

Оценки характеристик кодов Таннера на графе проективного пространства

А. А. Юсуфова*, Г. В. Калачев†

В работе рассматриваются коды Таннера, построенные на графе инцидентности точек и гиперплоскостей проективного пространства, с проективными кодами Рида-Маллера в качестве компонентных кодов. Сопоставление символов локальных кодов рёбрам производится таким образом, чтобы получаемый код Таннера обладал симметрией проективного пространства. В работе получены нижние оценки минимального расстояния и размерности таких кодов. В частности, показано, что при определённых значениях параметров эти коды являются асимптотически хорошими.

Ключевые слова: коды Таннера, граф инцидентности, проективное пространство, минимальное расстояние, размерность кода.

1. Введение

В данной работе изучаются коды Таннера, построенные на графе инцидентности точек и гиперплоскостей проективного пространства $\mathbb{P}_q^D$ над конечным полем $\mathbb{F}_q$. В качестве локальных кодов используются проективные коды Рида-Маллера, а сопоставление символов локальных кодов рёбрам графа производится таким образом, чтобы получаемый код обладал симметрией проективного пространства: группа изометрий кода включает в себя группу проективных преобразований $\text{PGL}(D+1, q)$. Такая симметрия важна для потенциальных применений этих кодов в качестве локальных кодов в симплицальных комплексах с соответствующими локальными симметриями.

Одна из основных мотиваций для изучения таких кодов связана с задачей построения локально тестируемых и квантовых LDPC кодов

* Юсуфова Алина Алмасовна — студент магистратуры, филиал МГУ в г. Ташкенте, e-mail: yusufova.alinochka@mail.ru, ORCID: 0009-0007-4090-8215.

Yusufova Alina Almasovna — Master's student, Lomonosov Moscow State University branch in Tashkent.

† Калачев Глеб Вячеславович — канд. физ.-мат. наук, науч. сотр. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: gleb.kalachev@yandex.ru, ORCID: 0000-0003-2695-3179.

Kalachev Gleb Vyacheslavovich — Candidate of Physical and Mathematical Sciences, Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

на основе симплициальных комплексов Рамануджана типа $\tilde{A}_d$ [1]. Графы инцидентности проективных пространств возникают как локальные структуры (линки) в таких комплексах, а коды Таннера, определённые на линках, играют ключевую роль при определении глобального кода на комплексе. Для построения хорошего глобального кода необходимо, чтобы локальные коды Таннера обладали необходимой симметрией, достаточной размерностью, минимальным расстоянием, а также свойством тестируемости на согласованность (agreement testability). Симплициальные комплексы Рамануджана потенциально могли бы дать семейства хороших локально тестируемых или квантовых LDPC кодов с высокой симметрией, чего пока не удаётся достичь с использованием конструкций, основанных на произведениях кодов (например, [2]). В данной работе мы фокусируемся на исследовании размерности и минимального расстояния.

Двумерный случай ($D = 2$), то есть конструкции на графах инцидентности аффинных и проективных плоскостей, изучен достаточно подробно. Оценки размерности кодов Таннера на таких графах получены в [3–5], а оценки минимального расстояния — в [3, 6, 7]. В [8] для кодов на аффинной плоскости, помимо расстояния и размерности, исследуется также свойство тестируемости на согласованность, важное для построения локально тестируемых кодов. Многомерный случай изучался только для локальных кодов степени один [9]. Настоящая работа рассматривает одно из естественных обобщений: проективные пространства произвольной размерности с локальными кодами более высокой степени.

Основные результаты работы состоят в следующем. Для кода Таннера на графе инцидентности проективного пространства с произвольными локальными кодами с достаточно большим минимальным расстоянием получена нижняя оценка минимального расстояния глобального кода, основанная на спектральном расширении графа и оценке Сипсера–Спилмана. Для кодов с проективными кодами Рида–Маллера в качестве локальных кодов получена нижняя оценка размерности, а также нижние оценки минимального расстояния как в случае проективной плоскости, так и в больших размерностях. Из полученных оценок следует, что при определённых соотношениях между параметрами эти коды являются асимптотически хорошими. Также проверено, что предложенная конструкция действительно наследует симметрию проективного пространства.

Статья организована следующим образом. В разделе 2 приведены основные определения и обозначения, относящиеся к кодам Таннера, построенным на графе инцидентности проективного пространства, и формулируются основные результаты работы. Раздел 3 содержит вспомогательные сведения о кодах Рида–Маллера, графах-расширителях и спектре графа инцидентности, необходимые для дальнейших доказа-

тельств. В разделе 4 приведены доказательства оценок минимального расстояния и размерности рассматриваемых кодов, а также исследуется их инвариантность относительно действия групп симметрий. В разделе 5 сформулированы основные выводы. В приложении А приведены результаты численного эксперимента, посвящённого вычислению размерности кода в двумерном случае.

2. Основные определения и результаты

2.1. Линейные коды

Обозначим через $\mathbb{F}_q^n$ — n -мерное векторное пространство над $\mathbb{F}_q$. Ниже приведём основные определения (см., например, [10, стр. 198]).

Линейным кодом длины n и размерности k (сокращённо $[n, k]$ -кодом) называется произвольное линейное k -мерное подпространство n -мерного векторного пространства $\mathbb{F}_q^n$. Элементы линейного кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ называются *кодowymi словами*. Отношение $R = k/n$ линейного кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется *скоростью кода* (*code rate*). *Вес вектора* $v \in \mathbb{F}_q^n$ — количество ненулевых элементов вектора. Вес будем обозначать через $|v|$. *Расстояние Хэмминга* между векторами $x, y \in \mathbb{F}_q^n$ определим как

$$d(x, y) = |x - y|,$$

то есть как число позиций, в которых x и y не совпадают. Минимальное расстояние между различными кодowymi словами кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется *расстоянием кода*. Обозначим его через $d_{\min}(\mathcal{C})$. Иногда удобнее использовать *относительное минимальное расстояние* $\delta_{\min}(\mathcal{C}) := d_{\min}(\mathcal{C})/n$. Легко показать, что в линейном коде $\mathcal{C}$ кодовое расстояние равно весу его минимального ненулевого элемента:

$$d_{\min}(\mathcal{C}) = \min_{c \in \mathcal{C} \setminus \{0\}} |c|.$$

2.2. Коды Таннера

Нас будет интересовать класс линейных кодов, которые определяются на графах через набор локальных проверок. В дальнейшем будем следовать изложению определения таких кодов из работы [11].

Пусть A и B — произвольные множества. Через A^B понимаются множества всех функций (отображений), определённых на B и принимающих значения в A .

Определение 1 (Код Таннера). Пусть $G = (V, E)$ — w -регулярный граф, в котором все рёбра, выходящие из вершины v , занумерованы от 1 до w , обозначим их $e_{v,1}, \dots, e_{v,w}$. Пусть также есть набор линейных кодов $\mathcal{C} = (\mathcal{C}_v)_{v \in V}$, $\mathcal{C}_v \subseteq \mathbb{F}_q^w$. Код Таннера $\mathcal{T}(G, \mathcal{C})$ — это линейный код, состоящий из всех кодовых слов $c \in \mathbb{F}_q^E$, таких что $c_v \in \mathcal{C}_v$ для всех вершин $v \in V$, где $c_v = (c(e_{v,1}), \dots, c(e_{v,w}))$.

2.2.1. Граф инцидентности проективного пространства

Мы будем исследовать коды Таннера на двудольном графе $\Gamma_{D,q}$ инцидентности прямых и гиперплоскостей $(D+1)$ -мерного пространства $\mathbb{F}_q^{D+1}$ (который можно также интерпретировать как граф инцидентности точек и гиперплоскостей D -мерного проективного пространства над полем $\mathbb{F}_q$). Определим этот граф в том виде, как нам будет удобно его использовать, приводя заодно некоторые вспомогательные определения из [12, стр. 9]. Напомним, что *степенью вершины* v в графе G называется число инцидентных ей рёбер. Граф G называется *регулярным (или однородным)* графом, если степени всех его вершин равны.

Нам будет удобно задавать двудольный граф тройкой $G = (V_0, V_1, E)$, где V_0, V_1 — множества вершин первой и второй доли, $E \subseteq V_0 \times V_1$ — множество рёбер.

Обозначим $\text{Gr}_q(D, k) := \{V \subseteq \mathbb{F}_q^D \mid \dim V = k\}$ — множество всех k -мерных подпространств D -мерного пространства над полем $\mathbb{F}_q$.

Тогда $\Gamma_{D,q} = (\text{Gr}_q(D+1, 1), \text{Gr}_q(D+1, D), E)$, где

$$E = \{(\ell, h) \in \text{Gr}_q(D+1, 1) \times \text{Gr}_q(D+1, D) \mid \ell \subseteq h\}.$$

Определим скалярное произведение $\langle \alpha, \beta \rangle := \sum_{i=0}^D \alpha_i \beta_i$ векторов $\alpha, \beta \in \mathbb{F}_q^{D+1}$. Каждую прямую $\ell \in \text{Gr}_q(D+1, 1)$ можно однозначно задать ненулевым вектором (*представителем*) $\hat{\ell} \in \mathbb{F}_q^{D+1}$ на этой прямой, а каждую гиперплоскость $h \in \text{Gr}_q(D+1, D)$ можно задать ненулевым вектором (*представителем*) $\hat{h}$, ортогональным данной гиперплоскости. Поскольку представители $\hat{\ell}$ и $\hat{h}$ определены с точностью до умножения на константу, для определённости потребуем, чтобы у представителей первая ненулевая координата была равна 1.

Представители прямых и гиперплоскостей можно естественным образом взаимно-однозначно отождествить с точками проективного пространства

$$\mathbb{P}_q^D = (\mathbb{F}_q^{D+1} \setminus \{0\}) / \sim,$$

где $x \sim y$, если $x = \gamma y$ для некоторого $\gamma \in \mathbb{F}_q \setminus \{0\}$ для $x, y \in \mathbb{F}_q^{D+1} \setminus \{0\}$. Каждой точке $x \in \mathbb{P}_q^D$ сопоставляется вектор длины $D+1$ её однородных координат.

Теперь мы можем ввести чуть более удобное определение $\Gamma_{D,q} = (\mathbb{P}_q^D, \mathbb{P}_q^D, E)$, где

$$E = \{(x, y) \in \mathbb{P}_q^D \times \mathbb{P}_q^D \mid \langle x, y \rangle = 0\}.$$

2.2.2. Код на графе проективного пространства

Введём ещё нескольких необходимых определений и обозначений. Пусть $f \in \mathbb{F}_q[x_1, \dots, x_n]$ — полином, тогда его *степень* $\deg_{x_{i_1}, x_{i_2}, \dots, x_{i_m}} f$ по переменным $x_{i_1}, x_{i_2}, \dots, x_{i_m}$ определим как максимальную степень его монома по этим переменным, где степень монома определяется как

$$\deg_{x_{i_1}, \dots, x_{i_m}} (cx_1^{d_1} x_2^{d_2} \dots x_n^{d_n}) = d_{i_1} + d_{i_2} + \dots + d_{i_m}.$$

В частности, *степенью* полинома f называется степень по всем его переменным:

$$\deg f = \deg_{x_1, \dots, x_n} f.$$

Полином называется *однородным по переменным* $x_{i_1}, \dots, x_{i_m}$, если для любого монома, входящего в данный полином, его степень по переменным $x_{i_1}, \dots, x_{i_m}$ равна одной и той же величине d . Полином называется *однородным степени* d , если степень всех его мономов равна d .

Введём несколько обозначений.

1. $\mathbb{F}_q[x_1, \dots, x_n]$ — кольцо полиномов от переменных $x_1, \dots, x_n$ над полем $\mathbb{F}_q$;
2. $\mathbb{F}_q[x_1, \dots, x_n]_{\leq \nu}$ — множество полиномов степени не выше ν над полем $\mathbb{F}_q$;
3. $\mathbb{F}_q[x_1, \dots, x_n]_{\nu}$ — множество однородных полиномов степени ν над полем $\mathbb{F}_q$, включающее в себя нулевой полином.

Зафиксируем $D \geq 2$, $m < (q-1)D$. Определим код $\mathcal{C}_{D,q,m}$ как множество функций $c : E(\Gamma_{D,q}) \rightarrow \mathbb{F}_q$ таких, что для любого $\gamma \in \mathbb{P}_q^D$ существуют однородные полиномы $f_\gamma, f^\gamma \in \mathbb{F}_q[x_0, \dots, x_D]_m$ такие, что $c(\alpha, \beta) = f_\alpha(\beta) = f^\beta(\alpha)$ для всех рёбер $(\alpha, \beta) \in E(\Gamma_{D,q})$.

Замечание. Код $\mathcal{C}_{D,q,m}$ является кодом Таннера на графе $\Gamma_{D,q}$, в котором для различных вершин могут использоваться различные локальные коды.

2.3. Полученные результаты

Теорема 1. Пусть для каждой вершины $v \in V$ графа $\Gamma_{D,q}$ выбран локальный код $\mathcal{C}_v \subseteq \mathbb{F}_q^w$, $w = \frac{q^D-1}{q-1}$. Обозначим за $\mathcal{C} = \{\mathcal{C}_v\}_{v \in V}$ — семейство таких кодов, где длина каждого кода составляет w и расстояние не меньше εw . Тогда относительное минимальное расстояние кода $\mathcal{T} = \mathcal{T}(\Gamma_{D,q}, \mathcal{C})$ удовлетворяет оценке:

$$\delta_{\min}(\mathcal{T}) \geq \varepsilon \left(\varepsilon - \sqrt{q^{1-D}} \right).$$

Теорема 2. Пусть $0 \leq m < q$. Тогда $\delta_{\min}(\mathcal{C}_{2,q,m}) \geq \varepsilon^3$, где $\varepsilon = \frac{q-m}{q}$.

Теорема 3. Пусть $m < q$, $D \geq 3$. Тогда

$$\delta_{\min}(\mathcal{C}_{D,q,m}) \geq \frac{(q-m)^2(q-2)}{q^3}.$$

Теорема 4. Пусть $1 \leq m < q/2$. Тогда

$$\dim \mathcal{C}_{D,q,m} \geq \frac{2m+D}{D} \binom{m+D-1}{D-1}^2.$$

Таким образом, для случая проективной плоскости ($D = 2$) получаем следствие

Следствие 1. Пусть $1 \leq m < q/2$. Тогда

$$\dim \mathcal{C}_{2,q,m} \geq (m+1)^3. \quad (1)$$

Отметим, что аналогичные результаты для кодов на графах аффинных плоскостей получены в работах [3–5, 8]. В [5] также без доказательства упомянуто, что оценки для аффинного случая переносятся на проективный, однако это не всегда выполняется и требует дополнительного исследования¹. Более того, на основании результатов численного эксперимента, в котором размерность кода $\mathcal{C}_{2,q,m}$ оценивалась по рангу его проверочной матрицы, можно также выдвинуть следующее предположение:

Гипотеза 1. Пусть $q/2 \leq m < q$. Тогда

$$\dim \mathcal{C}_{2,q,m} \geq (2m+1-q)(q^2+q+1) + (q-m)^3.$$

¹В частности, при $q = 9, m = 3$ в аффинном случае размерность 66 [4], а в проективном 64 (см. Приложение А)

Заметим, что в случае $q = 9, m = 4$ размерность равна 131, что выше оценки (1). В [3, 4] детально исследован аффинный случай и показано, что для кодов на графе аффинной плоскости для $q = 9, k = 4$ (в наших обозначениях это соответствует $m = 3$): размерность равна 66, что выше общей нижней оценки $k^3 = 64$.

Для линейных кодов $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ линейное отображение $\varphi : \mathcal{C}_1 \rightarrow \mathcal{C}_2$ называется *изометрией* кодов $\mathcal{C}_1$ и $\mathcal{C}_2$, если $\varphi(\mathcal{C}_1) = \mathcal{C}_2$ и φ сохраняет вес Хэмминга, то есть $|\varphi(x)| = |x|$ для любого $x \in \mathcal{C}_1$. Коды $\mathcal{C}_1$ и $\mathcal{C}_2$ называются *эквивалентными*, если между ними существует изометрия. *Мономиальным преобразованием* пространства $\mathbb{F}_q^n$ называется композиция перестановки координат и умножения каждой координаты на ненулевой элемент поля. Любое мономиальное преобразование является изометрией кодов.

Следующее утверждение показывает, что код $\mathcal{C}_{D,q,m}$ обладает определённой симметрией.

Для любого вектора $\alpha = (\alpha_0, \dots, \alpha_D) \in \mathbb{F}_q^{D+1} \setminus \{0\}$ обозначим через $\hat{\alpha}$ нормированный вектор, где первая ненулевая компонента равна 1. Здесь

$$\hat{\alpha} = \frac{\alpha}{\alpha_i} = \left(0, \dots, 0, \underbrace{1}_i, \frac{\alpha_{i+1}}{\alpha_i}, \dots, \frac{\alpha_D}{\alpha_i}\right),$$

где $i = \min\{k \in \{0, \dots, D\} \mid \alpha_k \neq 0\}$. Таким образом, $\hat{\alpha}$ — однородные координаты точки проективного пространства $\mathbb{P}_q^D$, соответствующей прямой, проходящей через точку α .

Утверждение 1. Пусть $D \geq 2, 1 \leq m < (q-1)D, E = E(\Gamma_{D,q}), \mathcal{C} = \mathcal{C}_{D,q,m}$. Для любой матрицы $A \in \text{GL}(D+1, q)$ существует набор ненулевых констант $a = (a_{(\alpha,\beta)})_{(\alpha,\beta) \in E} \in \mathbb{F}_q^E$ такой, что для любого кодового слова $c \in \mathcal{C}$ существует кодовое слово $c' \in \mathcal{C}$, удовлетворяющее условию:

$$c'(\alpha, \beta) = a_{(\alpha,\beta)} c(\widehat{A\alpha}, \widehat{A^*\beta}) \quad \text{для всех } (\alpha, \beta) \in E,$$

где $A^* = (A^T)^{-1}$.

Из данного утверждения, в частности, следует, что группа изометрий кода $\mathcal{C}_{D,q,m}$ включает в себя группу проективных преобразований $\text{PGL}(D+1, q)$.

3. Вспомогательные результаты

3.1. Коды Рида-Маллера

Для доказательства основных результатов нам понадобятся известные результаты о размерности и минимальном расстоянии недвоичных ко-

дов Рида-Маллера. Пусть $\mathbb{F}_q^D = \{\alpha_1, \dots, \alpha_q^D\}$. Кодом Рида-Маллера порядка ν длины q^D над полем $\mathbb{F}_q$ называется множество

$$\text{RM}_q(\nu, D) := \left\{ (p(\alpha_i)_{i=1}^{q^D}) \mid p \in \mathbb{F}_q[x_1, \dots, x_D]_{\leq \nu} \right\}.$$

Известно [13, стр. 1568], что при $\nu < q$ коды Рида-Маллера имеют следующие параметры:

$$\begin{aligned} \dim \text{RM}_q(\nu, D) &= \binom{\nu + D}{D}, \\ d_{\min}(\text{RM}_q(\nu, D)) &= (q - \nu)q^{D-1}. \end{aligned}$$

Теперь определим проективные коды Рида-Маллера. Пусть $\mathbb{P}_q^D = (P_1, \dots, P_{n_D})$, где $n_D := |\mathbb{P}_q^D| = \frac{q^{D+1}-1}{q-1}$, P_i — однородные координаты i -й точки проективного пространства. Проективным кодом Рида-Маллера порядка ν длины n_D называется код

$$\text{PRM}_q(\nu, D) := \left\{ (p(P_i))_{i=1}^{n_D} \mid p \in \mathbb{F}_q[x_0, x_1, \dots, x_D]_{\nu} \right\}$$

Известно [13, Раздел III, Теорема 1, стр. 1568–1569], что при $1 \leq \nu < q$ проективные коды Рида-Маллера имеют следующие параметры:

$$\dim \text{PRM}_q(\nu, D) = \binom{\nu + D}{D}, \quad (2)$$

$$d_{\min}(\text{PRM}_q(\nu, D)) = (q - \nu + 1)q^{D-1}. \quad (3)$$

При этом при $\nu = 0$ код содержит только полиномы нулевой степени, то есть константы, поэтому $\text{PRM}_q(0, D)$ — это просто код с повторением длины n_D .

При $D = 1$ коды Рида-Маллера соответствуют расширенным кодам Рида-Соломона длины q , где значение полинома дополнительно вычисляется в точке 0. Проективные коды Рида-Маллера при $D = 1$ в точности соответствуют проективным кодам Рида-Соломона, где значение полинома дополнительно вычисляется в 0 и в бесконечно удалённой точке (старший коэффициент полинома), т.е.

$$\text{PRS}(q, k) = \text{PRM}_q(k - 1, 1).$$

В частности,

$$\begin{aligned} \dim \text{PRS}(q, k) &= k, \\ d_{\min}(\text{PRS}(q, k)) &= q - k + 2. \end{aligned}$$

Как и обычные коды Рида-Соломона, проективные коды Рида-Соломона являются MDS кодами, то есть для них достигается оценка Синглтона.

3.2. Графы–расширители (expander graphs)

Приведём определения разных видов расширения графов (см. [12, стр. 9], [14, стр. 7]).

Пусть дан регулярный граф G степени d с n вершинами, все вершины которого пронумерованы от 1 до n . Матрицей смежности $A(G)$ порядка $n \times n$ графа G называется симметричная бинарная матрица вида:

$$A_{ij} = \begin{cases} 1, & \text{если вершины } i \text{ и } j \text{ смежны;} \\ 0, & \text{в противном случае.} \end{cases}$$

Все собственные значения матрицы $A(G)$ упорядочим в виде:

$$\lambda_1 = d \geq \lambda_2 \geq \dots \geq \lambda_{n-1} \geq \lambda_n.$$

Второе по абсолютной величине собственное значение $\max(|\lambda_2|, |\lambda_n|)$ характеризует спектральное расширение графа. Для двудольных регулярных графов $\lambda_n = -d$, и таким образом $\lambda(G) = d$. Поэтому в этом случае используется ослабленный вариант спектрального расширения, которое характеризуется вторым собственным значением λ_2 .

Пусть V — множество вершин данного графа G и пусть $S, T \subseteq V$. Обозначим:

$$E(S, T) = \{(s, t) \in E \mid s \in S, t \in T\}, \quad E(S) := |E(S, S)|/2.$$

Заметим, что в $E(S, S)$ каждое ребро $\{u, v\}$ входит два раза: как (u, v) и как (v, u) ; поэтому при подсчёте числа рёбер $E(S)$, индуцированных на множестве вершин S , мы делим число пар в $E(S, S)$ пополам.

Нам потребуется следующая односторонняя версия леммы Алона-Чанга.

Лемма 1 (теорема 9.2.1 в [15]). Пусть G — d -регулярный граф порядка n , второе по убыванию собственное значение которого равно λ . Пусть $X \subset V(G)$ — произвольное подмножество вершин, такое что $|X| = \gamma n$ для некоторого $\gamma \in [0, 1]$. Тогда число рёбер, индуцированных на X , удовлетворяет неравенству

$$E(X) \leq \frac{dn}{2} \left(\gamma^2 + \frac{\lambda}{d} \gamma (1 - \gamma) \right).$$

3.2.1. Спектр графа инцидентности проективного пространства

Лемма 2. Матрица смежности графа $\Gamma_{D,q}$ имеет следующие собственные значения:

1. $\pm w$ кратности 1, где $w = \frac{q^D-1}{q-1}$ — степень вершины;
2. $\pm q^{\frac{D-1}{2}}$ кратности $n-1$, где $n = \frac{q^{D+1}-1}{q-1}$ — число вершин в каждой доле.

Доказательство. Матрица смежности графа $\Gamma_{D,q}$ имеет вид

$$A = \begin{pmatrix} 0 & M \\ M^T & 0 \end{pmatrix},$$

где $M = (M_{\alpha,\beta})_{\alpha,\beta \in \mathbb{P}_q^D}$,

$$m_{\alpha,\beta} = \begin{cases} 1, & \langle \alpha, \beta \rangle = 0, \\ 0, & \text{иначе.} \end{cases}$$

Здесь строки и столбцы матрицы M проиндексированы точками проективного пространства $\mathbb{P}_q^D$.

Для $\alpha \in \mathbb{P}_q^D$ введём обозначение

$$\alpha^\perp := \{\beta \in \mathbb{P}_q^D \mid \langle \alpha, \beta \rangle = 0\}.$$

Заметим, что $\alpha^\perp$ представляет собой $(D-1)$ -мерное проективное пространство, поэтому $|\alpha^\perp| = \frac{q^D-1}{q-1} = w$. Для различных $\alpha, \alpha' \in \mathbb{P}_q^D$ множество $\alpha^\perp \cap \alpha'^\perp$ представляет собой $(D-2)$ -мерное проективное пространство. Отсюда

$$|\alpha^\perp| = \frac{q^D-1}{q-1} = w, \tag{4}$$

$$|\alpha^\perp \cap \alpha'^\perp| = \frac{q^{D-1}-1}{q-1} =: s. \tag{5}$$

Вычислим матрицу MM^T , используя (4) и (5):

$$(MM^T)_{\alpha,\alpha'} = |\{\beta : \langle \alpha, \beta \rangle = \langle \alpha', \beta \rangle = 0\}| = |\alpha^\perp \cap \alpha'^\perp| = \begin{cases} w, & \alpha = \alpha', \\ s, & \alpha \neq \alpha'. \end{cases}$$

Таким образом,

$$MM^T = sJ_n + (w-s)I_n,$$

где J_n — $n \times n$ матрица из единиц, I_n — единичная матрица $n \times n$.

Пусть $\mathbf{1}$ — вектор длины n , все компоненты которого равны 1. Легко видеть, что $J_n \mathbf{1} = n\mathbf{1}$, а также $J_n x = 0$ для любого вектора x , ортогонального $\mathbf{1}$. Таким образом, матрица J_n имеет однократное собственное значение n и $(n-1)$ -кратное собственное значение 0. Значит, MM^T имеет спектр:

$$\lambda_2 = \dots = \lambda_n = w - s = \frac{q^D - q^{D-1}}{q - 1} = q^{D-1},$$

$$\lambda_1 = sn + (w - s) = \frac{(q^{D+1} - 1)(q^{D-1} - 1)}{(q - 1)^2} + q^{D-1} = \frac{q^{2D} - 2q^D + 1}{(q - 1)^2} = w^2.$$

Поскольку матрица M симметричная, то модули её собственных значений равны корню из собственных значений матрицы MM^T :

$$\lambda_1(M) = w, \quad |\lambda_2(M)| = \dots = |\lambda_n(M)| = \sqrt{q^{D-1}}.$$

Осталось заметить, что матрица

$$A = \begin{pmatrix} 0 & M \\ M^T & 0 \end{pmatrix}$$

имеет в спектре значения $\pm \lambda_i(M)$, $i = 1, \dots, n$. Лемма доказана. $\square$

4. Доказательство основных результатов

4.1. Оценка минимального расстояния

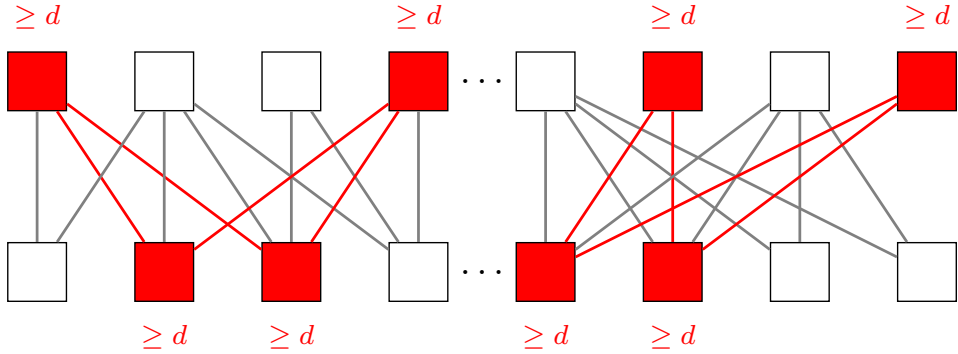
Семейство кодов назовём *асимптотически хорошим*, если минимальное расстояние пропорционально длине кода и скорость не меньше некоторого $R > 0$. В свою очередь, это означает, что для каждого кода из семейства минимальное расстояние $d_{\min}$ растёт линейно с длиной n , обычно так, что $d_{\min} \geq \alpha n$, где $\alpha > 0$ — фиксированная константа, $k \geq Rn$.

Приведём нижнюю оценку минимального расстояния, также упоминавшуюся в работах [3, 5, 7] для графовых кодов. Здесь мы приведём явное доказательство для графа проективной плоскости $\Gamma_{2,q}$.

Лемма 3. Пусть для каждой вершины $v \in V$ графа $\Gamma_{2,q}$ выбран локальный код $C_v \subseteq \mathbb{F}_q^{q+1}$. Через $\mathcal{C} = \{C_v\}_{v \in V}$ обозначим семейство таких кодов с расстоянием не меньше d . Будем считать, что в каждой вершине графа $\Gamma_{2,q}$ фиксирована нумерация инцидентных рёбер. Тогда код $\mathcal{T}(\Gamma_{2,q}, \mathcal{C})$ обладает минимальным расстоянием не меньше:

$$d_{\min}(\mathcal{T}(\Gamma_{2,q}, \mathcal{C})) \geq d(d-1+1).$$

В частности, при выборе $\mathcal{C} \equiv \mathcal{C}_0$ для всех $v \in V$ получаем конструкцию кода Таннера вида $\mathcal{T}(\Gamma_{2,q}, \mathcal{C}_0)$.



Доказательство. Для краткости обозначим $\Gamma := \Gamma_{2,q}$, $E := E(\Gamma)$ — множество рёбер графа Γ . Рассмотрим ненулевое кодовое слово $c \in \mathcal{T}(\Gamma, \mathcal{C})$ минимального веса. Напомним, что кодовое слово кода $\mathcal{T}(\Gamma, \mathcal{C})$ — это функция, определённая на множестве рёбер графа Γ . *Активными* назовём те рёбра $e \in E$, для которых $c(e) \neq 0$, таким образом $d(\mathcal{T}(\Gamma, \mathcal{C})) = |c|$ равно числу активных рёбер. Вершину графа Γ назовём *активной*, если из неё исходит хотя бы одно активное ребро. Напомним, что каждой вершине графа соответствует точка или прямая проективной плоскости. Точку или прямую будем называть *активной*, если соответствующая вершина графа $\Gamma_{2,q}$ активна.

Так как код Таннера $\mathcal{T}(\Gamma, \mathcal{C})$ состоит из всех кодовых слов $c \in \mathbb{F}_q^E$ таких, что $c_v \in \mathcal{C}_v$ для всех вершин $v \in V$, где $c_v = (c(e_{v,1}), \dots, c(e_{v,w}))$, то рассмотрим произвольную активную прямую, из которой исходит не менее d активных рёбер. Поскольку эта прямая инцидентна по меньшей мере d активным точкам, то на ней расположены как минимум d активных точек. В свою очередь, через каждую активную точку рассматриваемой прямой проходит ещё не менее $d - 1$ активных прямых по построению. Тогда всего активных прямых будет не менее $d(d - 1) + 1$. Как уже упоминалось ранее, из соответствующих вершин графа исходит как минимум d активных рёбер, таким образом общее число активных рёбер не меньше $d(d(d - 1) + 1)$. $\square$

Лемма 4. Пусть G — w -регулярный граф порядка n со вторым по величине собственным значением $\lambda \geq 0$. Пусть для каждой вершины $v \in V$ графа G сопоставлен линейный код $\mathcal{C}_v$ с длиной w и минимальным

расстоянием не меньше εw . Обозначим за $\mathcal{C} = \{\mathcal{C}_v\}_{v \in V}$ — семейство таких кодов, тогда выполнена оценка:

$$\delta_{\min}(\mathcal{T}(G, \mathcal{C})) \geq \varepsilon \left(\varepsilon - \frac{\lambda}{w} \right).$$

Эта лемма аналогична [14, Lemma 15], но мы не предполагаем, что все локальные коды одинаковые. Приведём здесь доказательство, идея которого полностью аналогична той, что использовалась в [14, Lemma 15].

Доказательство. При $\lambda/w \geq \varepsilon$ утверждение леммы тривиально. Поэтому далее рассматриваем случай $\lambda/w < \varepsilon$.

Пусть $c \in \mathcal{T}(G, \mathcal{C})$ — некоторое ненулевое кодовое слово минимального веса. Обозначим за S множество рёбер графа G с ненулевыми пометками и A — множество вершин, инцидентных рёбрам из S . Пусть

$$\gamma := \frac{|A|}{n}.$$

По лемме 1 выполнено

$$|S| \leq \frac{wn}{2} \left(\gamma^2 + \frac{\lambda}{w} (\gamma - \gamma^2) \right).$$

Поскольку каждое ребро из S инцидентно по крайней мере двум вершинам, значит в среднем на одну вершину из A приходится рёбер

$$\frac{2|S|}{|A|} \leq \frac{wn(\gamma^2 + \frac{\lambda}{w}(\gamma - \gamma^2))}{\gamma n} = w \left(\gamma + \frac{\lambda}{w} (1 - \gamma) \right).$$

По условию, из каждого локального кода $\mathcal{C}_v$ для $v \in A$ исходит не менее εw рёбер с ненулевыми пометками, поэтому

$$\gamma + \frac{\lambda}{w} (1 - \gamma) \geq \varepsilon \implies \gamma \geq \frac{\varepsilon - \frac{\lambda}{w}}{1 - \frac{\lambda}{w}} \geq \varepsilon - \frac{\lambda}{w}.$$

Также

$$|S| \geq \frac{1}{2} \varepsilon w |A| = \gamma \varepsilon \frac{wn}{2} = \gamma \varepsilon |E(G)|.$$

Таким образом, относительное число рассматриваемых рёбер будет не меньше

$$\frac{|S|}{|E(G)|} \geq \varepsilon \left(\varepsilon - \frac{\lambda}{w} \right),$$

что и доказывает утверждение леммы. $\square$

Теорема 1. Пусть для каждой вершины $v \in V$ графа $\Gamma_{D,q}$ выбран локальный код $\mathcal{C}_v \subseteq \mathbb{F}_q^w$, $w = \frac{q^D-1}{q-1}$. Обозначим за $\mathcal{C} = \{\mathcal{C}_v\}_{v \in V}$ — семейство таких кодов, где длина каждого кода составляет w и расстояние не меньше εw . Тогда относительное минимальное расстояние кода $\mathcal{T} = \mathcal{T}(\Gamma_{D,q}, \mathcal{C})$ удовлетворяет оценке:

$$\delta_{\min}(\mathcal{T}) \geq \varepsilon \left(\varepsilon - \sqrt{q^{1-D}} \right).$$

Доказательство. По лемме 2 второе собственное значение графа $\Gamma_{D,q}$ равно $\lambda = \sqrt{q^{D-1}}$. Согласно лемме 4, для $\mathcal{T}$ справедливо:

$$\delta_{\min}(\mathcal{T}) \geq \varepsilon \left(\varepsilon - \frac{\lambda}{w} \right) = \varepsilon \left(\varepsilon - \frac{\sqrt{q^{D-1}}}{w} \right).$$

Учитывая, что $w = \frac{q^D-1}{q-1} > q^{D-1}$, имеем

$$\delta_{\min}(\mathcal{T}) \geq \varepsilon \left(\varepsilon - \frac{\sqrt{q^{D-1}}}{q^{D-1}} \right) = \varepsilon \left(\varepsilon - \sqrt{q^{1-D}} \right). \quad \square$$

Лемма 5. Для кода $\mathcal{C}_{D,q,m}$ в каждой вершине $v \in V(\Gamma_{D,q})$ локальный код $\mathcal{C}_v$ эквивалентен проективному коду Рида-Маллера $\text{PRM}_q(m, D-1)$.

Доказательство. Обозначим $w := \frac{q^D-1}{q-1}$ — степень вершины $\Gamma_{D,q}$. В каждой вершине v графа $\Gamma_{D,q}$, соответствующей точке α проективного пространства, по определению локальный код $\mathcal{C}_v \subset \mathbb{F}_q^w$ задаётся следующим образом:

$$\mathcal{C}_v = \left\{ (f_\alpha(\beta))_{\beta \in \mathbb{P}_q^D: \langle \alpha, \beta \rangle = 0} \mid f_\alpha \in \mathbb{F}_q[a_0, \dots, a_D]_m \right\}.$$

Поскольку условие $\langle \alpha, x \rangle = \sum_{i=0}^D \alpha_i x_i = 0$ является линейным относительно переменных $x_0, \dots, x_D$, то, без ограничения общности полагая $\alpha_0 \neq 0$, можно выразить x_0 через $x_1, \dots, x_D$:

$$x_0 = - \sum_{i=1}^D \frac{\alpha_i}{\alpha_0} x_i.$$

Подставляя это выражение в $f_\alpha(x_0, \dots, x_D)$, получаем функцию

$$g_\alpha(x_1, \dots, x_D) := f_\alpha \left(- \sum_{i=1}^D \frac{\alpha_i}{\alpha_0} x_i, x_1, \dots, x_D \right).$$

Так как исходный полином f_α являлся однородным полиномом степени m от $D+1$ переменных, то полученный полином g_α является однородным полиномом степени m от D переменных. Таким образом, $\mathcal{C}_v$ является множеством векторов значений полиномов от D переменных, вычисленных в точках $(D-1)$ -мерного проективного пространства, но не на однородных координатах, а на точках, отличающихся в константу раз. Поэтому $\mathcal{C}_v$ изометричен коду $\text{PRM}_q(m, D-1)$, где изометрия задаётся умножением координат на константы, обусловленные выбором представителей точек $\mathbb{P}_q^{D-1}$.

В силу симметричности конструкции такие же рассуждения применимы для вершин графа $\Gamma_{D,q}$, соответствующих гиперплоскостям проективного пространства. $\square$

Используя известную оценку минимального расстояния проективного кода Рида-Маллера (3), при $m < q$ получаем следствие.

Следствие 2. Пусть $1 \leq m < q$, $D \geq 2$. Для кода $\mathcal{C}_{D,q,m}$ в каждой вершине $v \in V(\Gamma_{D,q})$ минимальное расстояние локального кода $\mathcal{C}_v$ равно $(q-m+1)q^{D-2}$.

Теорема 2. Пусть $0 \leq m < q$. Тогда $\delta_{\min}(\mathcal{C}_{2,q,m}) \geq \varepsilon^3$, где $\varepsilon = \frac{q-m}{q}$.

Доказательство. Рассмотрим случай при $m = 0$. В этом случае все локальные коды — коды с повторением, а значит и весь код $\mathcal{C}_{2,q,m}$ — код с повторением, значит его относительное минимальное расстояние равно 1; кроме того, $\varepsilon = \frac{q-m}{q} = 1$, таким образом утверждение теоремы выполнено.

Теперь рассмотрим основной случай $m \geq 1$. По лемме 5 все локальные коды кода $\mathcal{C}_{2,q,m}$ изометричны кодам Рида-Маллера $\text{PRM}_q(m, 1)$, то есть кодам Рида-Соломона $\text{PRS}(q, m+1)$. Значит по следствию 2 минимальное расстояние всех локальных кодов равно

$$d_0 = q + 1 - m = \varepsilon q + 1.$$

Согласно лемме 3:

$$d(\mathcal{C}_{2,q,m}) \geq d_0(d_0(d_0 - 1) + 1).$$

Так как $d_0 = \varepsilon q + 1$, то получим:

$$\begin{aligned} d(\mathcal{C}_{2,q,m}) &\geq (\varepsilon q + 1) \left((\varepsilon q + 1)(\varepsilon q + 1 - 1) + 1 \right) = (\varepsilon q + 1) \left((\varepsilon q + 1)\varepsilon q + 1 \right) = \\ &= (\varepsilon q + 1) \left(\varepsilon^2 q^2 + \varepsilon q + 1 \right) \geq \varepsilon^3 (q + 1) (q^2 + q + 1) = \varepsilon^3 n, \end{aligned}$$

где $n = (q+1)(q^2+q+1)$ — длина кода $\mathcal{C}_{2,q,m}$. $\square$

Теперь докажем оценку расстояния для размерности $D \geq 3$, используя теорему 1.

Теорема 3. Пусть $m < q$, $D \geq 3$. Тогда

$$\delta_{\min}(\mathcal{C}_{D,q,m}) \geq \frac{(q-m)^2(q-2)}{q^3}.$$

Доказательство. Заметим, что при $m = 0$ все локальные коды — коды с повторением, а значит и весь код $\mathcal{C}_{D,q,m}$ — код с повторением, значит его относительное минимальное расстояние равно 1, и утверждение теоремы выполнено. Далее предполагаем, что $m \geq 1$.

Пусть $w := \frac{q^D-1}{q-1}$ — степень вершины графа $\Gamma_{D,q}$. По следствию 2 все локальные коды кода $\mathcal{C}_{D,q,m}$ имеют минимальное расстояние

$$d_0 = (q-m+1)q^{D-2}.$$

Значит относительное минимальное расстояние можно оценить следующим образом:

$$\varepsilon = \frac{d_0}{w} = \frac{(q+1-m)q^{D-2}}{\frac{q^D-1}{q-1}} \geq \frac{(q+1-m)(q-1)}{q^2} \geq \frac{q-m}{q}.$$

Здесь мы использовали, что $(q+1-m)(q-1) = (q-m)q+m-1 \geq (q-m)q$. По теореме 1 получим оценку

$$\delta_{\min}(\mathcal{C}_{D,q,m}) \geq \varepsilon \left(\varepsilon - \sqrt{q^{1-D}} \right).$$

Поскольку $D \geq 3$, то $\sqrt{q^{1-D}} \leq 1/q$, значит

$$\varepsilon - \sqrt{q^{1-D}} \geq \frac{(q+1-m)(q-1)}{q^2} - \frac{1}{q} = \frac{(q+1-m)(q-1) - q}{q^2}$$

или

$$\varepsilon - \sqrt{q^{1-D}} \geq \frac{(q-m)(q-1) - 1}{q^2} \geq \frac{(q-m)(q-2)}{q^2}.$$

Отсюда

$$\delta_{\min}(\mathcal{C}_{D,q,m}) \geq \frac{(q-m)}{q} \cdot \frac{(q-m)(q-2)}{q^2} \geq \frac{(q-m)^2(q-2)}{q^3}. \quad \square$$

4.2. Оценка размерности

Далее будем считать, что размер поля q , параметр $m \in \mathbb{N}$ и размерность пространства $D \geq 2$ фиксированы. Далее опустим индексы и положим $\Gamma := \Gamma_{D,q}$, $E := E(\Gamma)$, $\mathcal{C} := \mathcal{C}_{D,q,m}$.

Введём 2 группы переменных $x = (x_0, \dots, x_D)$ и $a = (a_0, \dots, a_D)$. Через P обозначим кольцо полиномов от $2(D+1)$ переменных над конечным полем $\mathbb{F}_q$:

$$P = \mathbb{F}_q[x_0, \dots, x_D, a_0, \dots, a_D].$$

Обозначим $B(x, a) := \langle x, a \rangle = \sum_{i=0}^D a_i x_i$ — полином, задающий скалярное произведение.

Для $s \geq 0$ через P_s обозначим множество полиномов из P , однородных по переменным $x_0, \dots, x_D$ и по переменным $a_0, \dots, a_D$, таких, что $\deg_x(p) = \deg_a(p) = s$; также включим в P_s нулевой полином, чтобы оно было линейным пространством.

Рассмотрим отображение:

$$\sigma : P_m \rightarrow \mathbb{F}_q^E,$$

где

$$\sigma(p) = p|_E, \quad \sigma(p; \alpha, \beta) = p(\alpha, \beta),$$

где $(\alpha, \beta) \in E$.

Лемма 6. Пусть $1 \leq m < q/2$. Тогда для любого $p \in P_m$ выполняется $\sigma(p) = 0$ тогда и только тогда, когда $B \mid p$. Другими словами, $\ker \sigma = P_{m-1} \cdot B$.

Доказательство.

Достаточность. Докажем, что если для $p \in P_m$ выполнено $B \mid p$, то $\sigma(p) = 0$. Напомним, что множество E представлялось в виде:

$$E = \{(\alpha, \beta) \in \mathbb{P}_q^D \times \mathbb{P}_q^D \mid B(\alpha, \beta) = 0\}.$$

Поскольку $p = Br$ для некоторого $r \in P$, то в силу делимости имеем:

$$p|_E = \underbrace{B|_E}_{\equiv 0} \cdot r|_E \equiv 0.$$

Необходимость. Докажем, что если для $p \in P_m$ верно, что $\sigma(p) = 0$, то $B \mid p$. Зафиксируем произвольный многочлен $p \in P_m$ такой, что $\sigma(p) = 0$, то есть $p|_E = 0$.

Домножим данный многочлен на a_0^m и получим:

$$a_0^m p(x, a)$$

Введём замену:

$$u = B(x, a).$$

Выразим:

$$a_0 x_0 = u - \sum_{i=1}^D a_i x_i. \quad (6)$$

Заметим, что

$$\deg_{x_0} p \leq \deg_x p = m.$$

Поскольку $\deg_{x_0} p \leq m$, то в каждом мономе $a_0^m p$ степень a_0 не меньше, чем степень x_0 . Поэтому существует такой многочлен $\hat{p} \in \mathbb{F}_q[u, x_1, \dots, x_D, a_0, \dots, a_D]$, что

$$\hat{p}(B(x, a), x_1, \dots, x_D, a_0, \dots, a_D) = a_0^m p(x, a).$$

Каждому моному $\prod_{s=0}^D x_s^{i_s} a_s^{j_s}$ многочлена p соответствует слагаемое

$$a_0^{m-i_0} \left(u - \sum_{s=1}^D a_s x_s \right)^{i_0} a_0^{j_0} \prod_{s=1}^D x_s^{i_s} a_s^{j_s}$$

в полиноме $\hat{p}$. Отсюда

$$\deg_{u, x_1, \dots, x_D} \hat{p} = \deg_x p = m.$$

Кроме того, поскольку $\sum_{s=0}^D j_s = \deg_a p = m$, то

$$\deg_a a_0^{m-i_0} \left(u - \sum_{s=1}^D a_s x_s \right)^{i_0} a_0^{j_0} \prod_{s=1}^D x_s^{i_s} a_s^{j_s} = m - i_0 + i_0 + \sum_{s=0}^D j_s = 2m < q,$$

значит $\deg_a \hat{p} < q$. Таким образом, степень $\hat{p}$ по каждой переменной не выше $q - 1$.

Положим

$$\tilde{E} := \left\{ (u, x_1, \dots, x_D, a_0, \dots, a_D) \in \mathbb{F}_q^{2D+2} \mid u = 0 \right\}.$$

Тогда для любой точки

$$(0, x_1, \dots, x_D, a_0, \dots, a_D) \in \tilde{E}, \quad a_0 \neq 0$$

возьмём

$$x_0 = -a_0^{-1} \sum_{i=1}^D a_i x_i,$$

тогда точка (x, a) лежит на конусе, образованном прямыми из E . Отсюда $p(x, a) = 0$, и по определению многочлена $\hat{p}$ имеем

$$\hat{p}(0, x_1, \dots, x_D, a_0, \dots, a_D) = a_0^m p(x, a) = 0.$$

Осталось рассмотреть случай $a_0 = 0$. Покажем, что $\hat{p}$ делится на a_0 . Сгруппируем в полиноме p все мономы, где x_0 входит в степени m , не содержащие a_0 :

$$p(x, a) = x_0^m h(a_1, \dots, a_D) + a_0 q(x, a) + \sum_{s=1}^D x_s q_s(x, a),$$

где h — однородный полином степени m по переменным $a_1, \dots, a_D$, а $q, q_1, \dots, q_D$ — некоторые полиномы.

Покажем, что $h \equiv 0$. Предположим противное. Тогда найдётся набор

$$(a_1, \dots, a_D) \neq 0$$

такой, что

$$h(a_1, \dots, a_D) \neq 0.$$

Рассмотрим точку

$$x = (1, 0, \dots, 0), \quad a = (0, a_1, \dots, a_D).$$

Для неё

$$B(x, a) = a_0 x_0 + \sum_{s=1}^D a_s x_s = 0 \cdot 1 + \sum_{s=1}^D a_s \cdot 0 = 0,$$

поэтому $(x, a) \in E$. Так как $\sigma(p) = 0$, имеем

$$p(x, a) = 0.$$

С другой стороны, из приведённого разложения следует

$$p(1, 0, \dots, 0, 0, a_1, \dots, a_D) = h(a_1, \dots, a_D) \neq 0,$$

поскольку $a_0 = 0$ и $x_1 = \dots = x_D = 0$. Получено противоречие. Значит, $h \equiv 0$. Тогда в каждом слагаемом полинома $\hat{p}$

$$a_0^{m-i_0} \left(u - \sum_{s=1}^D a_s x_s \right)^{i_0} a_0^{j_0} \prod_{s=1}^D x_s^{i_s} a_s^{j_s}$$

либо $i_0 < m$, либо $j_0 > 0$. Следовательно, каждое слагаемое полинома $\hat{p}$ содержит множитель a_0 , значит

$$a_0 \mid \hat{p}.$$

Таким образом, в случае $a_0 = 0$, также имеем

$$\hat{p}(0, x_1, \dots, x_D, a_0, \dots, a_D) = 0.$$

Следовательно, если $p|_E = 0$, то и $\hat{p}|_{\bar{E}} = 0$.

Покажем, что $u \mid \hat{p}$. Пусть $c_{i_0, \dots, i_D, j_0, \dots, j_D} \in \mathbb{F}_q$ — коэффициент при мономе $u^{i_0} a_0^{j_0} \prod_{s=1}^D x_s^{i_s} a_s^{j_s}$ в полиноме $\hat{p}$. Тогда

$$\hat{p}(0, x_1, \dots, x_D, a_0, \dots, a_D) = \sum_{i_1, \dots, i_D, j_0, \dots, j_D} c_{0, i_1, \dots, i_D, j_0, \dots, j_D} \cdot a_0^{j_0} \prod_{s=1}^D x_s^{i_s} a_s^{j_s}. \quad (7)$$

Предположим, что существует хотя бы один коэффициент

$$c_{0, i_1, \dots, i_D, j_0, \dots, j_D} \neq 0 \quad \text{при некоторых } 0 \leq i_1, \dots, i_D, j_0, \dots, j_D < q.$$

Зная, что степень $\hat{p}$ по каждой переменной не выше $q - 1$ и используя тот факт, что любая функция, заданная на конечном множестве $\mathbb{F}_q$, однозначно представима в виде многочлена степени не выше $q - 1$, следует, что многочлен (7) не может быть тождественно равен нулю, если хотя бы один коэффициент $c_{0, i_1, \dots, i_D, j_0, \dots, j_D}$ не равен нулю. Это противоречит условию $\hat{p}|_{\bar{E}} = 0$, а значит все эти коэффициенты должны быть нулевыми, и, следовательно, в $\hat{p}$ нет мономов, не содержащих u . Таким образом, $\hat{p} = u \cdot r$ для некоторого $r \in \mathbb{F}_q[u, x_1, \dots, x_D, a_0, \dots, a_D]$, а значит

$$a_0^m p = B \cdot r(B(x, a), x_1, \dots, x_D, a_0, \dots, a_D).$$

Поскольку B неприводим и $B \nmid a_0^m$, то $B \mid p$, что и требовалось доказать. $\square$

Лемма 7. Если $p \in P_m$, то $\sigma(p) \in \mathcal{C}$, где $0 \leq m \leq q - 1$.

Доказательство. Напомним, что код $\mathcal{C}$ определялся как множество функций $c : E \rightarrow \mathbb{F}_q$, для которых для каждой точки $\alpha \in \mathbb{P}_q^D$ существуют однородные полиномы f_α и f^α степени m от $D + 1$ переменной, такие что $f_\alpha(\beta) = c(\alpha, \beta) = f^\beta(\alpha)$ для всех $(\alpha, \beta) \in E$, то есть удовлетворяющих условию $\langle \alpha, \beta \rangle = 0$.

Для произвольного $\alpha \in \mathbb{P}_q^D$ определим функции $f_\alpha \in \mathbb{F}_q[a_0, \dots, a_D]$, $f^\alpha \in \mathbb{F}_q[x_0, \dots, x_D]$:

$$f_\alpha(a) := p(\alpha, a), \quad f^\alpha(x) := p(x, \alpha).$$

Тогда для всех $\alpha, \beta \in \mathbb{P}_q^D$, таких что $\langle \alpha, \beta \rangle = 0$ верно:

$$\sigma(p)(\alpha, \beta) = f_\alpha(\beta) = f^\beta(\alpha).$$

Кроме того, поскольку p однороден по группам переменных a и x и имеет степень m по каждой из групп, то f_α и f^α также являются однородными полиномами степени m . Таким образом, отображение $\sigma(p)$ удовлетворяет обоим условиям определения кода $\mathcal{C}$ и, следовательно,

$$\sigma(p) \in \mathcal{C},$$

что и требовалось доказать. $\square$

Теорема 4. Пусть $1 \leq m < q/2$. Тогда

$$\dim \mathcal{C}_{D,q,m} \geq \frac{2m+D}{D} \binom{m+D-1}{D-1}^2.$$

Доказательство. Оценим размерность пространства полиномов P_m . Базисом линейного пространства полиномов над $\mathbb{F}_q$ является множество мономов

$$\left\{ \prod_{s=0}^D a_s^{i_s} x_s^{j_s} \mid \sum_{s=0}^D i_s = \sum_{s=0}^D j_s = m \right\}.$$

Есть $\binom{m+D}{D}$ способов разбить число m в сумму $D+1$ целых неотрицательных слагаемых, а значит мощность базиса и размерность пространства P_m равны

$$\dim P_m = \binom{m+D}{D}^2.$$

По лемме 6 выполнено $\ker \sigma = B \cdot P_{m-1}$, значит

$$\begin{aligned} \dim \operatorname{Im} \sigma &= \dim P_m - \dim \ker \sigma = \\ &= \dim P_m - \dim P_{m-1} = \\ &= \binom{m+D}{D}^2 - \binom{m-1+D}{D}^2. \end{aligned}$$

Учитывая, что $\binom{m+D}{D} = \frac{m+D}{D} \binom{m+D-1}{D-1}$, $\binom{m-1+D}{D} = \frac{m}{D} \binom{m+D-1}{D-1}$, имеем

$$\begin{aligned} \dim \operatorname{Im} \sigma &= \left(\left(\frac{m+D}{D} \right)^2 - \left(\frac{m}{D} \right)^2 \right) \binom{m+D-1}{D-1}^2 = \\ &= \frac{m^2 + 2mD + D^2 - m^2}{D^2} \binom{m+D-1}{D-1}^2 = \\ &= \frac{2m+D}{D} \binom{m+D-1}{D-1}^2. \end{aligned}$$

По лемме 7 выполнено $\sigma(P_m) \subseteq \mathcal{C}_{D,q,m}$, значит

$$\dim \mathcal{C}_{D,q,m} \geq \dim \operatorname{Im} \sigma \geq \frac{2m+D}{D} \binom{m+D-1}{D-1}^2. \quad \square$$

4.3. Симметрия кода $\mathcal{C}_{D,q,m}$

Автоморфизмом линейного кода $\mathcal{C} \subseteq \mathbb{F}_q^n$ называется частный случай изометрии, когда $\mathcal{C}' = \mathcal{C}$. Можно показать, что любой автоморфизм задаётся мономиальным преобразованием $\varphi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, переводящим $\mathcal{C}$ в себя.

Напомним, что $\Gamma_{D,q} = (\mathbb{P}_q^D, \mathbb{P}_q^D, E)$ — двудольный граф с множеством рёбер

$$E = \{(\alpha, \beta) \in \mathbb{P}_q^D \times \mathbb{P}_q^D \mid \langle \alpha, \beta \rangle = 0\}.$$

Код $\mathcal{C} \subseteq \mathbb{F}_q^E$ понимается как некоторое линейное множество функций $c: E \rightarrow \mathbb{F}_q$.

Каждая невырожденная матрица $A \in \operatorname{GL}(D+1, q)$ определяет проективное преобразование $\alpha \mapsto \widehat{A\alpha}$ и $\beta \mapsto \widehat{A^*\beta}$, где $A^* = (A^T)^{-1}$, $\alpha \in \mathbb{P}_q^D$, $\beta \in \mathbb{P}_q^D$. Введём отображения

$$\begin{aligned} \varphi_A &: (\alpha, \beta) \mapsto (A\alpha, A^*\beta) \\ \hat{\varphi}_A &: (\alpha, \beta) \mapsto (\widehat{A\alpha}, \widehat{A^*\beta}). \end{aligned}$$

Для любых $(\alpha, \beta) \in E$ выполнено

$$\langle A\alpha, A^*\beta \rangle = (A\alpha)^T ((A^T)^{-1}\beta) = \alpha^T A^T (A^T)^{-1} \beta = \alpha^T \beta = \langle \alpha, \beta \rangle = 0,$$

а значит и $\langle \widehat{A\alpha}, \widehat{A^*\beta} \rangle = 0$, то есть $\hat{\varphi}_A(\alpha, \beta) \in E$. Таким образом, $\hat{\varphi}_A$ задаёт автоморфизм графа $\Gamma_{D,q}$.

Покажем, что любое такое преобразование задаёт некоторый автоморфизм кода $\mathcal{C}_{D,q,m}$.

Утверждение 1. Пусть $D \geq 2$, $1 \leq m < (q-1)D$, $E = E(\Gamma_{D,q})$, $\mathcal{C} = \mathcal{C}_{D,q,m}$. Для любой матрицы $A \in \operatorname{GL}(D+1, q)$ существует набор ненулевых констант $a = (a_{(\alpha,\beta)})_{(\alpha,\beta) \in E} \in \mathbb{F}_q^E$ такой, что для любого кодового слова $c \in \mathcal{C}$ существует кодовое слово $c' \in \mathcal{C}$, удовлетворяющее условию:

$$c'(\alpha, \beta) = a_{(\alpha,\beta)} c(\widehat{A\alpha}, \widehat{A^*\beta}) \quad \text{для всех } (\alpha, \beta) \in E,$$

где $A^* = (A^T)^{-1}$.

Доказательство. Для вектора $\alpha \in \mathbb{F}_q^{D+1} \setminus \{0\}$ определим величину $\kappa(\alpha)$, равную первой ненулевой координате в векторе α . Тогда $\alpha = \kappa(\alpha)\hat{\alpha}$.

Для каждой пары $(\alpha, \beta) \in E$ положим

$$a_{(\alpha, \beta)} := (\kappa(A\alpha) \cdot \kappa(A^*\beta))^m.$$

Зафиксируем кодовое слово $c \in \mathcal{C}$ и определим c' как в условии теоремы:

$$c'(\alpha, \beta) := a_{(\alpha, \beta)} c(\widehat{A\alpha}, \widehat{A^*\beta}) \quad \text{для всех } (\alpha, \beta) \in E.$$

Покажем, что $c' \in \mathcal{C}$. Рассмотрим проекции f'_α (соотв., f'^α) функции c' на окрестности вершин α левой (соотв., правой) доли графа $\Gamma_{D,q}$, тогда

$$f'_\alpha(\beta) = c'(\alpha, \beta) = f'^\beta(\alpha) \quad \text{для всех } (\alpha, \beta) \in E.$$

Убедимся, что для всех $\alpha \in \mathbb{P}_q^D$ функции f'_α и f'^α являются кодовыми словами локальных кодов, то есть задаются однородными полиномами степени m . Зафиксируем произвольное $\alpha \in \mathbb{P}_q^D$, тогда для всех β таких, что $\langle \alpha, \beta \rangle = 0$, выполнено

$$f'_\alpha(\beta) = c'(\alpha, \beta) = a_{(\alpha, \beta)} c(\widehat{A\alpha}, \widehat{A^*\beta}) = \kappa(A\alpha)^m \cdot \kappa(A^*\beta)^m \cdot f_{\widehat{A\alpha}}(\widehat{A^*\beta}).$$

Поскольку $c \in \mathcal{C}$, то $f_{\widehat{A\alpha}}$ — однородный полином степени m , значит

$$\kappa(A^*\beta)^m \cdot f_{\widehat{A\alpha}}(\widehat{A^*\beta}) = f_{\widehat{A\alpha}}(\underbrace{\kappa(A^*\beta) \cdot \widehat{A^*\beta}}_{A^*\beta}) = f_{\widehat{A\alpha}}(A^*\beta).$$

Поскольку преобразование $x \mapsto A^*x$ задаёт линейную подстановку, то

$$\deg f'_\alpha = \deg f_{\widehat{A\alpha}}(A^*x) = \deg f_{\widehat{A\alpha}} = m.$$

Аналогично для фиксированного $\beta \in \mathbb{P}_q^D$ и всех $\alpha \in \mathbb{P}_q^D$ таких, что $\langle \alpha, \beta \rangle = 0$, получим

$$f'^\beta(\alpha) = c'(\alpha, \beta) = a_{(\alpha, \beta)} c(\widehat{A\alpha}, \widehat{A^*\beta}) = \kappa(A\alpha)^m \cdot \kappa(A^*\beta)^m \cdot f^{\widehat{A^*\beta}}(\widehat{A\alpha}).$$

Поскольку $f^{\widehat{A^*\beta}}$ является также однородным полиномом степени m , то

$$\kappa(A\alpha)^m \cdot f^{\widehat{A^*\beta}}(\widehat{A\alpha}) = f^{\widehat{A^*\beta}}(\underbrace{\kappa(A\alpha) \cdot \widehat{A\alpha}}_{A\alpha}) = f^{\widehat{A^*\beta}}(A\alpha).$$

В силу линейности преобразования $x \mapsto Ax$ имеем

$$\deg f'^\beta = \deg f^{\widehat{A^*\beta}}(Ax) = \deg f^{\widehat{A^*\beta}} = m.$$

Это означает, что c' удовлетворяет всем локальным ограничениям кода $\mathcal{C}$, значит $c' \in \mathcal{C}$. $\square$

5. Заключение

В настоящей работе была рассмотрена конструкция кодов Таннера на графе инцидентности точек и гиперплоскостей D -мерного проективного пространства $\mathbb{P}^D(\mathbb{F}_q)$, где в роли локальных проверок — проективные коды Рида–Маллера. Получены нижние оценки на минимальное расстояние таких кодов и их размерности, а также сформулирована гипотеза для более широкого диапазона параметров на основе результатов численного эксперимента.

Также было показано, что описанные коды инвариантны при действии группы $\text{PGL}(D+1, \mathbb{F}_q)$, что позволит использовать их как локальные коды при построении кодов с высокой симметрией на комплексах Рамануджана.

Список литературы

- [1] A. Lubotzky, “High dimensional expanders”, *Proceedings of the International Congress of Mathematicians (ICM 2018, Rio de Janeiro)*, **2**, World Scientific, 2019, 705–730. DOI: 10.1142/9789813272880_0027.
- [2] Г. В. Калачев, П. А. Пантелеев, “Семейство асимптотически хороших квантовых и локально тестируемых классических LDPC-кодов”, *Математические вопросы кибернетики*, Вып 21, ФИЗМАТЛИТ, М, 2023, 111–155. DOI: 10.20948/mvk-2023-111.
- [3] F. Piñero, *An algebraic approach to graph codes*, PhD thesis, Technical University of Denmark, 2015.
- [4] P. Beelen, T. Høholdt, F. Piñero, J. Justesen, “On the Dimension of Graph Codes with Reed–Solomon Component Codes”, *2013 IEEE International Symposium on Information Theory Proceedings*, IEEE, 2013, 1227–1231. DOI: 10.1109/ISIT.2013.6620422.
- [5] T. Høholdt, J. Justesen, “Graph codes with Reed–Solomon component codes”, *2006 IEEE International Symposium on Information Theory*, IEEE, 2006, 2022–2026. DOI: 10.1109/ISIT.2006.261904.
- [6] H. Janwa, A. K. Lal, “On Tanner Codes: Minimum Distance and Decoding”, *Applicable Algebra in Engineering, Communication and Computing*, **13** (2003), 335–347. DOI: 10.1007/s00200-003-0098-4.
- [7] T. Høholdt, J. Justesen, “The Minimum Distance of Graph Codes”, *Coding and Cryptology (IWCC 2011)*, Lecture Notes in Computer Science, **6639**, Springer, 2011, 201–212. DOI: 10.1007/978-3-642-20901-7_12.
- [8] I. Dinur, S. Liu, R. Y. Zhang, “New codes on high dimensional expanders”, *40th Computational Complexity Conference (CCC 2025)*, Leibniz International Proceedings in Informatics, **339**, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025, 27:1–27:42. DOI: 10.4230/LIPIcs.CCC.2025.27.
- [9] F. Rodier, “Codes from flag varieties over a finite field”, *Journal of Pure and Applied Algebra*, **178**:2 (2003), 203–214. DOI: 10.1016/S0022-4049(02)00188-3.

- [10] А. В. Чашкин, *Лекции по дискретной математике*, Физматлит, М, 2007, 416 с.
- [11] R. Tanner, “A recursive approach to low complexity codes”, *IEEE Transactions on Information Theory*, **27**:5 (1981), 533–547. DOI: 10.1109/TIT.1981.1056404.
- [12] В. А. Емельичев, О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич, *Лекции по теории графов*, Наука, М, 1990, 384 с.
- [13] A. B. Sorensen, “Projective Reed–Muller Codes”, *IEEE Transactions on Information Theory*, **37**:6 (1991), 1567–1576. DOI: 10.1109/18.104317.
- [14] M. Sipser, D. A. Spielman, “Expander codes”, *IEEE Transactions on Information Theory*, **42**:6 (1996), 1710–1722. DOI: 10.1109/18.556667.
- [15] N. Alon, J. H. Spencer, *The Probabilistic Method*, 3, John Wiley & Sons, 2008. DOI: 10.1002/9780470277331.

Приложение А. Численный эксперимент

В данном разделе приведены результаты вычисления размерности кода $\mathcal{C}_{2,q,m}$. Исходный код, который использовался в данном эксперименте, доступен по ссылке: https://github.com/Alinemsu/Tanner_matrix

Результаты подсчёта характеристик проверочных матриц и параметров кода $\mathcal{C}_{2,q,m}$ для $q \in \{2, 3, 4, 5, 7, 8, 9, 11\}$ приведены в таблице ниже.

q	m	Ранг	Размерность	Высота	Ширина
2	0	20	1	28	21
2	1	13	8	14	21
3	0	51	1	78	52
3	1	44	8	52	52
3	2	25	27	26	52
4	0	104	1	168	105
4	1	97	8	126	105
4	2	76	29	84	105
4	3	41	64	42	105
5	0	185	1	310	186
5	1	178	8	248	186
5	2	159	27	186	186
5	3	116	70	124	186
5	4	61	125	62	186
7	0	455	1	798	456
7	1	448	8	684	456

7	2	429	27	570	456
7	3	392	64	456	456
7	4	315	141	342	456
7	5	220	236	228	456
7	6	113	343	114	456
8	0	656	1	1168	657
8	1	649	8	1022	657
8	2	630	27	876	657
8	3	593	64	730	657
8	4	520	137	584	657
8	5	411	246	438	657
8	6	284	373	292	657
8	7	145	512	146	657
9	0	909	1	1638	910
9	1	902	8	1456	910
9	2	883	27	1274	910
9	3	846	64	1092	910
9	4	779	131	910	910
9	5	664	246	728	910
9	6	519	391	546	910
9	7	356	554	364	910
9	8	181	729	182	910
11	0	1595	1	2926	1596
11	1	1588	8	2660	1596
11	2	1569	27	2394	1596
11	3	1532	64	2128	1596
11	4	1471	125	1862	1596
11	5	1380	216	1596	1596
11	6	1205	391	1330	1596
11	7	1000	596	1064	1596
11	8	771	825	798	1596
11	9	524	1072	532	1596
11	10	265	1331	266	1596

Статья поступила 29 апреля 2026 г.

Bounds on the parameters of Tanner codes on the graph of projective space

A. A. Yusufova, G. V. Kalachev

This paper considers Tanner codes constructed on the incidence graph of points and hyperplanes of a projective space, with projective Reed–Muller codes as component codes. The assignment of symbols of local codes to edges is performed so that the resulting Tanner code inherits the symmetry of the projective space. Lower bounds on the minimum distance and dimension of such codes are obtained. In particular, it is shown that, for certain parameter values, these codes are asymptotically good.

Keywords: Tanner codes, incidence graph, projective space, minimum distance, code dimension.

References

- [1] A. Lubotzky, “High dimensional expanders”, *Proceedings of the International Congress of Mathematicians (ICM 2018, Rio de Janeiro)*, **2**, World Scientific, 2019, 705–730. DOI: 10.1142/9789813272880_0027.
- [2] G. V. Kalachev, P. A. Panteleev, “A family of asymptotically good quantum and locally testable classical LDPC codes”, *Matematicheskie voprosy kibernetiki*, Issue 21, FIZMATLIT, M., 2023, 111–155 (in Russian. DOI: 10.20948/mvk-2023-111).
- [3] F. Piñero, *An algebraic approach to graph codes*, PhD thesis, Technical University of Denmark, 2015.
- [4] P. Beelen, T. Høholdt, F. Piñero, J. Justesen, “On the Dimension of Graph Codes with Reed–Solomon Component Codes”, *2013 IEEE International Symposium on Information Theory Proceedings*, IEEE, 2013, 1227–1231. DOI: 10.1109/ISIT.2013.6620422.
- [5] T. Høholdt, J. Justesen, “Graph codes with Reed–Solomon component codes”, *2006 IEEE International Symposium on Information Theory*, IEEE, 2006, 2022–2026. DOI: 10.1109/ISIT.2006.261904.
- [6] H. Janwa, A. K. Lal, “On Tanner Codes: Minimum Distance and Decoding”, *Applicable Algebra in Engineering, Communication and Computing*, **13** (2003), 335–347. DOI: 10.1007/s00200-003-0098-4.
- [7] T. Høholdt, J. Justesen, “The Minimum Distance of Graph Codes”, *Coding and Cryptology (IWCC 2011)*, Lecture Notes in Computer Science, **6639**, Springer, 2011, 201–212. DOI: 10.1007/978-3-642-20901-7_12.

- [8] I. Dinur, S. Liu, R. Y. Zhang, “New codes on high dimensional expanders”, *40th Computational Complexity Conference (CCC 2025)*, Leibniz International Proceedings in Informatics, **339**, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025, 27:1–27:42. DOI: 10.4230/LIPIcs.CCC.2025.27.
- [9] F. Rodier, “Codes from flag varieties over a finite field”, *Journal of Pure and Applied Algebra*, **178**:2 (2003), 203–214. DOI: 10.1016/S0022-4049(02)00188-3.
- [10] A. V. Chashkin, *Lektsii po diskretnoi matematike*, Fizmatlit, M, 2007 (in Russian), 416 pp.
- [11] R. Tanner, “A recursive approach to low complexity codes”, *IEEE Transactions on Information Theory*, **27**:5 (1981), 533–547. DOI: 10.1109/TIT.1981.1056404.
- [12] V. A. Emelichev, O. I. Melnikov, V. I. Sarvanov, R. I. Tyshkevich, *Lektsii po teorii grafov*, Nauka, M, 1990 (in Russian), 384 pp.
- [13] A. B. Sorensen, “Projective Reed–Muller Codes”, *IEEE Transactions on Information Theory*, **37**:6 (1991), 1567–1576. DOI: 10.1109/18.104317.
- [14] M. Sipser, D. A. Spielman, “Expander codes”, *IEEE Transactions on Information Theory*, **42**:6 (1996), 1710–1722. DOI: 10.1109/18.556667.
- [15] N. Alon, J. H. Spencer, *The Probabilistic Method*, 3, John Wiley & Sons, 2008. DOI: 10.1002/9780470277331.

Received on April 29, 2026