ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 21

Г. В. Калачев,
П. А. Пантелеев

Семейство асимптотически хороших квантовых и локально тестируемых классических LDPC-кодов

Рекомендуемая форма библиографической ссылки: Калачев Г. В., Пантелеев П. А. Семейство асимптотически хороших квантовых и локально тестируемых классических LDPC-кодов // Математические вопросы кибернетики. Вып. 21. — М.: ФИЗМАТЛИТ, 2023. — С. 111–155. URL: https://library.keldysh.ru/mvk.asp?id=2023-111 DOI: 10.20948/mvk-2023-111

СЕМЕЙСТВО АСИМПТОТИЧЕСКИ ХОРОШИХ КВАНТОВЫХ И ЛОКАЛЬНО ТЕСТИРУЕМЫХ КЛАССИЧЕСКИХ LDPC-КОДОВ

Г. В. КАЛАЧЕВ, П. А. ПАНТЕЛЕЕВ

(МОСКВА)

§ 1. Введение

Классические LDPC-коды [21], а также их квантовые аналоги [42] имеют много важных приложений в теории и практике. Эти коды представлены разреженными проверочными матрицами, где термин *разреженность* обычно означает, что соответствующие графы Таннера имеют ограниченную степень вершин. Помимо многочисленных практических применений в системах хранения и передачи данных, такие коды используются для построения классических и квантовых локально тестируемых кодов [2, 18, 34], где разреженность кода обеспечивает свойство константной локальности. Неформально говоря, классический локально тестируемый код (LTC) — это код, для которого существует эффективная недетерминированная процедура, позволяющая с наперед заданной вероятностью проверить, является ли заданная последовательность битов близкой к некоторому кодовому слову, просматривая очень малое, обычно константное число случайно выбранных битов из этой последовательности. Существует несколько способов формального определения LTC [23]. В данной работе мы используем очень простое комбинаторное определение (см. [40, Definition 11]), которое подразумевает довольно сильную форму локальной тестируемости. Согласно этому определению, линейный код $\mathscr{C} \subseteq \mathbb{F}_q^n$ называется (ω, s)-*локально тестируемым*, если он имеет проверочную матрицу $H \in \mathbb{F}_q^{m \times n}$ со строками веса не более ω такую, что для любого вектора $x \in \mathbb{F}_q^n$ имеем

$$\frac{1}{m}|Hx| \geqslant \frac{s}{n} d(x, \mathscr{C}),$$

где $d(x, \mathscr{C}) := \min\limits_{c \in \mathscr{C}} d(x, c)$. Здесь $d(\cdot, \cdot)$ — расстояние Хэмминга, а $|\cdot|$ — вес Хэмминга. Параметры ω и s — положительные вещественные числа, называемые *локальность* и *корректность* соответственно. Как мы уже упоминали выше, это определение подразумевает сильную форму локальной тестируемости. Действительно, если наша процедура тестирования выбирает равномерно случайным образом строку матрицы H и находит соответствующую компоненту синдрома, то вероятность непрохождения теста

DOI: 10.20948/mvk-2023-111

$\mathrm{rej}_H(x) = \frac{1}{m}|Hx|$ возрастает, по крайней мере, линейно с ростом относительного минимального расстояния $\frac{1}{n}d(x, \mathscr{C})$ от проверяемого вектора $x \in \mathbb{F}_q^n$ до кода $\mathscr{C}$. Заметим, что для любого семейства LDPC-кодов с $m = \Theta(n)$, где веса строк и столбцов в H ограничены сверху константой ω (такие коды называются *ω-ограниченными*), следует, что $\frac{1}{m}|Hx|$ не может расти *более* чем линейно с ростом $\frac{1}{n}d(x, \mathscr{C})$, поскольку для каждого $x \in \mathbb{F}_q^n$ мы получаем $|Hx| \leqslant \omega \cdot d(x, \mathscr{C})$.

В случае квантовых локально тестируемых кодов (qLTC), введенных в работе [2], можно дать подобное вышеприведенному определение, если разреженную проверочную матрицу H заменить локальным гамильтонианом $\mathscr{H}$, определяющим квантовый код. Однако для квантового CSS кода $\mathscr{Q}$ (см. [10, 51]), полученного из пары классических кодов $\mathscr{C}_X$ и $\mathscr{C}_Z$, можно [2, 40] вывести локальную тестируемость $\mathscr{Q}$ из локальной тестируемости $\mathscr{C}_X$ и $\mathscr{C}_Z$. Напомним, что квантовый CSS код $\mathscr{Q}$ *размерности* k определяется парой классических линейных кодов $\mathscr{C}_X, \mathscr{C}_Z \subseteq \mathbb{F}_q^n$ таких, что $\mathscr{C}_Z^\perp \subseteq \mathscr{C}_X$, и $k = \dim \mathscr{C}_X/\mathscr{C}_Z^\perp$. Его *минимальное расстояние* d определяется как $\min(d_X, d_Z)$, где d_X и d_Z — минимальные веса Хэмминга для векторов из $\mathscr{C}_X \setminus \mathscr{C}_Z^\perp$ и $\mathscr{C}_Z \setminus \mathscr{C}_X^\perp$ соответственно. В этом случае мы, как правило, говорим, что $\mathscr{Q}$ является $[\![n, k, d]\!]_q$ кодом. Коды $\mathscr{C}_X$ и $\mathscr{C}_Z$ обычно представляются соответственно проверочными матрицами H_X и H_Z, а условие $\mathscr{C}_Z^\perp \subseteq \mathscr{C}_X$ эквивалентно $H_X H_Z^* = 0$, где H_Z^* — транспонированная матрица H_Z. В [40, Lemma 13] было показано, что если CSS-код $\mathscr{Q}$ определяется двумя классическими (ω, s)-локально тестируемыми кодами с проверочными матрицами H_X и H_Z, то квантовый код $\mathscr{Q}$ является (ω, s')-локально тестируемым, где $s' := s \min\left(\frac{m_X}{m_X + m_Z}, \frac{m_Z}{m_X + m_Z}\right)$, а m_X (соответственно m_Z) — число строк в матрице H_X (соответственно H_Z).

Классические и квантовые LTC имеют много интересных приложений в теоретической информатике, поскольку они тесно связаны с рядом важных проблем в теории сложности [2, 17]. Основной открытой проблемой, также известной как *c^3-гипотеза* (в контексте классических кодов [14]) и *qLTC-гипотеза* (в квантовом случае [2]), является вопрос о том, существуют ли такие коды с *константной* локальностью ω, *константной* скоростью и *линейным* минимальным расстоянием. В этом отношении ситуация для классических LTC намного лучше, чем для их квантовых аналогов, поскольку классические LTC с почти оптимальными параметрами известны уже давно [22]. Однако в квантовом случае, даже если свойство локальной тестируемости не требуется, все еще остается открытая проблема, известная как *qLDPC-гипотеза* [8] о существовании *асимптотически хорошего* семейства квантовых LDPC-(qLDPC)-кодов*), т. е. кодов с постоянной скоростью и линейным минимальным расстоянием. До самого последнего времени [7, 27, 28, 48] лучшие доказуемые нижние оценки минимального расстояния qLDPC-кодов были не более $\sqrt{n}$ с точностью до полилогарифмических множителей при числе кубитов $n \to \infty$ [13, 19, 20, 24, 32, 54]. В то же время асимптотически хорошие семейства классических LDPC-кодов известны с момента их введения Робертом Галлагером в 1960-х годах [21].

*) Заметим, что при выходе за рамки стандартного определения квантового LDPC-кода уже было известно о существовании кодов с очень хорошими параметрами [3, 5].

В данной работе мы доказываем существование классических LTC с постоянной скоростью, постоянной локальностью и линейным минимальным расстоянием. В частности, мы доказываем следующую теорему, которая дает положительный ответ на c^3-гипотезу. Напомним, что классический линейный код $\mathscr{C} \subseteq \mathbb{F}_q^n$ имеет параметры $[n, k, d]_q$, если $k = \dim \mathscr{C}$ и $d = \min\limits_{c \in \mathscr{C} \setminus \{0\}} |c|$.

Теорема 1. *Для любого $R \in (0, 1/2)$ и конечного поля $\mathbb{F}_q$ можно найти универсальные константы s и ω такие, что существует явное семейство (ω, s)-локально тестируемых классических LDPC-кодов с параметрами $[n, k \geqslant Rn, d = \Theta(n)]_q$ при $n \to \infty$.*

В квантовом случае мы доказали существование асимптотически хороших семейств qLDPC-кодов, необязательно локально тестируемых. Это дает утвердительный ответ на гипотезу qLDPC, оставляя открытым вопрос о существовании qLTC.

Теорема 2. *Для любого $R \in (0, 1)$ и конечного поля $\mathbb{F}_q$ существует явное семейство квантовых LDPC-кодов над $\mathbb{F}_q$ с параметрами $[\![n, k \geqslant Rn, d = \Theta(n)]\!]_q$ при $n \to \infty$.*

Замечание 1. Для классических кодов из Теоремы 1 относительно легко показать, что алгоритм, подобный алгоритму переключения битов (англ. bit-flipping algorithm), исправляет за линейное время любую ошибку веса вплоть до константной доли длины кода. Недавно, после опубликования препринта этой статьи, было показано [37,38], что для квантовых кодов из теоремы 2 это также возможно с использованием варианта алгоритма переключения малых подмножеств битов (англ. small-set-flip algorithm) из [39] (см. также [19]).

Коды из двух вышеприведенных теорем получены с помощью недавно введенной конструкции поднятого произведения [48], которую можно рассматривать как обобщение конструкции (тензорного) произведения для классических кодов [4, 43] и конструкции гиперграфового произведения для получения квантовых кодов из двух классических [53]. Похожее обобщение было также независимо предложено в работе [7], где была показана ее связь с операцией сбалансированного произведения из топологии. Перечисленные выше конструкции естественным образом формулируются в терминах гомологической алгебры как тензорное произведение модулей над групповой алгеброй*).

1.1. Цепные комплексы и коды. В последние годы идеи гомологической алгебры нашли много интересных приложений в области классических и квантовых кодов [6, 31, 49]. Кратко напомним, что *цепной комплекс* — это абелева группа $\mathscr{C} = \bigoplus\limits_{i \in \mathbb{Z}} \mathscr{C}_i$ с некоторым фиксированным морфизмом $\partial\colon \mathscr{C} \to \mathscr{C}$, называемым *оператором границы* таким, что $\partial^2 = 0$ и $\partial \mathscr{C}_i \subseteq \mathscr{C}_{i-1}$ для всех $i \in \mathbb{Z}$. Комплекс $(\mathscr{C}, \partial)$ обычно представляется последовательностью

$$\ldots \xrightarrow{\partial_{i+1}} \mathscr{C}_i \xrightarrow{\partial_i} \mathscr{C}_{i-1} \xrightarrow{\partial_{i-1}} \ldots$$

*) В этом тексте мы предполагаем, что читатель знаком со стандартными понятиями гомологической алгебры, такими как (ко)цепной комплекс и группы (ко)гомологий. Краткое введение в эту тему см. в [9].

абелевых групп $\mathscr{C}_i$ и морфизмов*) $\partial_i := \partial|_{\mathscr{C}_i} \colon \mathscr{C}_i \to \mathscr{C}_{i-1}$ таких, что $\partial_i \circ \partial_{i+1} = 0$ для всех $i \in \mathbb{Z}$. Пространство $\mathscr{C}_i$ в комплексе $\mathscr{C}$ называется группой i-*цепей*. Утверждение $\partial_i \circ \partial_{i+1} = 0$ эквивалентно $\operatorname{im} \partial_{i+1} \subseteq \ker \partial_i$, что позволяет нам рассматривать для каждого $i \in \mathbb{Z}$ факторгруппу $H_i(\mathscr{C}) = \ker \partial_i / \operatorname{im} \partial_{i+1}$, называемую i-*й группой гомологий* комплекса $\mathscr{C}$. Элементы из $Z_i(\mathscr{C}) := \ker \partial_i$ и $B_i(\mathscr{C}) := \operatorname{im} \partial_{i+1}$ называются i-*циклами* и i-*границами* из $\mathscr{C}$ соответственно. Абелевы группы в комплексе часто имеют некоторую дополнительную алгебраическую структуру, которая делает их векторными пространствами над полем $\mathbb{F}$ или модулями над кольцом R, и в этом случае предполагается, что все операторы границы являются линейными над данным полем или кольцом.

В контексте помехоустойчивых кодов нас интересуют цепные комплексы $\mathscr{C}$ над $\mathbb{F}_q$ с τ ненулевыми членами (τ-*членные* комплексы), где каждый член $\mathscr{C}_i$ имеет выделенный базис $X_i \subseteq \mathscr{C}_i$ над $\mathbb{F}_q$, элементы которого называются i-*клетками*. Во многих случаях удобно рассматривать i-цепи $c \in C_i$ как формальные $\mathbb{F}_q$-линейные комбинации

$$c = \sum_{x \in X_i} c_x x$$

i-клеток и отождествлять $\mathscr{C}_i$ с $\mathbb{F}_q^{n_i}$, где $n_i := |X_i|$. Заметим, что любое пространство формальных линейных комбинаций $\mathbb{F}_q S \cong \mathbb{F}_q^{|S|}$ снабжено стандартным *скалярным произведением* $\langle a, b \rangle := \sum_{s \in S} a_s b_s$ и *нормой Хэмминга* $|a| := |\operatorname{supp} a|$, где $\operatorname{supp} a := \{s \in S \mid a_s \neq 0\}$. Обычно мы интерпретируем члены таких цепных комплексов либо как пространство кодовых слов, либо как пространство синдромов линейного кода.

Удобно рассматривать множество $X = \bigsqcup_i X_i$ как градуированное множество, называемое *клеточным посетом* (англ. cell poset) комплекса $\mathscr{C} = \mathbb{F}_q X$. Пусть P является посетом с частичным порядком $\leqslant$. На множестве P можно ввести *отношение покрытия* $\prec$, где $a \prec b$ (эквивалентная запись $b \succ a$) для $a, b \in P$ тогда и только тогда, когда $a < b$ и нет элемента $c \in P$ такого, что $a < c < b$. Легко видеть, что любой конечный посет может быть однозначно определен отношением покрытия $\prec$, если положить $a \leqslant b$ тогда и только тогда, когда существует последовательность $c_0 \prec c_1 \prec \ldots \prec c_n$ элементов из P таких, что $c_0 = a$, $c_n = b$, и $n \geqslant 0$. Мы можем определить частичный порядок $\leqslant$ на выделенном базисе X, если для любых двух клеток $x, x' \in X$ положим $x' \prec x$ тогда и только тогда, когда $x' \in \operatorname{supp} \partial x$. Мы называем множество X с отношением $\leqslant$ *клеточным посетом* $\mathscr{C}$. Этот посет является *градуированным*, так как имеет естественную *функцию ранга* $\rho \colon X \to \mathbb{Z}$, определенную как $\rho(x) := i$, если $x \in X_i$, а множества X_i называются *уровнями* X. Во многих случаях элементы X можно интерпретировать как некоторые геометрические объекты (точки, ребра и т.д.), а градуировка соответствует их размерности.

Замечание 2. В этой работе мы также рассматриваем неориентированный граф Γ как градуированный посет с уровнями $V(\Gamma)$ и $E(\Gamma)$, где для каждого $v \in V(\Gamma)$ и $e \in E(\Gamma)$ мы имеем $v \prec e$ всегда, когда v инцидентно e.

*) Иногда, когда это не вызывает путаницы, мы опускаем индексы в отображениях ∂_i и просто пишем ∂ вместо ∂_i.

Фактически двухуровневые посеты эквивалентны *системам инцидентности* и поэтому могут быть использованы для представления неориентированных мультиграфов и гиперграфов.

Мы можем визуализировать τ-членный комплекс $\mathscr{C}$ с помощью τ-дольного графа $\mathscr{T}$, называемого *графом Таннера*, где X_i — множество вершин i-й доли, и у нас есть ребро (x, x'), помеченное элементом $a = \langle x', \partial x\rangle \in \mathbb{F}_q$ всякий раз, когда $x \succ x'$. Легко видеть, что $\mathscr{T}$ — это просто диаграмма Хассе клеточного посета X.

Рассмотрим несколько примеров. Во-первых, мы можем отождествить 2-членный цепной комплекс

$$\mathbb{F}_q^n \xrightarrow{\partial_1} \mathbb{F}_q^m$$

с классическим линейным кодом $\ker \partial_1$, определяемым *проверочной матрицей* $H := \partial_1$. Здесь пространство 1-цепей $\mathbb{F}_q^n$ соответствует n битам, а пространство 0-цепей $\mathbb{F}_q^m$ — m проверкам. В то же время, 3-членный цепной комплекс

$$\mathscr{C} := \left(\mathbb{F}_q^{m_Z} \xrightarrow{\partial_2} \mathbb{F}_q^n \xrightarrow{\partial_1} \mathbb{F}_q^{m_X}\right)$$

можно естественно отождествить с квантовым CSS $[\![n, k, d]\!]_q$ кодом $\mathscr{Q} = \mathscr{Q}(H_X, H_Z)$, определяемым проверочными матрицами $H_X := \partial_1$ и $H_Z := \partial_2^*$, где $\partial_2^*\colon \mathbb{F}_q^n \to \mathbb{F}_q^{m_Z}$ — транспонированные матрицы операторов границ $\partial_2\colon \mathbb{F}_q^{m_Z} \to \mathbb{F}_q^n$. В этом случае пространство 1-клеток $\mathbb{F}_q^n$ соответствует n кубитам, а пространство 0-клеток $\mathbb{F}_q^{m_X}$ (соответственно пространство 2-клеток $\mathbb{F}_q^{m_Z}$) — *X-проверкам* (соответственно *Z-проверкам*). Длина кода $\mathscr{Q}$ равна $n = \dim \mathbb{F}_q^n$, а размерность k равна размерности первой гомологической группы $H_1(\mathscr{C}) := \ker \partial_1 / \operatorname{im} \partial_2 = \mathscr{C}_X / \mathscr{C}_Z^{\perp}$, где $\mathscr{C}_X := \ker \partial_1$ и $\mathscr{C}_Z := \ker \partial_2^*$. Минимальное расстояние $d = d(\mathscr{Q})$ также может быть описано на языке гомологических групп, если мы рассмотрим векторное пространство $H_1(\mathscr{C})$ как метрическое пространство, где расстояние $d(A, B)$ между гомологическими классами $A, B \in H_1(\mathscr{C})$ определяется как $d(A, B) := |A - B|$ с использованием нормы Хэмминга $|A| := \min\limits_{a \in A} |a|$. Легко видеть, что $d = \min(d(H_1(\mathscr{C}), d(H_1(\mathscr{C}^*))$, где

$$\mathscr{C}^* := \left(\mathbb{F}_q^{m_X} \xrightarrow{\partial_1^*} \mathbb{F}_q^n \xrightarrow{\partial_2^*} \mathbb{F}_q^{m_Z}\right) \text{ —}$$

это *двойственный цепной комплекс* для $\mathscr{C}$. Заметим, что расстояния $d(H_1(\mathscr{C}))$ и $d(H_1(\mathscr{C}^*))$ иногда называют *1-систолическим* и *1-косистолическим расстояниями* для $\mathscr{C}$.

1.2. Поднятое произведение. В этой работе мы рассматриваем несколько новых семейств классических и квантовых LDPC-кодов с постоянной скоростью, основанных на недавно введенной конструкции поднятого произведения [48], которая обобщает многие известные конструкции квантовых LDPC-кодов [25, 26, 36, 42, 49, 53]. Основная идея поднятого произведения в его общем виде (см. [48, с. 3]) заключается в расширении стандартного тензорного произведения $\mathscr{A} \otimes_{\mathbb{F}_q} \mathscr{B}$ двух цепных комплексов $\mathscr{A}$ и $\mathscr{B}$ над $\mathbb{F}_q$ на более общее произведение $\mathscr{A} \otimes_R \mathscr{B}$, где $\mathscr{A}$, $\mathscr{B}$ — свободные

R-модули*), а $R=\mathbb{F}_qG$ — это групповая алгебра**) над $\mathbb{F}_q$ для некоторой конечной группы G.

Идея поднятого произведения была использована недавно в работе [48] для получения первого семейства qLDPC-кодов с почти линейным расстоянием. В последующей работе [7], где некоторые идеи из [48] были развиты независимо, очень похожая конструкция под названием *сбалансированное произведение* была использована для получения qLDPC-кодов с очень большими расстояниями***). Как и в случае поднятого произведения, сбалансированное произведение двух цепных комплексов $\mathscr{A}$ и $\mathscr{B}$ также можно рассматривать как тензорное произведение цепных комплексов $\mathscr{A}\otimes_R\mathscr{B}$ над групповой алгеброй $R=\mathbb{F}_qG$, но на этот раз $\mathscr{A}$ и $\mathscr{B}$ являются произвольными (т.е. необязательно свободными) R-модулями. Как было показано в работе [7], поднятое произведение и сбалансированное произведение можно рассматривать как частные случаи еще более общей топологической идеи, называемой *локально тривиальным расслоением*, предложенной в качестве способа построения qLDPC-кодов в прорывной работе [27], которая впервые преодолела порог $n^{1/2}\mathrm{polylog}(n)$ в нижних оценках расстояния qLDPC-кодов. Интересно также отметить, что коды, которые фактически были использованы для получения основных результатов в работах [7, 27, 48], относятся к более ограниченному классу кодов на основе поднятого произведения, которые ранее были изучены в работе [47] под названием GHP-коды, где было показано, что они удивительно хорошо работают на практике при использовании BP-OSD-декодера.

Пусть R — конечномерная алгебра над $\mathbb{F}_q$. Мы говорим, что векторное пространство V является *свободным R-модулем ранга n*, если $V\cong R^n$.

О п р е д е л е н и е 1. Пусть G — конечная группа. Рассмотрим два цепных комплекса $\mathscr{A}=\bigoplus\limits_{i=0}^{m}\mathscr{A}_i$ и $\mathscr{B}=\bigoplus\limits_{j=0}^{n}\mathscr{B}_j$ над $\mathbb{F}_q$ такие, что векторные пространства $\mathscr{A}_i$ и $\mathscr{B}_j$ также являются свободными R-модулями****) для $R=\mathbb{F}_qG$ и операторы границ $\partial_{\mathscr{A}}\colon\mathscr{A}\to\mathscr{A}$, $\partial_{\mathscr{B}}\colon\mathscr{B}\to\mathscr{B}$ также являются R-линейными. *Поднятое произведение* $\mathscr{A}$ и $\mathscr{B}$ над R — это комплекс, являющийся их *тензорным произведением* $\mathscr{A}\otimes_R\mathscr{B}$ (см. [9, p. 7]), где для $k=0,1,\ldots,m+n$ пространство k-цепей $(\mathscr{A}\otimes_R\mathscr{B})_k$ равно $\bigoplus\limits_{i+j=k}\mathscr{A}_i\otimes_R\mathscr{B}_j$, а оператор границы $\partial\colon\mathscr{A}\otimes_R\mathscr{B}\to\mathscr{A}\otimes_R\mathscr{B}$ определен для $a\in\mathscr{A}_i$, $b\in\mathscr{B}_j$ как*****)

$$\partial(a\otimes_R b):=\partial_{\mathscr{A}}a\otimes_R b+(-1)^i a\otimes_R\partial_{\mathscr{B}}b \tag{1}$$

*) Общее определение *тензорного произведения комплексов* $\mathscr{A}\otimes_R\mathscr{B}$ над произвольным кольцом R можно найти в работе [9, p. 7].

**) Элементами $\mathbb{F}_qG$ являются формальные суммы $\sum\limits_{g\in G}\alpha_g g$, где $\alpha_g\in\mathbb{F}_q$. Для элементов $a=\sum\limits_{g\in G}\alpha_g g$ и $b=\sum\limits_{g\in G}\beta_g g$ из $\mathbb{F}_qG$ их сумма $a+b$ и произведение ab определяются следующим образом: $a+b:=\sum\limits_{g\in G}(\alpha_g+\beta_g)g$, $\quad ab:=\sum\limits_{g\in G}\left(\sum\limits_{hr=g}\alpha_h\beta_r\right)g$.

***) Заметим, что коды из [48] являются кодами CSS, в то время как коды из [7] в целом относятся к более широкому классу квантовых кодов, называемых *подсистемными кодами*.

****) Если G неабелева, то далее мы предполагаем, что $R=\mathbb{F}_qG$ действует справа на $\mathscr{A}$ и слева на $\mathscr{B}$, т.е. $\mathscr{A}$ — правый свободный R-модуль, а $\mathscr{B}$ — левый свободный R-модуль.

*****) Надо отметить, что знак $(-1)^i$ в этом определении имеет значение только в случае конечных полей нечетной характеристики.

и расширяется по линейности на все пространство $\mathscr{A}_i \otimes \mathscr{B}_j$. Когда в пространствах $\mathscr{A}_i$ и $\mathscr{B}_j$ имеются выделенные базисы X_i и Y_j (над $\mathbb{F}_q$), мы предполагаем, что G действует свободно*) на них. В таких случаях, по определению, поднятое произведение $\mathscr{A} \otimes_R \mathscr{B}$ имеет выделенный базис (над $\mathbb{F}_q$), заданный следующим образом:

$$X \times_G Y := \{x \otimes_R y \mid x \in X, y \in Y\},$$

где $X := \bigsqcup_i X_i$, $Y := \bigsqcup_j Y_j$.

На самом деле, поднятое произведение также может быть использовано с произвольной конечномерной ассоциативной алгеброй R над $\mathbb{F}_q$, необязательно равной $\mathbb{F}_q G$. В настоящей работе мы рассматриваем только случай $R = \mathbb{F}_q G$. Обозначим комплекс $\mathscr{A} \otimes_R \mathscr{B}$ через $\mathscr{A} \otimes_G \mathscr{B}$ и $a \otimes_R b$ через $a \otimes_G b$, что согласуется с обозначениями из [7]. Заметим, что условие, что векторное пространство является свободным $\mathbb{F}_q G$-модулем, эквивалентно условию, что оно имеет базис над $\mathbb{F}_q$, на котором группа G действует свободно. Более того, отображение является $\mathbb{F}_q G$-линейным в точности тогда, когда это $\mathbb{F}_q$-линейное отображение, коммутирующее с действием группы G.

Поскольку множество $X \times_G Y$ из определения 1 является клеточным посетом для $\mathscr{A} \otimes_G \mathscr{B}$, оно также имеет частичный порядок. Для наших целей удобно определить множество $X \times_G Y$ для произвольных конечных множеств X и Y со свободным действием G. Скажем, что группа G *действует* на посете P, если она действует на P как на множестве, и для каждого $g \in G$, если $x \leqslant y$, то $gx \leqslant gy$ (или $xg \leqslant yg$ в случае правого действия). Легко видеть, что действие группы на графе $\Gamma = (V, E)$ также является действием на графе Γ как на 2-уровневом посете. Посет с действующей на нем группой G будем называть *G-посетом*.

Замечание 3. Для любого множества S с левым действием $(g, s) \mapsto g \cdot s$ (соотв. правым действием $(s, g) \mapsto s \cdot g$) группы G мы также можем рассмотреть соответствующее правое (соотв. левое) действие G, определенное как $(s, g) \mapsto g^{-1} \cdot s$ (или $(g, s) \mapsto s \cdot g^{-1}$). Поэтому если группа G имеет правое свободное действие на цепном комплексе $\mathscr{C}$, то она также имеет соответствующее левое свободное действие на $\mathscr{C}$, и наоборот. Это позволяет нам применять поднятое произведение $\mathscr{A} \otimes_G \mathscr{B}$ к двум правым G-модулям $\mathscr{A}$ и $\mathscr{B}$, если мы используем соответствующее левое действие G на $\mathscr{B}$.

Напомним, что если мы имеем свободное действие группы G на множестве S, то размер каждой орбиты равен $|G|$ и мы можем отождествить S с $(S/G) \times G$, где S/G — множество всех орбит под действием G. Важно ответить, что это множество не зависит от того, рассматривается ли левое или соответствующее ему правое действие. Если конечная группа G действует на посете S, то на множестве S/G естественным образом также определена структура посета, если для $A, B \in S/G$ мы положим, что $A \leqslant B$, если $x \leqslant y$ для некоторых $x \in A$, $y \in B$. Рефлексивность и транзитивность для посета S/G легко выводится из рефлексивности и транзитивности для посета $\leqslant_S$, а для доказательства антисимметричности необходимо также

*) *Левое* (соотв. *правое*) действие группы G множестве S называется *свободным*, если для каждого $g \in G$, когда мы имеем $gs = s$ (соотв. $sg = s$) для некоторого $s \in S$, то g является тождественным элементом G.

использовать условие конечности G. Действительно, если G конечно, то любые два различных элемента из одной орбиты из S/G будут несравнимы, поскольку в противном случае мы бы имели $x < gx$ для некоторого элемента x из этой орбиты, что влекло бы противоречие $x < gx < g^2x < \ldots < g^{|G|}x = x$. Тогда из $A < B$ и $B < A$ следовало бы $x < y$ и $y < gx$ для некоторых $x \in A$, $y \in B$ и $g \in G$, влекшее за собой $x < gx$, чего, как мы только что показали, быть не может.

Напомним, что *прямым произведением* посетов X и Y называется посет $X \times Y$, где $(x, y) \leqslant (x', y')$, если $x \leqslant_X x'$ и $y \leqslant_Y y'$. В дальнейшем нам понадобится естественное обобщение этого определения на случай G-посетов.

О п р е д е л е н и е 2. Рассмотрим конечную группу G, действующую справа на множестве X и слева на множестве Y. Их *сбалансированным произведением* называется посет $(X \times Y)/G$, где группа G действует антидиагонально на прямом произведении посетов $X \times Y$, т. е. как $(x, y) \mapsto (xg, g^{-1}y)$.

Заметим, что если действие G свободно, то посет $X \times_G Y$ как множество можно отождествить с $(X/G) \times G \times (Y/G)$. При этом отношение покрытия $\succ$ на нем задается следующим образом: $(x, g, y) \succ (x', g', y')$ тогда и только тогда, когда либо $x = x'$ и $(y, g) \succ_Y (y', g')$, либо $(x, g) \succ_X (x', g')$ и $y = y'$. Если $|G| = 1$, то очевидно, что $X \times_G Y = X \times Y$.

Нетрудно проверить, используя (1), что если $\mathscr{A}$ и $\mathscr{B}$ — комплексы с клеточными посетами X и Y, то клеточный посет $\mathscr{A} \otimes_G \mathscr{B}$ совпадает с тем, который дан в определении 2. Более того, базис для пространства k-цепей $(\mathscr{A} \otimes_R \mathscr{B})_k$ соответствует множеству $\bigsqcup_{i+j=k} X_i \times_G Y_j$.

З а м е ч а н и е 4. Если множества X и Y представляют собой клеточное разбиение некоторых топологических пространств M и N, то $X \times_G Y$ представляет собой клеточное разбиение их сбалансированного произведения*) $M \times_G N$ (см. [7]).

Для двух заданных классических линейных кодов, инвариантных относительно свободного действия группы G на их индексных множествах**), мы можем представить их как 2-членные цепные комплексы $\mathscr{A}\colon R^{n_a} \xrightarrow{A} R^{m_a}$ и $\mathscr{B}\colon R^{n_b} \xrightarrow{B} R^{m_b}$ над групповой алгеброй $R = \mathbb{F}_q G$, где $A \in R^{m_a \times n_a}$, $B \in R^{m_b \times n_b}$ — соответствующие проверочные матрицы***). Поднятое произведение $\mathscr{C} = \mathscr{A} \otimes_G \mathscr{B}$ является 3-членным комплексом

$$R^{n_a \times n_b} \xrightarrow{\partial_2} R^{n_a \times m_b} \oplus R^{m_a \times n_b} \xrightarrow{\partial_1} R^{m_a \times m_b}$$

с оператором границы $\partial\colon \mathscr{C} \to \mathscr{C}$, заданным следующей диаграммой:

$$\begin{array}{ccc} R^{n_a \times m_b} & \xrightarrow{A \otimes_R \mathrm{id}} & R^{m_a \times m_b} \\ {\scriptstyle -\mathrm{id} \otimes_R B}\uparrow & & \uparrow{\scriptstyle \mathrm{id} \otimes_R B} \\ R^{n_a \times n_b} & \xrightarrow[A \otimes_R \mathrm{id}]{} & R^{m_a \times n_b} \end{array},$$

*) *Сбалансированное произведение* двух топологических пространств X и Y с группой G, действующей непрерывными преобразованиями справа на X и слева на Y, является фактор-пространством $X \times_G Y := (X \times Y)/G$, где G действует антидиагонально.

**) Классический линейный код $\mathscr{C} \subseteq \mathbb{F}_q^n$ является *инвариантным* относительно действия группы G на индексном множестве $[n]$, если для всех $g \in G$ из $(c_i)_{i \in [n]} \in \mathscr{C}$ следует, что $(c_{\pi_g(i)})_{i \in [n]} \in \mathscr{C}$, где π_g — перестановка, соответствующая действию g на $[n]$.

***) Если G неабелева, то при умножении вектора над $R = \mathbb{F}_q G$ на матрицу A (соотв. B) мы предполагаем, что умножаем на элементы из R справа (соотв. слева).

что означает, что $\partial_2 := \left[\begin{smallmatrix} -\mathrm{id}\otimes_R B \\ A\otimes_R \mathrm{id}\end{smallmatrix}\right]$, $\partial_1 := [A\otimes_R \mathrm{id}, \mathrm{id}\otimes_R B]$. Можно легко проверить, что $\partial_1\circ\partial_2 = A\otimes_R B - A\otimes_R B = 0$, и $\mathscr{C}$ действительно является цепным комплексом. Теперь мы можем рассмотреть классический код $\ker\partial_2$ с проверочной матрицей ∂_2 и квантовый CSS-код $\mathscr{Q}(\partial_1, \partial_2^*)$, где $\mathscr{C}_X := \ker\partial_1$ и $\mathscr{C}_Z := \ker\partial_2^*$. Мы можем естественно отождествить эти коды со второй гомологической группой $H_2(\mathscr{C})$ и первой гомологической группой $H_1(\mathscr{C})$ комплекса $\mathscr{C}$ и использовать их для получения классических кодов из теоремы 1 и квантовых кодов из теоремы 2 соответственно. Заметим, что когда G является тривиальной группой, т. е. $|G| = 1$, то $R\cong\mathbb{F}_q$ и можно видеть, что $\ker\partial_2$ и $\mathscr{Q}(\partial_1, \partial_2^*)$ являются соответственно тензорным произведением и гиперграфовым произведением двух классических кодов $\ker A$ и $\ker B$. Следовательно, поднятое произведение комплексов $\mathscr{A}\otimes_G\mathscr{B}$, который мы также иногда обозначаем $\mathrm{LP}(A, B)$, можно рассматривать как обобщение этих двух конструкций, где вместо отдельных символов из $\mathbb{F}_q$ мы имеем блоки символов размера $|G|$, представленные элементами из $\mathbb{F}_qG\cong\mathbb{F}_q^{|G|}$.

1.3. Поднятые коды Таннера и их произведения. Очень важной составляющей конструкций из [7, 48] являются экспандерные коды [50], которые представляют собой коды Таннера [52], полученные из спектральных экспандеров. Отдельные символы экспандерного кода $\mathscr{T}(\Gamma; h)$, определенного для w-регулярного графа Γ и проверочной матрицы $h\in\mathbb{F}_q^{r\times w}$, присваиваются ребрам Γ, и мы получаем кодовое слово в точности тогда, когда для каждой вершины v из Γ символы на ребрах, инцидентных вершине v, дают кодовое слово *локального кода* $\ker h$.

Обычно мы отождествляем код $\mathscr{T}(\Gamma; h)$ с комплексом

$$\mathbb{F}_qE(\Gamma)\xrightarrow{\partial}\mathbb{F}_q^rV(\Gamma),$$

где ∂ — его проверочная матрица. Здесь $\mathbb{F}_qE(\Gamma)\cong\mathbb{F}_q^{|E(\Gamma)|}$ и $\mathbb{F}_q^rV(\Gamma)\cong\mathbb{F}_q^{r|V(\Gamma)|}$ — соответственно пространства формальных линейных комбинаций ребер (над $\mathbb{F}_q$) и вершин (над $\mathbb{F}_q^r$), которые мы также можем рассматривать как векторные пространства над $\mathbb{F}_q$.

В [48] графы-экспандеры Γ получаются как *G-поднятия* (т.е. регулярные $|G|$-кратные накрытия) некоторых малых базовых графов, где G — очень большая группа*).

О п р е д е л е н и е 3. (Левое) *G-поднятие базового графа***) Γ с некоторым фиксированным порядком $<$ вершин является графом $\widehat{\Gamma}$, полученным из Γ, если заменить каждую вершину $v\in V(\Gamma)$ на $|G|$ ее копий $\widehat{v}_g$, $g\in G$, и заменить каждое ребро $e\in E(\Gamma)$, соединяющее вершины $v, v'\in V(\Gamma)$, где $v<v'$, на $|G|$ его копий $\widehat{e}_g$, $g\in G$, таких, что: $\widehat{e}_g$ соединяет в $\widehat{\Gamma}$ вершины $\widehat{v}_g$ и $\widehat{v}'_{sg}$, где $s = s(v, v')\in G$.

На каждом G-поднятом (слева) графе $\widehat{\Gamma}$ естественным образом определено свободное правое действие, определенное как $\widehat{v}_g\cdot h := \widehat{v}_{gh}$, $\widehat{e}_g\cdot h := e_{gh}$ для $h\in G$. Нетрудно сделать полученные таким образом коды Таннера $\mathscr{T}(\Gamma; h)$ инвариантными относительно свободного действия G (мы называем

*) В [48] эта общая идея была применена к циклическим группам для получения основного результата.

**) В данной работе мы допускаем, что в базовом графе Γ есть кратные ребра, но *нет* петель.

их G-*поднятыми*). Класс таких G-поднятых кодов Таннера для заданного G-поднятого графа $\widehat{\Gamma}$ и проверочной матрицы h обозначим через $\mathfrak{T}_G(\Gamma; h)$. Поэтому такие коды могут быть использованы в операции поднятого произведения для получения 3-членного цепного комплекса $\mathscr{C}$, который также можно рассматривать как квантовый CSS-код.

В [48, Example 3] показано, что, используя поднятое произведение двух классических кодов, можно получить qLDPC-коды постоянной скорости*). В частности, если $\rho := 1 - m/n$ — нижняя оценка скорости классического кода $\ker A$, представленного комплексом $\mathscr{A} := R^n \xrightarrow{A} R^m$, то скорость квантового кода, представленного комплексом $\mathscr{A} \otimes_G \mathscr{A}^*$, не меньше $\dfrac{(n-m)^2}{n^2+m^2} = \dfrac{\rho^2}{1+(1-\rho)^2}$. Здесь $\mathscr{A}^* := R^m \xrightarrow{A^*} R^n$ — это *двойственный цепной комплекс* для $\mathscr{A}$, т. е. A^* — это транспонированная проверочная матрица A, рассматриваемая как матрица над $\mathbb{F}_q$. Следовательно, скорость квантовых кодов, полученных из $\mathscr{A} \otimes_G \mathscr{A}^*$, может быть сколь угодно близка к 1 при $\rho \to 1$. Более того, некоторые конкретные примеры таких кодов [48, Example 4], показывают, что они также могут иметь очень большие минимальные расстояния, близкие к расстояниям классических кодов $\ker A$, используемых в поднятом произведении. Однако если группа G абелева, то верхняя оценка на минимальное расстояние таких кодов [48, Eq. 24] является сильным аргументом в пользу того, что для получения асимптотически хорошего семейства qLDPC-кодов при помощи поднятого произведения необходимо использовать неабелевы группы.

Одна явная конструкция кодов, аналогичная вышеупомянутому поднятому произведению $\mathscr{A} \otimes_G \mathscr{A}^*$, была ранее рассмотрена в [7], где была высказана гипотеза, что данное семейство qLDPC-кодов является асимптотически хорошим. Однако наша стратегия доказательства не работает для комплексов вида $\mathscr{A} \otimes_G \mathscr{A}^*$ и данная гипотеза не может быть доказана с помощью методов, разработанных в данной работе. Вместо этого мы рассматриваем аналогичные комплексы $\mathscr{A} \otimes_G \mathscr{B}^*$, где 2-членные комплексы $\mathscr{A}$ и $\mathscr{B}$ соответствуют экспандерным кодам $\mathscr{T}(\Gamma; h_1)$ и $\mathscr{T}(\Gamma; h_2)$, определенным для *одного и того же* экспандера Γ, но для *различных* локальных кодов $\ker h_1$ и $\ker h_2$. Легко показать, подсчитав количество кодовых символов и проверочных соотношений в классическом коде $\ker \partial_2$ и квантовом коде $\mathscr{Q}(\partial_1, \partial_2^*)$, полученных из $\mathscr{A} \otimes_G \mathscr{B}^*$, что эти коды имеют постоянную скорость. Однако, чтобы наше доказательство теорем 1 и 2 сработало, пара локальных кодов, используемых в $\mathscr{A} \otimes_G \mathscr{B}^*$, не может быть произвольной и должна удовлетворять специальному свойству $\rho(\ker h_1, \ker h_2) \geqslant c$, где $\rho(\mathscr{C}_1, \mathscr{C}_2)$ — характеристика пары кодов, в некотором смысле являющаяся двумерным аналогом относительного минимального расстояния кода. Это свойство похоже на свойство *робастной тестируемости*, часто используемое в контексте локально тестируемых кодов [4, 16]. Мы докажем, что пара случайных линейных кодов обладает этим свойством с высокой вероятностью.

1.4. Двойные накрытия графов Кэли. Неформально говоря, свойство расширения произведения является *локальным* свойством комплекса $\mathscr{A} \otimes_G \mathscr{B}^*$, играющим роль, аналогичную роли минимального расстояния локальных кодов в классическом доказательстве Сипсера и Спилма-

*) Подобное наблюдение (без доказательства) также было сделано в [7].

на [50], что экспандерные коды имеют линейные минимальные расстояния. Однако для получения основного результата мы также используем *глобальное* свойство комплекса $\mathscr{A} \otimes_G \mathscr{B}^*$, связанное с *расширительными свойствами на малых множествах**) графа Γ, для экспандерных кодов $\mathscr{T}(\Gamma; h_1)$ и $\mathscr{T}(\Gamma; h_2)$. Наш основной технический результат (Утверждение 1) показывает, что общая конструкция $\mathscr{A} \otimes_G \mathscr{B}^*$ может быть использована с произвольным регулярным графом Γ, полученным как G-поднятие базового графа без петель, если Γ является достаточно хорошим экспандером малых множеств. Ниже будет показано, что спектральные экспандеры и их конечные накрытия обладают хорошими расширяющими свойствами на малых множествах. Следовательно, в качестве графа Γ мы можем взять двудольный граф, являющийся двойным накрытием графа Кэли для некоторой конечной группы G. Напомним, что для конечной группы G с некоторым симметричным порождающим множеством S (т.е. $S = \{s^{-1} \mid s \in S\}$) соответствующий (*левый*) *граф Кэли* — это простой граф $\mathrm{Cay}(G, S)$ с множеством вершин $V(\Gamma) := G$ и множеством ребер $E(\Gamma) := \{\{g, sg\} \mid g \in G, s \in S\}$. Двудольным двойным накрытием $\mathrm{Cay}(G, S)$ является граф $\mathrm{Cay}_2(G, S)$ с множеством вершин $V(\Gamma) := G \times \{0, 1\}$ и множеством ребер: $E(\Gamma) := \{\{(g, 0), (sg, 1)\} \mid g \in G, s \in S\}$.

Заметим, что мы имеем свободное правое действие группы G на $\mathrm{Cay}_2(G, S)$, определенное как $(g, a)t := (gt, a)$ и $\{(g, 0), (sg, 1)\}t := \{(gt, 0), (sgt, 1)\}$, где $g, t \in G$, $s \in S$, и $a \in \{0, 1\}$. Это важно для построения поднятого произведения, поскольку нам нужен классический код, инвариантный относительно свободного действия группы G. Пусть у нас есть проверочная матрица $h \in \mathbb{F}_q^{r \times w}$ и порождающее множество $S = \{s_1, \ldots, s_w\} \subseteq G$. Мы можем задать экспандерный код $\mathscr{T}(\Gamma; h)$ для $\Gamma = \mathrm{Cay}_2(G, S)$ его 2-членным комплексом $\mathbb{F}_q E(\Gamma) \xrightarrow{\partial} \mathbb{F}_q^r V(\Gamma)$. А именно, для каждого $e = \{(g, 0), (s_i g, 1)\} \in E(\Gamma)$, где $g \in G$ и $i \in [w]$, мы полагаем

$$\partial e = h_i \cdot (g, 0) + h_i \cdot (s_i g, 1).$$

Следовательно, для любого графа Кэли мы можем получить экспандерный код $\mathscr{T}(\Gamma; h)$ со свободным действием G. В нашем доказательстве мы применяем эту идею (см. пример 1) к рамануджановским графам Кэли [1, 41], которые также использовались в исходной конструкции экспандерных кодов [50] и в упомянутой ранее гипотезе из [7].

Основным техническим инструментом в доказательстве теорем 1 и 2 является понятие *локально минимальной* (ко)цепи, часто используемое в контексте многомерных экспандеров для доказательства свойств расширения в симплициальных комплексах [33]. Известно, что такие расширительные свойства могут быть использованы для доказательства локальной тестируемости классического кода [31] и для получения нижней оценки на минимальное расстояние квантового кода [19]. В настоящей работе мы обобщаем эти идеи на гораздо более общий контекст (ко)цепных комплексов с локальной системой коэффициентов, которые можно рассматривать как многомерные аналоги кодов Таннера, подобные тем, которые изучались

*) Неформально граф является *экспандером малых множеств*, если для каждого достаточно малого множества вершин S почти все ребра, соединенные с ним, выходят за пределы S (подробности см. в подразделе 4.2).

в работе [45]. Вместо графов такие обобщенные коды Таннера определены на многомерных комплексах, которые обычно формально представляются градуированными посетами. Поскольку поднятое произведение определено для произвольных комплексов, оно естественным образом может быть применено к графам, рассматриваемым как 1-мерные комплексы. Если рассматривать графы Γ и Γ' как топологические пространства, то их поднятое произведение (как топологическое пространство) можно рассматривать как сбалансированное произведение $\Gamma \times_G \Gamma'$ этих пространств [7]. На самом деле, можно показать, что произведения $\Gamma \times_G \Gamma'$ являются примерами известного класса 2-мерных комплексов, называемых *полными квадратными комплексами* [55]. Определяющим свойством полного квадратного комплекса является то, что линки всех его вершин изоморфны *полному* двудольному графу. Поскольку полные двудольные графы являются совершенными экспандерами, то в некотором смысле это свойство аналогично свойству многомерных экспандеров иметь линки, которые являются хорошими экспандерами [33].

Используя рассмотренные выше G-поднятые произведения экспандерных кодов над неабелевыми группами G, мы покажем, что можно получить qLDPC-коды с параметрами как в Теореме 2. Это дает положительный ответ на вопросы, поставленные в [48, Заключение] и в [7, Заключение] о том, могут ли соответственно поднятые и сбалансированные произведения классических кодов дать асимптотически хорошее семейство qLDPC-кодов. Более того, мы также показываем, что при некоторых дополнительных предположениях, если H_X и H_Z являются проверочными матрицами таких qLDPC-кодов, то классический код $\ker H_Z^*$ является локально тестируемым с параметрами как в Теореме 1.

З а м е ч а н и е. Отметим, что результат, аналогичный нашей Теореме 1 для случая двоичного поля $\mathbb{F}_2$, был независимо получен в [15]. При этом 3-членный комплекс, использованный в работе [15] для получения основного результата, эквивалентен сбалансированному произведению над G экспандерных кодов [7, 8], определенных на *двух различных* графах Кэли для *одной и той же* группы G. Интересно отметить, что эта конструкция похожа на конструкцию поднятого произведения из [46, Remark 5]), где вместо произведения $\mathscr{A} \otimes_G \mathscr{B}^*$ мы предлагаем использовать произведение $\mathscr{A} \otimes_G \mathscr{B}$ и предполагаем, что таким образом тоже можно получить асимптотически хорошие LTC. Диаграммы для $\mathscr{A} \otimes_G \mathscr{B}$ и $\mathscr{A} \otimes_G \mathscr{B}^*$ задаются соответственно как

$$\begin{array}{ccc} R^{n_a \times m_b} & \xrightarrow{A \otimes_R \mathrm{id}} & R^{m_a \times m_b} \\ {\scriptstyle -\mathrm{id} \otimes_R B}\uparrow & & \uparrow{\scriptstyle \mathrm{id} \otimes_R B} \\ R^{n_a \times n_b} & \xrightarrow[A \otimes_R \mathrm{id}]{} & R^{m_a \times n_b} \end{array}, \qquad \begin{array}{ccc} R^{n_a \times m_b} & \xrightarrow{A \otimes_R \mathrm{id}} & R^{m_a \times m_b} \\ {\scriptstyle -\mathrm{id} \otimes_R B^*}\downarrow & & \downarrow{\scriptstyle \mathrm{id} \otimes_R B^*} \\ R^{n_a \times n_b} & \xrightarrow[A \otimes_R \mathrm{id}]{} & R^{m_a \times n_b} \end{array}.$$

Можно легко проверить, что графы Таннера комплексов $\mathscr{A} \otimes_G \mathscr{B}$ и $\mathscr{A} \otimes_G \mathscr{B}^*$ изоморфны. Отличается здесь интерпретация вершин графа Таннера как *кодовых символов* и *проверок на четность*, когда мы из комплекса делаем код. В некотором смысле произведение $\mathscr{A} \otimes_G \mathscr{B}$ лучше подходит для LTC, поскольку оно дает классические коды со скоростью, произвольно близкой к 1. В то же время конструкция $\mathscr{A} \otimes_G \mathscr{B}^*$, которую мы

используем для доказательства основных результатов, гораздо лучше подходит для qLDPC-кодов, так как она симметрична. Эта симметрия позволяет нам доказать нижнюю оценку на Z-расстояние нашего qLDPC-кода таким же способом, как и на X-расстояние. Кроме того, мы можем сделать равное количество X-проверок и Z-проверок, что дает qLDPC-коды со скоростями, произвольно близкими к 1.

§ 2. Предварительные сведения и определения

2.1. Произведения графов. Если X и Y — два графа (рассматриваемые как 2-уровневые посеты), то с геометрической точки зрения посет $X\times Y$ соответствует прямому произведению X и Y (как топологических графов). В то же время геометрическая интерпретация посета $X\times_G Y$ (см. Определение 2) может быть дана в терминах сбалансированного произведения графов [7]. Заметим, что 1-*остов* графа $X\times Y$, т. е. его ограничение на первые два уровня, является 2-уровневым посетом, представляющим граф $X\square Y$, которое обычно называют *декартовым произведением* графов X и Y. Напомним, что для каждого G-поднятого графа Γ группа G свободно действует на Γ.

О п р е д е л е н и е 4. Мы определяем *поднятое декартово произведение* $\widehat{X}\square_G\widehat{Y}$ для G-поднятий $\widehat{X}$, $\widehat{Y}$ базовых графов X, Y как 1-остов $\widehat{X}\times_G\widehat{Y}$.

Нетрудно проверить, что граф $\widehat{X}\square_G\widehat{Y}$ является $|G|$-кратным накрытием для стандартного декартова произведения $X\square Y$. Более того, если группа G абелева, то это накрытие регулярно, т. е. $\widehat{X}\square_G\widehat{Y}$ является G-поднятием $X\square Y$.

Предположим, что $\widehat{\Gamma}$ является G-поднятием некоторого базового графа Γ. Мы можем рассматривать Γ как фактор $\widehat{\Gamma}$ по модулю действия G, т. е. $V(\Gamma)=V(\widehat{\Gamma})/G$ и $E(\Gamma)=E(\widehat{\Gamma})/G$. Рассмотрим клеточный посет $\widetilde{X}:=\widehat{\Gamma}\times_G\widehat{\Gamma}$ и представим его элементы тройками $x\cdot g\cdot y$, где $x,y\in V(\Gamma)\cup E(\Gamma)$ и $g\in G$. Удобно интерпретировать посет $\widetilde{X}$ как 2-мерный геометрический объект. Элемент $x\cdot g\cdot y\in\widetilde{X}$ называется:

— *вершиной*, если $x\in V(\Gamma), y\in V(\Gamma)$;

— *горизонтальным ребром*, если $x\in E(\Gamma), y\in V(\Gamma)$;

— *вертикальным ребром*, если $x\in V(\Gamma), y\in E(\Gamma)$;

— *гранью*, если $x\in E(\Gamma), y\in E(\Gamma)$,

и соответствующие подмножества элементов обозначим как $V=V(\widetilde{X})$, $E_{\rightarrow}=E_{\rightarrow}(\widetilde{X})$, $E_{\uparrow}=E_{\uparrow}(\widetilde{X})$, и $F=F(\widetilde{X})$. Также определим множество $E(\widetilde{X}):=E_{\rightarrow}(\widetilde{X})\cup E_{\uparrow}(\widetilde{X})$.

З а м е ч а н и е 5. Заметим, что $V=V(\widehat{\Gamma})\times_G V(\widehat{\Gamma})$, $E_{\rightarrow}=E(\widehat{\Gamma})\times_G V(\widehat{\Gamma})$, $E_{\uparrow}=V(\widehat{\Gamma})\times_G E(\widehat{\Gamma})$ и $F=E(\widehat{\Gamma})\times_G E(\widehat{\Gamma})$.

Если P является посетом, то через P^* обозначим *двойственный посет*, т. е. $x\leqslant_{P^*}y$ всякий раз, когда $y\leqslant_P x$. В дальнейшем нам понадобится также

посет $X := \widehat{\Gamma} \times_G \widehat{\Gamma}^*$, который определен на том же множестве, что и $\widetilde{X} = \widehat{\Gamma} \times_G \widehat{\Gamma}$, но имеет *другой* частичный порядок. Клеточный посет $\widetilde{X}$ имеет 3 уровня: $\widetilde{X}_0 := V$, $\widetilde{X}_1 := E_\uparrow \cup E_\rightarrow$, и $\widetilde{X}_2 := F$, а уровни для X следующие: $X_0 := E_\uparrow$, $X_1 := F \cup V$ и $X_2 := E_\rightarrow$.

Замечание 6. Как будет видно в разделе 4.3, посет $X = \widehat{\Gamma} \times_G \widehat{\Gamma}^*$ соответствует комплексу поднятого произведения $\mathcal{T}(\Gamma; h_1) \otimes_G \mathcal{T}^*(\Gamma; h_2)$, который мы используем для доказательства основного результата. Однако уровни в посете X не соответствуют естественной геометрической размерности клеток, и в доказательстве нашего основного результата удобнее работать с посетом $\widetilde{X} = \widehat{\Gamma} \times_G \widehat{\Gamma}$, определенным на том же множестве, что и X, но дающим ему естественную геометрическую интерпретацию как 2-мерного комплекса. Для этого определим отношение инцидентности $\mathrm{inc}(\cdot, \cdot)$ на множестве $V \cup E_\rightarrow \cup E_\uparrow \cup F$ в стандартном геометрическом смысле, т. е. мы предполагаем, что $\mathrm{inc}(x, y)$ тогда и только тогда, когда $x \leqslant y$ или $y \leqslant x$, где $\leqslant$ — частичный порядок множества $\widetilde{X} = \widehat{\Gamma} \times_G \widehat{\Gamma}$. Если $x \in X$ и $S, T \subseteq X$, то мы также используем следующие обозначения:

$$S_x := \{y \in S \mid \mathrm{inc}(x, y)\},$$
$$S_T := \{y \in S \mid \mathrm{inc}(x, y) \text{ для некоторого } x \in T\}.$$

То есть S_x — это подмножество элементов из X, инцидентных x, а S_T — это подмножество элементов из S, инцидентных некоторому элементу из T. Например, $X_v = \{v\} \cup E_v \cup F_v$ — множество всех клеток, инцидентных v, называемое *звездой* v, где E_v (или F_v) — множество ребер (или граней), инцидентных v.

Для доказательства нашего основного результата нам также понадобится 1-остов $\Lambda := \widehat{\Gamma} \,\square_G\, \widehat{\Gamma}$ из $\widehat{\Gamma} \times_G \widehat{\Gamma}$ с множеством вершин $V(\Lambda) := V(\widetilde{X})$ и множеством ребер $E(\Lambda) := E(\widetilde{X})$.

Замечание 7. В разделе 4, когда мы упоминаем множества V, E, $E_\rightarrow$, $E_\uparrow$, F или граф Λ, мы ссылаемся на соответствующие множества и граф, определенные для множества $\widehat{\Gamma} \times_G \widehat{\Gamma}$ в этом разделе, если не указано иное.

2.2. Комплексы с локальной системой коэффициентов. В этом подразделе мы снова рассматриваем экспандерные коды и их поднятые произведения. Мы используем удобный способ, применяемый в работах [45], [7] для представления этих кодов на языке цепных комплексов и локальных систем. Локальные системы могут быть использованы для получения высокоуровневого представления цепного комплекса над $\mathbb{F}_q$. Основная идея состоит в том, чтобы позволить каждому элементу x из клеточного посета X иметь собственное векторное пространство коэффициентов $\mathcal{F}_x$.

Пусть X — некоторое конечное множество, которое мы будем использовать в качестве индексного множества. Если векторное пространство $\mathcal{C}$ является прямой суммой $\bigoplus_{x \in X} \mathcal{F}_x$ набора векторных пространств $\mathcal{F} = (\mathcal{F}_x)_{x \in X}$, то мы можем рассматривать элементы $\mathcal{C}$ как формальные суммы $\sum_{x \in X} a_x x$ элементов из X, где для каждого $x \in X$ коэффициент a_x из векторного пространства $\mathcal{F}_x$ называется *локальным пространством коэффициентов* элемента x. В таких случаях мы также обозначаем векторное пространство $\mathcal{C}$ через $\mathcal{F}X$ или через AX, когда все локальные пространства коэффициентов

равны одному пространству A. Если каждое локальное пространство коэффициентов $\mathscr{F}_x$ имеет выделенный базис $\widetilde{\mathscr{F}}_x$, то мы предполагаем, что выделенным базисом для $\mathscr{F}X$ является множество $\{ax \mid a \in \widetilde{\mathscr{F}}_x,\ x \in X\}$; в этом случае мы говорим, что $\mathscr{F}X$ *имеет выделенный базис*.

Рассмотрим цепной комплекс $\mathscr{C} = \mathscr{F}X$ с выделенным базисом над $\mathbb{F}_q$. Пусть $a = \sum\limits_{x \in X} a_x x \in \mathscr{C}$, где каждый коэффициент a_x из векторного пространства $\mathscr{F}_x$ над $\mathbb{F}_q$ с выделенным базисом. Обозначим через $\boldsymbol{wt}(a)$ стандартный вес Хэмминга для a, рассматриваемого как вектор над $\mathbb{F}_q$. Мы также рассмотрим *блочный вес* $\boldsymbol{wt}_X(a)$, определяемый как количество ненулевых блоков в a, рассматриваемых как блочный вектор $(a_x)_{x \in X}$, то есть

$$\boldsymbol{wt}_X(a) := \operatorname{card}\{x \in X \mid a_x \neq 0\}.$$

Иногда нам нужно учесть только те блоки, которые соответствуют некоторому подмножеству $S \subseteq X$. В этом случае мы можем определить вес блока $\boldsymbol{wt}_S(a) := \operatorname{card}\{x \in S \mid a_x \neq 0\}$ *относительно* подмножества $S \subseteq X$. Определим также $\operatorname{supp} a := \{x \in X \mid a_x \neq 0\}$ и $a|_S := \sum\limits_{x \in S} a_x$, где $a = \sum\limits_{x \in X} a_x x$.

Пусть $\partial\colon \mathscr{F}X \to \mathscr{F}X$ — оператор границы комплекса $\mathscr{C}$. В некоторых случаях мы хотим ограничить образ и прообраз ∂. Для каждого $S, T \subseteq X$ мы рассматриваем отображение $\partial_{S \to T}\colon \mathscr{F}S \to \mathscr{F}T$, определенное как $a \mapsto (\partial a)|_T$. Из определения ясно, что для каждого $a \in \mathscr{F}X$ мы имеем

$$(\partial(a|_S))|_T = \partial_{S \to T}(a|_S). \tag{2}$$

Мы можем представить код Таннера $\mathscr{T}(\Gamma; h)$ для графа Γ (рассматриваемого как 2-уровневый посет $\Gamma = V \sqcup E$) комплексом $\mathscr{F}\Gamma$, определяемым диаграммой

$$\mathbb{F}_q E \xrightarrow{\partial} \mathbb{F}_q^r V,$$

где $\mathscr{F}_v := \mathbb{F}_q^r$ для каждого $v \in V$ и $\mathscr{F}_e := \mathbb{F}_q$ для каждого $e \in E$.

Предположим, что у нас есть свободное действие группы G на клеточных посетах X и Y комплексов $\mathscr{A} = \mathscr{F}X$ и $\mathscr{B} = \mathscr{G}Y$ с локальными системами $\mathscr{F}$ и $\mathscr{G}$ соответственно (как обычно, справа на X и слева на Y). Кроме того, мы предполагаем, что $\mathscr{F}_{xg} = \mathscr{F}_x$ и $\mathscr{G}_{gy} = \mathscr{G}_y$ для каждого $x \in X$, $y \in Y$ и $g \in G$. Тогда нетрудно видеть, что $\mathscr{A} \otimes_G \mathscr{B} \cong (\mathscr{F} \otimes \mathscr{G})X \times_G Y$, где $\mathscr{F} \otimes \mathscr{G}$ — локальная система для $X \times_G Y$, определенная как $(\mathscr{F} \otimes \mathscr{G})_z := \mathscr{F}_x \otimes_{\mathbb{F}_q} \mathscr{G}_y$, где $z = x \otimes_G y \in X \times_G Y$. Заметим, что это определение верно, так как $\mathscr{F}_{xg} \otimes_{\mathbb{F}_q} \mathscr{G}_y = \mathscr{F}_x \otimes_{\mathbb{F}_q} \mathscr{G}_{gy}$.

Покажем, что комплекс поднятого произведения $\mathscr{C} = \mathscr{A} \otimes_G \mathscr{B}^*$, где $\mathscr{A} = \mathscr{T}(\Gamma; h_1)$ и $\mathscr{B} = \mathscr{T}(\Gamma; h_2)$ — коды Таннера, инвариантные относительно свободного действия G, также может быть представлен как комплекс $\mathscr{F}X$ с локальной системой на множестве $X := \Gamma \times_G \Gamma^*$. Действительно, в этом случае $\mathscr{A} = \left(\mathbb{F}_q E \xrightarrow{A} \mathbb{F}_q^r V\right)$, $\mathscr{B}^* = \left(\mathbb{F}_q^{r'} V \xrightarrow{B^*} \mathbb{F}_q E\right)$, а комплекс $\mathscr{F}X$ представлен правой частью уравнения:

$$\begin{array}{ccc} \mathbb{F}_q E & \xrightarrow{A} & \mathbb{F}_q^r V \\ \otimes_G & & \\ \mathbb{F}_q E & & \end{array} = \begin{array}{ccc} \mathbb{F}_q E & \mathbb{F}_q E \times_G E & \xrightarrow{A \otimes_G \mathrm{id}} \mathbb{F}_q^r V \times_G E \\ \uparrow{\scriptstyle B^*} & \uparrow{\scriptstyle -\mathrm{id} \otimes_G B^*} & \uparrow{\scriptstyle \mathrm{id} \otimes_G B^*} \\ \mathbb{F}_q^{r'} V & \mathbb{F}_q^{r'} E \times_G V & \xrightarrow[A \otimes_G \mathrm{id}]{} \mathbb{F}_q^{r \times r'} V \times_G V \end{array}.$$

Здесь мы отождествляем $\mathbb{F}_q^r \otimes \mathbb{F}_q^{r'}$ с $\mathbb{F}_q^{r \times r'}$. Таким образом, мы видим, что $\mathscr{C} = \mathscr{A} \otimes_G \mathscr{B}^*$ является следующим 3-членным комплексом:

$$\underbrace{\mathbb{F}_q^{r'} E \times_G V}_{\mathscr{C}_2} \xrightarrow{\partial_2} \underbrace{\mathbb{F}_q E \times_G E \oplus \mathbb{F}_q^{r \times r'} V \times_G V}_{\mathscr{C}_1} \xrightarrow{\partial_1} \underbrace{\mathbb{F}_q^r V \times_G E}_{\mathscr{C}_0}. \tag{3}$$

§ 3. Расширение произведения кодов

В этом разделе мы определим свойство произведения кодов, называемое *расширением*. Прежде чем продолжить, напомним некоторые стандартные определения и введем новые обозначения, связанные с произведениями кодов.

Напомним, что (*тензорным*) *произведением линейных кодов* $\mathscr{C}_1, \ldots, \mathscr{C}_m$ над $\mathbb{F}_q$ называется код

$$\mathscr{C}_1 \otimes \ldots \otimes \mathscr{C}_m := \{c \in \mathbb{F}_q^{n_1 \times \ldots \times n_m} \mid \forall i \in [m]\ \forall \ell \in \mathscr{L}_i \colon c|_\ell \in \mathscr{C}_i\},$$

где $\mathbb{F}_q^{n_1 \times \ldots \times n_m}$ — множество функций $c\colon [n_1] \times \ldots \times [n_m] \to \mathbb{F}_q$, а $\mathscr{L}_i$ — множество линий, параллельных i-й оси на m-мерной сетке $[n_1] \times \ldots \times [n_m]$, то есть

$$\mathscr{L}_i := \{\{x + s \cdot e_i \mid s \in [n_i]\} \mid x \in [n_1] \times \ldots \times [n_m], x_i = 0\}.$$

Здесь e_i обозначает вектор $(0, \ldots, 0, 1, 0 \ldots, 0) \in [n_1] \times \ldots \times [n_m]$, где 1 стоит на i-й позиции.

Удобно ввести обозначение для двойственного кода к произведению кодов [12, 56]. Для линейных кодов $\mathscr{C}_1 \subseteq \mathbb{F}_q^{n_1}$, $\mathscr{C}_2 \subseteq \mathbb{F}_q^{n_2}$ через $\mathscr{C}_1 \boxplus \mathscr{C}_2$ обозначим код $(\mathscr{C}_1^\perp \otimes \mathscr{C}_2^\perp)^\perp = \mathscr{C}_1 \otimes \mathbb{F}_q^{n_2} + \mathbb{F}_q^{n_1} \otimes \mathscr{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$. Для набора $\mathscr{C} = (\mathscr{C}_i)_{i \in [m]}$ линейных кодов над $\mathbb{F}_q$ мы можем определить коды

$$\mathscr{C}^{(i)} := \mathbb{F}_q^{n_1} \otimes \ldots \otimes \mathscr{C}_i \otimes \ldots \otimes \mathbb{F}_q^{n_m} = \{c \in \mathbb{F}_q^{n_1 \times \ldots \times n_m} \mid \forall \ell \in \mathscr{L}_i \colon c|_\ell \in \mathscr{C}_i\}.$$

Нетрудно видеть, что

$$\mathscr{C}_1 \otimes \ldots \otimes \mathscr{C}_m = \mathscr{C}^{(1)} \cap \ldots \cap \mathscr{C}^{(m)}, \qquad \mathscr{C}_1 \boxplus \ldots \boxplus \mathscr{C}_m = \mathscr{C}^{(1)} + \ldots + \mathscr{C}^{(m)}.$$

Заметим, что каждый код $\mathscr{C}^{(i)}$ является прямой суммой $|\mathscr{L}_i| = \dfrac{1}{n_i} \prod\limits_{i \in [m]} n_i$ копий кода $\mathscr{C}_i$. Для $x \in \mathbb{F}_q^{n_1 \times \ldots \times n_m}$ обозначим через $|x|_i$ число таких $\ell \in \mathscr{L}_i$, что $a|_\ell \neq 0$. Также всюду в данном разделе вес Хэмминга для краткости будем обозначать через $|\cdot|$.

О п р е д е л е н и е 5. Для линейных кодов $\mathscr{C}_1, \ldots, \mathscr{C}_m$, $\mathscr{C}_i \subseteq \mathbb{F}_q^{n_i}$, определим величину $\rho(\mathscr{C}_1, \ldots, \mathscr{C}_m)$. Это максимальное такое ρ, что каждое кодовое слово $c \in \mathscr{C}_1 \boxplus \ldots \boxplus \mathscr{C}_m$ может быть представлено как сумма $c = \sum\limits_{i \in [m]} a_i$, где $a_i \in \mathscr{C}^{(i)}$ для всех $i \in [m]$ и выполняется следующее неравенство:

$$\rho \sum_{i \in [m]} n_i \, |a_i|_i \leqslant |c|. \tag{4}$$

Код $\mathscr{C}_1 \boxplus \ldots \boxplus \mathscr{C}_m$ назовем ρ-*расширяющим*, если $\rho(\mathscr{C}_1, \ldots, \mathscr{C}_m) \geqslant \rho$.

Заметим, что если $n_i = n$, $i \in [m]$, то (4) может быть также переписано в виде

$$\sum_{i\in[m]} |a_i|_i \leqslant \frac{|c|}{\rho n}.$$

Заметим, что существует вырожденный случай, когда $\mathscr{C}_i = \mathbb{F}_q^{n_i}$ для некоторого $i \in [m]$, в этом случае мы называем этот набор кодов *вырожденным*. В этом случае $\mathscr{C}^{(i)} = \mathbb{F}_q^{n_1\times\cdots\times n_m}$, из чего следует $\mathscr{C}_1 \boxplus \cdots \boxplus \mathscr{C}_m = \mathbb{F}_q^{n_1\times\cdots\times n_m}$, и поэтому $\rho(\mathscr{C}_1, \ldots, \mathscr{C}_m) = 1/n_i$. Например, если $\mathscr{C}_i = \mathbb{F}_q$ $(n_i = 1)$, то $\rho(\mathscr{C}_1, \ldots, \mathscr{C}_m) = 1$, *независимо* от кодов $\mathscr{C}_j$, $j \neq i$.

Нетрудно показать, что для любого невырожденного набора кодов $\mathscr{C}_1, \ldots, \mathscr{C}_m$ выполнено $d(\mathscr{C}_i) \geqslant \rho n_i$ для всех $i \in [m]$.

Мы будем далее работать со случаем $m = 2$, когда каждое кодовое слово кода $\mathscr{C}_1 \otimes \mathscr{C}_2$ представляет собой таблицу, в которой каждая строка принадлежит коду $\mathscr{C}_1$, а каждый столбец — коду $\mathscr{C}_2$. Кодовое слово x кода $\mathscr{C}_1 \boxplus \mathscr{C}_2$ также можно интерпретировать в виде матрицы, которая представляется в виде суммы какого-то числа строк из $\mathscr{C}_1$ и какого-то числа столбцов из $\mathscr{C}_2$. Это условие может быть выражено через проверочные матрицы как $h_2 x h_1^* = 0$, где $\mathscr{C}_1 = \ker h_1$, $\mathscr{C}_2 = \ker h_2$.

З а м е ч а н и е 8. Заметим, что из определения расширения произведения сразу следует, что для любой пары кодов $(\mathscr{C}_1, \mathscr{C}_2)$, определяющей CSS код (т.е. для их проверочных матриц имеем $H_1 H_2^* = 0$), выполнено $\rho(\mathscr{C}_1, \mathscr{C}_2) \leqslant 1/n$, где n — длина кодов $\mathscr{C}_1$ и $\mathscr{C}_2$. Действительно, возьмем в качестве x единичную матрицу $(\delta_{ij})_{n\times n} \in \mathbb{F}_q^{n\times n}$, тогда $H_2 x H_1^* = H_2 H_1^* = 0$, значит, x является кодовым словом кода $\mathscr{C}_1 \boxplus \mathscr{C}_2$; при этом $(\delta_{ij})_{n\times n}$ нельзя получить суммой менее чем n строк или столбцов. Таким образом, код $\mathscr{C}_1 \boxplus \mathscr{C}_2$ *не* является ρ-расширяющим ни для какого фиксированного $\rho > 0$ при $n \to \infty$.

Обозначим через $\mathsf{Gr}(n, k)$ множество всех линейных подпространств в $\mathbb{F}_q^n$ размерности k. Основным результатом данного раздела является следующая теорема.

Т е о р е м а 3. *Для любых $\varepsilon_1 \in (0, 1)$, $\varepsilon_2 \in (0, 1)$ существует $\rho > 0$ такое, что доля пар кодов $(\mathscr{C}_1, \mathscr{C}_2) \in \mathsf{Gr}(n, n - r_1) \times \mathsf{Gr}(n, n - r_2)$, для которых выполнено $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$, стремится к 1 при $n \to \infty$, $r_1 \geqslant \varepsilon_1 n$, $r_2 \geqslant \varepsilon_2 n$.*

С л е д с т в и е 1. *Для каждого $R_1 \in (0, 1)$, $R_2 \in (0, 1)$ существует $\rho > 0$ такое, что доля пар кодов $(\mathscr{C}_1, \mathscr{C}_2) \in \mathsf{Gr}(n, k_1) \times \mathsf{Gr}(n, k_2)$, для которых $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$ и $\rho(\mathscr{C}_1^\perp, \mathscr{C}_2^\perp) \geqslant \rho$, стремится к 1 при $n \to \infty$, $k_1/n \to R_1$, $k_2/n \to R_2$.*

Мы часто будем использовать следующие сокращения:

$$x(I, \cdot) := x|_{I\times[n]}, \qquad x(\cdot, J) := x|_{[n]\times J}, \qquad x(I, J) := x|_{I\times J},$$

где $x \in \mathbb{F}_q^{n\times n}$, $I, J \subseteq [n]$. Если $I \subseteq [n]$, то обозначим через $\mathbb{F}_q^I$ линейное пространство $\{x \in \mathbb{F}_q^n \mid \forall i \in [n] \setminus I\colon x_i = 0\}$. То есть, по определению, мы предполагаем, что $\mathbb{F}_q^I \subseteq \mathbb{F}_q^n$.

Сначала приведем набросок доказательства теоремы 3. Рассмотрим два кода $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$ с минимальными расстояниями $d_1 = d(\mathscr{C}_1)$ и $d_2 = d(\mathscr{C}_2)$ соответственно. Мы говорим, что $x \in \mathbb{F}_q^{n\times n}$ имеет *нулевой прямоугольник* $A \times B$,

где $A, B \subseteq [n]$, если $|A| > n - d_1$, $|B| > n - d_2$, и $x(A, B) = 0$. Неформально доказательство состоит двух основных шагов:

1. Если кодовое слово $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ имеет нулевой прямоугольник $A \times B$, то x является суммой $n - |A|$ столбцов из $\mathscr{C}_2$ и $n - |B|$ строк из $\mathscr{C}_1$ (лемма 7).
2. Пара случайных линейных кодов с высокой вероятностью обладает свойством, что каждое кодовое слово $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ веса δn^2 имеет нулевой прямоугольник размера $n(1 - O(\delta)) \times n(1 - O(\delta))$.

В результате каждое кодовое слово $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ веса δn^2 может быть представлено как сумма $O(\delta)$ строк из $\mathscr{C}_1$ и столбцов из $\mathscr{C}_2$, что и требуется для доказательства результата. Основная трудность на этом пути заключается в доказательстве второго утверждения из вышеприведенного списка. Нам нужно доказать, что оно справедливо для всех кодовых слов веса $\leqslant \delta_0 n^2$, где $\delta_0 > 0$ — некоторый фиксированный параметр, не зависящий от n. Заметим, что число таких кодовых слов не превышает $q^{H_q(\delta_0)n^2}$.

На самом деле нетрудно показать, что для фиксированного x вероятность события $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ ограничена сверху как $q^{-\Omega(n \operatorname{rk} x)}$ (лемма 3). Для множества всех матриц x с $\operatorname{rk} x = \Omega(n)$ вероятность того, что хотя бы одна из них принадлежит коду $\mathscr{C}_1 \boxplus \mathscr{C}_2$, можно оценить сверху суммой вероятностей по всевозможным x. Основной проблемой являются матрицы x с маленьким рангом, т. е. у которых $\operatorname{rk} x = o(n)$, так как здесь такой оценки оказывается недостаточно. Мы покажем, что можно избежать этой проблемы, рассматривая только коды $\mathscr{C}_1$ и $\mathscr{C}_2$, обладающие специальным свойством, которое выполняется для случайных кодов с высокой вероятностью и исключает кодовые слова в $\mathscr{C}_1 \boxplus \mathscr{C}_2$ с малым рангом.

Для определения этого специального свойства введем понятие *α-разреженности*. Мы говорим, что вектор $v \in \mathbb{F}_q^n$ является *α-разреженным*, если его вес Хэмминга ограничен сверху αn. Подпространство $V \subseteq \mathbb{F}_q^n$ называется *α-разреженным*, если оно может быть порождено (нулем или более) α-разреженных векторов. Мы говорим, что подпространство $U \in \mathsf{Gr}(n, n-r)$ обладает свойством $(*)$, если для каждого α-разреженного подпространства V такого, что $\dim V \leqslant r$ и $\alpha = H_q^{-1}(r/8n)$ имеем $\dim(U \cap V) < \frac{1}{2} \dim V$. Путем прямого подсчета можно показать, что почти все подпространства U обладают свойством $(*)$ (лемма 4).

Это свойство мотивировано тем, что для матрицы $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ с пространством строк $X := \operatorname{im} x^*$ и пространством столбцов $Y := \operatorname{im} x$ мы имеем (лемма 8)

$$\operatorname{rk} x \leqslant \dim(\mathscr{C}_1 \cap X) + \dim(\mathscr{C}_2 \cap Y). \tag{5}$$

Если коды $\mathscr{C}_1$ и $\mathscr{C}_2$ обладают свойством $(*)$ и мы можем гарантировать, что пространства X и Y являются *α-разреженными*, то имеем $\operatorname{rk} x = \dim X = \dim Y > n - \max(\dim \mathscr{C}_1, \dim \mathscr{C}_2)$. Действительно, иначе по свойству $(*)$ получаем

$$\dim(\mathscr{C}_1 \cap X) + \dim(\mathscr{C}_2 \cap Y) < \frac{1}{2} \dim X + \frac{1}{2} \dim Y = \operatorname{rk} x,$$

что противоречит (5).

Теперь рассмотрим коды $\mathscr{C}_1$ и $\mathscr{C}_2$ такие, что они обладают свойством $(*)$, и код $\mathscr{C}_1 \boxplus \mathscr{C}_2$ не имеет кодовых слов малого веса и большого ранга. Из предыдущих наблюдений следует, что для достаточно малого δ_0 не существует кодовых слов $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ веса $\leqslant \delta_0 n^2$ с α-разреженными пространствами строк и столбцов.

Осталось показать, что для каждого кодового слова $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ малого веса $\leqslant \delta n^2$, $\delta \leqslant \delta_0$, либо x имеет нулевой прямоугольник размера $n(1-O(\delta)) \times n(1-O(\delta))$, либо существует кодовое слово x' веса $n^2 O(\delta)$ с α-разреженными пространствами строк и столбцов. Действительно, для любой матрицы x можно найти подмножество строк и столбцов веса $\geqslant \alpha n/2$. При достаточно малом $\delta_0 \leqslant \alpha^2/4$ остальные столбцы (индексное множество A) и строки (индексное множество B) либо образуют нулевой прямоугольник, либо веса строк и столбцов в подматрице $x(A,B)$ ограничены сверху $\alpha n/2$, где $|A|, |B| \geqslant n(1-2\delta/\alpha) = n(1-O(\delta))$. В последнем случае мы можем расширить $x(A,B)$ до кодового слова $x' \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ (т. е. $x'(A,B) = x(A,B)$) способом, гарантирующим, что все столбцы x' порождаются столбцами $x'(A,\cdot)$, а все строки x' порождаются строками $x'(\cdot,B)$ (лемма 9), при этом вес всех этих строк и столбцов не превышает α. Поэтому пространства строк и столбцов x' являются α-разреженными.

3.1. Свойства случайных линейных подпространств. Введем некоторые дополнительные обозначения, которые понадобятся нам в следующих леммах. Для $n \in \mathbb{N}$, $\alpha > 0$ определим множество $S(n,\alpha) := \{x \in \mathbb{F}_q^n \mid |x| \leqslant \alpha n\}$. Подпространство $\mathbb{F}_q^n$ называется *α-разреженным*, если оно имеет базис, состоящий из векторов из $S(n,\alpha)$. Нам также понадобится *q-арная функция энтропии* $H_q : [0,1] \to [0,1]$ и ее обратная $H_q^{-1} : [0,1] \to [0, 1-1/q]$:

$$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x)\log_q(1-x),$$

где $H_q^{-1}(y)$ — единственная*) точка $x \in [0, 1-1/q]$ такая, что $H_q(x) = y$.

В дальнейшем нам также понадобится множество $P(n, r_a, r_b) := \mathsf{Gr}(n, n-r_a) \times \mathsf{Gr}(n, n-r_b)$, где $\mathsf{Gr}(n,k)$ обозначает *грассманиан*, т. е. множество всех k-мерных подпространств $\mathbb{F}_q^n$. Известно, что $|\mathsf{Gr}(n,k)| = \binom{n}{k}_q$, где $\binom{n}{k}_q := \prod\limits_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1}$ — *q-биномиальный коэффициент*.

Теперь приведем некоторые известные оценки [35, Lemma 4] на q-биномиальные коэффициенты $\binom{n}{k}_q$.

Лемма 1. *Для q-биномиальных коэффициентов мы имеем следующие оценки:*

$$q^{k(n-k)} \leqslant \binom{n}{k}_q \leqslant 4q^{k(n-k)}.$$

Доказательство. Действительно, мы имеем:

$$\binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1} = q^{k(n-k)} \prod_{i=0}^{k-1} \frac{1-q^{i-n}}{1-q^{i-k}}.$$

*) Заметим, что на отрезке $[0, 1-1/q]$ функция H_q монотонна и принимает значения от 0 до 1, значит, она обратима, и обратная функция H_q^{-1} определена на отрезке $[0,1]$.

Так как $k \leqslant n$, то имеем $1 - q^{i-n} \geqslant 1 - q^{i-k}$. Значит $\prod\limits_{i=0}^{k-1} \frac{1-q^{i-n}}{1-q^{i-k}} \geqslant 1$. С другой стороны, мы видим, что

$$\prod_{i=0}^{k-1}(1-q^{i-k}) = \prod_{i=1}^{k}(1-q^{-i}) \geqslant (1-q^{-1})\Big(1-\sum_{i=2}^{\infty} q^{-i}\Big) = 1 - q^{-1} - q^{-2} \geqslant \frac{1}{4},$$

где последнее неравенство справедливо, так как $q \geqslant 2$. Таким образом, имеем

$$\prod_{i=0}^{k-1} \frac{1-q^{i-n}}{1-q^{i-k}} \leqslant \prod_{i=0}^{k-1} \frac{1}{1-q^{i-k}} \leqslant 4,$$

что завершает доказательство.

Теперь, прежде чем перейти к следующей лемме, отметим, что если $k \leqslant m \leqslant n$, то имеем

$$\frac{\binom{m}{k}_q}{\binom{n}{k}_q} = \prod_{i=0}^{k-1} \underbrace{\frac{q^m - q^i}{q^n - q^i}}_{\leqslant q^{m-n}} \leqslant q^{(m-n)k}.$$

Лемма 2. *Для любого подпространства $V \in \mathsf{Gr}(n, v)$ доля подпространств $U \in \mathsf{Gr}(n, u)$, для которых выполнено $\dim(U \cap V) \geqslant k$, не превосходит $4q^{-k(n+k-v-u)}$.*

Доказательство. Условие $\dim(U \cap V) \geqslant k$ означает, что существует k-мерное подпространство $W \subseteq V$ такое, что $W \subseteq U$, которое можно переписать как $U^\perp \subseteq W^\perp$, где $U^\perp$ — ортогональное подпространство к U. Следовательно, доля таких подпространств U не превышает

$$\frac{\binom{\dim V}{\dim W}_q \binom{\dim W^\perp}{\dim U^\perp}_q}{\binom{n}{\dim U}_q} = \binom{v}{k}_q \frac{\binom{n-k}{n-u}_q}{\binom{n}{n-u}_q} \leqslant 4q^{k(v-k)} \cdot q^{((n-k)-n)(n-u)} = 4q^{-k(-v+k+n-u)}.$$

Теперь получим верхнюю оценку на вероятность того, что для случайных кодов $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$ код $\mathscr{C}_1 \boxplus \mathscr{C}_2$ имеет некоторое фиксированное кодовое слово x большого ранга.

Лемма 3. *Для матрицы $x \in \mathbb{F}_q^{n\times n}$ ранга $\operatorname{rk} x \geqslant \min(r_1, r_2)$ вероятность того, что $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ для случайной пары кодов $(\mathscr{C}_1, \mathscr{C}_2) \in P(n, r_1, r_2)$, не превосходит $5q^{-\frac{1}{4}r_1 r_2}$, если $\min(r_1, r_2) \geqslant 2$.*

Доказательство. Пусть $h_i \in \mathbb{F}_q^{r_i \times n}$ — проверочная матрица кода $\mathscr{C}_i$, $i \in [2]$. Без потери общности будем считать, что $r_1 \leqslant r_2$. Рассмотрим $r' := \lfloor r_1/2 \rfloor$. Так как $r_2 \geqslant r_1 \geqslant 2$, то имеем $r_1/4 < r' \leqslant r_1/2$, $r_1 - r' \geqslant r_1/2$, $r_2 - r' \geqslant r_2/2$. Оценим количество кодов $\mathscr{C}_1 \in \mathsf{Gr}(n, n-r_1)$ таких, что $\operatorname{rk} x h_1^* \leqslant r'$. Пусть $X = \operatorname{im} x^*$ — пространство строк матрицы x, тогда для искомых кодов имеем

$$\begin{aligned} r' \geqslant \operatorname{rk} x h_1^* = \operatorname{rk} h_1 x^* = \dim \operatorname{im} h_1 x^* = \dim h_1 X = \dim(X/\ker h_1|_X) \\ = \underbrace{\dim(X)}_{\operatorname{rk} x} - \dim(\underbrace{\ker h_1}_{\mathscr{C}_1} \cap X), \end{aligned}$$

т. е. $\dim(X \cap \mathscr{C}_1) \geqslant \dim X - r' = \operatorname{rk} x - r' \geqslant r_1 - r' \geqslant r_1/2$. По лемме 2 имеем

$$\begin{aligned} \mathsf{P}(\operatorname{rk} x h_1^* \leqslant r') &\leqslant \mathsf{P}\big(\dim(X \cap \mathscr{C}_1) \geqslant \dim X - r'\big) \\ &\leqslant 4q^{-(\dim X - r')(n + (\dim X - r') - \dim X - (n - r_2))} \\ &= 4q^{-(\dim X - r')(r_2 - r')} \leqslant 4q^{-\frac{1}{4}r_1 r_2}. \end{aligned}$$

Теперь зафиксируем код $\mathscr{C}_1$ и матрицу h_1 такую, что $\operatorname{rk} xh_1^* \geqslant r'$, и оценим вероятность того, что $h_2 x h_1^* = 0$. Как уже отмечалось ранее, условие $h_2 x h_1^* = 0$ эквивалентно $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$, следовательно, выполняется оно или нет, зависит только от кодов $\mathscr{C}_1$ и $\mathscr{C}_2$ и не зависит от конкретного выбора проверочных матриц h_1 и h_2. Это можно переписать как $\operatorname{im} xh_1^* \subseteq \ker h_2 = \mathscr{C}_2$. Пусть $U := \operatorname{im} xh_1^*$, $u := \dim U = \operatorname{rk} xh_1^*$. Имеем $u \geqslant r'$,

$$\mathsf{P}(U \subseteq \mathscr{C}_2) = \mathsf{P}(\mathscr{C}_2^\perp \subseteq U^\perp) = \frac{\binom{n-u}{r_2}_q}{\binom{n}{r_2}_q} \leqslant q^{-ur_2} \leqslant q^{-r'r_2}.$$

Заметим, что $\mathsf{P}(\operatorname{rk} xh_1^* > r' \wedge h_2(xh_1^*) = 0) \leqslant q^{-r'r_2}$, потому что мы можем сначала выбрать $\mathscr{C}_1$, а когда $\mathscr{C}_1$ (и, следовательно, $U = \operatorname{im} xh_1^*$) фиксировано, мы независимо выбираем $\mathscr{C}_2$. Таким образом, мы можем оценить

$$\begin{aligned}\mathsf{P}(h_2 x h_1^* = 0) &\leqslant \mathsf{P}(\operatorname{rk} xh_1^* \leqslant r') + \mathsf{P}(\operatorname{rk} xh_1^* > r' \wedge h_2(xh_1^*) = 0) \\ &\leqslant 4q^{-\frac{1}{4}r_1 r_2} + q^{-r'r_2} \leqslant 5q^{-\frac{1}{4}r_1 r_2},\end{aligned}$$

что завершает доказательство.

Напомним, что подпространство $V \subseteq \mathbb{F}_q^n$ мы называем *α-разреженным*, если оно может быть порождено векторами с весом Хэмминга не более αn, а множество таких векторов мы обозначаем через $S(n, \alpha)$. Другими словами, V является α-разреженным тогда и только тогда, когда $V = \langle V \cap S(n, \alpha) \rangle$.

Лемма 4. *Для каждого $\rho \in (0, 1)$, $n \in \mathbb{N}$, $r \geqslant \rho n$ случайное подпространство $U \in \mathsf{Gr}(n, n-r)$ с вероятностью не менее $1 - 4\frac{q^{-r/8}}{1-q^{-r/8}}$ для всех $m \in [r]$ обладает следующим свойством:*

(*) для каждого α-разреженного $V \in \mathsf{Gr}(n, m)$ выполнено $\dim(U \cap V) < \frac{m}{2}$,

где $\alpha = H_q^{-1}(\rho/8)$.

Доказательство. Зафиксируем $m \in [1, r]$ и рассмотрим α-разреженное m-мерное подпространство $V \subseteq \mathbb{F}_q^n$. По лемме 2 вероятность того, что V является контрпримером к свойству $(*)$ для $(n-r)$-мерного подпространства U (т.е. $\dim(U \cap V) \geqslant m/2$), можно оценить следующим образом:

$$\mathsf{P}(\dim(U \cap V) \geqslant \lceil m/2 \rceil) \leqslant 4q^{-\lceil m/2 \rceil (n + \lceil m/2 \rceil - m - (n-r))} \leqslant 4q^{-m(r-m/2)/2} \leqslant 4q^{-mr/4}. \tag{6}$$

Заметим, что существует не более $|S(n, \alpha)|^m$ способов выбрать m базисных векторов для α-разреженного подпространства V. Мы можем оценить это число следующим образом:

$$|S(n, \alpha)|^m \leqslant \left(\sum_{i=0}^{\lfloor n\alpha \rfloor} \binom{n}{i} (q-1)^i \right)^m \leqslant q^{mnH_q(\alpha)} = q^{mn\rho/8} \leqslant q^{mr/8}.$$

Теперь мы можем получить верхнюю оценку на вероятность, что свойство $(*)$ не выполнено для случайного $U \in \mathsf{Gr}(n, n-r)$ и размерности m, просуммировав оценку (6) по всевозможным α-разреженным подпространствам V размерности m:

$$\begin{aligned}\mathsf{P}((*) \text{ не выполняется при } \dim V = m) &\leqslant \sum_V \overbrace{\mathsf{P}((*) \text{ не выполняется для } V)}^{\leqslant 4q^{-mr/4}} \\ &\leqslant q^{mr/8} \cdot 4q^{-mr/4} \leqslant 4q^{-mr/8}.\end{aligned}$$

Наконец, суммируя по всевозможным размерностям $m \in [r]$, мы имеем

$$\mathsf{P}((*)\text{не выполняется при } \dim V \in [r]) \leqslant 4 \sum_{m=1}^{r} q^{-mr/8} < 4 \frac{q^{-r/8}}{1-q^{-r/8}}.$$

Заметим, что если для $(n-r)$ размерного подпространства $U \subseteq \mathbb{F}_q^n$ выполнено свойство $(*)$ и $r \geqslant 2$, то минимальное расстояние кода U больше $2\alpha n$.

3.2. Доказательство теоремы 3. Начнем с доказательства некоторых вспомогательных лемм.

Мы будем пользоваться тем, что тензорное произведение пространств дистрибутивно относительно сумм и пересечений: для любых пространств $A, B, C \subseteq \mathbb{F}_q^n$ выполнено

$$(A+B) \otimes C = (A \otimes C) + (B \otimes C), \qquad (A \cap B) \otimes C = (A \otimes C) \cap (B \otimes C).$$

В доказательстве мы будем много раз применять следующую лемму.

Лемма 5. *Для любых линейных кодов $A, B, C, D, E, F \subseteq \mathbb{F}_q^n$ выполнено*

$$A \otimes B \cap (C \otimes D + E \otimes F) = A \otimes B \cap (C' \otimes D + E \otimes F),$$

где $C' = C \cap (A+E)$.

Доказательство. Включение правой части в левую очевидно. Поэтому остается проверить включение в обратном направлении. Пусть $x \in A \otimes B \cap (C \otimes D + E \otimes F)$. Тогда $x = x_1 + x_2$, где $x_1 \in C \otimes D$, $x_2 \in E \otimes F$. Поэтому получаем $x_1 = x - x_2 \in E \otimes F + A \otimes B \subseteq (E+A) \otimes (F+B)$. Однако, так как $x_1 \in C \otimes D$, получаем, что $x_1 \in (C \otimes D) \cap ((E+A) \otimes (F+B)) \subseteq (C \cap (A+E)) \otimes D$. Поэтому получаем $x = x_1 + x_2 \in ((C \cap (A+E)) \otimes D + E \otimes F) \cap A \otimes B$, и доказательство завершено.

Лемма 6. *Для линейных кодов $\mathscr{C}_1, \mathscr{C}_2, X, Y \subseteq \mathbb{F}_q^n$ имеем*

$$(X \otimes Y) \cap (\mathscr{C}_1 \boxplus \mathscr{C}_2) = (X \cap \mathscr{C}_1) \otimes Y + X \otimes (Y \cap \mathscr{C}_2).$$

Доказательство. Доказательство следует из следующей цепочки равенств:

$$\begin{aligned}
&= (X \otimes Y) \cap (\mathscr{C}_1 \boxplus \mathscr{C}_2) = (X \otimes Y) \cap (\mathscr{C}_1 \otimes \mathbb{F}_q^n + \mathbb{F}_q^n \otimes \mathscr{C}_2) = \\
&= (\text{применяем дважды лемму 5}) = (X \otimes Y) \cap (\mathscr{C}_1 \otimes \underline{(Y + \mathscr{C}_2)} + \underline{(X + \mathscr{C}_1)} \otimes \mathscr{C}_2) = \\
&= (\text{т.к. } \mathscr{C}_1 \otimes \mathscr{C}_2 \subseteq (X + \mathscr{C}_1) \otimes \mathscr{C}_2) = (X \otimes Y) \cap (\mathscr{C}_1 \otimes Y + (X + \mathscr{C}_1) \otimes \mathscr{C}_2) = \\
&= (\text{применяем лемму 5}) = (X \otimes Y) \cap (\mathscr{C}_1 \otimes Y + (X + \mathscr{C}_1) \otimes \underline{(\mathscr{C}_2 \cap Y)}) = \\
&= (\text{т.к. } \mathscr{C}_1 \otimes (\mathscr{C}_2 \cap Y) \subseteq \mathscr{C}_1 \otimes Y) = (X \otimes Y) \cap (\mathscr{C}_1 \otimes Y + X \otimes (\mathscr{C}_2 \cap Y)) = \\
&= (\text{применяем лемму 5}) = (X \otimes Y) \cap (\underline{(\mathscr{C}_1 \cap X)} \otimes Y + X \otimes (\mathscr{C}_2 \cap Y)) = \\
&= (\text{каждое слагаемое лежит в } X \otimes Y) = (\mathscr{C}_1 \cap X) \otimes Y + X \otimes (\mathscr{C}_2 \cap Y).
\end{aligned}$$

Лемма доказана.

Следующая лемма является аналогом для двойственных произведений кодов $\mathscr{C}_1 \boxplus \mathscr{C}_2$ «метода прямоугольников», первоначально разработанного для произведений кодов $\mathscr{C}_1 \otimes \mathscr{C}_2$ (см. [16, 44]).

Л е м м а 7. *Рассмотрим линейные коды* $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$. *Если* $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$, *и для* $A_1, A_2 \subseteq [n]$ *таких, что* $n - |A_i| < d(\mathscr{C}_i)$, $i \in [2]$, *имеем* $x(A_1, A_2) = 0$, *то* x *можно представить как сумму* $n - |A_1|$ *столбцов из* $\mathscr{C}_2$ *и* $n - |A_2|$ *строк из* $\mathscr{C}_1$.

Д о к а з а т е л ь с т в о.

Поскольку $n - |A_i| < d(\mathscr{C}_i)$, индексное множество A_i содержит информационное множество*) I_i кода $\mathscr{C}_i$, $i \in [2]$. Поэтому мы можем однозначно выбрать $\Delta_1 \in \mathscr{C}_1 \otimes \mathbb{F}_q^{\bar{A}_2}$ и $\Delta_2 \in \mathbb{F}_q^{\bar{A}_1} \otimes \mathscr{C}_2$ такие, что $\Delta_1(I_1, \bar{A}_2) = x(I_1, \bar{A}_2)$ и $\Delta_2(\bar{A}_1, I_2) = x(\bar{A}_1, I_2)$, где $\bar{I}_i := [n] \setminus I_i$, $\bar{A}_i := [n] \setminus A_i$. Рассмотрим $x' = x - \Delta_1 - \Delta_2$. Тогда имеем $x'(I_1, \cdot) = 0$, $x'(\cdot, I_2) = 0$, и поэтому $x' \in \mathbb{F}_q^{\bar{I}_1} \otimes \mathbb{F}_q^{\bar{I}_2}$ (правая часть на рис. 1). Так как $x' \in \mathscr{C}_1 \boxplus \mathscr{C}_2$, то по лемме 6 получаем

$$x' \in \underbrace{(\mathbb{F}_q^{I_1} \cap \mathscr{C}_1)}_{=\{0\}} \otimes \mathbb{F}_q^{I_2} + \mathbb{F}_q^{I_1} \otimes \underbrace{(\mathbb{F}_q^{I_2} \cap \mathscr{C}_2)}_{=\{0\}} = \{0\}.$$

Здесь $\mathbb{F}_q^{\bar{I}_i} \cap \mathscr{C}_i = \{0\}$, так как I_i является информационным множеством $\mathscr{C}_i$. Поэтому $x' = 0$ и $x = \Delta_1 + \Delta_2$ и, более того, Δ_1 является суммой не более $|\bar{A}_2| = n - |A_2|$ ненулевых строк из $\mathscr{C}_1$, а Δ_2 является суммой не более $|\bar{A}_1| = n - |A_1|$ ненулевых столбцов из $\mathscr{C}_2$, и лемма доказана.

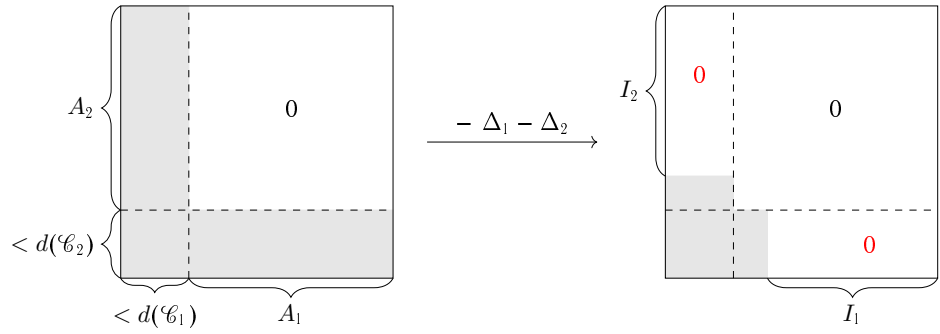


Рис. 1. Идея доказательства леммы о нулевых прямоугольниках

Л е м м а 8. *Рассмотрим линейные коды* $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$, *кодовое слово* $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$, *пространства* $X = \operatorname{im} x^*$ *и* $Y = \operatorname{im} x$, *порожденные соответственно строками и столбцами из* x. *Тогда мы имеем*

$$\operatorname{rk} x \leqslant \dim(X \cap \mathscr{C}_1) + \dim(Y \cap \mathscr{C}_2).$$

Д о к а з а т е л ь с т в о. Нетрудно проверить, что $x \in (X \otimes Y) \cap (\mathscr{C}_1 \boxplus \mathscr{C}_2)$. По лемме 6 имеем $x \in (X \cap \mathscr{C}_1) \otimes Y + X \otimes (Y \cap \mathscr{C}_2)$. Поэтому $x = x_1 + x_2$ для некоторых $x_1 \in (X \cap \mathscr{C}_1) \otimes Y$, $x_2 \in X \otimes (Y \cap \mathscr{C}_2)$. Отсюда для матриц x_1, x_2 мы имеем $\operatorname{rk} x_1 \leqslant \dim(X \cap \mathscr{C}_1)$, $\operatorname{rk} x_2 \leqslant \dim(Y \cap \mathscr{C}_2)$, и поэтому

$$\operatorname{rk} x \leqslant \operatorname{rk} x_1 + \operatorname{rk} x_2 \leqslant \dim(X \cap \mathscr{C}_1) + \dim(Y \cap \mathscr{C}_2).$$

*) Информационное множество для линейного кода $\mathscr{C} \subseteq \mathbb{F}_q^n$ — это наименьшее по включению индексное множество $I \subseteq [n]$ такое, что для каждого $c \in \mathscr{C}$ если $c|_I = 0$, то $c = 0$. Ясно, что для каждого $S \subseteq [n]$ такого, что $|S| > n - d(\mathscr{C})$, если для некоторого кодового слова $c \in \mathscr{C}$ имеем $c|_S = 0$, то $c = 0$. Следовательно, должно существовать информационное множество $I \subseteq S$.

Лемма 9. *Рассмотрим линейные коды* $\mathscr{C}_1$, $\mathscr{C}_2 \subseteq \mathbb{F}_q^n$, *и кодовое слово* $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$. *Тогда для каждого* $A_1, A_2 \subseteq [n]$ *существует* $x' \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ *такое, что**) $x'(A_1, A_2) = x(A_1, A_2)$ *и* $\operatorname{rk} x' = \operatorname{rk} x(A_1, A_2)$.

Доказательство. Сначала определим операторы проекции $\pi_i \colon \mathbb{F}_q^n \to \mathbb{F}_q^{A_i}$, $\pi_i x = x|_{A_i}$, $i \in [2]$. Рассмотрим $\mathscr{C}_i|_{A_i} := \pi_i \mathscr{C}_i$. Зафиксируем базис B_i^0 подпространства $\mathscr{C}_i|_{A_i}$ и расширим его до базиса B_i пространства $\mathbb{F}_q^{A_i}$. Теперь определим оператор g_i на базисе B_i. Поскольку для каждого вектора $e \in B_i^0$ существует вектор $\bar{e} \in \mathscr{C}_i$ такой, что $\pi \bar{e} = e$, мы можем положить по определению, что $g_i e := \bar{e}$. Поскольку для каждого вектора $e \in B_i \setminus B_i^0$ существует вектор $\bar{e} \in \mathbb{F}_q^n$ такой, что $\pi \bar{e} = e$, мы можем положить по определению $g_i e := \bar{e}$. Теперь из определения выше мы имеем $\pi_i g_i = \mathrm{id}$ и $g_i(\mathscr{C}_i|_{A_i}) \subseteq \mathscr{C}_i$.

Если положить $x' := (g_1 \otimes g_2) x(A_1, A_2)$, то получим

$$x'(A_1, A_2) = (\pi_1 \otimes \pi_2) x' = (\pi_1 \otimes \pi_2)(g_1 \otimes g_2) x(A_1, A_2) = x(A_1, A_2).$$

Заметим, что $x(A_1, A_2) = (\pi_1 \otimes \pi_2) x \in \mathscr{C}_1|_{A_1} \otimes \mathbb{F}_q^{A_2} + \mathbb{F}_q^{A_1} \otimes \mathscr{C}_2|_{A_2}$. Кроме того, $(g_1 \otimes g_2)(\mathscr{C}_1|_{A_1} \otimes \mathbb{F}_q^{A_2} + \mathbb{F}_q^{A_1} \otimes \mathscr{C}_2|_{A_2}) = g_1 \mathscr{C}_1|_{A_1} \otimes \operatorname{im} g_2 + \operatorname{im} g_1 \otimes g_2 \mathscr{C}_2|_{A_2} \subseteq \mathscr{C}_1 \otimes \mathbb{F}_q^n + \mathbb{F}_q^n \otimes \mathscr{C}_2$ и поэтому $x' \in \mathscr{C}_1 \boxplus \mathscr{C}_2$. Также легко видеть, что $\operatorname{rk} x' \leqslant \operatorname{rk} x(A_1, A_2)$. Наконец, поскольку $x'(A_1, A_2) = x(A_1, A_2)$, получаем $\operatorname{rk} x' = \operatorname{rk} x(A_1, A_2)$.

Лемма 10. *Рассмотрим линейные коды* $\mathscr{C}_1 \in \mathsf{Gr}(n, n - r_1)$, $\mathscr{C}_2 \in \mathsf{Gr}(n, n - r_2)$, *удовлетворяющие свойству* (*). *Тогда* $d(\mathscr{C}_i) > \alpha_i n$, *и каждое кодовое слово* $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ *с весом* $|x| \leqslant \alpha_1 \alpha_2 n^2/4$ *и рангом* $\operatorname{rk} x \leqslant \min(r_1, r_2)$ *имеет нулевой прямоугольник* $A_1 \times A_2$, *где* $\alpha_i := H_q^{-1}(\frac{r_i}{8n})$, $|A_1| \geqslant n - \dfrac{|x|}{\alpha_2 n/2}$, $|A_2| \geqslant n - \dfrac{|x|}{\alpha_1 n/2}$.

Доказательство. Сначала зафиксируем вектор $v \in \mathbb{F}_q^n$, $|v| \leqslant \alpha_i n$, определим одномерное пространство $V := \langle v \rangle \subseteq \mathbb{F}_q^n$ и используем свойство (*) для $\mathscr{C}_i$, $i \in [2]$. В результате получим $\dim(\mathscr{C}_i \cap V) < 1/2$, а значит $v \neq \mathscr{C}_i$. Отсюда $d(\mathscr{C}_i) > \alpha_i n$, $i \in [2]$.

Теперь рассмотрим кодовое слово $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ с весом $|x| < \alpha_1 \alpha_2 n^2/4$ и рангом $\operatorname{rk} x \leqslant \min(r_1, r_2)$. Пусть A_1 (соотв. A_2) — множество индексов столбцов (соотв. строк) матрицы x веса не более $\alpha_2 n/2$ (соотв. $\alpha_1 n/2$), $\bar{A}_i := [n] \setminus A_i$, $i \in [2]$. Тогда $|x| \geqslant \max(|\bar{A}_2|\alpha_1, |\bar{A}_1|\alpha_2) n/2$ и поэтому

$$|\bar{A}_1| \leqslant \frac{|x|}{\alpha_2 n/2} \leqslant \alpha_1 n/2 < d(\mathscr{C}_1), \qquad |\bar{A}_2| \leqslant \frac{|x|}{\alpha_1 n/2} \leqslant \alpha_2 n/2 < d(\mathscr{C}_2).$$

Это означает, что A_i содержит информационное множество кода $\mathscr{C}_i$, $i \in [2]$. Теперь предположим, что $A_1 \times A_2$ не является нулевым прямоугольником кодового слова x, т. е. $x(A_1, A_2) \neq 0$. По лемме 9 существует кодовое слово $x' \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ такое, что $x'(A_1, A_2) = x(A_1, A_2)$, все строки (соотв. столбцы) x' порождаются строками $x'(\cdot, A_2)$ (соотв. столбцами $x'(A_1, \cdot)$). Поскольку $|x'(i, \cdot)| \leqslant |x'(i, A_2)| + |\bar{A}_2| = |x(i, A_2)| + |\bar{A}_2| \leqslant \alpha_2 n$ для $i \in A_1$, пространство столбцов Y матрицы x' является α_2-разреженным. Аналогично пространство строк X матрицы x' является α_1-разреженным. Из свойства (*) для кодов $\mathscr{C}_1$ и $\mathscr{C}_2$ получаем $\dim(\mathscr{C}_1 \cap X) < \frac{1}{2} \dim X$, $\dim(\mathscr{C}_2 \cap Y) < \frac{1}{2} \dim Y$, и поэтому

*) Иначе говоря, все строки (соотв. столбцы) из x' являются линейными комбинациями строк из $x'(\cdot, A_2)$ (соотв. столбцов из $x(A_1, \cdot)$).

по лемме 8 получаем противоречие:

$$\operatorname{rk} x' \leqslant \dim(\mathscr{C}_1 \cap X) + \dim(\mathscr{C}_2 \cap Y) < \frac{1}{2}\dim X + \frac{1}{2}\dim Y = \operatorname{rk} x'.$$

Значит, $X(A_1, A_2) = 0$. Следовательно, $A_1 \times A_2$ — нулевой прямоугольник в x с требуемыми параметрами.

Т е о р е м а 3. *Для любых* $\varepsilon_1 \in (0,1)$, $\varepsilon_2 \in (0,1)$ *существует* $\rho > 0$ *такое, что доля пар кодов* $(\mathscr{C}_1, \mathscr{C}_2) \in \mathsf{Gr}(n, n-r_1) \times \mathsf{Gr}(n, n-r_2)$, *для которых выполнено* $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$, *стремится к* 1 *при* $n \to \infty$, $r_1 \geqslant \varepsilon_1 n$, $r_2 \geqslant \varepsilon_2 n$.

Д о к а з а т е л ь с т в о. Пусть $\alpha_i = H_q^{-1}(\varepsilon_i/8)$, $i \in [2]$,

$$\rho = \frac{1}{2}\min\left(\frac{\alpha_1\alpha_2}{4}, H_q^{-1}\left(\frac{\varepsilon_1\varepsilon_2}{8}\right)\right). \tag{7}$$

Рассмотрим $r_1 \geqslant \varepsilon_1 n$, $r_2 \geqslant \varepsilon_2 n$. Для простоты предположим, что n достаточно велико и $\min(r_1, r_2) \geqslant 8$. Рассмотрим два случая «плохих» пар кодов и оценим долю таких пар (эту долю мы также интерпретируем как вероятность, что случайно выбранная пара кодов — «плохая»).

1. Множество $P_1 \subseteq P(n, r_1, r_2)$ всех пар $(\mathscr{C}_1, \mathscr{C}_2)$ таких, что существует $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$ веса $|x| \leqslant 2\rho n^2$ и ранга $\operatorname{rk} x \geqslant \min(r_1, r_2)$. Используя лемму 3 и суммируя по всевозможным словам x веса не более $2\rho n^2$, получаем оценку:

$$\begin{aligned}\mathsf{P}(P_1) \leqslant \sum_{i=0}^{\lfloor 2\rho n^2 \rfloor} \binom{n^2}{i}(q-1)^i \cdot 5q^{-\frac{1}{4}r_1 r_2} &\leqslant q^{n^2 H_q(2\rho)} \cdot 5q^{-\frac{1}{4}n^2\varepsilon_1\varepsilon_2} \\ &\leqslant 5q^{\frac{1}{8}n^2\varepsilon_1\varepsilon_2 - \frac{1}{4}n^2\varepsilon_1\varepsilon_2} = 5q^{-\frac{1}{8}n^2\varepsilon_1\varepsilon_2}. \end{aligned} \tag{8}$$

2. Множество $P_2 \subseteq P(n, r_1, r_2)$ всех таких пар $(\mathscr{C}_1, \mathscr{C}_2)$, что один из кодов не обладает свойством $(*)$. По лемме 4 вероятность того, что $\mathscr{C}_i$ не обладает свойством $(*)$, не больше $4\frac{q^{-r_i/8}}{1-q^{-r_i/8}}$. Отсюда получаем:

$$\mathsf{P}(P_2) \leqslant 4\frac{q^{-r_1/8}}{1-q^{-r_1/8}} + 4\frac{q^{-r_2/8}}{1-q^{-r_2/8}} \leqslant 16q^{-\frac{1}{8}\min(r_1, r_2)} \leqslant 16q^{-\frac{1}{8}n\min(\varepsilon_1, \varepsilon_2)}. \tag{9}$$

Комбинируя (8) и (9), получаем $\mathsf{P}(P(n, r_1, r_2) \setminus P_1 \setminus P_2) \to 1$ при $n \to \infty$, $r_1 \geqslant \varepsilon_1 n$, $r_2 \geqslant \varepsilon_2 n$.

Остается показать, что $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$ для любой пары $(\mathscr{C}_1, \mathscr{C}_2) \in P(n, r_1, r_2) \setminus P_1 \setminus P_2$. Пусть у нас есть ненулевое кодовое слово $x \in \mathscr{C}_1 \boxplus \mathscr{C}_2$. Рассмотрим два случая:

1. Случай $|x| \geqslant 2\rho n^2$. Слово x всегда можно представить как сумму строк из $\mathscr{C}_1$ и столбцов из $\mathscr{C}_2$. Однако общее количество строк и столбцов равно $2n \leqslant \frac{|x|}{\rho n}$.

2. Случай $|x| < 2\rho n^2$. Поскольку $(\mathscr{C}_1, \mathscr{C}_2) \notin P_1$, то $\operatorname{rk} x < \min(r_1, r_2)$. Следовательно, так как $|x| \leqslant \frac{\alpha_1\alpha_2}{4}n^2$ и коды $\mathscr{C}_1, \mathscr{C}_2$ обладают свойством $(*)$, то по лемме 10 слово x имеет нулевой прямоугольник $A_1 \times A_2$, где $|A_1| \geqslant n - \frac{2|x|}{\alpha_2 n}$, $|A_2| \geqslant n - \frac{2|x|}{\alpha_1 n}$ и $d(\mathscr{C}_i) \geqslant \alpha_i n$. Тогда по лемме 7 слово x можно представить как сумму $n - |A_2|$ строк из $\mathscr{C}_1$ и $n - |A_1|$ столбцов из $\mathscr{C}_2$. Поэтому мы получаем оценку $(n - |A_1|) + (n - |A_2|) \leqslant \frac{2|x|}{\alpha_1 n} + \frac{2|x|}{\alpha_2 n} \leqslant \frac{|x|}{(\alpha_1\alpha_2/4)n} < \frac{|x|}{\rho n}$.

Итак, мы получили, что во всех случаях x можно представить не более чем $\frac{|x|}{\rho n}$ строк из $\mathscr{C}_1$ и столбцов из $\mathscr{C}_2$. А значит, $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$.

Следствие 1. *Для каждого* $R_1 \in (0,1)$, $R_2 \in (0,1)$ *существует* $\rho > 0$ *такое, что доля пар кодов* $(\mathscr{C}_1, \mathscr{C}_2) \in \mathsf{Gr}(n, k_1) \times \mathsf{Gr}(n, k_2)$, *для которых* $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$ *и* $\rho(\mathscr{C}_1^{\perp}, \mathscr{C}_2^{\perp}) \geqslant \rho$, *стремится к 1 при* $n \to \infty$, $k_1/n \to R_1$, $k_2/n \to R_2$.

Доказательство. Сначала заметим, что вместо фиксации $r_i = \lceil \varepsilon_i n \rceil$ в доказательстве теоремы 3 мы можем зафиксировать любое $r_i \geqslant \varepsilon_i n$, поэтому мы можем заменить $\lceil \varepsilon_i n \rceil$ на любое $r_i \geqslant \varepsilon_i n$ в утверждении теоремы без изменения доказательства.

Следовательно, $r_i \geqslant (R_i - \delta)n$ и $1 - r_i \geqslant (1 - R_i - \delta)n$. Зафиксируем $\delta = \min(R_1, R_2, 1 - R_1, 1 - R_2)/2$. Применяя теорему 3 с параметрами $\varepsilon_i = (1 - R_i - \delta)$, $i = 1, 2$, имеем, что для некоторого $\rho_1 > 0$ для случайной пары кодов $(\mathscr{C}_1, \mathscr{C}_2) \in P(n, r_1, r_2)$ с высокой вероятностью выполнено $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho_1$, если $r_i \geqslant (1 - R_i - \delta)n$, $i = 1, 2$. Применяя теорему 3 с параметрами $\varepsilon_i = (R_i - \delta)$, $i = 1, 2$, мы имеем, что для некоторого $\rho_2 > 0$ для случайной пары кодов $(\mathscr{C}_1^{\perp}, \mathscr{C}_2^{\perp}) \in P(n, n - r_1, n - r_2)$ с высокой вероятностью выполнено $\rho(\mathscr{C}_1^{\perp}, \mathscr{C}_2^{\perp}) \geqslant \rho_2$, если $n - r_i \geqslant (R_i - \delta)n$, $i = 1, 2$.

Поскольку $k_i/n \to R_i$, при достаточно большом n имеем $R_i - \delta \leqslant k_i/n \leqslant R_i + \delta$, $i = 1, 2$. Имеем $\mathsf{Gr}(n, k_1) \times \mathsf{Gr}(n, k_2) = P(n, r_1, r_2)$, где $r_i = n - k_i \in [(1 - R_i - \delta)n, (1 - R_i + \delta)n]$, $i = 1, 2$. Следовательно, если взять $\rho = \min(\rho_1, \rho_2)$, то для случайной пары кодов $(\mathscr{C}_1, \mathscr{C}_2) \in \mathsf{Gr}(n, k_1) \times \mathsf{Gr}(n, k_2)$ с высокой вероятностью выполнено $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$ и $\rho(\mathscr{C}_1^{\perp}, \mathscr{C}_2^{\perp}) \geqslant \rho$ при $n \to \infty$.

§ 4. Доказательство основных результатов

4.1. Локальная минимальность. Одной из ключевых идей, используемых в доказательстве нашего основного результата, является идея локальной минимальности. Ранее она применялась в контексте когомологии симплициальных комплексов с $\mathbb{F}_2$-коэффициентами [19, 33]. В настоящей работе мы распространяем эту идею на гораздо более общий контекст (ко)гомологии абстрактных клеточных комплексов с локальными системами коэффициентов.

Рассмотрим клеточный посет X и цепной комплекс $\mathscr{C} = \mathscr{F}X$ с выделенным базисом

$$\ldots \xrightarrow{\partial_{i+1}} \mathscr{C}_i \xrightarrow{\partial_i} \mathscr{C}_{i-1} \xrightarrow{\partial_{i-1}} \ldots$$

над $\mathbb{F}_q$, где $\mathscr{F}$ — локальная система на X. Для краткости обозначим через $|\cdot|_X$ блочный вес $\boldsymbol{wt}_X(\cdot)$, который делает каждый член $\mathscr{C}_i$ в этом комплексе нормированной абелевой группой с нормой $|\cdot|_X$ и позволяет нам определить расстояние стандартным образом: $d(a, b) := |a - b|_X$, $d(a, \mathscr{B}) := \min\limits_{b \in \mathscr{B}} |a - b|_X$. Мы также используем $|\cdot|_X$, чтобы определить для каждого $i \in \mathbb{Z}$ соответствующую норму на i-й гомологической группе $H_i(\mathscr{C}) = Z_i(\mathscr{C})/B_i(\mathscr{C})$, называемую *систолической нормой* по формуле $|\mathscr{A}|_X := \min\limits_{a \in \mathscr{A}} |a|_X$, где $\mathscr{A} \in H_i(\mathscr{C})$, $B_i(\mathscr{C}) = \operatorname{im} \partial_{i+1}$, $Z_i(\mathscr{C}) = \ker \partial_i$. Это, в свою очередь, позволяет нам определить расстояние на $H_i(\mathscr{C})$

как $d(\mathscr{A},\mathscr{B}) := |\mathscr{A}-\mathscr{B}|_X$ и рассмотреть минимальное расстояние $H_i(\mathscr{C})$, заданное стандартными формулами:

$$d(H_i(\mathscr{C})) := \min_{\substack{\mathscr{A}\neq\mathscr{B}\\ \mathscr{A},\mathscr{B}\in H_i(\mathscr{C})}} d(\mathscr{A},\mathscr{B}) = \min_{\mathscr{A}\in H_i(\mathscr{C})\setminus\{B_i(\mathscr{C})\}} |\mathscr{A}|_X = \min_{a\in Z_i(\mathscr{C})\setminus B_i(\mathscr{C})} |a|_X.$$

Заметим, что минимальное расстояние $H_i(\mathscr{C})$ также называется *i-систолическим расстоянием* $\mathscr{C}$, а расстояние $d(H_i(\mathscr{C}^*))$ двойственного цепного комплекса $\mathscr{C}^*$ называется его *i-косистолическим расстоянием*. Эти расстояния связаны с минимальным расстоянием $d(\mathscr{Q})$ квантового CSS-кода $\mathscr{Q}=\mathscr{Q}(\partial_i,\partial_{i+1}^*)$ над $\mathbb{F}_q$, определяемого тремя последовательными членами комплекса

$$\mathscr{C}_{i+1}\xrightarrow{\partial_{i+1}}\mathscr{C}_i\xrightarrow{\partial_i}\mathscr{C}_{i-1}.$$

Легко видеть, что $d(\mathscr{Q})\geqslant\min(d(H_i(\mathscr{C})),d(H_i(\mathscr{C}^*)))$, где мы имеем равенство, если $\mathscr{F}_x=\mathbb{F}_q$ для всех $x\in X$, поскольку блочный вес Хэмминга $\boldsymbol{wt}_X(\cdot)$ не превосходит обычного веса Хэмминга $\boldsymbol{wt}(\cdot)$.

О п р е д е л е н и е 6. Мы говорим, что i-цепь $c\in\mathscr{C}_i$, $i\in\mathbb{Z}$, является *локально минимальной* (*относительно* X), если $|c+\partial ax|_X\geqslant|c|_X$ для всех $x\in X(i+1)$ и $a\in\mathscr{F}_x$. Мы также определяем значение

$$d_{\mathrm{LM}}^{(i)}(\mathscr{C}) := \min\{|c|_X \mid c\in Z_i(\mathscr{C})\setminus\{0\}, c \text{ локально минимален}\}.$$

Если у нас нет ненулевых локально минимальных i-циклов, то мы предполагаем, что $d_{\mathrm{LM}}^{(i)}(\mathscr{C})=\infty$.

Заметим, что в общем случае $d_{\mathrm{LM}}^{(i)}(\mathscr{C})$ не равно минимальному расстоянию $Z_i(\mathscr{C})$, так как кодовые слова минимального веса из $Z_i(\mathscr{C})$ необязательно локально минимальны. Например, в контексте w-ограниченных qLDPC-кодов, где $|\partial x|\leqslant w$ для каждого $x\in X(i+1)$, и таким образом мы имеем $\partial x\in Z_i(\mathscr{C})$ и $d(Z_i(\mathscr{C}))\leqslant w$, то видно, что кодовое слово $c=\partial x$ не является локально минимальным, так как $|c-\partial x|=0<|c|$.

Следующая лемма связывает $d_{\mathrm{LM}}^{(i)}(\mathscr{C})$ со свойствами соответствующих квантовых и классических кодов, полученных из комплекса $\mathscr{C}$. Первое утверждение можно использовать для получения нижней оценки на минимальное расстояние $d(\mathscr{Q})$ соответствующего квантового CSS-кода $\mathscr{Q}$, а второе — для того, чтобы показать, что пространство $Z_{i+1}(\mathscr{C})$ является локально тестируемым кодом.

Л е м м а 11. *Пусть $\mathscr{C}=\mathscr{F}X$ — цепной комплекс, где $\mathscr{F}$ — локальная система на X. Тогда для каждого $i\in\mathbb{Z}$ имеем*

$$d(H_i(\mathscr{C}))\geqslant d_{\mathrm{LM}}^{(i)}(\mathscr{C}),$$

и для каждой цепи $c\in\mathscr{C}_{i+1}$ такой, что $|\partial c|_X<d_{\mathrm{LM}}^{(i)}(\mathscr{C})$, имеем

$$|\partial c|_X\geqslant d(c,Z_{i+1}(\mathscr{C})). \tag{10}$$

Д о к а з а т е л ь с т в о. По определению мы имеем

$$d(H_i(\mathscr{C}))=|c_0|_X,\quad\text{где}\quad c_0:=\operatorname*{arg\,min}_{c\in Z_i(\mathscr{C})\setminus B_i(\mathscr{C})}|c|_X.$$

Поскольку элемент c_0 имеет минимальную норму в смежном классе $c_0+B_i(\mathscr{C})$, то он также локально минимален. Следовательно, имеем $d(H_i(\mathscr{C}))=|c_0|_X\geqslant d_{\mathrm{LM}}^{(i)}(\mathscr{C})$.

Второе утверждение докажем индукцией по $|\partial c|_X$. Если $|\partial c|_X = 0$, то $d(c, Z_{i+1}(\mathscr{C})) = 0$ и (10) верно. Рассмотрим $c \in \mathscr{C}_{i+1}$ такой, что $0 < |\partial c|_X < d^{(i)}_{\mathrm{LM}}(\mathscr{C})$. Поскольку $\partial c \in Z_i(\mathscr{C})$ и $|\partial c|_X < d^{(i)}_{\mathrm{LM}}(\mathscr{C})$, мы видим, что ∂c не может быть локально минимальным, а значит, существуют $x \in X(i+1)$, $a \in \mathscr{F}_x$ такие, что $|\partial(c+ax)|_X \leqslant |\partial c|_X - 1$. Поэтому по предположению индукции имеем $|\partial(c+ax)|_X \geqslant d(c+ax, Z_{i+1}(\mathscr{C}))$. Таким образом, получаем

$$d(c, Z_{i+1}(\mathscr{C})) \leqslant d(c+ax, Z_{i+1}(\mathscr{C})) + |ax|_X \leqslant |\partial(c+ax)|_X + \underbrace{|ax|_X}_{=1} \leqslant |\partial c|_X,$$

что завершает доказательство второго утверждения.

4.2. Расширение графов. Пусть Γ — это граф с множеством вершин $V(\Gamma)$ и множеством ребер $E(\Gamma)$. Если вершины $v, v' \in V(\Gamma)$ соединены ребром $e \in E(\Gamma)$, мы называем v, v' *смежными* и обозначаем этот факт $v \leftrightarrow v'$ или $v \leftrightarrow_e v'$, когда хотим подчеркнуть ребро e. Граф Γ называется *w-регулярным*, если все его вершины имеют степень w. *Матрица смежности* графа Γ с $V(\Gamma) = \{v_1, \ldots, v_n\}$ — это матрица $A(\Gamma) = (a_{ij})_{n\times n}$, где a_{ij} — число ребер $e \in E(\Gamma)$ таких, что $v_i \leftrightarrow_e v_j$. Поскольку $A(\Gamma)$ — симметричная матрица, она имеет n вещественных собственных значений $\lambda_1 \geqslant \ldots \geqslant \lambda_n$. Пусть $\lambda_2(\Gamma) := \lambda_2$, и $\lambda(\Gamma) := \max(|\lambda_2|, |\lambda_n|)$. Очевидно, что $\lambda_2(\Gamma) \leqslant \lambda(\Gamma)$.

Определение 7. Мы говорим, что Γ является (n, w, λ)-*экспандером*, если это простой w-регулярный граф на n вершинах такой, что $\lambda = \lambda(G)$. Также мы будем называть граф Γ *односторонним* (n, w, λ)-*экспандером*, если $\lambda = \lambda_2(G)$.

Пример 1. Рассмотрим бесконечное семейство $(p+1)$-регулярных недвудольных графов Рамануджана $X^{p,q}$ из [41], где p и q — два различных простых числа таких, что $q > 2\sqrt{p}$, $p \equiv q \equiv 1 \pmod 4$, и $p^{(q-1)/2} \equiv 1 \pmod q$. Граф $X^{p,q}$ получен в [41] как граф Кэли $\mathrm{Cay}(G, S_{p,q})$, где*) $G := \mathrm{PSL}(\mathbb{F}_q^2)$ и $S_{p,q}$ — некоторое конкретное симметричное множество из $p+1$ генераторов. Обозначим через $\bar{X}^{p,q}$ соответствующее двойное накрытие $\mathrm{Cay}_2(G, S_{p,q})$. Следовательно, $\bar{X}^{p,q}$ — $(p+1)$-регулярный двудольный граф с $n = 2|G|$ вершинами, где $|G| = q(q^2-1)/2$. Поскольку в [41] доказано, что $\lambda(X^{p,q}) \leqslant 2\sqrt{p}$, то мы также имеем $\lambda_2(\bar{X}^{p,q}) \leqslant 2\sqrt{p}$.

Для любого графа Γ через Γ^2 обозначим граф с $V(\Gamma^2) = V(\Gamma)$ и $A(\Gamma^2) = (A(\Gamma))^2$, т. е. число ребер, соединяющих две вершины в Γ^2, равно числу соединяющих их путей длины 2 в Γ. В этом разделе мы докажем несколько технических лемм для установления расширяющих свойств графов Λ и Λ^2, где Λ — граф, определенный в подразделе 2.1. Если $\Gamma = (V, E)$ — граф (возможно, с кратными ребрами) и $S, T \subseteq V$, то $E_\Gamma(S, T)$ обозначает множество ориентированных ребер из S в T, то есть $E_\Gamma(S, T) := \{(s, e, t) \mid e \in E; s \in S, t \in T; s \leftrightarrow_e t\}$ (каждое ребро, соединяющее $s, t \in S \cap T$, учитывается дважды). Мы также обычно пишем $E(S, T)$ вместо $E_\Gamma(S, T)$, если граф Γ ясен из контекста.

Без доказательства приведем лемму Алона — Чанга для односторонних (n, w, λ)-экспандеров [29, Lemma 2.5].

Лемма 12 (Алона — Чанга, [29]). *Если $\Gamma = (V, E)$ — w-регулярный граф с n вершинами и $\lambda = \lambda_2(\Gamma)$, то для каждого $S \subseteq V$ имеем*

$$|E(S, S)| \leqslant \frac{1}{n}\left(w|S|^2 + \lambda|S|(n - |S|)\right).$$

*) Группа $\mathrm{PSL}(\mathbb{F}_q^2)$ — это *проективная специальная линейная* группа для $\mathbb{F}_q^2$, то есть факторгруппа матриц $A \in \mathbb{F}_q^{2\times 2}$ с $\det A = 1$ по модулю своей подгруппы $\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$.

Далее будет удобно определить понятие (a, λ)-расширяющего графа, которое характеризует реберное расширение для малых подмножеств вершин в графе.

Определение 8. Мы говорим, что граф Γ является (a, λ)-*расширяющим*, если для любого множества $S \subseteq V(\Gamma)$ такого, что $|S| \leqslant a$, выполняется следующее условие:

$$|E(S, S)| \leqslant \lambda |S|.$$

Заметим, что если (a, λ)-расширяющий граф содержит хотя бы одно ребро и $a \geqslant 2$, то, взяв в качестве S пару смежных вершин, мы получим $\lambda \geqslant 1$. Мы будем использовать эту простую нижнюю границу в доказательствах некоторых технических лемм.

Лемма 13. *Если граф* Γ *— односторонний* (n, w, λ)*-экспандер, то он является* $(\lambda n/w, 2\lambda)$*-расширяющим.*

Доказательство. Поскольку Γ является w-регулярным, то из леммы 12 следует, что для любого $S \subseteq V(\Gamma)$ такого, что $|S| \leqslant \lambda n/w$ имеем $|E(S, S)| \leqslant \frac{1}{n}\left(w|S|^2 + \lambda |S|(n - |S|)\right)$. Следовательно, имеем

$$|E(S, S)| \leqslant w\frac{|S|^2}{n} + \lambda |S|\frac{n - |S|}{n} \leqslant \left(\frac{\lambda n}{w} \cdot \frac{w}{n} + \lambda\right)|S| = 2\lambda |S|,$$

и лемма доказана.

Лемма 14. *Любой граф* $\bar{X}^{w-1,t}$ *из примера 1 является* $(n/\sqrt{w}, 4\sqrt{w})$*-расширяющим, где* $n = t(t^2 - 1)$ *— число его вершин.*

Доказательство. Поскольку $\lambda_2(\bar{X}^{w-1,t}) \leqslant 2\sqrt{w-1} \leqslant 2\sqrt{w}$, этот граф — односторонний $(n, w, 2\sqrt{w})$-экспандер и по лемме 13 он является $(2n/\sqrt{w}, 4\sqrt{w})$-расширяющим.

Замечание 9. Далее мы будем использовать следующие свойства (a, λ)-расширяющих графов, которые легко доказать.

1. Если граф Γ является (a, λ)-расширяющим, то Γ также является и (a', λ')-расширяющим для любых $a' \leqslant a$, $\lambda' \geqslant \lambda$.

2. Если граф $\Gamma = (V, E)$ является (a, λ)-расширяющим и $\Gamma' = (V, E')$ является подграфом Γ (т. е. $E' \subseteq E$), то Γ' также является (a, λ)-расширяющим.

3. Если графы $\Gamma_1, \ldots, \Gamma_m$ являются (a, λ)-расширяющими, то их объединение $\Gamma = \Gamma_1 \sqcup \ldots \sqcup \Gamma_m$ также является (a, λ)-расширяющим.

4. Если графы $\Gamma_1, \ldots, \Gamma_m$ имеют одинаковое множество вершин, и Γ_i является (a_i, λ_i)-расширяющим, то их объединение $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_m$ является $(\min\limits_{i \in [m]} a_i, \sum\limits_{i=1}^{m} \lambda_i)$-расширяющим.

4.3. Схема доказательства. В этом подразделе мы дадим некоторые определения и неформальное представление о доказательстве основных результатов. Пусть граф $\widehat{\Gamma} = (\widehat{E}, \widehat{V})$ является G-поднятием некоторого

базового графа Γ. Мы предполагаем, что $\widehat{\Gamma}$ является w-регулярным (a,λ)-расширяющим простым графом с n вершинами. Например, мы можем использовать граф из бесконечного семейства $\bar{X}^{w-1,t}$ из примера 1, для которого по лемме 14 имеем $a=2n/\sqrt{w}$, $\lambda=4\sqrt{w}$.

Пусть $h_1 \in \mathbb{F}_q^{r\times w}$, $h_2 \in \mathbb{F}_q^{r'\times w}$ — некоторые матрицы полного ранга, а $\mathscr{A}\in\mathfrak{T}_G(\widehat{\Gamma},h_1)$, $\mathscr{B}\in\mathfrak{T}_G(\widehat{\Gamma},h_2)$ — соответствующие G-поднятые коды Таннера:

$$\mathscr{A}=\left(\mathbb{F}_q\widehat{E}\xrightarrow{\partial_A}\mathbb{F}_q^r\widehat{V}\right),\qquad \mathscr{B}=\left(\mathbb{F}_q\widehat{E}\xrightarrow{\partial_B}\mathbb{F}_q^{r'}\widehat{V}\right).$$

Теперь, поскольку G свободно действует на $\mathscr{A}$ и $\mathscr{B}$, мы можем рассмотреть комплекс $\mathscr{C}:=\mathscr{A}\otimes_G\mathscr{B}^*$ над $\mathbb{F}_q$:

$$\underbrace{\mathbb{F}_q\widehat{E}\otimes_G\mathbb{F}_q^{r'}\widehat{V}}_{\mathscr{C}_2}\xrightarrow{\partial_2}\underbrace{\overbrace{\mathbb{F}_q\widehat{E}\otimes_G\mathbb{F}_q\widehat{E}}^{\mathscr{C}_F}\oplus\overbrace{\mathbb{F}_q^r\widehat{V}\otimes_G\mathbb{F}_q^{r'}\widehat{V}}^{\mathscr{C}_V}}_{\mathscr{C}_1}\xrightarrow{\partial_1}\underbrace{\mathbb{F}_q^r\widehat{V}\otimes_G\mathbb{F}_2\widehat{E}}_{\mathscr{C}_0}.$$

Удобно представлять $\mathscr{C}$ как цепной комплекс $\mathscr{F}X$, где $\mathscr{F}$ — локальная система коэффициентов на $X:=\widehat{\Gamma}\times_G\widehat{\Gamma}^*$. Поскольку множество X имеет три уровня: $X(2)=E_\rightarrow$, $X(1)=F\cup V$ и $X(0)=E_\uparrow$, нетрудно видеть, что $\mathscr{F}X$ имеет следующий вид:

$$\underbrace{\mathbb{F}_q^{r'}E_\rightarrow}_{\mathscr{C}_2}\xrightarrow{\partial_2}\underbrace{\overbrace{\mathbb{F}_qF}^{\mathscr{C}_F}\oplus\overbrace{\mathbb{F}_q^{r\times r'}V}^{\mathscr{C}_V}}_{\mathscr{C}_1}\xrightarrow{\partial_1}\underbrace{\mathbb{F}_q^rE_\uparrow}_{\mathscr{C}_0},$$

где $\mathbb{F}_q^r\otimes\mathbb{F}_q^{r'}$ мы отождествили с $\mathbb{F}_q^{r\times r'}$.

Замечание 10. Как мы видим, $\mathscr{F}X$ дает нам высокоуровневое представление комплекса $\mathscr{C}$. Например, слева на рис. 2 можно найти графическое представление комплекса тензорного произведения $\mathscr{A}\otimes\mathscr{B}^*$, где $\mathscr{A}\in\mathfrak{T}(D_w;h_1)$, $\mathscr{B}\in\mathfrak{T}(D_w;h_2)$, и $w=8$. Для простоты мы рассматриваем в этом примере обычное тензорное произведение вместо поднятого произведения. Справа на рис. 2 показана «часть» этого комплекса, соответствующая граням и ребрам, инцидентным одной конкретной вершине $v\in V$.

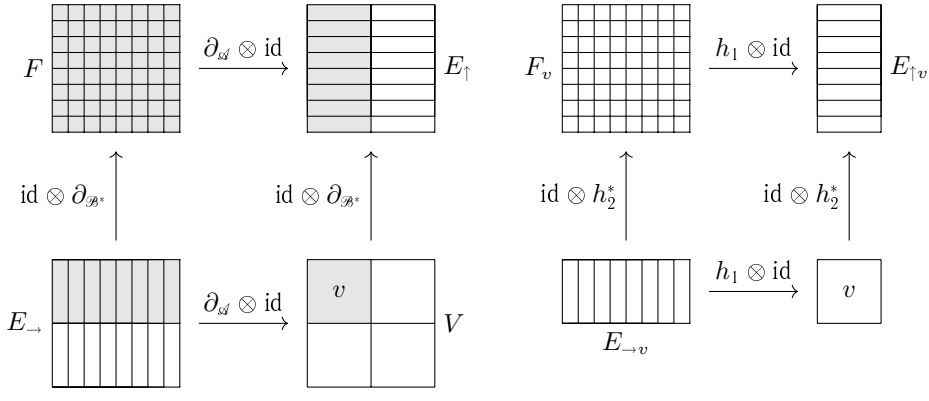


Рис. 2. Высокоуровневый вид комплекса тензорного произведения $\mathscr{A}\otimes\mathscr{B}^*$, где $\mathscr{A}\in\mathfrak{T}(D_w;h_1)$, $\mathscr{B}\in\mathfrak{T}(D_w;h_2)$, и $w=8$ (справа); его часть, соответствующая элементам из X, инцидентным вершине v (слева).

Теперь рассмотрим классический код $Z_2(\mathscr{C})=\ker\partial_2$ и квантовый код $\mathscr{Q}(\mathscr{C}):=\mathscr{Q}(\partial_1,\partial_2^*)$, и покажем, что для некоторого достаточно большого чис-

ла w мы можем выбрать матрицы h_1, h_2 такие, что $Z_2(\mathscr{C})$ и $\mathscr{Q}(\mathscr{C})$ удовлетворяют условиям теорем 1 и 2 соответственно. Самая сложная часть доказательства — показать, что код $Z_2(\mathscr{C})$ локально тестируемый, а $\mathscr{Q}(\mathscr{C})$ имеет линейное минимальное расстояние. Однако из леммы 11 легко следует, что если $\mathscr{C}$ имеет $d^{(1)}_{\mathrm{LM}}(\mathscr{C}) = \Theta(n)$ при $n \to \infty$, то $Z_2(\mathscr{C})$ и $\mathscr{Q}(\mathscr{C})$ обладают желаемыми свойствами. Поэтому нам нужно показать, что для каждого локально минимального 1-цикла $c \in Z_1(\mathscr{C})$ такого, что $\boldsymbol{wt}_X(c) = o(n)$ при $n \to \infty$, выполнено $c = 0$.

Зафиксируем произвольный ненулевой локально минимальный 1-цикл $c = \sum\limits_{x \in X(1)} c_x x \in Z_1(\mathscr{C})$. Тогда $c \neq 0$ и $\partial c = 0$. Имеем $c = c_F + c_V$, где $c_F := c|_F$ и $c_V := c|_V$. Ниже приведен ряд важных определений, используемых в остальной части статьи. Заметим, что некоторые из них зависят от 1-цикла c, который мы зафиксировали. Однако для краткости мы обычно не упоминаем c.

О п р е д е л е н и е 9. Элемент $x \in X(1)$ (вершина или грань) называется *активным*, если $c_x \neq 0$. Вертикальное ребро $e \in E_\uparrow$ называется *активным*, если оно инцидентно активной вершине или активной грани. Более того, ребро e называется *face-active*, если оно не инцидентно ни одной активной вершине (только активной грани).

Нам также потребуется определить множество вершин $L \subseteq V$. Это минимальное множество вершин такое, что:

1) L содержит все активные вершины;

2) если вершина v инцидентна 4 активным граням и $|E_\Lambda(\{v\}, L)| > 2\lambda$, то $v \in L$.

Константа 4 в определении лишь затем, чтобы размер множества L оценивался через вес c без дополнительных множителей: $|L| \leqslant \boldsymbol{wt}_X(c)$. Важным шагом в доказательстве будет показать, что для любой вершины $v \in L$ выполнено

$$|E_\Lambda(\{v\}, L)| > 2\lambda. \qquad (**)$$

В доказательстве, изложенном ниже, мы рассматриваем классические коды, которые являются двойственными кодами к произведениям кодов. В подразделе 4.4 мы определяем специальную характеристику пары кодов $\rho(C_1, C_2)$. Эта величина соответствует локальному расширению в комплексе $\mathscr{C}$. В некотором смысле она играет роль, аналогичную роли минимального расстояния локальных кодов в классическом доказательстве Сипсера и Спилмана из [50], где показано, что экспандерные коды имеют линейное минимальное расстояние.

Из следствия 1 следует, что для фиксированных параметров $R_1, R_2 \in (0, 1)$ (которые будут определять скорость полученного кода) мы можем найти $\rho > 0$, достаточно большое число w и матрицы h_1 и h_2 с w столбцами и примерно $R_1 w$ и $R_2 w$ строками соответственно такие, что выполнено $\rho(\operatorname{im} h_1^*, \ker h_2) \geqslant \rho$ и $\rho(\ker h_1, \operatorname{im} h_2^*) \geqslant \rho$.

В доказательстве мы часто используем расширяющие свойства графа $\Lambda := \widehat{\Gamma} \square_G \widehat{\Gamma}$, определенного в подразделе 2.1. Используя реберное расширение $\widehat{\Gamma}$, в лемме 16 мы покажем, что Λ является $(a, 2\lambda)$-расширяющим.

Предположим, что $\boldsymbol{wt}_X(c) = o(n)$, т. е. число активных вершин и граней относительно мало. Тогда доказательство состоит из следующих шагов.

1. Поскольку каждая вершина $v \in L$ либо сама активна, либо инцидентна активной грани, то $|L| \leqslant \boldsymbol{wt}_X(c) = o(n)$. Следовательно, мы можем использовать свойства расширения графа Λ.

2. Используя свойства расширения графа $\widehat{\Gamma}$, можно показать, что каждое активное ребро инцидентно вершине из L (лемма 18). Заметим, что $(**)$ имеет место для каждой неактивной вершины из L по определению.

3. Используя локальную минимальность c, свойство $\rho(\operatorname{im} h_1^*, \ker h_2) \geqslant \rho$ и пункт 2, мы можем показать, что $(**)$ имеет место для каждой активной вершины (ключевая лемма 19).

4. Из предыдущих двух пунктов следует, что $(**)$ имеет место для каждой вершины $v \in L$ (следствие 2).

5. Поскольку Λ является $(a = \Theta(n), 2\lambda)$-расширяющим и $|L| < a$, получаем, что $L = \varnothing$, следовательно, $c = 0$ (лемма 20).

Следовательно, каждый ненулевой локально минимальный 1-цикл c имеет вес $|c| = \Theta(n)$, значит $d_{\mathrm{LM}}^{(1)}(\mathscr{C}) = \Theta(n)$ при $n \to \infty$, которое, в свою очередь, того же порядка, что и длина классических или квантовых кодов, полученных из цепного комплекса $\mathscr{C}$. Следовательно, по лемме 11 мы получаем необходимые нижние оценки в теоремах 1 и 2.

4.4. Локальное расширение. В этом разделе мы переформулируем результаты из раздела 3 в том виде, в котором они будут использоваться в доказательстве.

Вектор $x \in \mathbb{F}_q^n$ назовем *Δ-минимальным* относительно кода $\mathscr{C} \subseteq \mathbb{F}_q^n$, если $\boldsymbol{wt}(x) \leqslant d(x^i, \mathscr{C}) + \Delta$, то есть мы не можем уменьшить вес x более чем на Δ, прибавляя кодовые слова из $\mathscr{C}$.

Лемма 15. *Пусть $\mathscr{C}_1, \mathscr{C}_2 \subseteq \mathbb{F}_q^n$ — линейные коды. Если $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$ и каждый столбец ненулевого кодового слова $x \in (\mathscr{C}_1 \boxplus \mathscr{C}_2) \setminus (\mathscr{C}_1 \otimes \mathbb{F}_q^w)$ является Δ-минимальным относительно кода $\mathscr{C}_2$, то $\boldsymbol{wt}(x) \geqslant \frac{1}{2}\rho w(\rho w - \Delta + 2)$.*

Доказательство. В силу условия $\rho(\mathscr{C}_1, \mathscr{C}_2) \geqslant \rho$ слово x представляется в виде суммы некоторых строк из $\mathscr{C}_1$ (пусть номера этих строк образуют множество B) и некоторых столбцов из $\mathscr{C}_2$ (пусть номера этих столбцов образуют множество A) таким образом, что $|A| + |B| \leqslant \frac{1}{\rho w}\boldsymbol{wt}(x)$. Поскольку $x \notin \mathscr{C}_1 \otimes \mathbb{F}_q^w$, то $A \neq \varnothing$. Тогда столбец x_i, $i \in A$, представляется в виде $x_i = u + v$, где $u \in \mathscr{C}_2 \setminus \{0\}$, $\operatorname{supp} v \subseteq B$. Поскольку по условию столбец x_i является Δ-минимальным относительно кода $\mathscr{C}_2$, то $\boldsymbol{wt}(x_i) \leqslant \boldsymbol{wt}(x_i - u) + \Delta$. Отсюда

$$\rho w \leqslant d(\mathscr{C}_2) \leqslant \boldsymbol{wt}(u) \leqslant \boldsymbol{wt}(x_i) + \boldsymbol{wt}(u - x_i) \leqslant 2\boldsymbol{wt}(u - x_i) + \Delta = \\ = 2\boldsymbol{wt}(v) + \Delta \leqslant 2|B| + \Delta.$$

Значит, $\boldsymbol{wt}(x) \geqslant \rho w(|B| + |A|) \geqslant \rho w\left(\frac{\rho w - \Delta}{2} + 1\right)$, что и требовалось.

4.5. Глобальное расширение. В этом подразделе граф Λ — это граф из подраздела 2.1.

Лемма 16. *Граф Λ является $(a, 2\lambda)$-расширяющим.*

Доказательство. Поскольку $E = E_{\rightarrow} \cup E_{\uparrow}$, мы можем разбить граф Λ как $\Lambda = \Lambda_{\rightarrow} \cup \Lambda_{\uparrow}$, где

$$\Lambda_{\rightarrow} := V \cup E_{\rightarrow} = \{x \cdot g \cdot y \mid x \in V(\Gamma) \cup E(\Gamma), y \in V(\Gamma), g \in G\},$$

$$\Lambda_{\uparrow} := V \cup E_{\uparrow} = \{x \cdot g \cdot y \mid x \in V(\Gamma), y \in V(\Gamma) \cup E(\Gamma), g \in G\}.$$

В терминах графов $\Lambda_{\rightarrow}$ — это подграф Λ, содержащий только горизонтальные ребра, а $\Lambda_{\uparrow}$ — это подграф Λ, содержащий только вертикальные ребра. Легко видеть, что

$$\Lambda_{\rightarrow} = \bigsqcup_{y \in V(\Gamma)} \Lambda_{\rightarrow}^{(y)}, \qquad \Lambda_{\uparrow} = \bigsqcup_{x \in V(\Gamma)} \Lambda_{\uparrow}^{(x)},$$

где

$$\Lambda_{\rightarrow}^{(y)} = \{x \cdot g \cdot y \mid x \in V(\Gamma) \cup E(\Gamma), g \in G\},$$
$$\Lambda_{\uparrow}^{(x)} = \{x \cdot g \cdot y \mid y \in V(\Gamma) \cup E(\Gamma), g \in G\}.$$

Поскольку графы $\Lambda_{\uparrow}^{(x)}$ и $\Lambda_{\rightarrow}^{(y)}$ изоморфны $\widehat{\Gamma}$, то они (a, λ)-расширяющие. Следовательно, по свойству 3 расширения (см. замечание 9) их дизъюнктные объединения $\Lambda_{\rightarrow}$ и $\Lambda_{\uparrow}$ тоже (a, λ)-расширяющие. Поэтому по свойству 4 расширения графов их объединение Λ является $(a, 2\lambda)$-расширяющим, и лемма доказана.

В остальной части этого подраздела мы предполагаем, что c — это некоторый фиксированный локально минимальный 1-цикл в комплексе $\mathcal{F}X$ из подраздела 4.3.

Лемма 17. *Если $\partial c = 0$ и вертикальное ребро e активно, но не инцидентно активным вершинам, то оно инцидентно по крайней мере $d(\ker h_1)$ активным граням.*

Доказательство. Напомним, что F_e — множество граней, инцидентных e, а V_e — множество (из двух) вершин, инцидентных e. По условию, $c|_{V_e} = 0$, но $c|_{F_e} \neq 0$ (поскольку ребро e — активное). Так как $(\partial c)|_e$ зависит только от $c|_{F_e}$ и $c|_{V_e}$, то, используя (2), имеем

$$0 = (\partial c)|_e = (\partial(c|_{F_e} + \underbrace{c|_{V_e}}_{=0}))|_e = \partial_{F_e \to e}(c|_{F_e}).$$

Поскольку $\partial_{F_e \to e} \sim h_1$, $c|_{F_e} \neq 0$, и $\partial_{F_e \to e}(c|_{F_e}) = 0$, мы имеем, что число активных граней, инцидентных ребру e, равно

$$\boldsymbol{wt}(c|_{F_e}) \geqslant d(\ker \partial_{F_e \to e}) = d(\ker h_1),$$

и лемма доказана.

Лемма 18. *Если $d(\ker h_1) \geqslant 6\lambda$, $\partial c = 0$ и $\boldsymbol{wt}_X(c) \leqslant a$, то каждое активное ребро инцидентно вершине из множества L.*

Доказательство. Пусть $S \subseteq E_{\uparrow}$ — множество активных ребер, не инцидентных вершинам из L, а $A \subseteq E_{\uparrow}$ — множество всех активных ребер.

Рассмотрим подпосет $\Lambda_\square = E_\uparrow \cup F$ посета X. Поскольку каждая грань из F инцидентна ровно двум вертикальным ребрам из $E_\uparrow$, то $\Lambda_\square$ можно интерпретировать как граф с $V(\Lambda_\square) = E_\uparrow$ и $E(\Lambda_\square) = F$. Имеем

$$\Lambda_\square = \{x \cdot g \cdot y \mid x \in V(\Gamma) \cup E(\Gamma), y \in E(\Gamma), g \in G\} = \bigsqcup_{y \in E(\Gamma)} \Lambda_\square^{(y)},$$

где

$$\Lambda_\square^{(y)} = \{x \cdot g \cdot y \mid x \in V(\Gamma) \cup E(\Gamma), g \in G\} \simeq \widehat{\Gamma}.$$

Множества S и A можно интерпретировать как множества вершин графа $\Lambda_\square$. Определим $S^{(y)} := S \cap \Lambda_\square^{(y)}$. Так как для фиксированного $y \in E(\Gamma)$ каждая вершина в V инцидентна ровно одному ребру из $\Lambda_\square^{(y)}$, то имеем $|S^{(y)}| \leqslant \boldsymbol{wt}_X(c) \leqslant a$. Поэтому из того, что $\Lambda_\square^{(y)} \simeq \widehat{\Gamma}$ является (a, λ)-расширяющим, имеем $|E_{\Lambda_\square}(S^{(y)}, S^{(y)})| \leqslant \lambda |S^{(y)}|$ и

$$|E_{\Lambda_\square}(S, S)| = \Big| \bigsqcup_{y \in E(\Gamma)} E_{\Lambda_\square^{(y)}}(S^{(y)}, S^{(y)}) \Big| \leqslant \lambda \sum_{y \in E(\Gamma)} |S^{(y)}| = \lambda |S|.$$

С другой стороны, по лемме 17, поскольку каждое ребро $e \in S$ активно и не инцидентно активным вершинам (поскольку любая активная вершина входит в L), то оно инцидентно по крайней мере $d = d(\ker h_1) \geqslant 6\lambda$ активным граням, каждая из которых соединяет его с другим активным ребром из множества A (поскольку по определению оба вертикальных ребра активной грани активны). Интерпретируя вертикальные ребра и грани соответственно как вершины и ребра графа $\Lambda_\square$, имеем $|E_{\Lambda_\square}(S, A)| \geqslant 6\lambda |S|$. Таким образом,

$$|E_{\Lambda_\square}(S, A \setminus S)| = |E_{\Lambda_\square}(S, A)| - |E_{\Lambda_\square}(S, S)| \geqslant 6\lambda |S| - \lambda |S| = 5\lambda |S|.$$

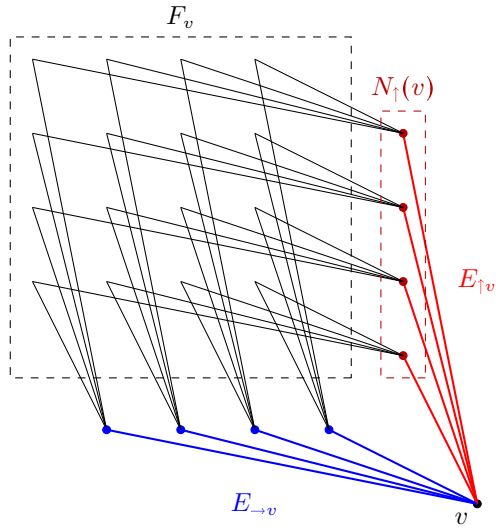
Предположим, что $|S| \neq \varnothing$. Тогда существует ребро $e \in S$, смежное с не менее 5λ ребрами $e_1, \ldots, e_m \in A \setminus S$ в $\Lambda_\square$, $m \geqslant 5\lambda$. По определению A и S каждое из ребер e_i инцидентно некоторой вершине $x_i \in L$, которая смежна с одной из двух вершин e в Λ. Следовательно, существует $m \geqslant 5\lambda$ различных вершин из L, смежных с одной из вершин ребра e, и поэтому одна из этих вершин смежна с более чем 2λ вершин из L; кроме того, она смежна с не менее $d \geqslant 6\lambda > 4$ активными гранями, поэтому по определению принадлежит L. Это противоречит тому, что ребро e из S и не может быть смежным с вершиной из L. Следовательно, $S = \varnothing$, и лемма доказана.

Л е м м а 19. *Предположим, что* $\rho(\ker h_1, \operatorname{im} h_2^*) \geqslant \rho$, *матрицы* h_1 *и* h_2 *имеют полный ранг,* $\rho^2 w > 16\lambda$. *Если* c — *локально минимальный* 1-*цикл, и* $\boldsymbol{wt}_X(c) \leqslant a$, *то* $|E_\Lambda(\{v\}, L)| > 2\lambda$ *для каждой вершины* $v \in L$.

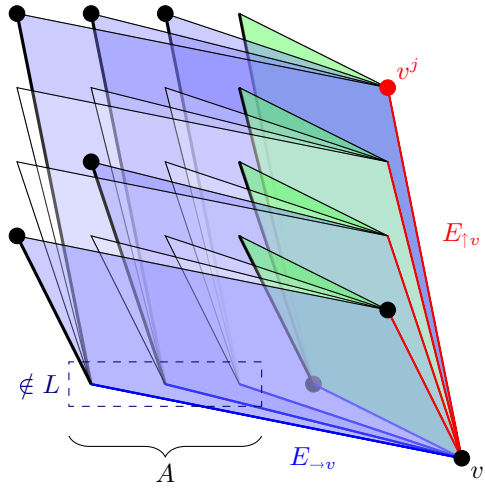
Д о к а з а т е л ь с т в о.

1. Сначала зафиксируем некоторую вершину $v \in L$, $v = v' \cdot g \cdot v''$, где $v', v'' \in V(\Gamma)$, $g \in G$. Пусть $y = c|_v \in \mathbb{F}_q^{r \times r'} v$, $f = c|_{F_v} \in \mathbb{F}_q F_v$. Тогда нетрудно заметить, что

$$\begin{aligned} E_{\to v} &= \{e' \cdot g' \cdot v' \in E_\to \mid \widehat{e}'_{g'} \succ_{\widehat{\Gamma}} \widehat{v}'_g\}, \\ E_{\uparrow v} &= \{v' \cdot g' \cdot e' \in E_\uparrow \mid \widehat{e}''_{g''} \succ_{\widehat{\Gamma}} \widehat{v}''_g\}, \\ F_v &= \{e' \cdot g' g^{-1} g' \cdot e' \in F \mid \widehat{e}'_{g'} \succ_{\widehat{\Gamma}} \widehat{v}'_g, \widehat{e}'_{g''} \succ_{\widehat{\Gamma}} \widehat{v}'_g\}. \end{aligned}$$



а



б

Рис. 3. а) окрестность вершины v в $\widehat{\Gamma} \times_G \widehat{\Gamma}^*$; б) активные грани и множество вершин L. Черные точки — вершины из L, красная точка — вершина v^j, для которой получаем противоречие (v^j смежна с многими вершинами из $L \Rightarrow v^j \in L$)

Поскольку каждая грань из F_v инцидентна одному ребру из $E_\uparrow$ и одному ребру из $E_\to$, то существует естественное взаимно-однозначное соответствие*) между F_v и $E_{\to v} \times E_{\uparrow v}$ (см. рис. 3,а). Поскольку $|E_{\to v}| = |E_{\uparrow v}| = w$, то мы можем представить проекцию $f = c|_{F_v}$ как матрицу $w \times w$ со строка-

*) Эквивалентный способ выразить это свойство состоит в том, чтобы сказать, что двумерный комплекс $\widetilde{X} = \widehat{\Gamma} \times_G \widehat{\Gamma}$ является *полным квадратным комплексом* (англ. *complete square complex*) [55], т.е. комплексом, где линк каждой вершины изоморфен полному двудольному графу.

ми и столбцами, индексированными ребрами из $E_{\uparrow v}$ и $E_{\rightarrow v}$ соответственно, то есть $f \in \mathbb{F}_q F_v \cong \mathbb{F}_q(E_{\rightarrow v} \times E_{\uparrow v})$. Определим множество

$$N_{\uparrow}(v) := \{v' \in V \mid v \leftrightarrow_e v',\ e \in E_{\uparrow}\},$$

которое состоит из вершин, соединенных с v вертикальными ребрами. Заметим, что множество элементов из $X(1) = V \cup F$, инцидентных элементам из $E_{\uparrow v} \subseteq X(0)$, равно $V_{E_{\uparrow v}} \cup F_{E_{\uparrow v}}$, где $V_{E_{\uparrow v}} = N_{\uparrow}(v) \cup \{v\}$ и $F_{E_{\uparrow v}} = F_v$. Отсюда получаем

$$(\partial c)|_{E_{\uparrow v}} = \big(\partial(c|_v + c|_{F_v} + c|_{N_{\uparrow}(v)})\big)|_{E_{\uparrow v}} = \underbrace{\partial_{v \to E_{\uparrow v}}}_{\mathrm{id} \otimes \partial_{\mathscr{B}}^{(v'')^*}}(y) + \underbrace{\partial_{F_v \to E_{\uparrow v}}}_{\partial_{\mathscr{A}}^{(v')} \otimes \mathrm{id}}(f) + \partial_{N_{\uparrow}(v) \to E_{\uparrow v}}(c|_{N_{\uparrow}(v)}).$$

Поскольку $\mathscr{A} \in \mathfrak{T}_G(\widehat{\Gamma}; h_1)$, $\mathscr{B} \in \mathfrak{T}_G(\widehat{\Gamma}; h_2)$, имеем $\partial_{\mathscr{A}}^{(v')} \sim h_1$ и $\partial_{\mathscr{B}}^{(v')} \sim h_2$, поэтому при правильном упорядочении ребер в E_v мы можем отождествить $\partial_{v \to E_{\uparrow v}}$ с $I_r \otimes h_2^*$ и $\partial_{F_v \to E_{\uparrow v}}$ с $h_1 \otimes I_w$. Пусть $z_v := (I_r \otimes h_2^*)y$, $z_F := (h_1 \otimes I_w)f$ и $z_N := \partial_{N_{\uparrow}(v) \to E_{\uparrow v}}(c|_{N_{\uparrow}(v)})$. Тогда имеем

$$0 = (\partial c)|_{E_{\uparrow v}} = z_v + z_F + z_N.$$

Пусть $A \subseteq E_{\rightarrow v}$ (соотв. $B \subseteq E_{\uparrow v}$) — это множество горизонтальных (соотв. вертикальных) ребер, ведущих из v вне множества L. Мы также будем использовать дополнение $\bar{A} := E_{\rightarrow v} \setminus A$ (соотв. $\bar{B} := E_{\uparrow v} \setminus B$), которое является множеством горизонтальных (соотв. вертикальных) ребер, соединяющих v с вершинами из L. Каждая пара ребер в $A \times B$ определяет грань, инцидентную v и не инцидентную вершинам из L, смежным с v в Λ.

2. Докажем от противного, что условие леммы выполнено для вершины v. Предположим обратное, тогда

$$2\lambda \geqslant |E_{\Lambda}(\{v\}, L)| = |\bar{A} \cup \bar{B}| \geqslant \max(|\bar{A}|, |\bar{B}|).$$

Заметим, что поскольку z_N — это образ активных вершин, смежных с v, под действием оператора ∂, то $\operatorname{supp} z_N \subseteq \bar{B}$. Кроме того, поскольку матрица h_1 полного ранга, то оператор h_2 сюръективен, значит, существует $t \in \mathbb{F}_q^w \otimes \mathbb{F}_q \bar{B}$ такая, что $(h_1 \otimes I_w)t = z_N$. Тогда

$$(h_1 \otimes I_w)(f + t) = z_N + z_F = -z_v \in \operatorname{im}(I_r \otimes h_2^*),$$

значит, $f' := (f+t) \in \ker h_1 \otimes \mathbb{F}_q^w + \mathbb{F}_q^w \otimes \operatorname{im} h_2^* = \ker h_1 \boxplus \operatorname{im} h_2^*$. Проверим условия леммы 15. Поскольку h_2 — матрица полного ранга, то $z_v = h_2^* y \neq 0$, значит, $f' \notin \ker h_1 \otimes \mathbb{F}_q^w$.

2a. Покажем от противного, что каждый столбец матрицы $f' := f + t$ является $(4\lambda + 2)$-минимальным относительно кода $\operatorname{im} h_2^*$. Допустим, существует столбец f'_e, $e \in E_{\rightarrow}$ (напомним, что мы индексируем столбцы матрицы элементами из $E_{\rightarrow}$) и элемент $u \in \mathbb{F}_q^{r'}$ такой, что $\boldsymbol{wt}(f'_e - h_2^* u) < \boldsymbol{wt}(f'_e) - 2 - 4\lambda$. Но тогда

$$\boldsymbol{wt}(f_e - h_2^* u) - \boldsymbol{wt}(f_e) \leqslant \boldsymbol{wt}(f'_e - h_2^* u) + \underbrace{\boldsymbol{wt}(t_e)}_{\leqslant |B|} - \boldsymbol{wt}(f_e) < -2 - 4\lambda + 2|\bar{B}| \leqslant -2,$$

$$\boldsymbol{wt}_X(c-\partial(ue))-\boldsymbol{wt}_X(c)\leqslant\underbrace{\boldsymbol{wt}_X(\partial(ue)|_V)}_{\leqslant 2}+\overbrace{\boldsymbol{wt}_F(\underbrace{c|_{F_e}}_{f_e}-\underbrace{\partial_{e\to F_e}(ue)}_{h_2^*u})-\boldsymbol{wt}(c|_{F_e})}^{<-2}<0,$$

что противоречит локальной минимальности c.

2b. Таким образом, мы можем применить лемму 15 к кодовому слову $f+t$ и получить оценку

$$\boldsymbol{wt}(f+t)\geqslant\tfrac{1}{2}\rho w(\rho w-(4\lambda+2)+2)\geqslant\left(\tfrac{1}{2}\rho^2 w-2\lambda\right)w>6\lambda w.$$

Оценим вес $f|_{[w]\times B}$. Поскольку $t|_{[w]\times B}=0$, то

$$\boldsymbol{wt}(f|_{[w]\times B})=\boldsymbol{wt}((f+t)|_{[w]\times B})\geqslant\boldsymbol{wt}(f+t)-w|\bar{B}|>6\lambda w-2\lambda w\geqslant 4\lambda w.$$

Это означает, что существует строка f^j, $j\in B$ веса $\boldsymbol{wt}(f^j)>4\lambda$. Поскольку $|\bar{A}|\leqslant 2\lambda$, то $\boldsymbol{wt}(f^j|_A)>2\lambda$.

2c. Рассмотрим активную грань $x=(i,j)\in A\times\{j\}$. Она инцидентна 4 вершинам v,v^j,v_i,v_i^j, 2 вертикальным ребрам $e_{\uparrow}^j$, $e_{i\uparrow}^j$, $v\leftrightarrow_{e_{\uparrow}^j}v^j$, $v_i\leftrightarrow_{e_{i\uparrow}^j}v_i^j$ и 2 горизонтальным ребрам $\vec{e}_i$, $\vec{e}_i^{\,j}$, $v\leftrightarrow_{\vec{e}_i}v_i$, $v^j\leftrightarrow_{\vec{e}_i^{\,j}}v_i^j$. Заметим, что $d(\ker h_1)\geqslant\rho w>6\lambda$, значит, условия леммы 18 выполнены. Поскольку грань x активна, то инцидентное ей вертикальное ребро $e_{i\uparrow}^j$ тоже активно, значит, по лемме 18 оно инцидентно некоторой вершине из L. Но поскольку $i\in A$, то $v_i\notin L$, а значит, $v_i^j\in L$. Таким образом, ребро $\vec{e}_i^{\,j}$ соединяет вершину v^j с вершиной из L, то есть $\vec{e}_i^{\,j}\in E_\Lambda(\{v^j\},L)$. При этом по построению различным i соответствуют различные ребра $\vec{e}_i^{\,j}$ (даже если некоторые вершины v_i^j совпадают), значит, $|E_\Lambda(\{v^j\},L)|\geqslant\boldsymbol{wt}(f^j|_A)>2\lambda$, кроме того, v^j инцидентна $\geqslant\boldsymbol{wt}(f^j)>4\lambda\geqslant 4$ активным граням, значит, по определению $v^j\in L$ (Рис. 3б). Получили противоречие с тем, что $j\in B$.

Из леммы 19 и определения множества L мы получаем следующий результат.

Следствие 2. *Предположим, что пара* $\rho(\ker h_1,\operatorname{im}h_2^*)\geqslant\rho$, *матрицы* h_1 *и* h_2 *имеют полный ранг,* $\rho^2 w>16\lambda$. *Если* c *— локально минимальный* 1*-цикл, и* $\boldsymbol{wt}_X(c)\leqslant a$, *то* $|E_\Lambda(\{v\},L)|>2\lambda$ *для каждой вершины* $v\in L$.

Доказательство. Если вершина v активна, то утверждение верно по лемме 19. Иначе оно выполнено по второму пункту определения множества L.

Лемма 20. *Предположим, что* $\rho(\ker h_1,\operatorname{im}h_2^*)\geqslant\rho$, *матрицы* h_1 *и* h_2 *имеют полный ранг,* $\rho^2 w>16\lambda$. *Если* c *— локально минимальный* 1*-цикл, и* $\boldsymbol{wt}_X(c)\leqslant a$, *то* $c=0$.

Доказательство. Предположим, что $|c|>0$, тогда $|L|>0$.

Тогда в соответствии со следствием 2 для каждой вершины $v\in L$ имеем $E_\Lambda(\{v\},L)>2\lambda$, следовательно,

$$E_\Lambda(L,L)>2\lambda|L|. \tag{11}$$

Так как каждая помеченная вершина v либо активна ($v\in\operatorname{supp}c_V$) либо инцидентна по крайней мере 4 активным граням, получаем

$$|L|\leqslant\boldsymbol{wt}_X(c_V)+4\boldsymbol{wt}_X(c_F)\leqslant\boldsymbol{wt}_X(c_V)+4\boldsymbol{wt}_X(c_F)/4=\boldsymbol{wt}_X(c)\leqslant a.$$

Но так как граф Λ является $(a,2\lambda)$-расширяющим, то $E_\Lambda(L,L)\leqslant 2\lambda|L|$, что противоречит (11). Значит предположение неверно и $c=0$.

Утверждение 1. *Для каждого конечного поля* $\mathbb{F}_q$, *интервалов* $(\rho_0, \rho_1), (\rho'_0, \rho'_1) \subseteq (0,1)$, *постоянной* $\mu \geqslant 1$, *бесконечного множества* $W \subseteq \mathbb{N}$, *достаточно больших* $w \in W$ *и любых* $r_1, r_2 \in \mathbb{N}$ *таких, что* $r_1/w \in (\rho_0, \rho_1)$, $r_2/w \in (\rho'_0, \rho'_1)$, *существуют матрицы* $h_1 \in \mathbb{F}_q^{r_1 \times w}$, $h_2 \in \mathbb{F}_q^{r_2 \times w}$ *такие, что для каждого* G*-поднятого одностороннего* $(n, w, \mu\sqrt{w})$*-экспандера без петель* $\widehat{\Gamma}$ *и кодов Таннера* $\mathscr{A} \in \mathfrak{T}_G(\widehat{\Gamma}; h_1)$, $\mathscr{B} \in \mathfrak{T}_G(\widehat{\Gamma}; h_2)$ *со свободным действием группы* G *имеем*

$$d^{(1)}_{\mathrm{LM}}(\mathscr{A} \otimes_G \mathscr{B}^*) \geqslant n/\sqrt{w},$$

$$d^{(1)}_{\mathrm{LM}}(\mathscr{B} \otimes_G \mathscr{A}^*) \geqslant n/\sqrt{w}.$$

Доказательство. Пусть w — параметр, который мы зафиксируем позже. Определим $r_1 := \left\lfloor \frac{1}{2}(\rho_0 + \rho_1)w \right\rfloor$, $r_2 := \left\lfloor \frac{1}{2}(\rho'_0 + \rho'_1)w \right\rfloor$. Так как $r_1/w \to \frac{1}{2}(\rho_0 + \rho_1)$, $r_2/w \to \frac{1}{2}(\rho'_0 + \rho'_1)$ как $w \to \infty$, по следствию 1 существует $\rho > 0$ такое, что при любом достаточно большом w для случайного $[w, w-r_1]_q$ кода C_1 и случайного $[w, w-r_2]_q$ кода C_2 с большой вероятностью выполнено $\rho(C_1, C_2) \geqslant \rho$ и $\rho(C_1^\perp, C_2^\perp) \geqslant \rho$. В частности, мы можем выбрать w_0 достаточно большим, что для любого $w > w_0$

1) существует $[w, w - r_1]_q$ код C_1 и $[w, w - r_2]_q$ код C_2 такие, что $\rho(C_1, C_2) \geqslant \rho$ и $\rho(C_1^\perp, C_2^\perp) \geqslant \rho$;

2) $\rho w > 32\mu\sqrt{w}$.

Поскольку множество W бесконечно, мы можем взять $w := \min\{w \in W \mid w \geqslant w_0\}$ и зафиксировать некоторую пару (C_1, C_2), удовлетворяющую условию 1. Теперь рассмотрим G-поднятый односторонний $(n, w, \mu\sqrt{w})$-экспандер $\widehat{\Gamma}$ и некоторые G-поднятые коды Таннера $\mathscr{A} \in \mathfrak{T}_G(\widehat{\Gamma}; h_1)$, $\mathscr{B} \in \mathfrak{T}_G(\widehat{\Gamma}; h_2)$. По лемме 14 граф $\widehat{\Gamma}$ является $(\mu n/\sqrt{w}, \lambda)$-расширяющим, где $\lambda = 2\mu\sqrt{w}$.

Поскольку $\rho w > 32\mu\sqrt{w} = 16\lambda$, мы можем применить лемму 20 к паре кодов $(\ker h_1, \operatorname{im} h_2^*)$ и получить, что каждый ненулевой локально минимальный 1-цикл цепного комплекса $\mathscr{A} \otimes_G \mathscr{B}^*$ имеет вес по крайней мере a. Отсюда следует, что

$$d^{(1)}_{\mathrm{LM}}(\mathscr{A} \otimes_G \mathscr{B}^*) \geqslant \mu n/\sqrt{w} \geqslant n/\sqrt{w}.$$

Поскольку лемма 20 применима и к паре $(\ker h_2, \operatorname{im} h_1^*)$, имеем

$$d^{(1)}_{\mathrm{LM}}(\mathscr{B} \otimes_G \mathscr{A}^*) \geqslant \mu n/\sqrt{w} \geqslant n/\sqrt{w},$$

что завершает доказательство.

Теорема 4. *Для любого* $R \in (0, 1/2)$ *и конечного поля* $\mathbb{F}_q$ *можно найти универсальные константы* s *и* ω *такие, что существует явное семейство* (ω, s)*-локально тестируемых классических LDPC-кодов с параметрами* $[n, k \geqslant Rn, d = \Theta(n)]_q$ *при* $n \to \infty$.

Доказательство. Зафиксируем произвольное число $R \in (0, 1/2)$ и положим $\varepsilon := (1-2R)/(6-2R)$. Заметим, что для любого w из бесконечного множества $W := \{p+1 \in \mathbb{N} \mid p \equiv 1 \mod 4$ и p является простым$\}$ существует бесконечное семейство односторонних $(n_0(t), w, 2\sqrt{w})$-экспандеров $\bar{X}^{w-1,t}$ из примера 1, где $n_0(t) = t(t^2-1) = |V(\bar{X}^{w-1,t})|$. Рассмотрим цепной комплекс

$$\mathscr{C} := \mathscr{T}(\bar{X}^{w-1,t}, h_1) \otimes_G \mathscr{T}^*(\bar{X}^{w-1,t}, h_2),$$

с граничным оператором ∂, где $G := \mathrm{PSL}(\mathbb{F}_t^2)$, а h_1, h_2 — проверочные матрицы локальных кодов, которые мы зафиксируем позже. Пусть $|\cdot|_X$ — блочный вес $\boldsymbol{wt}_X(\cdot)$, определенная на $\mathscr{C}$, рассматриваемом как цепной комплекс с локальной системой на клеточном посете $X = \bar{X}^{w-1,t} \times_G (\bar{X}^{w-1,t})^*$. По утверждению 1 для интервалов $(1-\varepsilon, 1)$, $(0, \varepsilon)$ и параметра $\mu = 2$, существуют $w \in W$ и матрицы $h_1 \in \mathbb{F}_q^{r_1 \times w}$, $h_2 \in \mathbb{F}_q^{r_2 \times w}$ такие, что для каждого $\bar{X}^{w-1,t}$ мы имеем

$$d_{\mathrm{LM}}^{(1)}(\mathscr{C}) \geqslant n_0(t)/\sqrt{w},$$

где $r_1/w > 1-\varepsilon$, $r_2/w < \varepsilon$. Пусть $n := \dim \mathscr{C}_2$ и $m := \dim \mathscr{C}_1$, тогда $n = n_0(t)rw$, $m = \frac{1}{2} n_0(t)(w^2 + 4rr')$. Отсюда $d_{\mathrm{LM}}^{(1)}(\mathscr{C}) \geqslant \frac{n}{wr\sqrt{w}} > \frac{n}{w^{5/2}}$. По лемме 11 для всех $c \in \mathscr{C}_2$ имеем

$$|\partial c|_X \geqslant \min(d_{\mathrm{LM}}^{(1)}(\mathscr{C}), |c + Z_2(\mathscr{C})|_X).$$

Поскольку $|y|_X \leqslant \boldsymbol{wt}(y)$ для $y \in \mathscr{C}$, то $\boldsymbol{wt}(c) \leqslant r_1 |c|_X \leqslant w|c|_X$ для $c \in \mathscr{C}_2$. Учитывая, что $n \geqslant \boldsymbol{wt}(c + Z_2(\mathscr{C}))$, окончательно получаем

$$\boldsymbol{wt}(\partial c) \geqslant |\partial c|_X \geqslant \min\left(\frac{n}{w^{5/2}}, \frac{\boldsymbol{wt}(c + Z_2(\mathscr{C}))}{w}\right) \geqslant \frac{1}{w^{5/2}} \boldsymbol{wt}(c + Z_2(\mathscr{C})).$$

Мы имеем

$$\frac{m}{n} = \frac{w^2 + 4r_1 r_2}{2rw} = \frac{1 + 4\frac{r_1}{w} \cdot \frac{r_2}{w}}{2r_1/w} \leqslant \frac{1 + 4\varepsilon}{2(1-\varepsilon)} = 1 - R.$$

В частности, мы имеем $m < n$ и поэтому

$$\frac{1}{m} \boldsymbol{wt}(\partial c) \geqslant \frac{w^{-5/2}}{m} \boldsymbol{wt}(c + Z_2(\mathscr{C})) \geqslant \frac{w^{-5/2}}{n} \boldsymbol{wt}(c + Z_2(\mathscr{C})).$$

Поэтому код $Z_2(\mathscr{C})$ является (ω, s)-локально тестируемым, где $\omega := 2w$ и $s := w^{-5/2}$. Для размерности $k = \dim Z_2(\mathscr{C})$ мы имеем оценку $k \geqslant n - m \geqslant Rn$.

Для завершения доказательства нам также нужно показать, что линейный код $Z_2(\mathscr{C})$ имеет минимальное расстояние $\Theta(n)$ при $n \to \infty$. Нетрудно видеть, что минимальное расстояние $Z_2(\mathscr{C})$ не меньше расстояния компонентного кода Таннера $\mathscr{T}(\bar{X}^{w-1,t}, h_1)$, который является классическим экспандерным кодом [50]. Таким образом, как следует из доказательства предложения 1, мы можем найти достаточно большое число w такое, что $d(\ker h_1) > \lambda_2(\bar{X}^{w-1,t})$, и получить $d(\mathscr{T}(\bar{X}^{w-1,t}, h_1)) = \Theta(n)$ при $n \to \infty$.

Теорема 5. *Для любого $R \in (0, 1)$ и конечного поля $\mathbb{F}_q$ существует явное семейство квантовых LDPC-кодов над $\mathbb{F}_q$ с параметрами $[\![n, k \geqslant Rn, d = \Theta(n)]\!]_q$ при $n \to \infty$.*

Доказательство. Зададим некоторое $R \in (0,1)$. Заметим, что для каждого w из бесконечного множества $W := \{p+1 \in \mathbb{N} \mid p \equiv 1 \bmod 4$ и p простое$\}$ существует бесконечное семейство односторонних $(n_0(t), w, 2\sqrt{w})$-экспандеров $\bar{X}^{w-1,t}$ из примера 1, где $n_0(t) = t(t^2-1) = |V(\bar{X}^{w-1,t})|$.

Как и в доказательстве теоремы 1, мы рассматриваем комплекс $\mathscr{C} = \mathscr{T}(\bar{X}^{w-1,t}, h_1) \otimes_G \mathscr{T}^*(\bar{X}^{w-1,t}, h_2)$ с оператором границы ∂, где $G = \mathrm{PSL}(\mathbb{F}_t^2)$. Пусть $|\cdot|_X$ — блочный вес, определенный на $\mathscr{C}$. По утверждению 1, для $\rho_0 = \rho_0' = 0$, $\rho_1 = \rho_1' = (1-R)/4$ и $\mu = 2$, существуют $w \in W$ и матрицы $h_1 \in \mathbb{F}_q^{r \times w}$, $h_2 \in \mathbb{F}_q^{r \times w}$ такие, что для всех $\bar{X}^{w-1,t}$ имеем

$$d_{\mathrm{LM}}^{(1)}(\mathscr{C}) \geqslant n_0(t)/\sqrt{w}, \qquad d_{\mathrm{LM}}^{(1)}(\mathscr{C}^*) \geqslant n_0(t)/\sqrt{w},$$

где $r = \lfloor w(1-R)/4 \rfloor$. Пусть $n := \dim \mathscr{C}_1$, тогда $n = \frac{1}{2} n_0(t)(w^2 + 4r^2) < w^2 n_0(t)$. Следовательно, $d_{\mathrm{LM}}^{(1)}(\mathscr{C}) \geqslant \frac{n}{4w^3\sqrt{w}} > \frac{n}{4w^{7/2}}$. Цепной комплекс $\mathscr{C}$ определяет квантовый CSS код $\mathscr{Q} = \mathscr{Q}(H_X, H_Z)$ с матрицами проверки четности $H_X := \partial_1$ и $H_Z := \partial_2^*$. По лемме 11 для комплекса $\mathscr{C}$ имеем

$$d_X(\mathscr{Q}) = d(H_1(\mathscr{C})) \geqslant d_{\mathrm{LM}}^{(1)}(\mathscr{C}) \geqslant \frac{n_0(t)}{\sqrt{w}} > \frac{n}{w^{5/2}}.$$

Аналогично, поскольку двойственный цепной комплекс $\mathscr{C}^*$ изоморфен *) цепному комплексу $\mathscr{B} \otimes_G \mathscr{A}^*$, то по лемме 11 имеем

$$d_Z(\mathscr{Q}) = d(H_1(\mathscr{C}^*)) \geqslant d_{\mathrm{LM}}^{(1)}(\mathscr{C}^*) > \frac{n}{w^{5/2}},$$

и поэтому $d(\mathscr{Q}) = \min(d_X(\mathscr{Q}), d_Z(\mathscr{Q})) \geqslant n/w^{5/2}$. Для завершения доказательства нам также нужно оценить размерность $k = \dim(H_1(\mathscr{C}))$ квантового кода $\mathscr{Q}$. Мы имеем

$$\dim \mathscr{C}_0 = n_0(t) r w = 2n \frac{rw}{w^2 + 4r^2} < n(1-R)/2,$$

$$\dim \mathscr{C}_2 = n_0(t) r' w = 2n \frac{r'w}{w^2 + 4r^2} < n(1-R)/2,$$

и поэтому

$$k = \dim(H_1(\mathscr{C})) \geqslant n - \dim \mathscr{C}_0 - \dim \mathscr{C}_2 > n - n(1-R)/2 - n(1-R)/2 = nR.$$

Таким образом, $\mathscr{Q}$ является ограниченным квантовым CSS-кодом с параметрами $[\![n, k \geqslant Rn, d \geqslant n/w^{5/2}]\!]_q$. Заметим, что по сути «каркасом» для построения конструкции из теоремы 2 является поднятие объединения левого и правого графов Кэли группы $\mathrm{PSL}(\mathbb{F}_t^2)$ в 4 раза. Однако в общем случае рассматриваемая в данной работе конструкция не сводится к графам Кэли, которые были использованы в работе [15] для построения LTC. В качестве примера приведем другой результат, который также является следствием утверждения 1. Вместо экспандерных кодов, основанных на графах Кэли, нужно взять квазициклические коды, которые использовались, например,

*) Мы говорим, что два базисных цепных комплекса $\mathscr{C}$ и $\mathscr{C}'$ над $\mathbb{F}_q$ *изоморфны*, если существует взаимно-однозначное $\mathbb{F}_q$-линейное отображение $f\colon \mathscr{C} \to \mathscr{C}'$ такое, что $f(\widetilde{\mathscr{C}}_i) = \widetilde{\mathscr{C}}'_i$ для каждого $i \in \mathbb{Z}$.

в работе [48] для построения квантовых кодов с почти линейным расстоянием. Применяя предложение 1 к этому семейству графов, мы получим семейство почти асимптотически хороших квазициклических кодов с большим размером циркулянта:

Утверждение 2. *Для каждого* $R \in (0,1)$ *и конечного поля* $\mathbb{F}_q$ *существует семейство квазициклических квантовых LDPC-кодов над* $\mathbb{F}_q$ *с параметрами* $[\![n, k \geqslant Rn, d = \Theta(n/\log n)]\!]_q$ *и размером циркулянта* $\Theta(n/\log^2 n)$ *как* $n \to \infty$.

Выводы

В этой работе мы показали, что существует семейство асимптотически хороших квантовых LDPC-кодов, что доказывает qLDPC-гипотезу. Построенные qLDPC-коды были получены при помощи тензорного произведения над групповой алгеброй $\mathbb{F}_q G$ двух G-поднятых кодов Таннера, рассмотренных как цепные комплексы над $\mathbb{F}_q G$, а для получения qLDPC-кодов с линейно растущим минимальным расстоянием использовалась неабелева группа G. На самом деле, нетрудно видеть, что из предложения 1 следует, что использование данной конструкции для двух $\boldsymbol{C}_\ell$-поднятых кодов Таннера из [48], где $\boldsymbol{C}_\ell$ — циклическая группа размера $\ell = \Theta(n/\log^2 n)$, можно получить квазициклические qLDPC-коды с параметрами $[\![n, k = \Theta(n), d = \Theta(n/\log n)]\!]_q$ при $n \to \infty$. Заметим, что недавние результаты о явных $\boldsymbol{C}_\ell$-поднятых экспандерах из [30] означают, что конструкция этих qLDPC-кодов также может быть сделана явной.

Кроме того, в процессе нашего доказательства qLDPC-гипотезы мы показали, что вторые гомологические группы построенных в этой работе цепных комплексов могут быть использованы для получения асимптотически хороших семейств классических LDPC-кодов, которые также локально тестируемы с постоянными параметрами локальности и корректности. Это доказывает важную гипотезу в области локально тестируемых кодов*).

Хотя все предложенные нами конструкции можно считать явными, локальные коды постоянного размера, используемые в наших экспандерных кодах, по-прежнему получаются вероятностными методами. Мы считаем, что найти явную конструкцию таких кодов является интересной открытой проблемой. Одним из возможных вариантов может быть использование MDS-кодов таких, как коды Рида — Соломона. На самом деле, такие небинарные локальные коды можно использовать, даже если мы хотим получить коды над $\mathbb{F}_2$, поскольку каждый классический или квантовый код над $\mathbb{F}_{2^s}$ можно также рассматривать как код над $\mathbb{F}_2$, а скорость и минимальное расстояние такого кода асимптотически не хуже, чем у небинарного, если s фиксировано. Однако неясно, можно ли найти пару MDS-кодов, удовлетворяющую свойству расширения произведения, необходимому для работы нашего доказательства.

Мы также надеемся, что некоторые из методов, разработанных в данной работе, могут быть использованы для доказательства существования локально тестируемых qLDPC-кодов, необходимых для доказательства

*) Независимое доказательство этой гипотезы было также предложено в работе [15].

qLTC-гипотезы. Естественным кандидатом на такой код был бы 5-членный цепной комплекс, где три средних члена соответствуют асимптотически хорошему qLDPC-коду, а два крайних члена представляют его X- и Z-метапроверки (т. е. проверки на проверках). На самом деле, подобные 5-членные комплексы уже использовались ранее в контексте однократного декодирования qLDPC-кодов [11, figure 1].

Перечень символов и стандартных обозначений

$[n]$	множество $\{1, 2, \ldots, n\}$
$\mathbb{F}_q$	конечное поле с q элементами
$R^{m\times n}$	множество $m \times n$ матриц над R
I_n	единичная матрица $n \times n$
$\ker A$	ядро линейного оператора $v \mapsto Av$
$\operatorname{im} A$	образ линейного оператора $v \mapsto Av$
A^*	сопряженный оператор или транспонированная матрица для A
$\mathscr{C}^*$	двойственный цепной комплекс
$\mathscr{F}X$	абелева группа формальных сумм $\sum_{x\in X} a_x x$ с коэффициентами $a_x \in \mathscr{F}_x$ в локальной системе $\mathscr{F}$
$\boldsymbol{wt}(a)$	вес Хэмминга элемента $a \in \mathbb{F}_q^n$
$\boldsymbol{wt}_S(a)$	блочный вес Хэмминга $a \in \mathscr{F}X$ относительно подмножества $S \subseteq X$
$\lvert a\rvert$	норма $a \in A$ в нормированной абелевой группе A
$\operatorname{supp} a$	носитель $\{x \in X \mid a_x \neq 0\}$ для $a \in \mathscr{F}X$
$a\lvert_S$	ограничение $\sum_{x\in S} a_x x$ на подмножество $S \subseteq X$ формальной суммы $a = \sum_{x\in X} a_x x \in \mathscr{F}X$ или вектора $a \in \mathbb{F}_q^X$
$\mathbb{K}G$	групповая алгебра над $\mathbb{K}$ для группы G
$v \leftrightarrow_e v'$	ребро e соединяет вершины v и v'
G-поднятие	$\lvert G\rvert$-кратное регулярное накрытие
$A(\Gamma)$	матрица смежности графа Γ
Γ^2	квадрат графа Γ, т. е. $A(\Gamma^2) = (A(\Gamma))^2$
$E_\Gamma(S, T)$	множество ориентированных ребер из S в T в Γ
$x \succ_P y$	x покрывает y в посете P
$\bar{X}^{p,q}$	двойное накрытие графа Рамануджана $X^{p,q}$
$\mathscr{A} \times_G \mathscr{B}$	поднятое произведение комплексов $\mathscr{A}$ и $\mathscr{B}$
$X \times_G Y$	поднятое произведение множеств X и Y
$\mathfrak{T}(\Gamma; h)$	коды Таннера на Γ с локальным кодом $\ker h$
$\mathfrak{T}_G(\widehat{\Gamma}; h)$	G-поднятые коды Таннера из $\mathfrak{T}(\widehat{\Gamma}; h)$

$A \sim B$	перестановочно эквивалентные коды или матрицы
$Z_i(\mathscr{C})$, $B_i(\mathscr{C})$	пространства i-циклов и i-границ для $\mathscr{C}$
$H_i(\mathscr{C})$	i-я гомологическая группа комплекса $\mathscr{C}$
$\partial_{S\to T}$	ограничение $\partial_{S\to T}\colon \mathscr{F}S \to \mathscr{F}T$ оператора границы $\partial\colon \mathscr{F}X \to \mathscr{F}X$ комплекса $\mathscr{F}X$

СПИСОК ЛИТЕРАТУРЫ

1. Маргулис Г. А. Явные теоретико-групповые конструкции комбинаторных схем и их применения в построении расширителей и концентраторов // Проблемы передачи информации. — 1988. — Т. 24, №1. — С. 51–60.
2. Aharonov D., Eldar L. Quantum Locally Testable Codes // SIAM Journal on Computing. — Society for Industrial and Applied Mathematics, 2015. — Vol. 44, N5. — P. 1230–1262.
3. Bacon D., Flammia S. T., Harrow A. W., Shi J. Sparse quantum codes from quantum circuits // IEEE Transactions on Information Theory. — 2017. — Vol. 63, N4. — P. 2464–2479.
4. Ben-Sasson E., Sudan M. Robust locally testable codes and products of codes // Random Structures & Algorithms. — 2006. — Vol. 28, N4. — P. 387–402.
5. Bohdanowicz T. C., Crosson E., Nirkhe C., Yuen H. Good approximate quantum LDPC-codes from spacetime circuit Hamiltonians // Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing. — New York, NY, USA: Association for Computing Machinery, 2019. — P. 481–490.
6. Bravyi S., Hastings M. B. Homological product codes // Proceedings of the forty-sixth annual ACM symposium on theory of computing. — New York, NY, USA: ACM, 2014. — P. 273–282.
7. Breuckmann N. P., Eberhardt J. N. Balanced Product Quantum Codes // IEEE Transactions on Information Theory. — 2021. — Vol. 67, N10. — P. 6653–6674.
8. Breuckmann N. P., Eberhardt J. N. Quantum Low-Density Parity-Check Codes // PRX Quantum. — 2021. — Vol. 2, N4. — P. 040101.
9. Brown K. S. Some Homological Algebra // Graduate Texts in Mathematics. — New York, NY: Springer, 2007. — P. 4–32.
10. Calderbank A. R., Shor P. W. Good quantum error-correcting codes exist // Phys. Rev. A. — 1996. — Vol. 54, N2. — P. 1098–1105.
11. Campbell E. T. A theory of single-shot error correction for adversarial noise // Quantum Science and Technology. — IOP Publishing, 2019. — Vol. 4, N2. — P. 025006.
12. Chien R., Ng S. Dual Product Codes for Correction of Multiple Low-Density Burst Errors // IEEE Transactions on Information Theory. — 1973. — Vol. 19, N5. — P. 672–677.
13. Dennis E., Kitaev A., Landahl A., Preskill J. Topological quantum memory // Journal of Mathematical Physics. — 2002. — Vol. 43, N9. — P. 4452–4505.
14. Dikstein Y., Dinur I., Harsha P., Ron-Zewi N. Locally testable codes via high-dimensional expanders // arXiv:2005.01045 [cs], 2020.
15. Dinur I., Evra S., Livne R., Lubotzky A., Mozes S. Locally Testable Codes with constant rate, distance, and locality // arXiv:2111.04808 [cs, math], 2021.
16. Dinur I., Sudan M., Wigderson A. Robust Local Testability of Tensor Products of LDPC-Codes // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. Lecture Notes in Computer Science. — Berlin, Heidelberg: Springer, 2006. — P. 304–315.
17. Dinur I. The PCP theorem by gap amplification // Journal of the ACM. — 2007. — Vol. 54, N3. — P. 6653–6674.
18. Eldar L., Harrow A. W. Local Hamiltonians Whose Ground States Are Hard to Approximate // 2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS). — Berkeley, CA, USA: IEEE, 2017. — P. 4452–4505.

19. Evra S., Kaufman T., Zémor G. Decodable quantum LDPC codes beyond the square root distance barrier using high dimensional expanders // 2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS). — Durham, NC, USA: IEEE, 2020. — P. 218–227.
20. Freedman M. H., Meyer D. A., Luo F. $\mathbb{Z}_2$-systolic freedom and quantum codes // Mathematics of quantum computation. — New York: Chapman & Hall/CRC, 2002. — P. 287–320.
21. Gallager R. G. Low-density parity-check codes. — Cambridge, MA: M.I.T. Press, 1963.
22. Goldreich O., Sudan M. Locally testable codes and PCPs of almost-linear length // The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings. — Vancouver, BC, Canada: IEEE, 2002. — P. 13–22.
23. Goldreich O. Short Locally Testable Codes and Proofs: A Survey in Two Parts // Property Testing: Current Research and Surveys. Lecture Notes in Computer Science. — Berlin, Heidelberg: Springer, 2010. — P. 65–104.
24. Guth L., Lubotzky A. Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds // Journal of Mathematical Physics. — American Institute of Physics, 2014. — Vol. 55, N8. — P. 082202.
25. Haah J. Local stabilizer codes in three dimensions without string logical operators // Physical Review A. — American Physical Society, 2011. — Vol. 83, N4. — P. 042330.
26. Hagiwara M., Imai H. Quantum quasi-cyclic LDPC-codes // 2007 IEEE international symposium on information theory. — Nice, France: IEEE, 2007. — P. 806–810.
27. Hastings M. B., Haah J., O'Donnell R. Fiber bundle codes // Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing. — New York, NY, USA: ACM, 2021. — P. 1276–1288.
28. Hastings M. B. On Quantum Weight Reduction // arXiv:2102.10030 [quant-ph], 2021.
29. Hoory S., Linial N., Wigderson A. Expander Graphs and Their Applications // Bull. Amer. Math. Soc. — American Mathematical Society, 2006. — Vol. 43, N4. — P. 439–562.
30. Jeronimo F. G., Mittal T., O'Donnell R., Paredes P., Tulsiani M. Explicit Abelian Lifts and Quantum LDPC-Codes // 13th Innovations in Theoretical Computer Science Conference (ITCS 2022). Leibniz International Proceedings in Informatics (LIPIcs). — Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. — Vol. 215, — P. 88:1–88:21.
31. Kaufman T., Lubotzky A. High dimensional expanders and property testing // Proceedings of the 5th conference on Innovations in theoretical computer science. — New York, NY, USA: Association for Computing Machinery, 2014. — P. 501–506.
32. Kaufman T., Tessler R. J. New cosystolic expanders from tensors imply explicit Quantum LDPC codes with $\Omega(\sqrt{n}\log^k n)$ distance // Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing. — New York, NY, USA: Association for Computing Machinery, 2021. — P. 1317–1329.
33. Kaufman T., Kazhdan D., Lubotzky A. Ramanujan Complexes and Bounded Degree Topological Expanders // 2014 IEEE 55th Annual Symposium on Foundations of Computer Science. — Philadelphia, PA, USA: IEEE, 2012. — P. 484–493.
34. Kaufman T., Sudan M. Sparse Random Linear Codes are Locally Decodable and Testable // 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). — Providence, RI, USA, 2007. — P. 590–600.
35. Koetter R., Kschischang F. R. Coding for Errors and Erasures in Random Network Coding // IEEE Transactions on Information Theory. — 2008. — Vol. 54, N8. — P. 3579–3591.
36. Kovalev A. A., Pryadko L. P. Quantum Kronecker sum-product low-density parity-check codes with finite rate // Physical Review A. — American Physical Society, 2013. — Vol. 88, N1. — P. 012311.
37. Leverrier A., Zémor G. Decoding quantum Tanner codes // arXiv:2208.05537 [quant-ph], 2022.
38. Leverrier A., Zémor G. Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes // arXiv:2206.07571 [quant-ph], 2022.
39. Leverrier A., Tillich J.-P., Zémor G. Quantum Expander Codes // 2015 IEEE 56th Annual Symposium on Foundations of Computer Science. — Berkeley, CA, USA: IEEE, 2015. — P. 810–824.

40. Leverrier A., Londe V., Zémor G. Towards local testability for quantum coding // Quantum. — Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften, 2022. — Vol. 6. — P. 661.
41. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. — 1988. — Vol. 8, N3. — P. 261–277.
42. MacKay D. J. C., Mitchison G., McFadden P. L. Sparse-graph codes for quantum error correction // IEEE Transactions on Information Theory. — 2004. — Vol. 50, N10. — P. 2315–2330.
43. MacWilliams F. J., Sloane N. J. A. The Theory of Error-Correcting Codes. — Amsterdam: North Holland Publishing Co., 1977.
44. Meir O. On the rectangle method in proofs of robustness of tensor products // Information Processing Letters. — 2012. — Vol. 112, — P. 257–260.
45. Meshulam R. Graph codes and local systems // arXiv:1803.05643 [math], 2018.
46. Panteleev P., Kalachev G. Asymptotically Good Quantum and Locally Testable Classical LDPC-Codes // arXiv:2111.03654 [quant-ph], 2021.
47. Panteleev P., Kalachev G. Degenerate Quantum LDPC-Codes With Good Finite Length Performance // Quantum. — Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften, 2021. — Vol. 5. — P. 585.
48. Panteleev P., Kalachev G. Quantum LDPC-Codes With Almost Linear Minimum Distance // IEEE Transactions on Information Theory. — 2022. — Vol. 68, N1. — P. 213–229.
49. Pryadko L. P., Zeng W. Higher-dimensional quantum hypergraph-product codes with finite rates // Physical Review Letters. — American Physical Society, 2019. — Vol. 122, N23. — P. 230501.
50. Sipser M., Spielman D. A. Expander codes // IEEE Transactions on Information Theory. — 1996. — Vol. 42, N6. — P. 1710–1722.
51. Steane A. M. Error Correcting Codes in Quantum Theory // Phys. Rev. Lett. — American Physical Society, 1996. — Vol. 77, N5. — P. 793–797.
52. Tanner R. A recursive approach to low complexity codes // IEEE Transactions on Information Theory. — 1981. — Vol. 27, N5. — P. 533–547.
53. Tillich J., Zémor G. Quantum LDPC-codes with positive rate and minimum distance proportional to the square root of the blocklength // IEEE Transactions on Information Theory. — 2014. — Vol. 60, N2. — P. 1193–1202.
54. Tillich, J. and Zémor, G. Quantum LDPC-codes with positive rate and minimum distance proportional to $n^{1/2}$ // 2009 IEEE international symposium on information theory. — Seoul, Korea (South): IEEE, 2009. — P. 799–803.
55. Wise D. T. Complete square complexes // Commentarii Mathematici Helvetici. — 2007. — Vol. 82, N4. — P. 683–724.
56. Wolf J. On Codes Derivable from the Tensor Product of Check Matrices // IEEE Transactions on Information Theory. — 1965. — Vol. 11, N2. — P. 281–284.

Поступило в редакцию 9 X 2023