрощая соотношение $\frac{\left(n-\frac{n-1}{q}\right)q^2}{2n(q-1)} \leqslant 2$, получаем неравенство

$$n\left(5-q-\frac{4}{q}\right) \geqslant 1,$$

которое имеет место тогда и только тогда, когда $q \in \{2, 3\}$, $n \in \mathbb{N}$. Таким образом, оценка при $q = 3$ принимает вид

$$3^{\frac{n}{2}} \left(1 - \frac{1}{n}\right)^{\frac{n}{2}} \left(1 + \frac{3}{2(n-1)}\right)^{\frac{2n+1}{6}}.$$

В результате несложных вычислений видим, что последнее выражение при больших n ведёт себя как $3^{\frac{n}{2}}(1 - O(1/n))$. Следствие 1 доказано.

В следствии мы исключили случай $q = 2$, так как выше упоминалась достижимая нижняя оценка для этого случая.

3. Верхняя оценка мощности минимального битрейда

Построим 1-совершенный трейд, имеющий на сегодняшний день рекордно минимальную мощность. Идея построения исходит из конструкций 1-совершенных кодов на основе латинских гиперкубов (эквивалентно, мультиарных квазигрупп) [6, 7]. Аналогично построению 1-совершенных кодов из латинских гиперкубов можно строить 1-совершенные трейды из латинских трейдов. Не вдаваясь в подробности общих конструкций, приведём явную конструкцию полученного трейда.

Пусть $n = qm+1$, где q — степень простого числа, а $f(x_1, \ldots, x_{q-1}) = x_1 + \ldots + x_{q-1}$ и $g(x_1, \ldots, x_{q-1}) = \gamma_1 x_1 + \ldots + \gamma_{q-1} x_{q-1}$, где $\gamma_1, \ldots, \gamma_{q-1}$ — все ненулевые элементы поля $\mathrm{GF}(q)$. Определим два множества T_0 и T_1 слов длины $n = qm + 1$:

$$T_\sigma = \big\{ \big(x_1^1, \ldots, x_{q-1}^1, g\big(x_1^1, \ldots, x_{q-1}^1\big), x_1^2, \ldots, x_{q-1}^2, g\big(x_1^2, \ldots, x_{q-1}^2\big), \ldots, x_1^m, \ldots, x_{q-1}^m, g\big(x_1^m, \ldots, x_{q-1}^m\big), \bigoplus_{i=1}^{m} f\big(x_1^i, \ldots, x_{q-1}^i\big) \oplus \sigma\big) \mid f\big(x_1^i, \ldots, x_{q-1}^i\big) \in \{0,1\},\ i \in \{1, \ldots, m\} \big\}.$$

Предложение 2. *Пара (T_0, T_1) является 1-совершенным битрейдом с мощностью $q^{\frac{(q-2)(n-1)}{q}} 2^{\frac{(n-1)}{q}}$ каждого из составляющих.*

Доказательство. Сначала удостоверимся, что мощность множества T_σ равна $q^{n-2m-1}2^m$. Действительно, для любого i от 1 до m значения $x_1^i, \ldots, x_{q-2}^i$ могут быть выбраны произвольно, после чего существует два значения для x_{q-1}^i, удовлетворяющих условию $f\big(x_1^i, \ldots, x_{q-1}^i\big) \in \{0, 1\}$. Значения остальных $m + 1$ координат слова T_σ вычисляются однозначно.

В силу выбора функций f и g любые два различных набора вида $(x_1, \ldots, x_{q-1}, g(x_1, \ldots, x_{q-1}), f(x_1, \ldots, x_{q-1}))$ отличаются не менее чем

в трёх элементах. Отсюда следует, что два слова из T_σ не могут различаться только в одной или только в двух позициях, т. е. каждый шар радиуса 1 содержит не более одного слова из T_σ.

Остаётся показать, что $\Omega(T_0) = \Omega(T_1)$, где $\Omega(T_\sigma)$ — множество слов на расстоянии не больше 1 от T_σ. Это нетрудно проверить и непосредственно перебором вариантов, но поступим иначе. Опишем множество таких слов.

Набор $(x_1, \ldots, x_{q-1}, x_0)$ назовём *хорошим*, если $f(x_1, \ldots, x_{q-1}) \in \{0, 1\}$ и $x_0 = g(x_1, \ldots, x_{q-1})$, и *плохим*, если $x_0 \neq g(x_1, \ldots, x_{q-1})$. Число хороших наборов равно $G = 2q^{q-2}$, а число плохих — $B = q^{q-1}(q-1)$. Слово $\left(x_1^1, \ldots, x_{q-1}^1, x_0^1, \ldots, x_1^m, \ldots, x_{q-1}^m, x_0^m, x_0^0\right)$ назовём *правильным*, если все наборы $\left(x_1^i, \ldots, x_{q-1}^i, x_0^i\right)$, $i = 1, \ldots, m$, хорошие, либо один из них плохой, а остальные хорошие, и при этом $x_0^0 \in \{0, 1\}$.

Легко видеть, что $\Omega(T_\sigma)$ состоит только из правильных слов. Действительно, любое слово из T_σ содержит m хороших наборов, а отступая от него на расстояние 1, либо меняем последнюю координату, либо делаем один из хороших блоков плохим. С другой стороны, число правильных слов равно

$$G^m \cdot q + m \cdot G^{m-1} \cdot B \cdot 2 = (2q^{q-2})^m \cdot (mq^2 - mq + q) \\ = |T_\sigma| \cdot (n(q-1) + 1) = |\Omega(T_\sigma)|.$$

Таким образом, как $\Omega(T_\sigma)$, так и $\Omega(T_\sigma)$ совпадают с множеством правильных слов, откуда $\Omega(T_0) = \Omega(T_1)$. Предложение 2 доказано.

Следствие 2. *Пусть $q, n \in \mathbb{N}$, $n \equiv 1 \bmod q$ и q — степень простого числа. Тогда существует функция $f : H(n, q) \to \{-1, 0, 1\}$, $f \in V_{n-\frac{n-1}{q}}$, такая, что $|S(f)| = q^{\frac{(q-2)(n-1)}{q}} 2^{\frac{n-1}{q}+1}$.*

Следствие 1 даёт нижнюю оценку мощности 1-совершенного битрейда в $H(n, q)$, $q \geqslant 3$, которая значительно лучше полученной ранее в [9]. Однако зазор между новой нижней оценкой и верхней оценкой, полученной в следствии 2, всё ещё остаётся существенным.

В заключение стоит обратить внимание на то, что техника, используемая в доказательстве теоремы 1, может оказаться полезной для оценки мощности носителей собственных функций и 1-совершенных битрейдов и в других дистанционно-регулярных графах.

ЛИТЕРАТУРА

1. **Дельсарт Ф.** Алгебраический подход к схемам отношений теории кодирования. — М.: Мир, 1976. — 136 с.
2. **Потапов В. Н.** Многомерные латинские битрейды // Сиб. мат. журн. — 2013. — Т. 52, № 2. — С. 317–324.
3. **Cavenagh N. J.** The theory and application of latin bitrades: a survey // Math. Slovaca. — 2008. — Vol. 58, N 6. — P. 691–718.
4. **Etzion T., Vardy A.** Perfect binary codes: constructions, properties, and enumeration // IEEE Trans. Inform. Theory. — 1994. — Vol. 40, N 3. — P. 754–763.
5. **Hedayat A. S., Khosrovshahi G. B.** Trades // CRC Handbook of Combinatorial Designs. — Boca Raton; London; New York: Chapman and Hall/CRC, 2006. — P. 644–648.
6. **Heden O., Krotov D. S.** On the structure of non-full-rank perfect q-ary codes // Adv. Math. Comm. — 2011. — Vol. 5, N 2. — P. 149–156.
7. **Phelps K. T.** A product construction for perfect codes over arbitrary alphabets // IEEE Trans. Inf. Theory. — 1984. — Vol. 30, N 5. — P. 769–771.
8. **Phelps K. T., Rifà J., Villanueva M.** Kernels and p-kernels of p^r-ary 1-perfect codes // Des. Codes Cryptogr. — 2005. — Vol. 37, N 2. — P. 243–261.
9. **Potapov V. N.** On perfect 2-colorings of the q-ary n-cube // Discrete Math. — 2012. — Vol. 312, N 8. — P. 1269–1272.
10. **Solov'eva F. I.** Structure of i-components of perfect binary codes // Discrete Appl. Math. — 2001. — Vol. 111, N 1–2. — P. 189–197.

Воробьёв Константин Васильевич,
e-mail: vorobev@math.nsc.ru
Кротов Денис Станиславович,
e-mail: krotov@math.nsc.ru

Статья поступила
23 октября 2014 г.

Переработанный вариант —
10 ноября 2014 г.