ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 60 **2024** **Вып. 3**

УДК 621.391 : 519.725

© 2024 г. **Ц. Байчева**[1], **С. Топалова**[2]

НОВЫЕ РЕЗУЛЬТАТЫ ОБ ОПТИМАЛЬНЫХ ДВОИЧНЫХ ЦИКЛИЧЕСКИ ПЕРЕСТАНОВОЧНЫХ РАВНОВЕСНЫХ $(v, 4, 1)$-КОДАХ

Построены новые двоичные циклически перестановочные равновесные коды (ЦПР-коды) с параметрами $(v, 4, 1)$ для длин $v \leqslant 136$, а также исправлено несколько табличных значений из работы авторов [1].

Ключевые слова: двоичный циклически перестановочный равновесный код, оптический ортогональный код, циклическая схема, классификация, автоморфизмы циклической группы.

DOI: 10.31857/S0555292324030021, **EDN:** PDKCCX

§ 1. Введение

Начнем с обозначений для рассматриваемых комбинаторных структур. Более подробную информацию об отношениях между ними можно найти в [1–3]. Обозначим через $\mathbb{Z}_v$ аддитивную группу целых чисел по модулю v.

Пусть $V = \{P_i\}_{i=1}^{v}$ – конечное множество *точек*, а $\mathcal{B} = \{B_j\}_{j=1}^{b}$ – конечный набор k-элементных подмножеств множества V, называемых *блоками*. Тогда $D = (V, \mathcal{B})$ называется *схемой* (или *дизайном*) с параметрами 2-$(v, k, 1)$ (системой Штейнера $S(2, k, v)$), если любое подмножество размера 2 множества V содержится ровно в одном блоке из $\mathcal{B}$. Две 2-$(v, k, 1)$-схемы D и D' *изоморфны*, если существует перестановка точек, переводящая каждый блок из D в блок из D'. Схема 2-$(v, k, 1)$ называется *циклической*, если у нее имеется автоморфизм α_v, переставляющий ее точки в одном цикле, и *строго циклической*, если орбита каждого блока под действием этого автоморфизма имеет длину v (нет коротких орбит). Две циклические 2-$(v, k, 1)$-схемы D и D' *мультипликаторно эквивалентны*, если существует автоморфизм $\mathbb{Z}_v$, отображающий каждый блок из D в блок из D'.

Пусть $M = \{m_1, m_2, \ldots, m_k\}$ – некоторое подмножество размера k аддитивной группы G. Тогда через $M + t$ обозначим t-сдвиг множества M, т.е.

$$M + t = \{m_1 + t, m_2 + t, \ldots, m_k + t\},$$

где $t \in G$.

Разностным $(v, k, 1)$-семейством называется множество $\mathcal{D} = \{M_1, \ldots, M_s\}$, где $M_i = \{m_{i_1}, m_{i_2}, \ldots, m_{i_k}\}$ – k-элементные подмножества аддитивной группы G порядка v, такие что любой ненулевой элемент группы G единственным образом представляется в виде некоторой разности $m_{i_j} - m_{i_\ell}$ для $1 \leqslant i \leqslant s$ и $1 \leqslant j \neq \ell \leqslant k$. Два

[1] Работа выполнена при частичной финансовой поддержке Министерства образования и науки Республики Болгария (номер гранта D01-325/01.12.2023).

[2] Работа выполнена при частичной финансовой поддержке Национального научного фонда Болгарии (номер контракта КР-06-Н62/2/13.12.2022).

разностных семейства над G эквивалентны, если существует автоморфизм α группы G, переводящий каждое k-элементное подмножество первого семейства в некоторый сдвиг подмножества из второго семейства. Если G – циклическая группа, то и разностное семейство циклическое. В дальнейшем мы будем рассматривать циклические разностные семейства для $G = \mathbb{Z}_v$.

Двоичный циклически перестановочный равновесный код (ЦПР-код) с параметрами $(v, k, 1)$ (или оптический ортогональный $(v, k, 1)$-код) можно определить как набор $\mathcal{C} = \{C_1, \ldots, C_s\}$, состоящий из k-подмножеств группы $\mathbb{Z}_v$ (*кодовых слов*), таких что любые два сдвига одного кодового слова имеют не более одного общего элемента и любые два сдвига двух различных кодовых слов также имеют не более одного общего элемента:

$$|C_i \cap (C_i + t)| \leqslant 1, \quad 1 \leqslant i \leqslant s, \quad 1 \leqslant t \leqslant v-1, \tag{1}$$

$$|C_i \cap (C_j + t)| \leqslant 1, \quad 1 \leqslant i < j \leqslant s, \quad 0 \leqslant t \leqslant v-1. \tag{2}$$

Первое из этих свойств называется свойством автокорреляции, а второе – свойством кросс-корреляции.

Два $(v, k, 1)$-ЦПР-кода C и C' *изоморфны*, если существует перестановка φ группы $\mathbb{Z}_v$, переводящая набор сдвигов каждого кодового слова из C в набор сдвигов кодового слова из C'. Эти два кода *мультипликаторно эквивалентны*, если φ является автоморфизмом группы $\mathbb{Z}_v$.

Рассмотрим кодовое слово $C = \{c_1, c_2, \ldots, c_k\}$. Обозначим через ΔC мультимножество, состоящее из значений разностей $c_i - c_j$, $i \neq j$, $i, j = 1, 2, \ldots, k$. Свойство автокорреляции означает, что все разности кодовых слов $(v, k, 1)$-ЦПР-кода различны. Свойство кросс-корреляции означает, что $\Delta C_1 \cap \Delta C_2 = \varnothing$ для любых двух кодовых слов C_1 и C_2. Если все возможные $v-1$ ненулевых разностей покрываются разностями кодовых слов, то $(v, k, 1)$-ЦПР-код называется *совершенным* и соответствует циклическому $(v, k, 1)$-разностному семейству и циклической 2-$(v, k, 1)$-схеме. Блоки этой схемы соответствуют кодовым словам и их сдвигам. Эта схема является строго циклической. Каждое кодовое слово со своими сдвигами соответствуют одной блоковой орбите длины v под действием α_v.

Для $(v, k, 1)$-ЦПР-кода его мощность s – это число его кодовых слов. Она не может превышать

$$\left\lfloor \frac{v-1}{k(k-1)} \right\rfloor.$$

ЦПР-коды, достигающие этой границы, называются оптимальными. Если мощность кода в точности равна $(v-1)/k(k-1)$, то этот $(v, k, 1)$-ЦПР-код совершенный. Тем самым, оптимальные $(v, 4, 1)$-ЦПР-коды совершенны тогда и только тогда, когда $v = 12n + 1$.

ЦПР-коды имеют различные применения [4–6] и широко изучены (см., например, [2, 7–10]). Существование оптимальных $(v, 4, 1)$-ЦПР-кодов рассматривалось в [11–17]. Известно, что оптимальные $(v, 4, 1)$-ЦПР-коды существуют для всех рассматриваемых нами длин. Нам не известны какие-либо результаты классификации для $(v, 4, 1)$-ЦПР-кодов или циклических схем при $v > 76$. Системы $S(2, 4, v)$ представляют собой особенно интересный класс систем Штейнера, им было посвящено множество исследований [18], и в частности, изучались циклические $S(2, 4, v)$-системы [19].

Недавно на портале `arXiv` была опубликована небольшая заметка [20]. В ней было получено несколько новых результатов о разностных семействах. Ее автор также проверил некоторые уже известные результаты из [1] и [21]. Для всех проверенных случаев он получил те же самые значения, за исключением разностных семейств

с параметрами $(73, 4, 1)$. Для них он получил 1428546 не эквивалентных разностных $(73, 4, 1)$-семейств, что больше, чем число 1426986 таких семейств, полученное в [1]. Мы повторили наши вычисления, и оказалось, что значение, приведенное в [20], является верным. Неверный результат в работе [1] связан с ошибкой в программе, которая использовалась для классификации в этой работе, он не имеет отношения к алгоритму и не затрагивает наших результатов классификации для ЦПР-кодов (оптических ортогональных кодов) с другими параметрами, опубликованных в других работах. Повторение всех вычислений из [1] на компьютере с частотой 3,2 ГГц не заняло много времени, и поэтому мы решили также рассмотреть и бóльшие длины.

В настоящей статье мы вначале корректируем результаты, полученные в [1] для $(v, 4, 1)$-ЦПР-кодов с длинами 41, 46, 53, 58, 71 и 73. Затем мы приводим классификацию с точностью до изоморфизма оптимальных $(85, 4, 1)$-ЦПР-кодов и циклических $2 - (85, 4, 1)$- и $2 - (88, 4, 1)$-схем (соответствующих неэквивалентным циклическим разностным $(85, 4, 1)$- и $(88, 4, 1)$-семействам). Наконец, получено несколько тысяч оптимальных $(v, 4, 1)$-ЦПР-кодов с длинами $76 < v \leqslant 136$. В § 2 представлены исправления к [1], в § 3 – новые результаты и алгоритмы, использованные для $76 < v \leqslant 136$, а в § 4 дано краткое заключение и описание открытых вопросов. Файлы со всеми построенными нами $(v, 4, 1)$-ЦПР-кодами можно загрузить с сайта `http://www.moi.math.bas.bg/~tsonka/`, а также `https://zenodo.org/records/13771464`. Расширенное изложение результатов настоящей статьи содержится в [22].

§ 2. Исправления к работе [1]

Значения числа мультипликаторно неэквивалентных оптимальных $(v, 4, 1)$-ЦПР-кодов с длинами 41, 46, 53, 58, 71, 73 и 74 отличаются от значений, указанных в [1]. Правильные значения приведены в табл. 1.

Таблица 1

Уточненные количества оптимальных $(v, 4, 1)$-ЦПР-кодов из [1]

Длина	Мощность	Число кодов
41	3	340
46	3	10016
53	4	28680
58	4	1013340

Длина	Мощность	Число кодов
71	5	425832736
73	6	1428546
74	6	2148852

§ 3. $(v, 4, 1)$-ЦПР-коды для $76 < v \leqslant 136$

3.1. Об основном алгоритме и справедливости компьютерных результатов. Вопрос о надежности наших компьютерных программ закономерно возникает после того как были обнаружены ошибки в наших предыдущих вычислениях. Никогда нельзя быть абсолютно уверенным в том, что какая-либо сложная программа работает правильно во всех случаях, потому что обычно какие-то очень мелкие детали могут приводить к ошибкам. Чтобы проверить надежность нашей программы, мы всегда тестировали ее на всех ранее известных результатах. Для [1] это были результаты классификации для циклических $(v, 4, 1)$-схем с $v \leqslant 64$ [19], которые совпали с нашими. Позже мы усовершенствовали эту программу для построения оптимальных $(v, k, 1)$-ЦПР-кодов для любого k (не только для $k = 4$) и протестировали ее на всех известных результатах классификации, а именно на циклических $(v, 3, 1)$-схемах с $v \leqslant 57$ [23] и циклических $(v, 5, 1)$-схемах с $v \leqslant 65$ [19]. Когда в [20] появилась информация об ошибке в нашем результате для $(73, 4, 1)$, мы повторили

с помощью этой более общей программы все вычисления из [1]; полученные при этом результаты приведены в предыдущем параграфе. Также в [20] отмечено, что за исключением случая $(73, 4, 1)$ алгоритм, описанный в [20], во всех других случаях, представленных в [21], дал то же самое число неэквивалентных циклических разностных семейств.

Для классификации оптимальных ЦПР-кодов и циклических схем с точностью до мультипликаторной эквивалентности используется обратный поиск с проверкой на минимальность некоторых частичных решений. Перед началом поиска строятся все возможные кодовые слова (блоки орбит по действию α_v, если строятся схемы), которые упорядочиваются как в лексикографическом порядке, так и по действию автоморфизмов циклической группы порядка v. Это позволяет задать лексикографический порядок и на решениях, а также с легкостью проверить с помощью теста на минимальность, можно ли с помощью какого-либо автоморфизма циклической группы порядка v перевести решение в лексикографически меньшее. Если можно, то решение отбрасывается. Таким образом, строятся только мультипликаторно неэквивалентные коды (циклические схемы). Подробности можно найти в [1], а в [22] приведен небольшой пример, иллюстрирующий работу алгоритма.

3.2. Классификация циклических 2-$(85, 4, 1)$- и 2-$(88, 4, 1)$-схем с точностью до изоморфизма. Вначале была проведена классификация совершенных $(85, 4, 1)$-ЦПР-кодов (циклических 2-$(85, 4, 1)$-схем) и циклических 2-$(88, 4, 1)$-схем с точностью до мультипликаторной эквивалентности с помощью параллельной версии основного алгоритма. Каждая из этих двух задач выполнялась в 96 процессах на высокопроизводительном компьютере "Авитохол" Болгарской академии наук (подробнее см. благодарности в конце статьи), и эта задача была выполнена за четыре дня. Таким образом мы выяснили, что с точностью до мультипликаторной эквивалентности имеется 228406824 совершенных $(85, 4, 1)$-ЦПР-кода и 149494720 2-$(88, 4, 1)$-схем. Это также количества неэквивалентных разностных $(85, 4, 1)$- и $(88, 4, 1)$-семейств.

Две циклические комбинаторные структуры на $v = p{\cdot}q$ точках (где p и q – различные простые числа) изоморфны тогда и только тогда, когда они мультипликаторно эквивалентны [24]. Поэтому все эти 228406824 циклические 2-$(85, 4, 1)$-схемы не изоморфны. Две циклические схемы на $v = 88$ точках, однако, могут быть мультипликаторно не эквивалентны, но изоморфны, если их полная группа автоморфизмов имеет порядок выше, чем 88. С помощью "Авитохола" мы вычислили порядки групп автоморфизмов всех 149494720 схем и установили, что все они имеют порядок 88. Это означает, что эти схемы не изоморфны. Компьютерное время, необходимое для нахождения групп автоморфизмов схем, оказалось в 5 раз выше времени их построения.

3.3. Оптимальные ЦПР-коды для $76 < v \leqslant 136$. Обычно, когда программа пытается получить слишком много результатов или требует слишком много времени для выполнения поставленной задачи, ее просто прерывают и пытаются использовать результаты, полученные к этому моменту. Однако полученные таким образом коды, как правило, оказывались очень похожими друг на друга – они отличались лишь несколькими последними кодовыми словами. Поэтому здесь мы использовали другой подход, немного модифицировав основной алгоритм. Если найдено частичное решение из m кодовых слов, то алгоритм классификации пытается дополнить его до частичного решения из $m + 1$ кодовых слов всеми возможными способами, а модифицированный алгоритм пытается дополнить частичное решение из m кодовых слов $(m > 1)$ до частичного решения из $m + 1$ кодовых слов не всеми, а лишь не более чем e возможными способами.

Тест на минимальность отвергает код C, если он переводится некоторым автоморфизмом в лексикографически меньший код C'. При этом мы должны быть уверены, что код C' уже построен. Поэтому когда для $(m + 1)$-го кодового слова существует

более e возможностей, используются только e лексикографически наименьших. Тем самым, для $m > 1$ рассматривается не более e ветвей узлов дерева поиска. Таким образом строятся коды со всеми возможностями для первого и второго кодового слова, и каждый из полученных кодов отличается от большинства других кодов по многим кодовым словам. Построенные коды доступны онлайн.

§ 4. Заключение и открытые вопросы

Пересмотр нашей работы 2011 года показал, что более мощные параллельные компьютеры, доступные в настоящее время, позволяют получать результаты классификации для бóльших длин, но чрезвычайно большое количество кодов делает эти результаты сложными для использования. Поэтому мы пытались строить только "репрезентативную" часть кодов, а именно коды, существенно отличающиеся друг от друга. Мы надеемся, что онлайн-доступность построенных оптимальных $(v, 4, 1)$-ЦПР-кодов сделает их полезными как для приложений, так и для будущих исследований. Другой подход может заключаться в построении только тех кодов, которые обладают определенными свойствами, например, группами автоморфизмов, или свойствами, важными для того или иного конкретного приложения. Задачи полной классификации циклических разностных $(v, 4, 1)$-семейств с $v > 88$ и классификация оптимальных $(v, 4, 1)$-ЦПР-кодов с $v > 76$ и $v \neq 85$ остаются открытыми.

Авторы благодарны Ивану Гетману за оперативное информирование о его результатах, представленных в [20].

Исследования, которые привели к данным результатам, проводились с использованием инфраструктуры, приобретенной в рамках Национальной дорожной карты для исследовательской инфраструктуры, финансовую координацию которой осуществляет Министерство образования и науки Республики Болгария (грант № D01-325/01.12.2023).

СПИСОК ЛИТЕРАТУРЫ

1. *Байчева Ц., Топалова С.* Классификация оптимальных двоичных циклически перестановочных равновесных $(v, 4, 1)$-кодов и циклических 2-$(v, 4, 1)$-дизайнов для $v \leqslant 76$ // Пробл. передачи информ. 2011. V. 47. № 3. P. 10–18. https://www.mathnet.ru/rus/ppi2051
2. *Moreno O., Zhang Z., Kumar P.V., Zinoviev V.A.* New Constructions of Optimal Cyclically Permutable Constant Weight Codes // IEEE Trans. Inform. Theory. 1995. V. 41. № 2. P. 448–455. https://doi.org/10.1109/18.370146
3. *Abel R.J.R., Buratti M.* Difference Families // Handbook of Combinatorial Designs. Boca Raton: Chapman & Hall/CRC, 2007. Sec. VI.16. P. 392–410.
4. *Chung F.R.K., Salehi J.A., Wei V.K.* Optical Orthogonal Codes: Design, Analysis, and Applications // IEEE Trans. Inform. Theory. 1989. V. 35. № 3. P. 595–604. https://doi.org/10.1109/18.30982
5. *Bird I.C.M., Keedwell A.D.* Design and Applications of Optical Orthogonal Codes—A Survey // Bull. Inst. Combin. Appl. 1994. V. 11. P. 21–44.
6. *Colbourn C.J., Dinitz J.H., Stinson D.R.* Applications of Combinatorial Designs to Communications, Cryptography, and Networking // Surveys in Combinatorics, 1999. Cambridge: Cambridge Univ. Press, 1999. P. 37–100.
7. *Nguyen Q.A., Gyöfri L., Massey J.L.* Constructions of Binary Constant-Weight Cyclic Codes and Cyclically Permutable Codes // IEEE Trans. Inform. Theory. 1992. V. 38. № 3. P. 940–949. https://doi.org/10.1109/18.135636
8. *Bitan S., Etzion T.* Constructions for Optimal Constant Weight Cyclically Permutable Codes and Difference Families // IEEE Trans. Inform. Theory. 1995. V. 41. № 1. P. 77–87. https://doi.org/10.1109/18.370117

9. *Fuji-Hara R., Miao Y.* Optical Orthogonal Codes: Their Bounds and New Optimal Constructions // IEEE Trans. Inform. Theory. 2000. V. 46. № 7. P. 2396–2406. https://doi.org/10.1109/18.887852
10. *Baicheva T., Topalova S.* Classification of Optimal $(v, k, 1)$ Binary Cyclically Permutable Constant Weight Codes with $k = 5$, 6 and 7 and Small Lengths // Des. Codes Cryptogr. 2019. V. 87. № 2–3. P. 365–374. https://doi.org/10.1007/s10623-018-0534-x
11. *Brickell E.F., Wei V.K.* Optical Orthogonal Codes and Cyclic Block Designs // Congr. Numer. 1987. V. 58. P. 175–182.
12. *Chen K., Zhu L.* Existence of $(q, k, 1)$ Difference Families with q a Prime Power and $k = 4, 5$ // J. Combin. Des. 1999. V. 7. № 1. P. 21–30. https://doi.org/10.1002/(SICI)1520-6610(1999)7:1<21::AID-JCD4>3.0.CO;2-Y
13. *Buratti M.* Cyclic Designs with Block Size 4 and Related Optimal Optical Orthogonal Codes // Des. Codes Cryptogr. 2002. V. 26. № 1–3. P. 111–125. https://doi.org/10.1023/A:1016505309092
14. *Chang Y., Fuji-Hara R., Miao Y.* Combinatorial Constructions of Optimal Optical Orthogonal Codes with Weight 4 // IEEE Trans. Inform. Theory. 2003. V. 49. № 5. P. 1283–1292. https://doi.org/10.1109/TIT.2003.810628
15. *Abel R.J.R., Buratti M.* Some Progress on $(v, 4, 1)$ Difference Families and Optical Orthogonal Codes // J. Combin. Theory Ser. A. 2004. V. 106. № 1. P. 59–75. https://doi.org/10.1016/j.jcta.2004.01.003
16. *Buratti M., Pasotti A.* Further Progress on Difference Families with Block Size 4 or 5 // Des. Codes Cryptogr. 2010. V. 56. № 1. P. 1–20. https://doi.org/10.1007/s10623-009-9335-6
17. *Wang X., Chang Y.* Further Results on $(v, 4, 1)$-Perfect Difference Families // Discrete Math. 2010. V. 310. № 13-14. P. 1995–2006. https://doi.org/10.1016/j.disc.2010.03.017
18. *Reid C., Rosa A.* Steiner Systems $S(2, 4, v)$—A Survey // Electron. J. Combin., Dynamic Survey DS18. 2010. https://doi.org/10.37236/39
19. *Colbourn M.J., Mathon R.A.* On Cyclic Steiner 2-Designs // Ann. Discrete Math. 1980. V. 7. P. 215–253. https://doi.org/10.1016/S0167-5060(08)70182-1
20. *Hetman I.* Steiner Systems $S(2, 6, 121/126)$ Based on Difference Families, https://arxiv.org/abs/2401.08274 [math.CO], 2024.
21. *Baicheva T., Topalova S.* Classification Results for $(v, k, 1)$ Cyclic Difference Families with Small Parameters // Mathematics of Distances and Applications. Sofia: ITHEA, 2012. P. 24–30. Available at http://www.foibg.com/ibs_isc/ibs-25/ibs-25-p02.pdf.
22. *Baicheva T., Topalova S.* An Update on Optimal $(v, 4, 1)$ Binary Cyclically Permutable Constant Weight Codes and Cyclic 2-$(v, 4, 1)$ Designs with Small v // Probl. Inf. Transm. 2024. V. 60. № 3. P. 189–198. https://doi.org/10.1134/S0032946024030037
23. *Colbourn C.J., Rosa A.* Triple Systems, Oxford: Clarendon; New York: Oxford Univ. Press, 1999.
24. *Pálfy P.* Isomorphism Problem for Relational Structures with a Cyclic Automorphism // European J. Combin. 1987. V. 8. № 1. P. 35–43. https://doi.org/10.1016/S0195-6698(87)80018-5

Байчева Цонка
Топалова Светлана
Институт математики и информатики
Болгарской академии наук, София, Болгария
tsonka@math.bas.bg
svetlana@math.bas.bg

Поступила в редакцию
11.07.2024
После доработки
25.09.2024
Принята к публикации
07.10.2024