

УДК 621.391 : 519.725

© 2024 г. Ф. Амирзаде, Д. Панарио, М.-Р. Садеги

**КВАНТОВЫЕ КВАЗИЦИКЛИЧЕСКИЕ МПП-КОДЫ С ВЕСОМ
СТОЛБЦОВ НЕ МЕНЕЕ 3 ИМЕЮТ ОБХВАТ НЕ ВЫШЕ 6**

Квантовые квазициклические МПП-коды (ККЦ-МПП-коды) исследуются с точки зрения их циклов. Показано, что все ККЦ-МПП-коды с весом столбцов не менее 3 имеют обхват не выше 6. Известно, что нижняя граница на минимальное расстояние квазициклического МПП-кода с обхватом 6 и весом столбцов 3 равна 4. По ККЦ-МПП-кодам с весом столбцов не менее 3 строятся ККЦ-МПП-коды с весом столбцов 3 и минимальным расстоянием не менее 6.

Ключевые слова: квантовые квазициклические МПП-коды, обхват, граф Таннера.

DOI: 10.31857/S0555292324020013, EDN: LWLTFH

§ 1. Введение

Квантовые компьютеры в перспективе смогут решать некоторые задачи, например, задачу факторизации (разложения на множители) целых чисел, гораздо быстрее, чем классические компьютеры. В 1982 году в работе Вуттерса и Зурека [1] была сформулирована теорема о невозможности определенных квантовых вычислений, известная как *теорема о запрете клонирования*. Согласно этой теореме невозможно создать независимую тождественную копию произвольного неизвестного квантового состояния.

В 1995 году Шор предложил код, в котором один кубит отображается в девять кубитов, с условием, что исходный кубит можно восстановить после декогеренции (т.е. нарушения когерентности) [2]. При использовании этого квантового кода, имеющего скорость $1/9$, можно декодировать только один кубит.

Одними из наиболее распространенных квантовых кодов, исправляющих ошибки, являются *стабилизаторные коды*. Эти коды позволяют хранить и передавать k битов квантовой информации, используя $n > k$ квантовых битов, таким образом, что переданную квантовую информацию можно восстановить, если некоторое подмножество из n квантовых битов содержит ошибки, представляющие собой битовые ошибки, фазовые ошибки и любые их линейные комбинации с тождественным оператором. В 1996 году Калдербэнк и Шор показали, что методы исправления ошибок работают эффективно, если декогеренция различных кубитов возникает независимо [3].

Калдербэнк, Шор и Стин показали как на основе классических линейных кодов можно построить некоторый класс квантовых кодов, называемых *CSS-кодами*. Эти коды являются частным случаем стабилизаторных кодов (см. [4]) и строятся по паре классических линейных кодов. Для восстановления кубита, подвергшегося воздействию окружающей среды, используется проверочное измерение, известное в квантовой теории информации как *стабилизаторный формализм*.

Для двух линейных кодов C и C' код C' называется двойственным кодом для C , т.е. $C' = C^\perp$, если любое кодовое слово кода C' является линейной комбинацией строк проверочной матрицы кода C . Иными словами, если код C' является двойственным кодом для C , а через c мы обозначаем кодовые слова кода C , то код C' определяется следующим образом:

$$C' = \{d \in \mathbb{F}_2^n : d \times c^T = 0, \forall c \in C\},$$

где через c^T обозначен транспонированный вектор c .

CSS-код с параметрами $[[n, k_1 - k_2]]$ строится по двум классическим линейным кодам $[[n, k_1]]$ -коду C_1 и $[[n, k_2]]$ -коду C_2 , таким что $C_2 \subset C_1$ и при этом как минимальное расстояние $d_{\min}(C_1)$ кода C_1 , так и дуальное расстояние $d_{\min}(C_2^\perp)$ кода C_2 равно d . Такой $[[n, k_1 - k_2]]$ -CSS-код исправляет $t = \frac{d-1}{2}$ битовых ошибок и $t = \frac{d-1}{2}$ фазовых ошибок.

Два линейных кода C_1 и C_2 удовлетворяют *условию скрученности* (twisted condition), если $C_1^\perp \subset C_2$ и $C_2^\perp \subset C_1$. Пара линейных кодов C_1 и C_2 , удовлетворяющих условию скрученности, порождает CSS-код [5]. При этом, если H_1 и H_2 – проверочные матрицы кода C_1 и кода, двойственного к C_2 , соответственно, то пара (H_1, H_2) является парой проверочных матриц для квантового кода тогда и только тогда, когда $H_{C_1} \times H_{C_2}^T = 0$. Если для $[[n, k_1 - k_2]]$ -CSS-кода выполнено условие $C_2 = C_1^\perp$, то такой квантовый код называется *содержащим двойственный* (dual-containing).

Коды с малой плотностью проверок (МПП-коды), введенные Галлагером в 1960-х годах [6], – это линейные коды (т.е. векторные пространства над конечными полями) с разреженными проверочными матрицами. МПП-код называется (m, n) -регулярным, если в каждом столбце и каждой строке проверочной матрицы содержится ровно m и n единиц соответственно. Число m называется весом столбцов, а n – весом строк. С каждым МПП-кодом связан двудольный *граф Таннера*, матрица смежности которого является проверочной матрицей кода. Длина кратчайшего цикла в графе Таннера называется обхватом кода.

Известно, что МПП-коды позволяют достигать пропускной способности канала при низкой сложности декодирования. Существуют различные конструкции МПП-кодов, такие как квазициклические МПП-коды (КЦ-МПП-коды), МПП-коды на основе алгебраических конструкций, а также МПП-коды, основанные на комбинаторных схемах. Высокая эффективность МПП-кодов является мотивацией для рассмотрения квантовых CSS-кодов, построенных по двум МПП-кодам C_1 и C_2 ; такие квантовые коды называются QLDPC-кодами [7]. Если H_1 и H_2 – проверочные матрицы кода C_1 и кода, двойственного к коду C_2 , соответственно, то проверочная матрица QLDPC-кода имеет вид

$$H = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}.$$

Согласно [8] в графе Таннера QLDPC-кода, содержащего двойственный, неизбежно присутствуют циклы длины 4, которые ухудшают эффективность этих кодов при использовании итерационных алгоритмов декодирования. Таким образом, все предлагаемые в литературе QLDPC-коды не являются кодами, содержащими двойственные, т.е. их графы Таннера не содержат циклов длины 4. Так, в работах [4, 5, 8], соответственно, для построения QLDPC-кодов с обхватом 6 использовались квадратично-вычетные множества, КЦ-МПП-коды и комбинаторные схемы.

КЦ-МПП-коды являются одними из самых популярных схем кодирования в каналах благодаря своей высокой эффективности при итеративном декодировании. Всякий (m, n) -регулярный КЦ-МПП-код описывается своей характеристической матрицей (exponent matrix) размера $m \times n$.

В настоящей статье рассматриваются QLDPC-коды, построенные по КЦ-МПП-кодам; такие коды мы будем называть *ККЦ-МПП-кодами*. Сначала доказывается, что граф Таннера этих кодов имеет обхват не выше 6, если вес столбцов их проверочной матрицы не меньше 3. Таким образом, все ККЦ-МПП-коды, предложенные в [5], имеют обхват 6. Так как минимальное расстояние кода с весом столбцов 3 не меньше 4 [9], то любая $(3 \times n)$ -подматрица характеристической матрицы из [5] имеет $d_{\min} \geq 4$. Мы укажем те подматрицы, минимальное расстояние которых не меньше 6.

Статья имеет следующую структуру. В § 2 приводятся основные обозначения и определения. Далее, § 3 посвящен анализу обхвата ККЦ-МПП-кодов с весом столбцов не менее 3. В § 4 получены ККЦ-МПП-коды с весом столбцов 3, обхватом 6 и $d_{\min} \geq 3$. В заключительном § 5 подводятся итоги.

§ 2. Предварительные сведения

Пусть $B = [b_{ij}]$ – характеристическая матрица размера $m \times n$ квазициклического МПП-кода (КЦ-МПП-кода) с размером циркулянта $N \times N$, где $b_{ij} \in \{0, 1, \dots, N-1\}$ или $b_{ij} = (\infty)$. Если целые числа в характеристической матрице заменить на циркулянтные перестановочные матрицы размера $N \times N$, первая строка которых содержит единицу в b_{ij} -м столбце и нули в остальных столбцах, а элемент (∞) заменить на нулевую матрицу размера $N \times N$, то в результате получается проверочная матрица КЦ-МПП-кода. Нулевое пространство этой проверочной матрицы и образует КЦ-МПП-код [10]. Число единиц в столбце проверочной матрицы называется *весом столбца*, а число единиц в ее строке – *весом строки*. Если проверочная матрица имеет постоянный вес столбцов m и постоянный вес строк n , то она соответствует (m, n) -регулярному КЦ-МПП-коду. Если все элементы характеристической матрицы – целые числа, то полученная проверочная матрица дает *полносвязный КЦ-МПП-код*. Ясно, что характеристическая матрица размера $m \times n$ с целочисленными элементами соответствует полносвязному (m, n) -регулярному КЦ-МПП-коду.

Для проверки наличия циклов длины $2k$ в графе Таннера КЦ-МПП-кода используется характеристическая матрица B и следующая лемма Фоссорье [10]: если

$$\sum_{i=0}^{k-1} (b_{m_i n_i} - b_{m_i n_{i+1}}) \equiv 0 \pmod{N}, \quad (1)$$

где $n_k = n_0$, $m_i \neq m_{i+1}$, $n_i \neq n_{i+1}$, а $b_{m_i n_i} - (m_i, n_i)$ -й элемент матрицы B , то в графе Таннера проверочной матрицы имеются циклы длины $2k$. Наименьшая длина цикла в графе Таннера равна *обхвату* графа Таннера, который обозначается через g .

При проверке циклов длины $2k$ следует учитывать, что уравнение (1) содержит k слагаемых, причем пара последовательных слагаемых, таких как $(b_{m_i n_i} - b_{m_i n_{i+1}})$ и $(b_{m_{i+1} n_{i+1}} - b_{m_{i+1} n_{i+2}})$, имеет различные номера строк m_i и m_{i+1} . Более того, номера строк первого и последнего слагаемых также различны, т.е. $m_0 \neq m_{k-1}$. Например, при проверке циклов длины 6, если в первом слагаемом номер строки равен m_0 , во втором m_1 , а в третьем m_2 , то поскольку m_0 и m_1 – номера строк двух последовательных слагаемых, имеем $m_0 \neq m_1$, а так как m_1 и m_2 – тоже номера строк двух последовательных слагаемых то и $m_1 \neq m_2$. Более того, поскольку m_0 и m_2 – номера строк первого и последнего слагаемых, то $m_0 \neq m_2$. Таким образом, при проверке циклов длины 6 в условии (1) участвуют три *различные* строки. Ситуация с номерами столбцов схожая. А именно, в каждом слагаемом $(b_{m_i n_i} - b_{m_i n_{i+1}})$ участвуют два разных номера столбцов n_i и n_{i+1} , а в паре последовательных слагаемых $(b_{m_i n_i} - b_{m_i n_{i+1}})$ и $(b_{m_{i+1} n_{i+1}} - b_{m_{i+1} n_{i+2}})$ номер столбца второго элемента $b_{m_i n_{i+1}}$ в слагаемом $(b_{m_i n_i} - b_{m_i n_{i+1}})$ равен номеру столбца первого элемента $b_{m_{i+1} n_{i+1}}$ в другом слагаемом. Кроме того, номера столбцов первого

и последнего элементов в уравнении (1) одинаковы, т.е. $n_0 = n_k$. Отсюда получаем, что при проверке циклов длины 6 в условии (1) участвуют три разных номера столбцов. Следовательно, для проверки циклов длины 6 в графе Таннера необходимо рассмотреть каждую (3×3) -подматрицу характеристической матрицы. Для облегчения понимания дальнейшего изложения рассмотрим поподробнее процедуру обнаружения коротких циклов в графе Таннера КЦ-МПП-кода:

а) Для проверки циклов длины 4 с помощью условия (1) в (2×2) -подматрице характеристической матрицы $B = [b_{ij}]_{m \times n}$ вычисляются величины

$$(b_{i_1 j_1} - b_{i_1 j_2}) + (b_{i_2 j_2} - b_{i_2 j_1}) \equiv 0 \pmod{N}, \quad i_1 \neq i_2, \quad j_1 \neq j_2.$$

Чтобы рассмотреть все циклы длины 4 в графе Таннера, требуется проверить условие (1) для каждой (2×2) -подматрицы характеристической матрицы.

б) Для каждой (3×3) -подматрицы характеристической матрицы $B = [b_{ij}]_{m \times n}$ для проверки циклов длины 6 из условия (1) получаем шесть уравнений, одним из которых, например, является

$$(b_{i_1 j_1} - b_{i_1 j_2}) + (b_{i_2 j_2} - b_{i_2 j_3}) + (b_{i_3 j_3} - b_{i_3 j_1}) \equiv 0 \pmod{N}, \quad i_1 \neq i_2 \neq i_3, \quad j_1 \neq j_2 \neq j_3.$$

Поскольку номера строк и столбцов попарно не совпадают, для проверки циклов длины 6 в графе Таннера условие (1) необходимо проверить для каждой (3×3) -подматрицы характеристической матрицы. Теперь для каждой (3×3) -подматрицы B мы укажем шесть случаев, которые требуется рассмотреть при проверке циклов длины 6. В каждом случае элементы подматрицы, не входящие в уравнение, обозначены символом “*”:

$$\begin{aligned} & \begin{bmatrix} b_{i_1 j_1} & b_{i_1 j_2} & * \\ * & b_{i_2 j_2} & b_{i_2 j_3} \\ b_{i_3 j_1} & * & b_{i_3 j_3} \end{bmatrix}, \quad \begin{bmatrix} b_{i_1 j_1} & * & b_{i_1 j_2} \\ * & b_{i_2 j_2} & b_{i_2 j_3} \\ b_{i_3 j_1} & b_{i_3 j_2} & * \end{bmatrix}, \quad \begin{bmatrix} * & b_{i_1 j_2} & b_{i_1 j_3} \\ b_{i_2 j_1} & * & b_{i_2 j_3} \\ b_{i_3 j_1} & b_{i_3 j_2} & * \end{bmatrix}, \\ & \begin{bmatrix} * & b_{i_1 j_2} & b_{i_1 j_3} \\ b_{i_2 j_1} & b_{i_2 j_2} & * \\ b_{i_3 j_1} & * & b_{i_3 j_3} \end{bmatrix}, \quad \begin{bmatrix} b_{i_1 j_1} & * & b_{i_1 j_3} \\ b_{i_2 j_1} & b_{i_2 j_2} & * \\ * & b_{i_3 j_2} & b_{i_3 j_3} \end{bmatrix}, \quad \begin{bmatrix} b_{i_1 j_1} & b_{i_1 j_2} & * \\ b_{i_2 j_1} & * & b_{i_2 j_3} \\ * & b_{i_3 j_2} & b_{i_3 j_3} \end{bmatrix}. \end{aligned} \quad (2)$$

Из вышесказанного следует, что существование цикла длины 6 в графе Таннера означает, что характеристическая матрица обязательно имеет не менее трех строк и трех столбцов, т.е. $m \geq 3$ и $n \geq 3$. В противном случае в графе Таннера заведомо нет циклов длины 6.

Следующая теорема дает необходимое и достаточное условие того, что из пары КЦ-МПП-кодов получается квантовый код.

Теорема 1 [5]. Пусть $C = [c_{ij}]$ и $D = [d_{ij}]$ – характеристические матрицы размера $m \times n$ некоторых КЦ-МПП-кодов. Пара (C, D) является парой характеристических матриц ККЦ-МПП-кода тогда и только тогда, когда для строк с номерами $i, i' \in \{1, \dots, m\}$ каждый элемент множества

$$R_{i, i'} = \{(c_{ij} - d_{i'j}) \bmod N, 1 \leq j \leq n\}$$

встречается четное число раз.

§ 3. ККЦ-МПП-коды с весом столбцов $m \geq 3$

В этом параграфе мы докажем, что графы Таннера двух характеристических матриц ККЦ-МПП-кода с весом столбцов не менее 3 имеют обхват не выше 6. Затем мы рассмотрим графические структуры графов Таннера ККЦ-МПП-кодов, предложенные в [5]. Для проверки циклов длины 4 с помощью условия (1) в (2×2) -под-

матрице характеристической матрицы $B = [b_{ij}]_{m \times n}$ вычисляются величины

$$(b_{i_1 j_1} - b_{i_1 j_2}) + (b_{i_2 j_2} - b_{i_2 j_1}) \equiv 0 \pmod{N}, \quad i_1 \neq i_2, \quad j_1 \neq j_2.$$

Чтобы рассмотреть все циклы длины 4 в графе Таннера, условие (1) необходимо проверить для каждой (2×2) -подматрицы характеристической матрицы. Следующая лемма дает необходимое и достаточное условие существования в графе Таннера ККЦ-МПП-кода циклов длины 4, наличия которых следует избегать.

Лемма 1 [11]. Пусть $C = [c_{ij}]$ и $D = [d_{ij}]$ – характеристические матрицы размера $m \times n$ двух КЦ-МПП-кодов C_1 и C_2 , причем граф Таннера кода C_1 имеет обхват не менее 6. Коды C_1 и C_2 порождают ККЦ-МПП-код с обхватом не менее 6 тогда и только тогда, когда для любых двух равных элементов $c_{ij} - d_{i'j}$ и $c_{ij'} - d_{i'j'}$ множество $R_{i,i'}$ для двух номеров строк $i \neq i' \in \{1, 2, \dots, m\}$, где $j \neq j' \in \{1, 2, \dots, n\}$, и множества $R_{i,i''}$ и $R_{i'',i'}$ удовлетворяют следующим условиям:

- а) $c_{ij} - d_{i''j} \not\equiv c_{ij'} - d_{i''j'} \pmod{N}$;
- б) $c_{i''j} - d_{i'j} \not\equiv c_{i''j'} - d_{i'j'} \pmod{N}$.

Следующие теоремы задают ограничения на построение ККЦ-МПП-кодов с конкретным обхватом.

Теорема 2 [11]. Любой ККЦ-МПП-код с характеристической матрицей размера 3×4 имеет обхват 4.

Теорема 3. ККЦ-МПП-коды с весом столбцов не менее 3 имеют обхват не выше 6.

Доказательство. Пусть $C = [c_{ij}]$ и $D = [d_{ij}]$ – характеристические матрицы ККЦ-МПП-кода. Согласно теореме 1 каждый элемент множества $R_{i,i'}$ встречается четное число раз. Таким образом, без ограничения общности будем считать, что в множестве

$$R_{1,1} = \{(c_{1j} - d_{1j}), 1 \leq j \leq n\}$$

выполнено $c_{11} - d_{11} = c_{12} - d_{12}$. Тогда по лемме 1 существует целое число $j \neq 2$, для которого $c_{11} - d_{21} = c_{1j} - d_{2j}$ в множестве $R_{1,2}$. Аналогично, в множестве $R_{1,3}$ имеем $j' \neq j$ и $j' \neq 2$, откуда $c_{11} - d_{31} = c_{1j'} - d_{3j'}$. Продолжая этот процесс, можно показать, что существуют номера столбцов k, k' , такие что $c_{12} - d_{22} = c_{1k} - d_{2k}$ и $c_{12} - d_{32} = c_{1k'} - d_{3k'}$. Таким образом, для элементов $d_{11}, d_{21}, d_{31}, d_{22}$ и d_{32} получаем следующие выражения:

$$\begin{aligned} d_{11} &= c_{11} - c_{12} + d_{12}, & d_{21} &= c_{11} - c_{1j} + d_{2j}, & d_{31} &= c_{11} - c_{1j'} + d_{3j'}, \\ d_{22} &= c_{12} - c_{1k} + d_{2k}, & d_{32} &= c_{12} - c_{1k'} + d_{3k'}. \end{aligned}$$

Подставим их в первые три строки характеристической матрицы D , которые обозначим через D' :

$$D' = \begin{bmatrix} c_{11} - c_{12} + d_{12} & d_{12} & \dots & d_{1j} & \dots & d_{1j'} & \dots \\ c_{11} - c_{1j} + d_{2j} & c_{12} - c_{1k} + d_{2k} & \dots & d_{12j} & \dots & d_{2j'} & \dots \\ c_{11} - c_{1j'} + d_{3j'} & c_{12} - c_{1k'} + d_{3k'} & \dots & d_{3j} & \dots & d_{3j'} & \dots \end{bmatrix}.$$

Теперь, проверяя условие (1) для циклов длины 6, для выделенных элементов приведенной выше матрицы D получаем следующее уравнение:

$$\begin{aligned} (D_{11} - D_{12}) + (D_{22} - D_{2j'}) + (D_{3j'} - D_{31}) &= \\ = (c_{11} - c_{12} + d_{12} - d_{12}) + (c_{12} - c_{1k} + d_{2k} - d_{2j'}) + (d_{3j'} - c_{11} + c_{1j'} - d_{3j'}) &= \\ = (c_{11} - c_{12}) + (c_{12} - c_{1k} + d_{2k} - d_{2j'}) + (c_{1j'} - c_{11}) &= \\ = -c_{1k} + d_{2k} - d_{2j'} + c_{1j'}. \end{aligned}$$

Если для любых j' и k правая часть этого уравнения не равна нулю, т.е.

$$(-c_{1k} + d_{2k}) + (c_{1j'} - d_{2j'}) \not\equiv 0 \pmod{N},$$

то $c_{1j'} - d_{2j'} \neq c_{1k} - d_{2k}$, откуда следует, что в множестве $R_{1,2}$ существует элемент типа $c_{1j'} - d_{2j'}$, который встречается один раз, а это противоречит условию четности кратности в множестве $R_{i,i'}$ из теоремы 1. Таким образом, найдется столбец с номером j' , для которого

$$(-c_{1k} + d_{2k}) + (c_{1j'} - d_{2j'}) \equiv 0 \pmod{N},$$

что и доказывает существование циклов длины 6. $\blacktriangle$

Теперь рассмотрим циклы длины 6 для ККЦ-МПП-кодов, приведенных в [5] и имеющих характеристические матрицы вида $C = [P|Q]$ и $D = [-Q^T|-P^T]$. Существование цикла длины $2k$ в графе Таннера, соответствующем характеристической матрице C , равносильно существованию цикла длины $2k$ в графе Таннера, соответствующем характеристической матрице D . Действительно, любое уравнение для цикла длины $2k$ из условия (1) для характеристической матрицы D можно получить, переписав уравнение для цикла длины $2k$ из (1) для характеристической матрицы C . Например, пусть $\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$ – подматрица матрицы C из ее первой части P , приводящая к циклу длины 4 в графе Таннера. Тогда соответствующее уравнение цикла длины 4 имеет вид

$$(c_{11} - c_{12}) + (c_{22} - c_{21}) \equiv 0 \pmod{N}.$$

Но согласно определению матрицы D ее вторая часть $-P^T$ содержит подматрицу $\begin{bmatrix} -c_{11} & -c_{21} \\ -c_{12} & -c_{22} \end{bmatrix}$. Применяя условие (1) к этой подматрице D , получаем выражение $(-c_{11} + c_{21}) + (-c_{22} + c_{12})$, преобразуя которое, видим, что

$$-[(c_{11} - c_{12}) + (c_{22} - c_{21})] \equiv 0 \pmod{N}.$$

Таким образом, граф Таннера ККЦ-МПП-кода с характеристической матрицей D содержит цикл длины $2k$ тогда и только тогда, когда граф Таннера ККЦ-МПП-кода с характеристической матрицей C содержит цикл длины $2k$. Согласно условию (1) и результатам работы [12] уравнения для циклов длины 6 для характеристической матрицы B имеют следующий вид, где $0 \leq e_i \leq N - 1$:

1. $(b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1}) = e_1$;
2. $(b_{i_1j_1} - b_{i_1j_3}) + (b_{i_2j_3} - b_{i_2j_2}) + (b_{i_3j_2} - b_{i_3j_1}) = e_2$;
3. $(b_{i_1j_2} - b_{i_1j_3}) + (b_{i_2j_3} - b_{i_2j_1}) + (b_{i_3j_1} - b_{i_3j_2}) = e_3$;
4. $(b_{i_1j_3} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_1}) + (b_{i_3j_1} - b_{i_3j_3}) = e_4$;
5. $(b_{i_1j_3} - b_{i_1j_1}) + (b_{i_2j_1} - b_{i_2j_2}) + (b_{i_3j_2} - b_{i_3j_3}) = e_5$;
6. $(b_{i_1j_2} - b_{i_1j_1}) + (b_{i_2j_1} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_2}) = e_6$.

Каждое из этих шести уравнений соответствует одной из шести (3×3) -матриц, перечисленных в (2). Для записи циклов длины 6, связанных с характеристической матрицей с номерами столбцов j_1, j_2, j_3 , будем использовать следующее обозначение: $[[j_1, j_2, j_3], [e_1, e_2, \dots, e_6]]$.

Пример 1. Пусть $C = [c_{ij}]$ и $D = [d_{ij}]$ – характеристические матрицы ККЦ-МПП-кода, приведенного в [5], с $N = 7$:

$$C = \begin{bmatrix} 1 & 2 & 4 & 3 & 6 & 5 \\ 4 & 1 & 2 & 5 & 3 & 6 \\ 2 & 4 & 1 & 6 & 5 & 3 \end{bmatrix}, \quad D = \begin{bmatrix} 4 & 2 & 1 & 6 & 3 & 5 \\ 1 & 4 & 2 & 5 & 6 & 3 \\ 2 & 1 & 4 & 3 & 5 & 6 \end{bmatrix}.$$

Соответствующие циклы длины 6 для матрицы C такие:

$$\begin{aligned} &[[0, 1, 2], [4, 0, 1, 2, 0, 0]], \quad [[0, 1, 4], [0, 6, 0, 0, 3, 5]], \quad [[0, 2, 3], [5, 0, 3, 6, 0, 0]], \\ &[[0, 4, 5], [0, 2, 0, 0, 1, 4]], \quad [[1, 2, 5], [0, 5, 0, 0, 6, 3]], \quad [[1, 3, 5], [4, 0, 1, 2, 0, 0]], \\ &[[2, 3, 4], [0, 1, 0, 0, 4, 2]], \quad [[3, 4, 5], [5, 0, 3, 6, 0, 0]]. \end{aligned}$$

Любой нулевой элемент в векторе $[e_1, e_2, \dots, e_6]$ означает существование семи циклов длины 6 в графе Таннера, так как для этого графа $N = 7$. Таким образом, количество циклов длины 6 в графе Таннера, соответствующем матрице C , равно $24 \times 7 = 168$.

§ 4. $(3, n)$ -регулярные ККЦ-МПП-коды с $d_{\min} \geq 6$

Теперь рассмотрим некоторые графические структуры в графах Таннера, играющие ключевую роль в определении минимального расстояния МПП-кода. Эти графические структуры известны как *тупиковые множества* (trapping sets). *Тупиковым (a, b) -множеством* называется подграф графа Таннера, состоящий из a символьных вершин и соседних с ними проверочных вершин, b из которых имеют нечетную степень, а число проверочных вершин четной степени произвольно.

Известно, что код C имеет минимальное расстояние $d_{\min}$ тогда и только тогда, когда граф Таннера не содержит тупиковых $(a, 0)$ -множеств при $a < d_{\min}$ и при этом существует хотя бы одно тупиковое $(d_{\min}, 0)$ -множество. Для регулярного МПП-кода с обхватом не менее 6 и весом столбцов $m = 3, 4, 5, 6$ наименьший размер тупикового $(a, 0)$ -множества равен $a = 4, 5, 6, 7$ соответственно [13]. Таким образом, согласно сказанному выше, для (m, n) -регулярного МПП-кода с $m = 3, 4, 5$ и 6 имеем $d_{\min} \geq 4$, $d_{\min} \geq 5$, $d_{\min} \geq 6$ и $d_{\min} \geq 7$ соответственно. В общем случае нижней границей на минимальное расстояние (m, n) -регулярного МПП-кода с обхватом не менее 6 является $m + 1$ (см. [9]).

Согласно теореме 3 обхват всех (m, n) -регулярных ККЦ-МПП-кодов с $m \geq 3$ равен 6. Отсюда следует, что нижняя граница на минимальное расстояние этих кодов равна $m + 1$. Таким образом, для ККЦ-МПП-кода с $m = 3$ имеем $d_{\min} \geq 4$. Например, наличие тупиковых $(4, 0)$ -множеств в графах Таннера ККЦ-МПП-кода из примера 1 свидетельствует о том, что минимальное расстояние этого кода равно 4. Далее мы укажем подматрицы характеристических матриц из работы [5], приводящие к $(3, n)$ -регулярным ККЦ-МПП-кодам с $d_{\min} \geq 6$.

Пример 2. Пусть следующие матрицы $C = [c_{ij}]$ и $D = [d_{ij}]$ представляют собой характеристические матрицы ККЦ-МПП-кода из работы [5] с $N = 101$:

$$C = \begin{bmatrix} 1 & 95 & 36 & 87 & 84 & 2 & 89 & 72 & 73 & 67 \\ 84 & 1 & 95 & 36 & 87 & 67 & 2 & 89 & 72 & 73 \\ 87 & 84 & 1 & 95 & 36 & 73 & 67 & 2 & 89 & 72 \\ 36 & 87 & 84 & 1 & 95 & 72 & 73 & 67 & 2 & 89 \\ 95 & 36 & 87 & 84 & 1 & 89 & 72 & 73 & 67 & 2 \end{bmatrix},$$

$$D = \begin{bmatrix} 99 & 34 & 28 & 29 & 12 & 100 & 17 & 14 & 65 & 6 \\ 12 & 99 & 34 & 28 & 29 & 6 & 100 & 17 & 14 & 65 \\ 29 & 12 & 99 & 34 & 28 & 65 & 6 & 100 & 17 & 14 \\ 28 & 29 & 12 & 99 & 34 & 14 & 65 & 6 & 100 & 17 \\ 34 & 28 & 29 & 12 & 99 & 17 & 14 & 65 & 6 & 100 \end{bmatrix}.$$

Поскольку вес столбцов равен 5, минимальное расстояние не меньше 6. Каждая из этих характеристических матриц содержит 150 подматриц размера 3×3 с векторами $[e_1, e_2, \dots, e_6]$, содержащими только один нулевой элемент. Таким образом, количе-

ство циклов длины 6 в каждом графе Таннера равно $150 \times 101 = 15150$. Более того, матрицы C и D не имеют подматриц размера 3×10 , не содержащих циклов длины 6. Используя метод, предложенный в [14, теоремы 4, 6, 7], можно доказать, что любая (3×10) -подматрица матриц C и D с номерами строк

$$(i_1, i_2, i_3) \in \{(1, 2, 3), (1, 2, 5), (1, 4, 5), (2, 3, 4), (3, 4, 5)\}$$

приводит к $(3, 10)$ -регулярному ККЦ-МПП-коду, граф Таннера которого не содержит тупиковых $(4, 0)$ -множеств, а значит, его минимальное расстояние не меньше 6. Если же выбрать три строки, отличные от указанных, то минимальное расстояние будет равно 4.

§ 5. Заключение

В статье исследованы графы Таннера ККЦ-МПП-кодов с точки зрения их коротких циклов и обхвата. Доказано, что любой (m, n) -регулярный ККЦ-МПП-код с $m \geq 3$ имеет обхват не менее 6 и минимальное расстояние $d_{\min} \geq m + 1$.

СПИСОК ЛИТЕРАТУРЫ

1. Wooters W.K., Zurek W.H. A Single Quantum Cannot be Cloned // Nature. 1982. V. 299. № 5886. P. 802–803. <https://doi.org/10.1038/299802a0>
2. Shor P.W. Scheme for Reducing Decoherence in Quantum Computer Memory // Phys. Rev. A. 1995. V. 52. № 4. P. R2493–R2496. <https://doi.org/10.1103/PhysRevA.52.R2493>
3. Calderbank A.R., Shor P.W. Good Quantum Error-Correcting Codes Exist // Phys. Rev. 1996. V. 54. № 2. P. 1098–1105. <https://doi.org/10.1103/PhysRevA.54.1098>
4. Xie X., Yang J., Sun Q.T. Design of Quantum LDPC Codes From Quadratic Residue Sets // IEEE Trans. Commun. 2018. V. 66. № 9. P. 3721–3735. <https://doi.org/10.1109/TCOMM.2018.2827945>
5. Hagiwara M., Imai H. Quantum Quasi-cyclic LDPC Codes // Proc. 2007 IEEE Int. Symp. on Information Theory (ISIT'2007). Nice, France. June 24–29, 2007. P. 806–810. <https://doi.org/10.1109/ISIT.2007.4557323>
6. Галлагер Р.Дж. Коды с малой плотностью проверок на четность. М.: Мир, 1966.
7. Postol M.S. A Proposed Quantum Low-Density Parity-Check Code. <https://arxiv.org/abs/quant-ph/0108131>, 2001.
8. Babar Z., Botsinis P., Alanis D., Ng S.X., Hanzo L. Construction of Quantum LDPC Codes From Classical Row-Circulant QC-LDPCs // IEEE Commun. Lett. 2016. V. 20. № 1. P. 9–12. <https://doi.org/10.1109/LCOMM.2015.2494020>
9. Huang Q., Diao Q., Lin S., Abdel-Ghaffar K. Trapping Sets of Structured LDPC Codes // Proc. 2011 IEEE Int. Symp. on Information Theory (ISIT'2011). St. Petersburg, Russia. July 31–Aug. 5, 2011. P. 1086–1090. <https://doi.org/10.1109/ISIT.2011.6033698>
10. Fossorier M.P.C. Quasi-cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices // IEEE Trans. Inform. Theory. 2004. V. 50. № 8. P. 1788–1793. <https://doi.org/10.1109/TIT.2004.831841>
11. Amirzade F., Panario D., Sadeghi M.-R. Girth Analysis of Quantum Quasi-Cyclic LDPC Codes // Probl. Inf. Transm. 2024. V. 60. № 2. P. 71–89. <https://doi.org/10.1134/S0032946024020017>
12. Amirzade F., Sadeghi M.-R., Panario D. QC-LDPC Construction Free of Small Size Elementary Trapping Sets Based on Multiplicative Subgroups of a Finite Field // Adv. Math. Commun. 2020. V. 14. № 3. P. 397–411. <https://doi.org/10.3934/amc.2020062>
13. Amirzade F., Sadeghi M.-R. Analytical Lower Bounds on the Size of Elementary Trapping Sets of Variable-Regular LDPC Codes with Any Girth and Irregular Ones with Girth 8 // IEEE Trans. Commun. 2018. V. 66. № 6. P. 2313–2321. <https://doi.org/10.1109/TCOMM.2018.2805834>

14. *Amirzade F., Sadeghi M.-R., Panario D.* Construction of Protograph-Based LDPC Codes with Chordless Short Cycles // IEEE Trans. Inform. Theory. 2023. V. 70. № 1. P. 51–74. <https://doi.org/10.1109/TIT.2023.3307583>

Амирзаде Фарзана (Amirzade, Farzane)

Школа математики и статистики,
Карлтонский университет, Оттава, Канада

Факультет математики и информатики,

Технологический университет имени Амира Кабира

(Тегеранский политехнический институт), Тегеран, Иран

farzaneamirzadedana@cunet.carleton.ca, famirzade@gmail.com

Панарио Даниэль (Panario, Daniel)

Школа математики и статистики,

Карлтонский университет, Оттава, Канада

daniel@math.carleton.ca

Садеги Мохаммад-Реза[✉] (Sadeghi, Mohammad-Reza)

Школа математики и статистики,

Карлтонский университет, Оттава, Канада

Факультет математики и информатики,

Технологический университет имени Амира Кабира

(Тегеранский политехнический институт), Тегеран, Иран

[✉]msadeghi@aut.ac.ir, msadeghi@math.carleton.ca

Поступила в редакцию

16.12.2023

После доработки

18.07.2024

Принята к публикации

29.08.2024