О кодовом расстоянии в одном классе квантовых LDPC кодов

Калачев Г.В.[1], Пантелеев П.А.[2]

В работе рассматривается одно семейство квантовых LDPC кодов с весом стабилизатора 6 и двумя логическими кубитами, где имеется фрактальная структура некоторых логических операторов. Эти коды можно представить в виде локальных кодов на трёхмерной решётке $L \times L \times L$ с периодическими граничными условиями. Для этого семейства кодов доказана нижняя оценка кодового расстояния $\Omega(L^\alpha)$, где $\alpha = \log_2(2(\sqrt{5}-1)) \approx 1.306$.

Ключевые слова: квантовый LDPC код, локальный квантовый код, кодовое расстояние, линейный клеточный автомат, фрактальная размерность.

1. Введение

Одним из основных препятствий на пути к созданию полноценного универсального квантового компьютера является достаточно высокая ненадёжность его компонент. Данное обстоятельство прежде всего связано с невозможностью в процессе вычисления на квантовом компьютере идеально изолировать от окружающей среды элементарные ячейки его памяти — *кубиты*, хранящие текущее состояние. Идея квантовых кодов, предложенная П. Шором [1], теоретически позволяют решить данную проблему за счёт кодирования абстрактного k-кубитного состояния квантового компьютера (*логические* кубиты) физически реализуемым n-кубитным состоянием (*физические* кубиты). При этом параметр $R = k/n < 1$, называемый *скоростью* кода, характеризует избыточность

[1] *Калачев Глеб Вячеславович* — к.ф.-м.н., м.н.с. лаборатории проблем теоретической кибернетики мех.-мат. ф-та МГУ, e-mail: gleb.kalachev@yandex.ru.

Kalachev Gleb Vyacheslavovich — Candidate of Physical and Mathematical Sciences, Junior Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Problems of Theorecical Cybernetics Lab.

[2] *Пантелеев Павел Анатольевич* — к.ф.-м.н., н.с. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: panpavel@yandex.ru.

Panteleev Pavel Anatolyevich — Candidate of Physical and Mathematical Sciences, Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

такого кодирования. Другой важной характеристикой квантового кода, показывающей его способность исправлять ошибки, возникающие в физических кубитах, является *кодовое расстояние*. Аналогично классическим кодам, *кодовое* (*минимальное*) *расстояние* квантового кода можно определить как максимальное число d такое, что любая ошибка, изменяющая квантовое состояние и затрагивающая менее чем d физических кубитов, может быть обнаружена.

В квантовой механике состояние n-кубитной квантовой системы может быть описано вектором из 2^n-мерного комплексного гильбертова пространства $\mathbb{C}^{2^n}$ и, в общем случае, квантовый код определяется формально как 2^k-мерное подпространство Q пространства $\mathbb{C}^{2^n}$, где параметры n и k называются его *длинной* и *размерностью*, соответственно. При идеальном функционировании квантового компьютера, защищённого кодом Q, его состояние должно быть одним из элементов Q, которые по аналогии с классическими кодами называют (*квантовыми*) *кодовыми словами*. Однако, вследствие ошибок, возникающих в кубитах, состоянием квантового компьютера являются искажённые квантовые кодовые слова, и задача декодера для Q состоит в периодическом обнаружении и исправлении этих ошибок.

Легко видеть, что приведённое выше определение квантового кода очень общее, и, вообще говоря, не является конструктивным, так как для фиксированных n и k существует континуум различных квантовых кодов. Поэтому, как правило, рассматриваются какие-то специальные классы квантовых кодов, которые можно задать конструктивно. Один из наиболее известных таких классов — это класс *стабилизирующих квантовых кодов*[1] (анг. stabilizer codes) [2], являющихся, в некотором смысле, квантовым аналогом классических линейных кодов. В данной работе мы рассматриваем частный случай стабилизирующих кодов, называемых кодами Кальдербанка-Шора-Стина (CSS коды) [3, 4].

Важным достоинством CSS кодов, выделяющим их в классе стабилизирующих кодов, является простота их задания и естественная связь с классическими линейными кодами. Фактически, можно рассматривать CSS код как пару классических двоичных линейных кодов одинаковой длины n, заданных проверочными матрицами H_X и H_Z такими, что любая строка H_X ортогональна[2] любой строке H_Z. В дальнейшим под словом квантовый код мы всегда будем подразумевать CSS код.

Со строками проверочных матриц H_X и H_Z связывают эрмитовы операторы, называемые *стабилизаторами*, описывающие квантовые изме-

[1] В литературе эти коды также еще называются *симплектическими* или *аддитивными*.

[2] Ортогональность двоичных векторов $(u_1, \ldots, u_n)$ и $(v_1, \ldots, v_n)$ понимается как выполнение тождества $\sum_{i=1}^{n} u_i v_i \equiv 0 \pmod 2$.

рения над n физическими кубитами. Случайный вектор s, являющийся результатом этих измерений, представляет собой аналог синдрома для классических линейных кодов. Он подаётся на вход декодеру, который пытается определить и исправить ошибку в n-кубитном квантовом состоянии. Отметим, что условие ортогональности строк матриц H_X и H_Z эквивалентно попарной коммутативности стабилизаторов, т.е. возможности совместного измерения всех компонент вектора s.

По определению, *весом* стабилизатора будем называть число ненулевых компонент в соответствующей строке проверочной матрицы. С физической точки зрения вес стабилизатора — это число физических кубитов с которыми надо провзаимодействовать для выполнения соответствующего квантового измерения. Поэтому с практической точки зрения особый интерес представляют квантовые LDPC коды (QLDPC коды), у которых обе проверочные матрицы H_X и H_Z разрежены. При этом разреженность обычно понимается как существование константы w, ограничивающей сверху веса строк и столбцов матриц H_X и H_Z при росте длины кода n. Последнее условие эквивалентно тому, что в каждом квантовом измерении участвует не более w физических кубитов, и каждый кубит участвует не более чем в $2w$ измерениях. В отличии от классического случая, подобные ограничения чрезвычайно важны для квантовых кодов, так как в процессе измерения мы взаимодействуем с кубитами, и тем самым вносим в них ошибки.

На данный момент неизвестно, существуют ли семейства QLDPC кодов, имеющие линейно растущее кодовое расстояние d даже при фиксированной размерности кода k. Однако имеются некоторые общие конструкции [6], позволяющие строить QLDPC коды с расстоянием, растущим, как $\Theta(\sqrt{n})$ и фиксированной скоростью кода k/n. Одно из лучших семейств QLDPC кодов, для которых известны оценки кодового расстояния, основано на специальном семействе метрик на некотором многообразии [7]. У этих кодов кодовое расстояние имеет порядок[3] $\sqrt{n\sqrt{\log n}}$. Отметим, что в недавних работах [8, 9] данный результат был несколько улучшен и получено семейство QLDPC кодов с расстоянием, растущим, как $\Omega(\sqrt{n}\log^k n)$ для любого k.

Также для физической реализации очень важно чтобы кубиты можно было расположить в D-мерном пространстве, где $D \leqslant 3$, так, чтобы связанные общим проверочным соотношением[4] кубиты были бы расположены локально, т.е. расстояние между ними ограничено константой при увеличении длины кода n. Квантовые LDPC коды, для которых такое расположение возможно, называются *D-локальными* или просто *ло-*

[3] В оригинальной работе [7] этот порядок ошибочно указан как $\sqrt{n\log n}$.

[4] Проверочные соотношения CSS кода — это проверочные соотношения двух соответствующих классических кодов.

кальными, если из контекста ясно о каком D идёт речь. Для локальных кодов известна [10] верхняя оценка $d = O(n^{(D-1)/D})$, которая при $D = 2$ достигается на торическом коде [16, с. 97][17]. Для $D > 2$ неизвестно кодов, на которых эта оценка достигается. При $D = 3$ есть несколько семейств кодов [11, 14, 15], для которых потенциально расстояние может асимптотически расти быстрее чем $\sqrt{n}$, однако все известные нижние оценки на кодовое расстояние этих кодов не превосходят $\Omega(n^{\frac{1}{3}})$. У таких кодов некоторые логические операторы (недетектируемые ошибки, изменяющие квантовое состояние) имеют фрактальную структуру, поэтому их иногда называют *фрактальными*[5].

В работе рассматривается одно семейство QLDPC кодов с весом стабилизатора 6 и двумя логическими кубитами (т.е., $k = 2$), где также имеется фрактальная структура некоторых логических операторов. Эти коды можно представить в виде локальных кодов на трёхмерной решётке $\mathbb{Z}_L^3$ с периодическими граничными условиями, где $\mathbb{Z}_L$ — кольцо вычетов по модулю L. При этом в каждом узле решётки $\mathbb{Z}_L^3$ находится по два кубита, и тем самым общее число кубитов $n = 2L^3$. Для этого семейства кодов доказана нижняя оценка кодового расстояния $d = \Omega(L^\alpha) = \Omega(n^{\frac{1}{3}\alpha})$, где $\alpha = \log_2(2(\sqrt{5} - 1)) \approx 1.306$.

2. Определения и обозначения

2.1. Классические и квантовые коды

Обозначим через $\mathbb{F}_2$ конечное поле из двух элементов, а через $\mathbb{F}_2^n$ — n-мерное координатное векторное пространство над $\mathbb{F}_2$, элементы которого мы будем понимать как двоичные векторы-столбцы $(v_1, \ldots, v_n)^T$. *Весом* вектора $v \in \mathbb{F}_2^n$ будем называть количество его ненулевых элементов и обозначать $|v|$. Если у нас имеется $m \times n$ матрица A над $\mathbb{F}_2$, то через $\langle A \rangle$ будем обозначать линейную оболочку строк матрицы A, а через $\ker A$ ядро линейного оператора $v \mapsto Av$.

Напомним, что классическим двоичным линейным C кодом *длины* n и *размерности* k называют произвольное k-мерное линейное подпространство n-мерного векторного пространства $\mathbb{F}_2^n$, элементы которого называются *кодовыми словами*. Важной характеристикой кода, которая описывает его способность исправлять ошибки, является *кодовое* (*минимальное*) *расстояние* d, равное, в случае линейных кодов, минимальному весу ненулевого кодового слова, т.е. $d = \min_{v \in C \setminus \{0\}} |v|$. Так как C является k-мерным линейным подпространством в $\mathbb{F}_2^n$, его можно задать как $C = \langle G \rangle$, т.е. как линейные комбинации строк некоторой матрицы G,

[5] Также широко используется название *квантовая фрактальная жидкость* (анг. quantum fractal liquid).

называемой *порождающей*. Линейное подпространство $C \subseteq \mathbb{F}_2^n$ можно также задать как $C = \ker H$, т.е. как множество решений системы линейных однородных уравнений, где матрица H называется *проверочной*. При этом строки проверочной матрицы H соответствуют уравнениям данной системы, которые мы будем называть *проверочными соотношениями* для кода C.

Обычно кодовые слова классического линейного кода $C \subseteq \mathbb{F}_2^n$, заданного проверочной матрицей H, понимаются как двоичные n-битные последовательности, которые мы передаём по каналу с ошибками. Однако кодовые слова из C можно также интерпретировать и как вектора ошибок $x \in \mathbb{F}_2^n$, возникающие с передаваемыми n битами, которые мы не можем детектировать при помощи проверочной матрицы H, т.е. когда $Hx = 0$. При этом самим векторам ошибок x естественно соответствуют операторы ошибок $E_x \colon v \mapsto v + x$ действующие на множестве n-битных векторов. Если $c' = E_x(c)$, где $c \in C$, есть искажённое кодовое слово с которым произошла ошибка x, то вектор $s = Hc'$ называют *синдромом*. Поскольку $s = H(c + x) = Hx$ мы видим, что синдром не зависит от самого кодового слова c, а зависит только от произошедшей с ним ошибки x. Поэтому проверочные соотношения, соответствующие строкам проверочной матрицы H, можно также понимать как «элементарные измерения», которые мы производим над искажённым кодовым словом c' для выявлении информации о произошедшей с ним ошибке x. Результатом такого измерения для i-й строки является значение i-й компоненты синдрома. При этом очевидно выполняются следующие условия:

- результат всех элементарных измерений равен нулю в точности для кодовых слов;
- для кодовых слов, искажённых оператором ошибки E_x, результат измерений описывается синдромом $s = Hx$.

В кубитах, в отличии от битов, может возникать континуум различных ошибок[6]. Однако можно показать [5, Глава 10], что для n-кубитного состояния защищённого квантовым кодом значение имеют только выделенное конечное подмножество ошибок $\mathcal{E}_n$, состоящее из 2^{2n} ошибок $E_{x,z}$, параметризованных всевозможными $x, z \in \mathbb{F}_2^n$. Напомним, что квантовым кодом C называют произвольное 2^k-мерное подпространство 2^n-мерного комплексного гильбертова пространства $\mathbb{C}^{2^n}$, элементы которого мы называем (*квантовыми*) *кодовыми словами*.

Основная идея квантового CSS кода C состоит в том, чтобы паре двоичных матриц H_X и H_Z с числом столбцов n, играющих роль прове-

[6] С точки зрения квантовой механики ошибкам над n-кубитным состоянием соответствуют унитарные операторы действующие на $\mathbb{C}^{2^n}$.

рочных матриц, сопоставить последовательность элементарных квантовых измерений[7] над n-кубитным состоянием (по одному измерению для каждой строки H_X и H_Z) так, чтобы:

- результат всех элементарных квантовых измерений детерминированный и равен нулю в точности для квантовых кодовых слов;
- для квантовых кодовых слов, искажённых оператором ошибки $E_{x,z}$, результат измерений также детерминированный, и описывается векторами $s_X = H_X z$, $s_Z = H_Z x$, которые, как и в случае классических линейных кодов, называются *синдромами*.

Как видно синдром s_X (соответственно s_Z) содержит информацию о компоненте z (соответственно x) ошибки $E_{x,z} \in \mathcal{E}_n$ произошедшей с n-кубитным квантовым состоянием. На основании данной информации декодер для квантового CSS кода пытается найти наиболее вероятную ошибку $E_{x,z} \in \mathcal{E}_n$ и исправить ее.

Как хорошо известно, в квантовой механике в силу принципа неопределённости Гейзенберга не любые два измерения могут давать полностью детерминированный результат одновременно. Достаточным условием для этого является коммутируемость самосопряжённых операторов, соответствующих этим измерениям. По этой причине для возможности одновременного измерения всех компонент синдромов s_X и s_Z требуется, чтобы операторы, соответствующие элементарным измерениям для матриц H_X и H_Z, были попарно коммутативны. Можно показать [5, с. 561], что последнее условие эквивалентно тому, что любая строка в матрице H_X ортогональна любой строке в H_Z с точки зрения стандартного скалярного произведения в векторном пространстве $\mathbb{F}_2^n$. Данное условие можно компактно сформулировать в матричном виде как:

$$H_X H_Z^T = 0. \tag{1}$$

В дальнейшем CSS код C, заданный парой матриц H_X и H_Z над полем $\mathbb{F}_2$ с одинаковым числом столбцов n, удовлетворяющих соотношению (1), будем обозначать через $\mathrm{CSS}(H_X, H_Z)$ и отождествлять с парой (C_Z, C_X) классических двоичных линейных кодов $C_Z, C_X \subseteq \mathbb{F}_2^n$, заданных проверочными матрицами H_X, H_Z, соответственно. Заметим, что ошибки вида $E_{0,z}$ и $E_{x,0}$, где $z \in C_Z$, $x \in C_X$ не будут обнаружены квантовым кодом, поскольку в этом случае $s_X = s_Z = 0$. По этой причине далее кодовые слова из C_Z (соответственно C_X) мы будем называть *Z-ошибками* (соответственно *X-ошибками*) кода $\mathrm{CSS}(H_X, H_Z)$.

[7] Результатом каждого элементарного квантового измерения является один бит, причём в общем случае этот результат не является детерминированным.

Отметим, что поскольку, в силу условия (1), строки матриц H_X и H_Z попарно ортогональны друг другу, каждая строка матрицы H_X является X-ошибкой, а матрицы H_Z — Z-ошибкой. Следовательно $\langle H_X \rangle \subseteq C_X$ и $\langle H_Z \rangle \subseteq C_Z$.

Когда мы рассматривали классические коды мы подмечали, что множество кодовых слов в точности совпадает со множеством всех ошибок $x \in \mathbb{F}_2^n$ которые мы не можем детектировать при вычислении синдрома. Однако, нулевому кодовому слову соответствует оператор ошибки $E_0 : x \mapsto x$, не изменяющий передаваемые по каналу кодовые слова. Оказывается, что в квантовом случае подобная ситуация встречается значительно чаще и можно показать [5, Глава 10], что любой оператор вида $E_{x,z}$, где $x \in \langle H_X \rangle$ и $z \in \langle H_Z \rangle$ тождественно действует на множестве квантовых кодовых слов. При этом любой другой оператор $E_{x,z}$ уже действует нетождественно на этом множестве. Данное обстоятельство мотивирует приведённое ниже определение.

Определение 1. X-ошибка $x \in C_X$ (соответственно, Z-ошибка $z \in C_Z$) называется *вырожденной*, если $x \in \langle H_X \rangle$ (соответственно, $z \in \langle H_Z \rangle$).

Заметим, что две X-ошибки $x, x' \in C_X$, отличающиеся на вырожденную X-ошибку (т.е. $x - x' \in \langle H_X \rangle$), задают операторы $E_{x,0}$ и $E_{x',0}$, действующие одинакового на множестве квантовых кодовых слов. Аналогичное утверждение справедливо и для Z-ошибок. Подобные ошибки, действующие одинаково на множестве квантовых кодовых слов, мы будем называть *эквивалентными*. Соответствующие данному отношению классы эквивалентности обычно называют *логическими ошибками*. Поэтому логические X-ошибки (соответственно Z-ошибки) представляют собой элементы факторпространства $C_X / \langle H_X \rangle$ (соответственно, $C_Z / \langle H_Z \rangle$).

Определение 2. *Размерностью* CSS кода называется размерность пространства его логических ошибок.

Убедимся, что определение корректно, т.е. размерности пространств логических X- и Z-ошибок совпадают. Действительно:

$$\dim(C_X / \langle H_X \rangle) = \dim(\ker H_Z) - \dim \langle H_X \rangle = n - \operatorname{rank} H_Z - \operatorname{rank} H_X,$$
$$\dim(C_Z / \langle H_Z \rangle) = \dim(\ker H_X) - \dim \langle H_Z \rangle = n - \operatorname{rank} H_X - \operatorname{rank} H_Z.$$

Таким образом, формула для размерности CSS кода имеет вид

$$\dim Q = n - \operatorname{rank} H_X - \operatorname{rank} H_Z. \tag{2}$$

Можно показать [5, с. 553], что введённое сейчас понятие размерности CSS кода согласуется с введённым ранее понятием размерности квантового кода общего вида, т.е. множество квантовых кодовых слов CSS кода образует 2^k-мерное подпространство в $\mathbb{C}^{2^n}$.

Определение 3. *Кодовым* (*минимальным*) расстоянием CSS кода называется минимальный вес невырожденной X- или Z-ошибки.

В данной работе рассматриваются CSS коды специального вида [21], а именно, когда матрицы H_X и H_Z состоят из двух квадратных блоков одинакового размера. Блочные матрицы будем писать в квадратных скобках. Если матрица состоит из двух блоков A и B, будем для наглядности разделять их вертикальной чертой: $[A \mid B]$. В этих обозначениях рассматриваемое семейство кодов задаётся матрицами

$$H_X = [A \mid B],$$
$$H_Z = \left[B^T \mid A^T\right],$$

где матрицы A и B коммутируют, т.е. $AB = BA$. Покажем, что в таком случае матрицы H_X и H_Z задают CSS код. Для этого достаточно убедится, что выполняется равенство (1). Действительно, имеем:

$$H_X H_Z^T = A(B^T)^T + B(A^T)^T = AB + BA = 0.$$

Кубиты полученного квантового кода естественно разбиваются на две группы одинакового размера — левую и правую, в зависимости от того, к какому блоку (левому или правому) матриц H_X и H_Z они относятся. В случаях когда кубиты будут размещаться в узлах какой-либо геометрической решётки мы будем размещать левый и соответствующий ему правый кубит в одном узле.

2.2. Задание кодов через групповые алгебры

Важный частный случай кодов из описанного выше семейства получается если матрицы A и B могут быть заданы элементами некоторой групповой алгебры [11, 14]. В связи с этим введём ещё несколько обозначений.

Циклическую группу порядка ℓ, порождённую элементом x будем обозначать $\langle x \rangle_\ell$.

Пусть G — группа. Через $\mathbb{F}_2^G$ будем обозначать групповую алгебру группы G над полем $\mathbb{F}_2$. Заметим, что если G — абелева, то её можно представить в виде произведения циклических групп $\langle x_1 \rangle_{a_1} \times \cdots \times \langle x_n \rangle_{a_n}$. В этом случае групповая алгебра $\mathbb{F}_2^G$ изоморфна факторкольцу полиномов $\mathbb{F}_2[x_1, ..., x_n]/(x_1^{a_1} + 1, ..., x_n^{a_n} + 1)$.

Через $\mathcal{M}_G(\mathbb{F}_2)$ обозначим алгебру матриц $|G| \times |G|$, у которых строки и столбцы индексируются элементами группы G. Определим вложение $\mathbb{F}_2^G \hookrightarrow \mathcal{M}_G(\mathbb{F}_2)$, которое определим на базисе (элементах группы G):

$$g \in G \longrightarrow M_G(g) = \{a_{ij}\}_{i,j \in G} \in \mathcal{M}_G(\mathbb{F}_2), \text{ где } a_{ij} = \begin{cases} 1, & \text{если } i = gj, \\ 0, & \text{иначе.} \end{cases}$$

Далее будем отождествлять элемент $g \in \mathbb{F}_2^G$ с соответствующей матрицей $M_G(g)$ в тех случаях, где группа G однозначно определяется из контекста.

Также нам понадобится ставить в соответствие элементам групповой алгебры $\mathbb{F}_2^G$ векторы длины $|G|$. Определим $V_G : \mathbb{F}_2^G \to \mathbb{F}_2^{|G|}$, где $V_G(g)$ — первый столбец матрицы $M_G(g)$. Заметим, что при таком определении выполнено свойство $V_G(gh) = M_G(g)V_G(h)$. Отметим, что в отличие от M_G, отображение V_G — биекция.

Введём операцию $\bar{\cdot}\colon \mathbb{F}_2^G \to \mathbb{F}_2^G$, соответствующую транспонированию матрицы:

$$g = \sum_{\alpha \in G} c_\alpha \alpha \quad \longmapsto \quad \overline{g} = \sum_{\alpha \in G} c_\alpha \alpha^{-1}.$$

Тогда $M_G(\overline{g}) = (M_G(g))^T$.

Классический линейный код с проверочной матрицей $M_G(g)$ будем обозначать через $\mathcal{C}(G, g)$.

Если G — группа и элементы $g, h \in \mathbb{F}_2^G$ коммутируют, то квантовый CSS код, задаваемый матрицами

$$\begin{aligned} H_X &= [M_G(g) \mid M_G(h)], \\ H_Z &= \left[M_G(\overline{h}) \mid M_G(\overline{g})\right] \end{aligned}$$

будем обозначать через $\mathcal{Q}(G, g, h)$.

Пример 1. $\mathcal{Q}\left(\langle x\rangle_L \times \langle y\rangle_L, 1 + x, 1 + y\right)$ представляет собой торический код [16, 17] с минимальным расстоянием L.

Пример 2. Семейство фрактальных кодов

$$\mathcal{Q}\left(\langle x\rangle_L \times \langle y\rangle_L \times \langle z\rangle_L, y + r(x), z + q(x)\right),$$

где p и q — некоторые многочлены, были исследованы в работе Йошиды [14, 15], однако для них неизвестно нижних оценок по порядку выше L, но несмотря на это есть гипотеза [14, 15], что расстояние этих кодов может быть выше $L^{3/2} = \Omega(\sqrt{n})$.

Пример 3. Кубический код Хааха [11] задаётся следующим образом:

$$\mathrm{Haah}(L) = \mathcal{Q}\left(\langle x\rangle_L \times \langle y\rangle_L \times \langle z\rangle_L, 1 + x + y + z, 1 + xy + xz + yz\right).$$

Торический код и фрактальные коды представляют собой два крайних случая: у торических кодов все логические ошибки являются цепями в графе Таннера, и для них легко находится точное значение минимального расстояния, а у фрактальных кодов логические ошибки минимального веса все имеют фрактальную структуру, и известные нижняя и верхняя оценка очень сильно расходятся.

В данной работе рассматривается промежуточный вариант кодов, у которых часть есть логические ошибки в виде цепей, а есть ошибки фрактального вида. Для этих кодов так же, как и для фрактальных кодов верхняя оценка на кодовое расстояние выше $\sqrt{n}$, а нижняя – ниже $\sqrt{n}$, где n — длина кодового слова, но мы покажем, что для них возможно доказать нижнюю оценку, которая существенно выше, чем известная оценка для фрактальных кодов.

Пример 4. Семейство кодов, рассматриваемых в данной работе, а именно:

$$\mathrm{SF}(r,t) = \mathcal{Q}\left(\langle x\rangle_{L^2} \times \langle y\rangle_L, 1+x, y+r(x^L)\right), \qquad \text{где } L = 2^t.$$

Видно, что в данном примере первый полином, как в торическом коде, второй — как во фрактальном коде. Поэтому назовём эти коды *полуфрактальными*.

Отметим, что элементы группы $\langle x\rangle_{L^2} \times \langle y\rangle_L$ имеют вид $x^{i+Lj}y^k = x^i z^j y^k$, где $z = x^L$; $0 \leqslant i,j,k < L$. Поэтому для фиксированного многочлена r семейство кодов $\mathrm{SF}(r,t)$ при $t \to \infty$, заданное многочленами $1+x$ и $y + r(z)$, является локальным при расположении кубитов на трёхмерной решётке $\mathbb{Z}_L^3$ с периодическими граничными условиями (узлы данной решётки можно расположить на трёхмерном торе).

Если C — код (классический или квантовый), то через $d(C)$ будем обозначать его кодовое расстояние.

Посмотрим, как выглядят кодовые слова кода $\mathcal{Q}(G,g,h)$. Уравнение $H_X v = 0$ в терминах групповой алгебры можно переписать, как

$$gs + ht = 0, \qquad \text{где } v = \begin{bmatrix} V_G(s) \\ V_G(t) \end{bmatrix}. \tag{3}$$

Таким образом, каждой Z-ошибке v можно поставить в соответствие пару (s,t), удовлетворяющую соотношению (3). Аналогично, каждой X-ошибке u можно поставить в соответствие пару (v,w), удовлетворяющую соотношению $\overline{h}v + \overline{g}w = 0$.

Условие вырожденности $v \in \langle H_Z\rangle = \left\langle \left[M_G(\overline{h}) \mid M_G(\overline{g})\right]\right\rangle$ означает, что существует вектор $V_G(a) \in \mathbb{F}_2^{|G|}$ такой, что $v = V_G(a)^T H_Z$, значит

$$v^T = H_Z^T V_G(a) = \begin{bmatrix} M_G(\overline{h})^T V_G(a) \\ M_G(\overline{g})^T V_G(a) \end{bmatrix} = \begin{bmatrix} V_G(ha) \\ V_G(ga) \end{bmatrix},$$

а это значит, что вектору v соответствует пара (ha, ga). Таким образом, множеству вырожденных Z-ошибок $\langle H_Z\rangle$ соответствует множество пар $\left\{(ha,ga) \mid a \in \mathbb{F}_2^G\right\}$. Аналогично, множеству вырожденных X-ошибок соответствует множество пар: $\left\{(\overline{g}a, \overline{h}a) \mid a \in \mathbb{F}_2^G\right\}$.

В данной работе нас будет интересовать случай, когда группа G абелева. В этом случае выполнено

$$\overline{gs} + \overline{h}\overline{t} = \overline{sg + th} = \overline{gs + ht},$$

поэтому отображение $(s, t) \mapsto (\overline{t}, \overline{s})$ задаёт изоморфизм между пространством X-ошибок и пространством Z-ошибок и сохраняет вес и вырожденность ошибки. Получим следующее утверждение.

Утверждение 1. *Пусть группа G абелева. Тогда для квантового кода $\mathcal{Q}(G, g, h)$ минимальный вес невырожденной X-ошибки равен минимальному весу невырожденной Z-ошибки, а также* $\operatorname{rank} H_X = \operatorname{rank} H_Z$.

Данное утверждение позволяет несколько упростить вычисление размерности CSS кода, которое даётся формулой (2). Но более важным следствием данного утверждения является возможность в дальнейшем при получении оценок на кодовое расстояние изучать только вес невырожденных Z-ошибок. Поэтому далее под словом ошибка мы будем иметь ввиду Z-ошибка.

3. Формулировка основных результатов

Сформулируем утверждение[8], выражающее размерность квантовых кодов, заданных элементами факторкольца многочленов, через размерность факторкольца многочленов, как векторного пространства над $\mathbb{F}_2$.

Утверждение 2. *Пусть* $Q = \mathcal{Q}\left(\langle x_1\rangle_{a_1} \times \cdots \times \langle x_n\rangle_{a_n}, p, q\right)$. *Тогда*

$$\dim Q = 2 \dim \left(\mathbb{F}_2[x_1, ..., x_n]/\left(x_1^{a_1} + 1, ..., x_n^{a_n} + 1, p, q\right)\right).$$

При доказательстве основного результата важной частью доказательства является лемма о выравнивании ошибок, которая может представлять независимый интерес. Рассмотрим код $Q = \mathcal{Q}\left(\langle x\rangle_{ac} \times H, 1 + x, g\right)$, где $g \in \mathbb{F}_2^{G'}$, $G' = \langle x^c\rangle \times H$. Поскольку x коммутирует со всеми элементами группы, в частности, с G, то квантовый код Q задан корректно. В лемме доказано, что для каждой логической ошибки минимального веса существует эквивалентная ей ошибка минимального веса, но в некотором смысле выровненная по элементам подгруппы G'.

Определение 4. Ошибка $e_Z = [p, q]$ кода Q называется *выровненной*, если $(1 + x)p \in \mathbb{F}_2^{G'}$ и $q \in \mathbb{F}_2^{G'}$.

[8] Аналогичное утверждение в значительно более общем виде может быть найдено в работе [12, Следствие 4.5].

Заметим, что выровненная ошибка кода Q всегда имеет вид

$$e_Z = \Big[p_0 \sum_{j=0}^{c-1} x^j,\ q_0\Big], \quad \text{где } p_0, q_0 \in \mathbb{F}_2^{G'}.$$

Лемма 1 (О выравнивании ошибок)**.** *Пусть $G = \langle x\rangle_\ell \times H$, $\ell = ac \geqslant 2$ и $g \in \mathbb{F}_2^{G'}$, где $G' = \langle x^c\rangle \times H \subseteq G$. Рассмотрим квантовый код $Q = \mathcal{Q}(G, 1+x, g)$. Для любой логической ошибки e_Z среди эквивалентных ей ошибок минимального веса существует выровненная ошибка e'_Z.*

Одним из применений этой леммы может быть поиск простых нижних оценок для квантовых кодов, описываемых в этой лемме. В качестве одного из примеров применения этой леммы будет доказано следующее утверждение.

Утверждение 3. *Пусть $G = \langle x\rangle_{ac} \times H$, $ac \geqslant 2$, $G' = \langle x^c\rangle \times H \subset G$, $g \in \mathbb{F}_2^{G'}$ имеет чётный вес, и минимальное расстояние классического кода $\mathcal{C}(G', g)$ равно d.*

Тогда $\mathcal{Q}(G, 1+x, g)$ — квантовый код с размерностью, отличной от 0 и минимальным расстоянием не меньше $\min(d, c)$.

Основным результатом данной работы является нижняя оценка кодового расстояния для полуфрактальных кодов, сформулированная в следующей теореме.

Теорема 1. *Если $L = 2^t$, то минимальное расстояние полуфрактального кода*

$$\mathrm{SF}(1+x+x^2, t) = \mathcal{Q}\left(\langle x\rangle_{L^2} \times \langle y\rangle_L, 1+x, y+1+x^L+x^{2L}\right)$$

ограничено снизу величиной $\Omega(L^\alpha)$, где $\alpha = \log_2(2(\sqrt{5}-1)) \approx 1.306$.

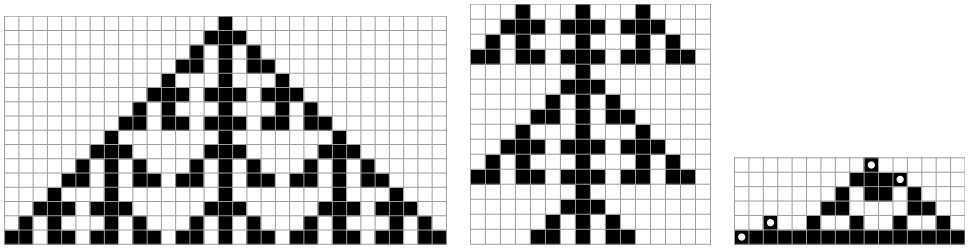
4. Доказательство

Для оценки кодового расстояния полуфрактальных кодов $\mathrm{SF}(r, t)$ нам понадобятся вспомогательные величины:

$$D_r(t) = \sum_{j=0}^{2^t-1} |r^j(x)|,$$

$$D_r^*(t) = \min_{\substack{p \in \mathbb{F}_2[x]/(x^{2^t}-1),\\ |p| \equiv 1 \mod 2}} \left| p(x) \sum_{j=0}^{2^t-1} (r(x)/y)^j \bmod (x^{2^t}-1, y^{2^t}-1) \right|,$$

$$\overline{D}_r(t) = \min_{h \in \mathbb{F}_2[x,y]} \left\{ |h(x,y)| \;\middle|\; h(x, r(x)) \equiv 1 + x + .. + x^{2^t-1} \mod x^{2^t}-1 \right\}.$$



(a) $D_{1+x+x^{-1}}(4) = 128$ (b) $D^*_{1+x+x^{-1}}(4) = 80$ (c) $\overline{D}_{1+x+x^{-1}}(4) = 4$

Рис. 1. Интерпретация величин D, D^* и $\overline{D}$ в терминах клеточных автоматов.

Величины D_r, D^*_r и $\overline{D}_r$ можно интерпретировать в терминах одномерного линейного клеточного автомата A_r с функцией перехода, задаваемой многочленом $r(x)$. Мы не будем использовать эту интерпретацию в формальных рассуждениях, однако иногда удобно её иметь в виду, чтобы удобнее представлять себе объекты, о которых будет идти речь. На рисунке 4 проиллюстрирована такая интерпретация на примере многочлена $r(x) = 1 + x + x^{-1}$, который соответствует элементарному клеточному автомату Rule 150 [19]. Отметим, что с величины $D_r, D^*_r, \overline{D}_r$ для многочленов $1 + x + x^{-1}$ и $1 + x + x^2$ совпадают, но в терминах клеточных автоматов многочлен $1 + x + x^{-1}$ более естественный, поскольку соответствует симметричной окрестности радиуса 1.

Величину $D_r(t)$ можно понимать, как количество единиц в эволюции одномерного линейного клеточного автомата [18, 19], с функцией перехода, задаваемой многочленом $r(x)$, в течение 2^t тактов (рисунок 1(a)). Для линейных клеточных автоматов определено понятие предельного множества и есть алгоритм вычисления фрактальной размерности этого множества [20]. Если a_r — фрактальная размерность, то $D_r(t) \asymp 2^{a_r t}$.

Величина $D^*_r(t)$ — минимальное число клеток в эволюции клеточного автомата A_r в полосе ширины 2^t с периодическими граничными условиями, на протяжении 2^t тактов, начиная с конфигурации с нечётным числом клеток (рисунок 1(b)).

Чтобы интерпретировать величину $\overline{D}_r(t)$, нужно рассмотреть автомат A_r с возможностью подавать на него управляющие сигналы. Один управляющий сигнал переключает состояние одной ячейки на противоположное. $\overline{D}_r(t)$ — минимальное число управляющих сигналов, которые необходимо подать, чтобы перевести состояние 00...00 в состояние 11...11 в полосе шириной 2^t. На рисунке 1(c) кружками отмечены места, где подаются управляющие сигналы. Для полосы ширины 16 достаточно всего 4 сигналов, чтобы получить конфигурацию из всех единиц.

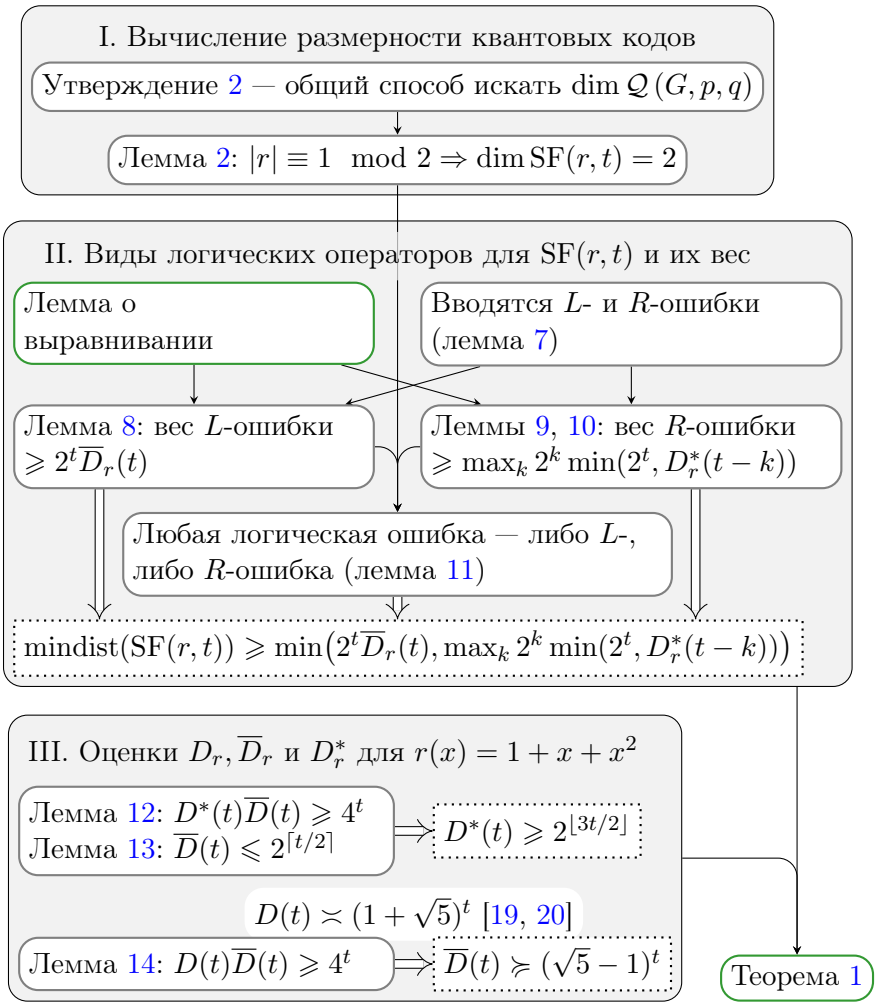


Рис. 2. Структура доказательства теоремы 1

Приведём общий план доказательства теоремы 1.

1) Утверждения о размерности квантовых кодов, заданных через групповые алгебры

   а) Общее утверждение 2, о кодовом расстоянии квантового кода $\mathcal{Q}(G, p, q)$ для коммутативной группы G.

   б) Для полуфрактального кода доказываем, что его размерность равна 2 (Лемма 2 с использованием утверждения 2). Как следствие получаем, что у такого кода есть 3 класса эквивалентности невырожденных ошибок.

2) Явный вид логических ошибок полуфрактальных кодов и нижние оценки их веса через величины $\overline{D}_r$ и D^*_r.

   а) Лемма о выравнивании, описывает класс, в котором содержатся ошибки минимального веса.

   б) Вводятся ошибки $L1, L2, L3$, и все ошибки делятся на L-ошибки и R-ошибки: в лемме 7, доказывается, что они являются логическими ошибками.

   в) В лемме 8 показано, что L-ошибки имеют вес не менее $2^t\overline{D}_r(t)$.

   г) В леммах 9, 10 показано, что вес любой R-ошибки не меньше $\max_k 2^k \min(2^t, D^*_r(t-k))$.

   д) В лемме 11 доказано, что $L1$, $L2$, $L3$ попарно неэквивалентны и невырожденные. Учитывая, что у кода всего 3 неэквивалентных невырожденных ошибки, получаем, что кроме $L1$, $L2$, $L3$ других невырожденных ошибок нет, значит любая ошибка – либо L-ошибка, либо R-ошибка.

   е) Из 2в, 2г, 2д получаем нижнюю оценку на кодовое расстояние

$$\operatorname{mindist}(\mathrm{SF}(r,t)) \geqslant \min\bigl(2^t\overline{D}_r(t), \max_k 2^k \min(2^t, D^*_r(t-k))\bigr).$$

3) Несколько лемм про соотношения между величинами D_r, $\overline{D}_r$ и D^*_r:

   а) $D_r(t)\overline{D}_r(t) \geqslant D^*_r(t)\overline{D}_r(t) \geqslant 4^t$ (леммы 12 и 14);

   б) $\overline{D}_{1+x+x^2}(t) \leqslant 2^{\lfloor t/2 \rfloor}$ (лемма 13);

   в) $D_{1+x+x^2}(t) \asymp (1+\sqrt{5})^t$ (известный результат [19, 20]).

4) Соединяя все оценки для $r(x) = 1 + x + x^2$, получаем оценку кодового расстояния в теореме 1.

Одна из причин, по которой было выбрано семейство кодов размерности 2 — то, что можно в явном виде выписать вид логических ошибок из каждого класса эквивалентности и изучать их по одиночке.

4.1. Леммы о размерности

Доказательство утверждения 2. Пусть $m = a_1 a_2 \cdots a_n$ — размерность групповой алгебры, изоморфной соответствующей факторалгебре многочленов

$$R = \mathbb{F}_2[x_1, ..., x_n]/(x_1^{a_1} + 1, ..., x_n^{a_n} + 1).$$

Длина кодового слова кода Q равна $2m$. Посчитаем размерность с использованием формулы (2). Учитывая, что $\operatorname{rank} H_X = \operatorname{rank} H_Z$ по утверждению 1, имеем $\dim Q = 2m - 2\operatorname{rank} H_X$.

$$\operatorname{rank} H_X = \dim \langle H_X \rangle = \dim \{sp + tq \mid s, t \in R\} = \dim(p, q),$$

где под (p, q) понимается идеал, порождённый элементами p и q в факторалгебре R. Тогда $\dim(g, h) = \dim R - \dim(R/(g, h)) = m - \dim(R/(g, h))$. Отсюда

$$\begin{aligned}\dim Q &= 2m - 2(m - \dim(R/(p, q))) = 2\dim(R/(p, q)) = \\ &= 2\dim\big(\mathbb{F}_2[x_1, ..., x_n]/(x_1^{a_1} + 1, ..., x_n^{a_n} + 1)/(p, q)\big) = \\ &= 2\dim\big(\mathbb{F}_2[x_1, ..., x_n]/(x_1^{a_1} + 1, ..., x_n^{a_n} + 1, p, q)\big).\end{aligned}$$

Утверждение доказано. □

С использованием доказанного утверждения посчитаем размерность полуфрактальных кодов.

Лемма 2. *Если вес многочлена r нечётный, то* $\dim \mathrm{SF}(r, t) = 2$.

Доказательство. Из утверждения 2 имеем

$$\dim \mathrm{SF}(r, t) = 2\dim\big(\mathbb{F}_2[x, y]/(x^{L^2} + 1, y^L + 1, 1 + x, y + r(x^L))\big)$$

Вес r нечётный, значит $r(x^L) \equiv r(1) = 1 \mod (1 + x)$, поэтому

$$(1+x, y+r(x^L), x^{L^2}+1, y^L+1) = (1+x, 1+y, x^{L^2}+1, y^L+1) = (1+x, 1+y).$$

Отсюда

$$\begin{aligned}\mathbb{F}_2[x, y]/(x^{L^2} + 1, y^L + 1, 1 + x, y + r(x^L)) = \mathbb{F}_2[x, y]/(1 + y)/(1 + x) \simeq \\ \simeq \mathbb{F}_2[x]/(1 + x) \simeq \mathbb{F}_2.\end{aligned}$$

Значит $\dim \mathrm{SF}(r, t) = 2\dim \mathbb{F}_2 = 2$. Лемма доказана. □

4.2. Лемма о выравнивании и её следствия

В этом разделе мы рассматриваем код $Q = \mathcal{Q}\left(\langle x \rangle_{ac} \times H, 1 + x, g\right)$ из леммы о выравнивании. Также используем обозначения: $G = \langle x \rangle_{ac} \times H$, $G' = \langle x^c \rangle \times H$.

Идея доказательства. Элементы $\mathbb{F}_2^G$ можно отождествить с подмножествами элементов группы G. Напомним, что ошибка $[p, q]$ является выровненной, если $(1 + x)p$ и q лежат в G'.

Для слова $[p, q] \in (\mathbb{F}_2^G)^2$ элемент $(1 + x)p$ назовём *левым синдромом*, а элемент gq назовём *правым синдромом*. Если $[p, q]$ — ошибка, то левый синдром должен совпасть с правым, давая в сумме 0, и в этом случае левый (и правый) синдромы назовём *полусиндромами*. Легко видеть, что ошибка является выровненной тогда и только тогда, когда соответствующий полусиндром лежит в $\mathbb{F}_2^{G'}$.

Срезом множества $X \subset G$ назовём множество вида $x^iG' \cap X$. Заметим, что срез правого синдрома, лежащий в x^iG', порождается элементом $q \in x^iG'$.

Основная идея состоит в том, что срез $X = gq_X$ полусиндрома $S = gq$ можно «сдвигать», постепенно прибавляя к кодовому слову вырожденные кодовые слова вида $[gq_X, (1+x)q_X]$ таким образом, что компонента X умножается на x. За i шагов можно «сдвинуть» X на i позиций (при этом X заменится на x^iX). И до тех пор, пока в $S \setminus X$ не пересекается с x^iX, с изменением i кусок границы X левой части кодового слова будет сдвигаться на i позиций, поэтому вес левой части ошибки меняется линейно по i (пусть он равен $w_0 + i\Delta w$), а вес правой части ошибки не меняется. В точке, где x^iX перестаёт пересекаться с $S \setminus X$, вес левой части кодового слова по-прежнему равен $w_0 + i\Delta w$, а вес правой части может быть такой же, как у исходного слова, а может быть меньше.

Таким образом, у нас получается семейство эквивалентных кодовых слов, параметризованных целым числом i, изменяющимся в пределах некоторого отрезка. При этом вес кодового слова в пределах этого отрезка линейно зависит от i, а на краях значение меньше или равно этой линейной функции. Отсюда можно заключить, что всегда можно взять i на одном из концов отрезка так, чтобы вес ошибки не увеличился.

То, что мы взяли i из края отрезка, означает, что у нас два среза полусиндрома «склеились», и число таких компонент уменьшилось на 1. Повторяя эту процедуру можно добиться, чтобы был лишь один непустой срез в полусиндроме. На последнем шаге следует так сдвинуть срез, чтобы он попал в G'. Вес на каждом шаге не увеличивается, и в результате мы получим искомое выровненное кодовое слово с меньшим или равным весом.

Введём обозначение

$$I(a, b) = \sum_{j=\min(a,b)}^{\max(a,b)-1} x^j.$$

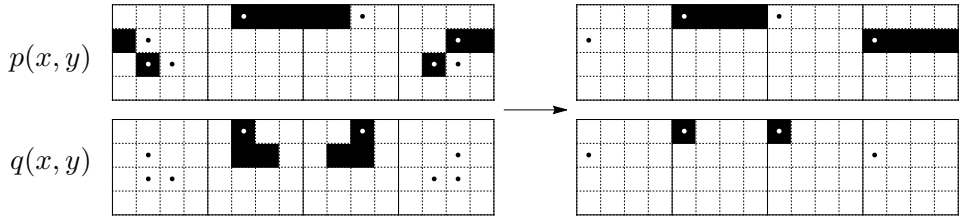


Рис. 3. Выравнивание логической ошибки $[p(x, y), q(x, y)]$ для кода $\mathrm{SF}(1 + x + x^{-1}, 2)$, $L = 4$. Каждая картинка изображает многочлен таким образом: чёрная клетка с координатами (i, j) соответствует слагаемому $x^i y^j$. Точка с координатами (i, j) соответствует слагаемому $x^i y^j$ в полусиндроме.

$I(a, b)$ обладает следующими свойствами:

$$I(l + a, r + a) = x^a I(l, r), \qquad I(l, r) + I(l', r') = I(l, l') + I(r, r'),$$
$$(1 + x)I(l, r) = x^l + x^r, \qquad I(l, l) = 0.$$

Если $0 \leqslant a \leqslant b \leqslant \ell c$, то $|I(a, b)| = b - a$.

Пусть задан набор v длины c, $v[i] \in \mathbb{Z}$. Введём оператор сдвига $S([p, q], v)$ для ошибки $[p, q]$. Пусть $q = \sum_{i=0}^{c-1} q_i x^i$, тогда

$$S([p, q], v) = [p, q] + [g, 1 + x] \sum_{i=0}^{c-1} q_i I(i, v[i]).$$

Лемма 3. *Если $[p, q]$ — ошибка, то $S([p, q], v)$ — эквивалентная ей ошибка.*

Доказательство. Утверждение следует из того, что $[p, q] + S([p, q], v]) = [g, 1 + x]a$ для $a = \sum_{i=0}^{c-1} q_i I(i, v[i]) \in \mathbb{F}_2^G$. □

Для удобства введём доопределённый вектор $v^*[i] := v[a] + cb$, если $i = a + cb$, $0 \leqslant a \leqslant c - 1$. Следующая лемма утверждает, что в представлении p в виде суммы «интервалов» $h_i I(l_i, r_i)$ после применения оператора S концы интервалов сдвигаются под действием отображения v^*.

Лемма 4. *Пусть $[p, q]$ — ошибка и*

$$p = \sum_{i=1}^{N} h_i I(l_i, r_i), \ \textit{где } h_i \in H, \ 0 \leqslant l_i < r_i \leqslant \ell c. \tag{4}$$

Тогда

$$S([p,q],v) = \Big[\sum_{i=1}^{N} h_i I(v^*[l_i], v^*[r_i]), \sum_{i=0}^{c-1} q_i x^{v[i]}\Big].$$

Доказательство. Пусть $[p',q'] = S([p,q],v)$. Тогда

$$q' = q + (1+x)\sum_{i=0}^{c-1} q_i I(i, v[i]) = \sum_{i=0}^{c-1} q_i x^i + \sum_{i=0}^{c-1} q_i (x^i + x^{v[i]}) = \sum_{i=0}^{c-1} q_i x^{v[i]}.$$

Чтобы проверить компоненту p', понадобится несколько обозначений. Представим l_i и r_i в виде

$$l_i = a_{2i-1} + cb_{2i-1}, \qquad r_i = a_{2i} + cb_{2i} \qquad \text{где } 0 \leqslant a_j \leqslant c-1,\ 0 \leqslant b_j \leqslant \ell.$$

Определим множества $M_j = \{i \mid a_i = j\}$. Пусть также $h'_{2i-1} = h'_{2i} = h_i$. Тогда

$$\begin{aligned}(1+x)p &= \sum_{i=1}^{N} h_i (1+x) I(l_i, r_i) = \\ &= \sum_{i=1}^{N} h_i (x^{l_i} + x^{r_i}) = \sum_{i=1}^{2N} h'_i x^{a_i} x^{cb_i} = \sum_{j=0}^{c-1} x^j \sum_{i \in M_j} h'_i x^{cb_i}.\end{aligned}$$

С другой стороны, поскольку $[p,q]$ — кодовое слово, имеем

$$(1+x)p = gq = \sum_{j=0}^{c-1} g q_j x^j.$$

Учитывая, что $gq_j \in \mathbb{F}_2^{G'}$ и $h'_i, x^{cb_i} \in \mathbb{F}_2^{G'}$, то $gq_j = \sum_{i \in M_j} h'_i x^{cb_i}$. Вычислим $\Delta p = p' + p$:

$$\begin{aligned}\Delta p &= \sum_{i=1}^{N} h_i \big(I(l_i, r_i) + I(v^*[l_i], v^*[r_i])\big) = \sum_{i=1}^{N} h_i \big(I(l_i, v^*[l_i]) + I(r_i, v^*[r_i])\big) = \\ &= \sum_{i=1}^{2N} h'_i\, I(a_i + cb_i, v[a_i] + cb_i) = \sum_{i=1}^{2N} h'_i x^{cb_i} I(a_i, v[a_i]) = \\ &= \sum_{j=0}^{c-1} I(j, v[j]) \sum_{i \in M_j^l} h'_i x^{cb_i} = \sum_{j=0}^{c-1} I(j, v[j]) q_j g.\end{aligned}$$

Лемма доказана. □

Покажем, что при условии $0 \leqslant v[i] \leqslant c$ отображение $v \mapsto v^*$ сохраняет монотонность.

Лемма 5. *Пусть*

$$0 = v[0] \leqslant v[1] \leqslant v[2] \leqslant \cdots \leqslant v[c-1] \leqslant c. \tag{5}$$

Тогда v^* монотонно на $\mathbb{Z}$.

Доказательство. Пусть $a < b$. Рассмотрим 2 случая.

1) Если $a < ct \leqslant b$ для некоторого $t \in \mathbb{Z}$, то

$$v^*[a] \leqslant c(t-1) + c = ct \leqslant v^*[b].$$

2) Иначе $ct \leqslant a \leqslant b < c(t+1)$. Тогда

$$v^*[a] = ct + v[a - ct] \leqslant ct + v[b - ct] = v^*[b].$$

Итак, в обоих случаях $v^*[a] \leqslant v^*[b]$. Лемма доказана. □

Доказательство леммы 1 о выравнивании ошибок. Зафиксируем произвольную ошибку $w = [p, q]$. Сначала посмотрим, как действует оператор сдвига на её левую часть p.

Представим p в виде суммы (4) таким образом, чтобы $\operatorname{supp} h_i I(l_i, r_i)$ не пересекались. Тогда $|p| = \sum_{i=1}^{N}(r_i - l_i)$.

Подберём такой вектор v, чтобы минимизировать величину

$$L(v) = \sum_{i=1}^{N}(v^*[r_i] - v^*[l_i])$$

при ограничении (5). Заметим, что v^* линейно по v, а целевая функция линейна по v^*, а значит и по v.

Для начальных значений $v_0[i] = i$ по построению $L(v_0) = |p|$.

Множество, задаваемое неравенствами (5), является $(c-1)$-мерным симплексом с вершинами $(0, \underbrace{0, 0, ..., 0}_{k}, \underbrace{c, ..., c}_{c-k-1})$, $k = 0, ..., c-1$. Поэтому минимум линейной функции $L(x)$ при ограничении (5) достигается в некоторой вершине v этого симплекса, причём $v[i] \in \{0, c\}$, значит $v[i]$ — целое и делится на c.

Положим $[p', q'] = S([p, q], v)$. Поскольку $v^*[l_i], v^*[r_i]$ делятся на c, то $I(v^*[l_i], v^*[r_i])$ делится на $I(0, c)$, а значит и p' делится на $I(0, c)$; также поскольку $v[i]$ делится на c, то $x^{v[i]} \in G'$, значит $q' \in \mathbb{F}_2^{G'}$, поэтому ошибка $[p', q']$ является выровненной, а по лемме 3 она эквивалентна $[p, q]$.

Осталось оценить вес $[p', q']$. Поскольку (5) выполнено, то v^* монотонно по лемме 5, значит $|I(v^*[l_i], v^*[r_i])| = v^*[r_i] - v^*[l_i]$. Отсюда, используя лемму 4, получим

$$|p'| = \Big|\sum_{i=1}^{N} h_i\, I(v^*[l_i], v^*[r_i])\Big| \leqslant \sum_{i=1}^{N} |h_i I(v^*[l_i], v^*[r_i])| =$$
$$= \sum_{i=1}^{N} (v^*[r_i] - v^*[l_i]) = L(v) \leqslant L(v_0) = |p|,$$
$$|q'| = \Big|\sum_{j=0}^{c-1} q_j x^{v[j]}\Big| \leqslant \sum_{j=0}^{c-1} |q_j| = |q|.$$

Отсюда $\big|[p', q']\big| \leqslant \big|[p, q]\big|$. Лемма доказана. □

Лемма 6. *Пусть $G = \langle x\rangle_\ell \times H$, $g \in \mathbb{F}_2^G$. Для того, чтобы размерность квантового кода $\mathcal{Q}(G, 1 + x, g)$ была отлична от 0, достаточно, чтобы вес g был чётным.*

Доказательство. Пусть $g = \sum_{i=1}^{2k} g_i$, $g_i \in G'$. Тогда

$$\Big(\sum_{v\in G} v\Big) g = \sum_{i=1}^{2k} \sum_{v\in G} v g_i = \big\langle v' = v g_i^{-1}\big\rangle = \sum_{i=1}^{2k} \sum_{v'\in G} v' = 2k \sum_{v'\in G} v' = 0.$$

Аналогично, поскольку $1 + x$ – чётного веса, то

$$\Big(\sum_{v\in G} v\Big)(1 + x) = 0.$$

Значит матрицы $H_X = [1 + x, g]$ и $H_Z = [\overline{g}, 1 + x^{-1}]$ вырожденные и $\operatorname{rank}[\overline{g}, 1 + x^{-1}] = \operatorname{rank}[1 + x, g] \leqslant |G| - 1$, значит размерность кода $\geqslant 2|G| - 2(|G| - 1) = 2$. Лемма доказана. □

Доказательство утверждения 3. Из того, что вес g чётный по лемме 6 получаем, что размерность кода $\mathcal{Q}(G, 1 + x, g)$ отлична от 0.

Рассмотрим ошибку минимального веса. По лемме 1 мы можем выбрать ошибку вида $e = \Big[p_0 \sum_{j=0}^{c-1} x^j,\ q_0\Big]$, где $p_0, q_0 \in \mathbb{F}_2^{G'}$. Рассмотрим 2 случая:

1) Если $p_0 = 0$, то $g q_0 = 0$, значит q_0 — кодовое слово классического кода, задаваемого элементом G, а по условию его расстояние d. Значит $|q_0| \geqslant d$.

2) Если $p_0 \neq 0$, тогда $|e| = |p_0| c + |q_0| \geqslant c$.

Лемма доказана. □

На самом деле, в случае $G' = H$, то есть, $\ell = 1$, код $\mathcal{Q}(G, 1+x, g)$ является [6] *гиперграфовым кодом-произведением* (анг. hypergraph product code) классических кодов $\mathcal{C}(\langle x \rangle_c, 1+x)$ и $\mathcal{C}(H, g)$, и оценка, даваемая утверждением 3, совпадает с оценкой из [6].

Пример 5. Положим $G' = H = \langle y \rangle$, $y^c = 1$, $g = 1 + y$. Получим торический код с матрицей $H_X = [1+x, 1+y]$ и кодовым расстоянием c. Легко видеть, что классический код, задаваемый элементом $1 + y$, является $[c, 1, c]$-кодом, где кодируемый бит просто повторяется c раз. Даваемая леммой нижняя оценка кодового расстояния c в данном случае является точной.

Чтобы получить коды, отличные от кодов из [6], нужно брать $\ell \geqslant 2$.

4.3. Виды логических ошибок $\mathrm{SF}(r,t)$ и их вес

Далее будем рассматривать полуфрактальные коды

$$\mathrm{SF}(r,t) = \mathcal{Q}\left(\langle x \rangle_{4^t} \times \langle y \rangle_{2^t}, 1+x, y + r(x^{2^t})\right),$$

в этом случае $H = \langle y \rangle_L$, $G = \langle x \rangle_{L^2} \times H$, $G' = \langle x^L \rangle \times H$, где $L = 2^t$.

Учитывая соотношения $x^{L^2} = y^L = 1$, будем использовать $1/x = x^{-1} = x^{L^2-1}$ и $1/y = y^{-1} = y^{L-1}$.

В лемме 2 мы показали, что размерность кода $\mathrm{SF}(r,t)$ равна 2. Таким образом, существует 4 логических ошибки, включая нулевую. Найдём 3 невырожденные ошибки. Введём следующие ошибки:

$$\Big[\sum_{j=0}^{L^2-1} x^j,\ \mathbf{0}\Big], \tag{$L1$}$$

$$\Big[\mathbf{0},\ \sum_{j=0}^{L-1} \big(r(x^L)/y\big)^j\Big], \tag{$L2$}$$

$$(L1) + (L2) = \Big[\sum_{j=0}^{L^2} x^j,\ \sum_{j=0}^{L-1} \big(r(x^L)/y\big)^j\Big] \tag{$L3$}.$$

Здесь ошибки заданы вектором из многочленов. Подразумевается, что каждому многочлену ставится в соответствие ошибка, в которой на позициях, соответствующих ненулевым коэффициентам многочлена стоит 1, на оставшихся позициях — 0.

Лемма 7. *$(L1)$, $(L2)$ и $(L3)$ являются ошибками для кода* $\mathrm{SF}(r,t)$.

Доказательство. Проверим, что ошибки $H_X L1 = H_X L2 = H_X L3 = 0$. Учитывая, что s и a — степени 2, получим

$$H_X L1 = (1+x)\sum_{i=0}^{L^2-1} x^j = 1 + x^{L^2} = 0.$$

$$H_X L2 = (r(x^L)+y)\sum_{j=0}^{L-1}\left(r(x^L)/y\right)^j =$$

$$= y(r(x^L)/y+1)\sum_{j=0}^{L-1}\left(r(x^L)/y\right)^j = y\left(\left(r(x^L)/y\right)^L + 1\right) = 0.$$

Здесь мы учли, что $y^L = 1$, $x^{L^2} = 1$ и

$$r^L(x^L) = r(x^{L^2}) = r(1) = |r| \mod 2 = 1,$$

поскольку в r — нечётное число ненулевых слагаемых. □

Ошибки, эквивалентные $L1$ будем называть *левыми* или L*-ошибками*, а эквивалентные $L2$ или $L3$ — *правыми* или R*-ошибками*. Ниже, в лемме 11, мы докажем, что их классы эквивалентности различны, но удобнее сначала получить оценки снизу на веса L- и R-ошибок.

Лемма 8. *Вес любой L-ошибки не меньше $L\overline{D}_r(t)$.*

Доказательство. Возьмём L-ошибку минимального веса вида

$$e = [p(x^L, y)(1 + x + ... + x^{L-1}), q(x^L, y)]$$

(по лемме 1 такая существует) и покажем, что $|p| \geqslant \overline{D}_r(t)$.

Поскольку e эквивалентна $L1$, то существует такой $f_0(x, y) \in \mathbb{F}_2[x, y]$, что

$$p(x^L, y)(1+x+...+x^{L-1}) + f_0(x, y)(y + r(x^L)) = \sum_{i=0}^{L-1} x^{iL}(1+x+...+x^{L-1}).$$

Здесь равенство в кольце $\mathbb{F}_2[x, y]/(x^{L^2} - 1, y^L - 1)$. Поскольку $r(x^L)^L = 1$, то мы можем подставить $y = r(x^L)$, тогда получим

$$p(x^L, r(x^L))(1 + x + ... + x^{L-1}) = \sum_{i=0}^{L-1} x^{iL}(1 + x + ... + x^{L-1}).$$

Отсюда, оставляя лишь коэффициенты при степенях x^{iL} и делая замену $z = x^L$, получим

$$p(z, r(z)) = 1 + z + ... + z^{L-1},$$

значит $\overline{D}_r(t) \leqslant |p|$, отсюда $|w| \geqslant L|p| \geqslant L\overline{D}_r(t)$, что и требовалось. □

Лемма 9. *Для любой R-ошибки (p, q) для всех $j = 0, ..., L-1$ вес q_j нечётный.*

Доказательство. Для любой вырожденной ошибки $[p', q']$ вес q'_j чётный, поскольку $q' = (1+x)s(x, y)$ для некоторого $s \in \mathbb{F}_2[x, y]/(y^L - 1, x^{L^2} - 1)$. Из любой R-ошибки прибавлением вырожденной ошибки можно получить либо $[p'', q''] = L2$, либо $[p'', q''] = L1 + L2$. В обоих случаях $q''_j(1) = r(1)^j = 1$, то есть q''_j имеет нечётный вес. А значит и $q_j = q'_j + q''_j$ имеет нечётный вес, что и требовалось. □

Следствие 1. *Для любой R-ошибки $[p, q]$ для всех $j = 1, ..., L-1$ выполнено $q_j \neq 0$.*

Лемма 10. *Вес любой R-ошибки не меньше*

$$\max_{1 \leqslant k \leqslant t} 2^k \min(L, D^*_r(t-k)).$$

Доказательство. Рассмотрим R-ошибку

$$w = [p(x^L, y)(1 + x + ... + x^{L-1}), q(x^L, y)]$$

минимального веса, (R-ошибка такого вида существует по лемме 1).

Зафиксируем произвольное $k \in \overline{1, t}$ и разделим левую и правую части ошибки на 2^k горизонтальных полос высоты 2^u, где $u = t - k$. Соответствующее представление в виде полиномов:

$$p(x) = \sum_{i=0}^{2^k-1} p_i(x, y), \qquad q(x) = \sum_{i=0}^{2^k-1} q_i(x, y),$$

где $p_i(x, y)$ и $q_i(x, y)$ содержат лишь степени y от $i2^u + 1$ до $(i+1)2^u$.

Покажем, что в каждой полосе либо $|q_i| \geqslant D^*_r(u)$, либо $|p_i| \neq 0$. Предположим, что $|p_i| = 0$. Тогда синдром

$$s_i = q_i(x, y)(y + r(x)) + p_i(x, y)(1 + x) = q_i(x, y)(y + r(x))$$

может содержать лишь y в степенях y^{i2^u} и $y^{(i+1)2^u}$, чтобы сократиться с s_{i+1} и s_{i-1}. Пусть

$$q_i(x, y) = y^{(i+1)2^u - 1} \sum_{j=0}^{2^u-1} q_i^j(x)/y^j.$$

Тогда при $0 < j < 2^k$ имеем $q_i^j(x) + r(x)q_i^{j-1} = 0$, отсюда $q_i^{j+1}(x) = q_i^j(x)r(x)$, значит

$$q_i(x, y) = y^{(i+1)2^u - 1} q_i^0(x) \sum_{j=0}^{2^u-1} (r(x)/y)^j,$$

Поскольку мы рассматриваем R-ошибку, то по лемме 9 вес всех q_i^j нечётный, в частности, нечётный вес имеет q_i^0. Тогда

$$|q_i(x,y)| = \left|q_i^0(x)\sum_{j=0}^{2^u-1}\frac{r^j(x)}{y^j}\right| \geqslant \left|q_i^0(x)\sum_{j=0}^{2^u-1}\frac{r^j(x)}{y^j} \bmod (x^{2^u}+1)\right| \geqslant D_r^*(u).$$

Итак, поскольку $|q_i| \geqslant D_r^*(t-k)$, либо $|p_i| \neq 0$, то

$$L|p_i| + |q_i| \geqslant \min(L, D_r^*(t-k)).$$

Суммируя по всем $i = 0, ..., 2^k - 1$, получим $|w| \geqslant 2^k \min(L, D_r^*(t-k))$. Поскольку k мы брали произвольным, то из этой оценки сразу следует утверждение леммы. □

Лемма 11. *Код* $\mathrm{SF}(r,t)$ *имеет размерность* 2, *и ошибки* $(L1)$, $(L2)$, $(L3)$ *являются различными невырожденными логическими ошибками.*

Доказательство. Для всех пар ошибок из $\{0, L1, L2, L3\}$ покажем, что они различны.

1) По лемме 9 у любой R-ошибки $[p,q]$ при каждой степени y в q многочлен от x имеет нечётный вес. А для 0-ошибки и $(L1)$ правая часть нулевая, поэтому $L2, L3 \not\sim 0, L1$.

2) $L1 \not\sim 0$ следует из леммы 8, поскольку минимальный вес L-ошибки больше 0.

3) $L3 + L2 = L1$, значит $L2$ и $L3$ — также различны.

Лемма доказана. □

Из леммы 11 следует, что любая невырожденная ошибка является либо L-ошибкой, либо R-ошибкой. Поэтому объединяя леммы 8 и 10, получим

Следствие 2. *Если многочлен* $r \in \mathbb{F}_2[x]$ *имеет нечётный вес, то*

$$\operatorname{mindist}\mathrm{SF}(r,t) \geqslant \min\bigl(2^t\overline{D}_r(t), \max_{1\leqslant k\leqslant t} 2^k \min(2^t, D_r^*(t-k))\bigr).$$

4.4. Соотношения между D, $\overline{D}$ и D^* и доказательство основной теоремы

Лемма 12. $D_r^*(t)\overline{D}_r(t) \geqslant 4^t$.

Доказательство. По определению $\overline{D}_r(t)$ существует многочлен $p(x,y)$ такой, что $|p| = \overline{D}_r(t)$ и $1 + x + ... + x^{2^t-1} = p(x, r(x))$ в факторкольце $\mathbb{F}_2[x]/(x^{2^t} - 1)$.

Обозначим $c_0(x,y) = \sum_{i=0}^{2^t-1}(r(x)/y)^j$. Далее все действия производятся в факторкольце $\mathbb{F}_2[x,y]/(x^{2^t} - 1, y^{2^t} - 1)$.

Рассмотрим многочлен $q \in \mathbb{F}_2[x]$ нечётного веса такой, что вес многочлена $w(x,y) = q(x)c_0(x,y)$ равен $D_r^*(t)$. Заметим, что если разложить многочлен $p(x,y)c_0(x,y)$ по степеням y, то при y^0 будет множитель $p(x, r(x)) = 1 + x + ... + x^{2^t-1}$. Поскольку $c_0(x,y)r(x)/y = c_0(x,y)$ в этом факторкольце, то при y^{L-j} будет множитель $r^j(x)p(x, r(x)) = 1 + x + ... + x^{2^t-1}$, значит

$$p(x,y)c_0(x,y) = \sum_{i=0}^{2^t-1}(1 + x + ... + x^{2^t-1})r(x)^j/y^j = \sum_{i,j=0}^{2^t-1} x^i/y^j,$$

то есть $|pc_0| = 4^t$. Отсюда

$$p(x,y)w(x,y) = q(x)c_0(x,y)p(x,y) = q(x)\sum_{i,j=0}^{2^t-1} x^i y^j = |q|\sum_{i,j=0}^{2^t-1} x^i y^j =$$

$$= \sum_{i,j=0}^{2^t-1} x^i y^j,$$

поскольку вес q нечётный. Теперь можем оценить вес w:

$$D_r^*(t)\overline{D}_r(t) = |w||p| \geqslant |pw| = 4^t,$$

что и требовалось. □

Лемма 13. $\overline{D}_{1+x+x^2}(t) \leqslant 2^{\lceil t/2 \rceil}$.

Доказательство. Определим последовательность многочленов $h_t(x,y)$ индуктивно:

$$h_0(x,y) = 1, \tag{6}$$

$$h_{t+1}(x,y) = \left(y^{4^t} + x^{3\cdot 4^t}\right) h_t(x,y). \tag{7}$$

Легко видеть, что $|h_{t+1}| \leqslant 2|h_t|$, значит $|h_t| \leqslant 2^t$. Проверим индукцией по t, что $h_t(x, 1 + x + x^2) = \sum_{i=0}^{4^t-1} x^i$.

База индукции: $t = 0$. $h_0(x, 1 + x + x^2) = 1 = \sum_{i=0}^{4^0-1} x^i$.

Шаг индукции $t \to t+1$. Поскольку всё происходит в поле характеристики 2, то $(1+x+x^2)^{4^t} = 1 + x^{4^t} + x^{2\cdot 4^t}$, значит

$$h_{t+1}(x, 1+x+x^2) = \left((1+x+x^2)^{4^t} + x^{3\cdot 4^t}\right) h_t(x, 1+x+x^2) =$$
$$= \left(1 + x^{4^t} + x^{2\cdot 4^t} + x^{3\cdot 4^t}\right) \sum_{i=0}^{4^t-1} x^i = \sum_{i=0}^{4^{t+1}-1} x^i.$$

Отсюда сразу следует, что $\overline{D}_{1+x+x^2}(2t) \leqslant |h_t| \leqslant 2^t$. Поскольку

$$\sum_{i=0}^{2^{2t+1}} x^i = (1+x^{4^t}) \sum_{i=0}^{2^{2t}} x^i = (1+x^{4^t}) h_t(x, 1),$$

то $\overline{D}_{1+x+x^2}(2t+1) \leqslant 2|h_t| \leqslant 2^{t+1}$. Лемма доказана. □

Лемма 14. $D_r(t)\overline{D}_r(t) \geqslant 4^t$.

Доказательство. В определении $D_r^*(t)$ подставим $p(x) = 1$, получим

$$D_r^*(t) \leqslant \left| \sum_{j=0}^{2^t-1} r^j(x)/y^j \bmod (x^{2^t}-1, y^{2^t}-1) \right| \leqslant \sum_{j=0}^{2^t-1} |r^j(x)| = D_r(t).$$

Используя лемму 12 получим $D_r(t)\overline{D}_r(t) \geqslant D_r^*(t)\overline{D}_r(t) \geqslant 4^t$. □

Доказательство теоремы 1. Известно [19, 20], что

$$D_{1+x+x^2}(t) \asymp (1+\sqrt{5})^t, \tag{8}$$

отсюда по лемме 14

$$\overline{D}_{1+x+x^2}(t) \succcurlyeq \left(\frac{4}{1+\sqrt{5}}\right)^t = \left(\sqrt{5}-1\right)^t. \tag{9}$$

По лемме 13 имеем

$$\overline{D}_{1+x+x^2}(t) \leqslant 2^{\lceil t/2 \rceil}, \tag{10}$$

отсюда по лемме 12 получаем

$$D^*_{1+x+x^2}(t) \geqslant 2^{\lfloor 3t/2 \rfloor}. \tag{11}$$

По лемме 8, учитывая (9), вес любой L-ошибки не меньше

$$2^t \overline{D}_{1+x+x^2}(t) \succcurlyeq 2^t(\sqrt{5}-1)^t = 2^{\alpha t}. \tag{12}$$

Учитывая (11) и подставляя $k = \lfloor t/3 \rfloor$ в лемму 10, получим, что вес любой R-ошибки не меньше

$$2^{\lfloor t/3 \rfloor} \min\left(2^t, D_r^*(\lceil 2t/3 \rceil)\right) \geqslant 2^{t/3-1} \min\left(2^t, 2^{\left\lfloor \frac{3}{2} \lceil \frac{2}{3} t \rceil \right\rfloor}\right) = 2^{\frac{4}{3}t-1} \succcurlyeq 2^{\alpha t}. \quad (13)$$

Последнее асимптотическое неравенство следует из числового неравенства $\alpha < 4/3$.

Учитывая (12) и (13), получаем, что вес любой логической ошибки по порядку не меньше $2^{\alpha t}$, что и требовалось. □

5. Заключение

В данной работе введён класс полуфрактальных квантовых кодов, для которых доказана нижняя оценка кодового расстояния. Мы здесь не приводим верхней оценки, но она выше $\sqrt{n}$, и есть основания полагать, что кодовое расстояние полуфрактальных кодов может оказаться выше, чем $\sqrt{n}$.

Для получения нижней оценки использовались простые соотношения между величинами D, $\overline{D}$ и D^*. Потенциально нижняя оценка может быть улучшена, если будут улучшены оценки на величины $\overline{D}(t)$ и $D^*(t)$.

Интерес представляет также рассмотрение других многочленов $r(x)$, отличных от $1 + x + x^2$.

Для рассмотрения более широких классов кодов необходимо обобщить лемму о выравнивании на случай кодов $\mathcal{Q}(G, p, q)$, когда многочлен p отличен от $1 + x$.

Далее перечислим некоторые гипотезы и соображения, как можно улучшить полученную в статье оценку, а также некоторые гипотезы.

Один из простейших способов улучшить оценку — рассмотреть код $\mathrm{SF}'(r, t, L') = \mathcal{Q}\left(\langle x \rangle_{LL'} \times \langle y \rangle_L, 1 + x, y + r(x^{L'})\right)$, $L = 2^t$, на решётке в виде параллелепипеда $L' \times L \times L$ вместо кубической решётки. Все оценки будут очень похожими, а именно, вес L-ошибки $\geqslant L'\overline{D}_r(t)$, а вес R-ошибки $\geqslant \max_k 2^k \min(L', D_r^*(t-k))$. При фиксированной длине кодового слова $L'L^2$ изменяя соотношение между L' и L можно максимизировать нижнюю оценку кодового расстояния.

Другим естественным шагом является улучшение оценок на $D^*(t)$ и $\overline{D}(t)$. Приведём здесь несколько гипотез относительно поведения этих величин.

Гипотеза 1. $D_r^*(t) \asymp D_r(t)$.

Заметим, что для величины D_r есть алгоритм вычисления асимптотики [20, Теорема 5.5], а для $D_r^*(t)$ асимптотика неизвестна даже для

конкретного случая $r(x) = 1 + x + x^2$. Соответствующая задача была явно сформулирована в статье [13], где исследовалось кодовое расстояние классических фрактальных кодов.

Отметим, что проведённые нами компьютерные эксперименты подтверждают правдоподобность данной гипотезы для многих многочленов $r(x)$ и параметра $t \leqslant 5$. Её также ещё можно переформулировать в терминах линейных клеточных автоматов.

Гипотеза 2 (переформулировка гипотезы 1)**.** *Для любого двоичного линейного клеточного автомата с периодическими граничными условиями плотность узора, порождаемого эволюцией одноклеточной начальной конфигурации, минимальна по порядку.*

Следующая гипотеза является в некотором смысле индикатором перспективности рассмотрения полуфрактальных кодов, как кандидатов на преодоление барьера кодового расстояния $\sqrt{n}\operatorname{polylog} n$.

Гипотеза 3. $\overline{D}_{1+x+x^2}(t) = 2^{\lceil t/2 \rceil}$.

Или в более слабой форме:

Гипотеза 4. *Существует многочлен $r \in \mathbb{F}_2[x]$ нечётного веса и $\varepsilon > 0$ такие, что*

$$D_r(t)\overline{D}_r(t) \succcurlyeq 4^{t(1+\varepsilon)} \qquad \textit{при } t \to \infty.$$

Гипотеза 3 основана лишь на верхней оценке и результатах компьютерных экспериментов для $t \leqslant 4$. Эту гипотезу можно пытаться опровергнуть, найдя экспериментально контрпример для $t \geqslant 5$, либо, если не получится, искать подходы к ее доказательству. В случае, если гипотеза верна, будут уже веские основания полагать, что кодовое расстояние кода $\mathrm{SF}(1 + x + x^2, t)$ превосходит n^γ, где $n = 8^t$ — длина кодового слова, $\gamma > 1/2$. Если же гипотеза 4 неверна, то кодовое расстояние полуфрактальных кодов будет не выше $\sqrt{n}\operatorname{polylog} n$.

Задача проверки гипотез 3 и 4 представляется ключевой и самой сложной частью исследования, связанного с кодовым расстоянием полуфрактальных кодов.

Список литературы

[1] P. Shor, “Scheme for reducing decoherence in quantum computer memory”, *Phys. Rev. A*, **52**:4 (1995), R2493–R2496.

[2] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. Thesis, California Institute of Technology, Pasadena, California, 2004 (Submitted May 21, 1997), 114 pp., arXiv: quant-ph/9705052.

[3] A. R. Calderbank, P. Shor, "Good quantum error-correcting codes exist", *Phys. Rev. A*, **54**:2 (1996), 1098–1105.

[4] A. M. Steane, "Error Correcting Codes in Quantum Theory", *Phys. Rev. Lett.*, **77**:5 (1996), 793–797.

[5] М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, Мир, М., 2006, 824 с.

[6] J. Tillich, G. Zémor, "Quantum LDPC Codes With Positive Rate and Minimum Distance Proportional to the Square Root of the Blocklength", *IEEE Transactions on Information Theory*, **60**:2 (Feb 2014), 1193–1202.

[7] M. H. Freedman, D. A. Meyer, F. Luo, "Z_2-systolic freedom and quantum codes", *Mathematics of quantum computation*, Computational Mathematics, ed. R. K. Brylinski, G. Chen, Chapman & Hall/CRC, 2002, 287–320.

[8] Sh. Evra, T. Kaufman, G. Zémor, *Decodable quantum LDPC codes beyond the $\sqrt{n}$ distance barrier using high dimensional expanders*, 2020, arXiv: quant-ph/2004.07935.

[9] T. Kaufman, R. J. Tessler, *Quantum LDPC codes with $\Omega(\sqrt{n}\log^k n)$ distance, for any k*, 2020, arXiv: quant-ph/2008.09495.

[10] S. Bravyi, B. Terhal, "A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes", *New Journal of Physics*, **11**:4 (Apr 2009), 043029.

[11] J. Haah, "Local stabilizer codes in three dimensions without string logical operators", *Phys. Rev. A*, **83**:4 (Apr 2011), 042330.

[12] J. Haah, "Commuting Pauli Hamiltonians as Maps between Free Modules", *Communications in Mathematical Physics*, **324**:2 (Oct 2013), 351–399.

[13] B. Yoshida, "Information storage capacity of discrete spin systems", *Annals of Physics*, **338** (Nov 2013), 134–166.

[14] B. Yoshida, "Exotic topological order in fractal spin liquids", *Phys. Rev. B*, **88**:12 (Sep 2013), 125122.

[15] B. Yoshida, *Classical and quantum fractal code*, `slides` (XVII Conference on Quantum Information Processing (QIP 14), Barcelona, Spain, Feb. 3–7, 2014).

[16] А. Ю. Китаев, "Квантовые вычисления: алгоритмы и исправление ошибок", *УМН*, **52**:6(318) (1997), 53–112; *Russian Math. Surveys*, **52**:6 (1997), 1191–1249.

[17] A. Yu. Kitaev, "Fault-tolerant quantum computation by anyons", *Annals of Physics*, **303**:1 (Jan 2003), 2–30.

[18] S. Amoroso, G. Cooper, "Tessellation structures for reproduction of arbitrary patterns", *Journal of Computer and System Sciences*, **5**:5 (Oct 1971), 455–464.

[19] S. Wolfram, "Statistical mechanics of cellular automata", *Rev. Mod. Phys.*, **55**:3 (Jul 1983), 601–644.

[20] S. J. Willson, "Computing fractal dimensions for additive cellular automata", *Physica D: Nonlinear Phenomena*, **24**:1 (1987), 190–206.

[21] A. A. Kovalev, L. P. Pryadko, "Quantum Kronecker sum-product low-density parity-check codes with finite rate", *Phys. Rev. A*, **88**:1 (Jul 2013), 012311.

On the minimum distance in one class of quantum LDPC codes
Kalachev G.V., Panteleev P.A.

We consider a family of quantum LDPC codes with weight-6 stabilizer generators and two logical qubits, where some logical operators have a fractal structure. These codes can be considered as local quantum codes on the $L \times L \times L$ cubic lattice with periodic boundary conditions. We prove that the minimum distance of codes from this family is bounded below by $\Omega(L^\alpha)$, where $\alpha = \log_2(2(\sqrt{5} - 1)) \approx 1.306$.

Keywords: quantum LDPC code, local quantum code, minimum distance, linear cellular automaton, fractal dimension.