MODELING AND ANALYSIS OF INFORMATION SYSTEMS, VOL. 29, NO. 3, 2022
journal homepage: www.mais-journal.ru

COMPUTER SYSTEM ORGANIZATION

On the Construction of Self-Complementary Codes and their Application in the Problem of Information Hiding

Y. V. Kosolapov[1], F. S. Pevnev[1], M. V. Yagubyants[1]

DOI: 10.18255/1818-1015-2022-3-182-198

[1]Southern Federal University, 105/42 Bolshaya Sadovaya str., Rostov-on-Don 344006, Russia.

MSC2020: 51E22, 94B05
Research article
Full text in Russian

Received May 27, 2022
After revision August 22, 2022
Accepted August 26, 2022

Line codes are widely used to protect against errors in data transmission and storage systems, to ensure the stability of various cryptographic algorithms and protocols, to protect hidden information from errors in a stegocontainer. One of the classes of codes that find application in a number of the listed areas is the class of linear self-complementary codes over a binary field. Such codes contain a vector of all ones, and their weight enumerator is a symmetric polynomial. In applied problems, self-complementary $[n, k]$-codes are often required for a given length n and dimension k to have the maximum possible code distance $d(k, n)$. For $n < 13$, the values of $d(k, n)$ are already known. In this paper, for self-complementary codes of length n=13, 14, 15, the problem is to find lower bounds on $d(k, n)$, as well as to find the values of $d(k, n)$ themselves. The development of an efficient method for obtaining a lower estimate close to $d(k, n)$ is an urgent task, since finding the values of $d(k, n)$ in the general case is a difficult task. The paper proposes four methods for finding lower bounds: based on cyclic codes, based on residual codes, based on the (u—u+v)-construction, and based on the tensor product of codes. On the joint use of these methods for the considered lengths, it was possible to efficiently obtain lower bounds, either coinciding with the found values of $d(k, n)$ or differing by one. The paper proposes a sequence of checks, which in some cases helps to prove the absence of a self-complementary $[n, k]$-code with code distance d. In the final part of the work, on the basis of self-complementary codes, a design for hiding information is proposed that is resistant to interference in the stegocontainer. The above calculations show the greater efficiency of the new design compared to the known designs.

Keywords: linear codes; self-complementary codes; information hiding

INFORMATION ABOUT THE AUTHORS

Yury V. Kosolapov correspondence author	orcid.org/0000-0002-1491-524X. E-mail: itaim@mail.ru associated professor, PhD.
Fedor S. Pevnev	orcid.org/0000-0003-3225-9992. E-mail: pevnev@sfedu.ru postgraduate student.
Margarita V. Yagubyants	orcid.org/0000-0001-9168-9875. E-mail: myagubyanc@sfedu.ru student.

For citation: Y. V. Kosolapov, F. S. Pevnev, and M. V. Yagubyants, "On the Construction of Self-Complementary Codes and their Application in the Problem of Information Hiding", *Modeling and analysis of information systems*, vol. 29, no. 3, pp. 182-198, 2022.

МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ, ТОМ 29, № 3, 2022
сайт журнала: www.mais-journal.ru

COMPUTER SYSTEM ORGANIZATION

О построении самодополнительных кодов и их приложении в задаче сокрытия информации

Ю. В. Косолапов [1], Ф. С. Певнев[1], М. В. Ягубянц[1]

DOI: 10.18255/1818-1015-2022-3-182-198

[1]Южный федеральный университет, ул. Большая Садовая, д. 105/42, г. Ростов-на-Дону, 344006 Россия.

УДК 519.7
Научная статья
Полный текст на русском языке

Получена 27 мая 2022 г.
После доработки 22 августа 2022 г.
Принята к публикации 26 августа 2022 г.

Линейные коды широко применяются для защиты от ошибок в системах передачи и хранения данных, обеспечения стойкости различных криптографических алгоритмов и протоколов, для защиты скрытой информации от ошибок в стегоконтейнере. Одним из классов кодов, находящих применение в ряде перечисленных областей, является класс линейных самодополнительных кодов над бинарным полем. Такие коды содержат вектор из всех единиц, а их нумератор весов является симметрическим многочленом. В прикладных задачах от самодополнительных $[n, k]$-кодов часто требуется при заданной длине n и размерности k иметь максимально возможное кодовое расстояние $d(k, n)$. Для $n < 13$ значения $d(k, n)$ уже известны. В настоящей работе для самодополнительных кодов длины n=13, 14, 15 ставится задача нахождения нижних оценок на $d(k, n)$, а также нахождение самих значений $d(k, n)$. Разработка эффективного способа получения нижней оценки, близкой к $d(k, n)$, является актуальной задачей, так как нахождение самих значений $d(k, n)$ в общем случае является трудной задачей. В работе предложены четыре способа нахождения нижних оценок: на основе циклических кодов, на основе остаточных кодов, на основе $(u|u + v)$-конструкции и на основе тензорного произведения кодов. На совместном использовании этих способов для рассмотренных длин удалось получить эффективным образом нижние оценки, либо совпадающие с найденными значениями $d(k, n)$, либо отличающиеся на единицу. В работе предложена последовательность проверок, которая в ряде случаев помогает доказать отсутствие самодополнительного $[n, k]$-кода с кодовым расстоянием d. В заключительной части работы на основе самодополнительных кодов предлагается конструкция для сокрытия информации, устойчивая к помехам в стегоконтейнере. Приведенные расчеты показывают большую эффективность новой конструкции по сравнению с известными конструкциями.

Ключевые слова: линейные коды; самодополнительные коды; сокрытие информации

ИНФОРМАЦИЯ ОБ АВТОРАХ

Юрий Владимирович Косолапов автор для корреспонденции	orcid.org/0000-0002-1491-524X. E-mail: itaim@mail.ru доцент, канд. техн. наук.
Федор Сергеевич Певнев	orcid.org/0000-0003-3225-9992. E-mail: pevnev@sfedu.ru аспирант.
Маргарита Владимировна Ягубянц	orcid.org/0000-0001-9168-9875. E-mail: myagubyanc@sfedu.ru студент.

Для цитирования: Y. V. Kosolapov, F. S. Pevnev, and M. V. Yagubyants, “On the Construction of Self-Complementary Codes and their Application in the Problem of Information Hiding”, *Modeling and analysis of information systems*, vol. 29, no. 3, pp. 182-198, 2022.

Введение

Линейным $[n, k]_q$-кодом C называется подпространство размерности k линейного пространства $\mathbb{F}_q^n$ над полем Галуа $\mathbb{F}_q$, состоящем из q элементов. Также для $[n, k]_q$-кода используют обозначение $[n, k, d]_q$, если известна характеристика d, называемая кодовым расстоянием, которая определяется как минимальное расстояние Хэмминга (количество несовпадающих координат) $\rho(\mathbf{c}, \mathbf{0}_n)$ от $\mathbf{c} \in C$ до нулевого вектора $\mathbf{0}_n = (0, ..., 0) \in \mathbb{F}_q^n$ по всем $\mathbf{c}$ из C, $\mathbf{c} \neq \mathbf{0}_n$. Число $\mathrm{wt}(\mathbf{c}) = \rho(\mathbf{c}, \mathbf{0}_n)$ называется весом Хэмминга вектора $\mathbf{c}$. Основным объектом исследования в настоящей работе являются коды над полем $\mathbb{F}_2$, поэтому для соответствующих кодов их характеристики в квадратных скобках будут указываться без нижнего индекса 2. $[n, k, d]$-код C, содержащий вектор из всех единиц $\mathbf{1}_n = (1, ..., 1)$, называется самодополнительным кодом (далее – просто СД-кодом или СД-кодом с параметрами $[n, k, d]$). Такие коды также называются антиподальными [1], так как для каждого вектора $\mathbf{c}$ из C в этом коде содержится его «антипод» (инверсия) вида $\mathbf{c} + \mathbf{1}_n$. СД-коды с параметрами $[n, k, d]$, кроме исправления ошибок в метрике Хэмминга и стираний [2], также могут использоваться для построения $[n - 1, k - 1]$-кодов, исправляющих помеху, приводящую к инверсии всех битов кодового слова [3]. Это свойство, в частности, используется в [4] для построения метода сокрытия информации, с одной стороны, эффективного в части отношения объема скрываемой информации к количеству изменений в контейнере, а с другой стороны, устойчивого к заранее определенному числу ошибок в стегоконтейнере.

Для СД-кода с параметрами $[n, k, d]$-кода C выполняется неравенство Грея-Рэнкина [5]

$$2^k \leqslant \frac{8d(n-d)}{n-(n-2d)^2}, \tag{1}$$

где n и d такие, что знаменатель положителен. В [6] найдены параметры всех СД-кодов, достигающих границы (1), а ряд работ (см., например, [7] и [8]) посвящен отысканию для фиксированных n, k и d числа неэквивалентных СД-кодов, достигающих границы Грея-Рэнкина.

Другой важной задачей для СД-кодов является нахождение максимально возможного кодового расстояния $d(k, n)$ для заданных k и n, и построение самодополнительного $[n, k, d(k, n)]$-кода (хотя бы одного). Актуальность этой задачи вызвана, например, тем, что для метода сокрытия [4] значения k и n являются его параметрами, и чем больше кодовое расстояние d СД-кода при этих параметрах, тем больше ошибок в стегоконтейнере может быть исправлено. В работе [9] при $n = 1, ..., 12$ найдены значения $d(k, n)$ для $k = 1, ..., n$, и приведены примеры порождающих матриц соответствующих СД-кодов. Целью настоящей работы является нахождение $d(k, n)$ для $n = 13, 14, 15$, $k = 1, ..., n$. В работе предлагаются способы оценки значений $d(k, n)$ снизу, аналитически находятся $d(k, n)$ при $n = 13, 14, 15$, а в приложении приводятся примеры порождающих матриц соответствующих СД-кодов. В этой части настоящая работа продолжает исследование, начатое в [9]. В заключительном разделе строится модификация стегоконструкции из [4]. Для повышения эффективности предлагается новый способ применения СД-кодов и для найденных в работе параметров СД-кодов приводятся результаты расчета эффективности.

1. Предварительные результаты

Порождающей матрицей G кода $C \subseteq \mathbb{F}_q^n$ размерности k называется $k \times n$-матрица, строки которой образуют базис C. Таким образом, линейная оболочка $\mathcal{L}(G)$, натянутая на строки матрицы G, совпадает с C. Говорят, что порождающая матрица $[n, k]_q$-кода имеет систематический вид, если ее первые k столбцов образуют единичную $k \times k$-матрицу E_k. Пусть $\langle \mathbf{x}, \mathbf{y} \rangle$ – скалярное произведение векторов $\mathbf{x}$ и $\mathbf{y}$. Для $[n, k]_q$-кода C код $C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{x}, \mathbf{c} \rangle = 0, \mathbf{c} \in C\}$ является $[n, n-k]_q$-кодом и называется дуальным к коду C. Порождающая $(n-k) \times n$-матрица H кода $C^\perp$ называется проверочной матрицей кода C. Нумератором весов $[n, k]$-кода C называется полином $W_C(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$, где

A_i — количество векторов веса i в коде C. Нумераторы весов кодов C и $C^\perp$ связаны тождеством Мак-Вильямс (см., например, [10]):

$$W_C(x, y) = |C^\perp|^{-1} W_{C^\perp}(y - x, x + y). \tag{2}$$

Утверждение 1. *Пусть C — СД-код, тогда $W_C(x, y) = W_C(y, x)$.*

Доказательство. Так как в СД-коде C длины n для каждого вектора $\mathbf{g}$ имеется вектор $\mathbf{g} + \mathbf{1}_n$, то в C векторов веса $\mathrm{wt}(\mathbf{g})$ столько же, сколько векторов веса $\mathrm{wt}(\mathbf{g} + \mathbf{1}_n)$. Таким образом, $W_C(x, y) = W_C(y, x)$, то есть нумератор является симметрическим многочленом. □

Утверждение 2. *Пусть C — СД-код, тогда в коде $C^\perp$ все ненулевые векторы имеют четный вес.*

Доказательство. Предположим, что существует вектор $\mathbf{g} \in C^\perp \subseteq \mathbb{F}_2^n$, причем $\mathrm{wt}(\mathbf{g})$ — нечетное число. Тогда $\langle \mathbf{g}, \mathbf{1}_n \rangle \neq 0$, что противоречит условию $\mathbf{g} \in C^\perp$. □

Напомним, что носителем вектора $\mathbf{c} = (c_1, ..., c_n) \in \mathbb{F}_q^n$ называется множество $\mathrm{supp}(\mathbf{c}) = \{i : c_i \neq 0\}$. В частности, $\mathrm{supp}(\mathbf{0}_n) = \varnothing$, $\mathrm{supp}(\mathbf{1}_n) = \{1, ..., n\}$ и $|\mathrm{supp}(\mathbf{c})| = \mathrm{wt}(\mathbf{c})$. Рассмотрим $[n, k, d]$-код C с порождающей матрицей G, первой строкой которой является вектор $\mathbf{g}$. Остаточным кодом $res(C, \mathbf{g})$, построенным по C относительно $\mathbf{g}$ называется код, порождённый строками матрицы G_0, где G_0 состоит из столбцов матрицы G с номерами из $\{1, 2, ..., n\} \setminus \mathrm{supp}(\mathbf{g})$. Известен следующий факт.

Теорема 1 ([11], лемма 2.13)**.** *Пусть C – $[n, k, d]$-код, $\mathbf{g} \in C$, $\mathbf{g} \neq \mathbf{0}$, $\mathrm{wt}(\mathbf{g})/2 < d$. Тогда, $res(C, \mathbf{g})$ является $[n - \mathrm{wt}(\mathbf{g}), k - 1, d']$, где $d' \geqslant d - \mathrm{wt}(\mathbf{g})/2$.*

Утверждение 3. *Пусть C – самодополнительный $[n, k, d]$-код, $\mathbf{g} \in C$, $\mathbf{g} \neq \mathbf{0}_n, \mathbf{1}_n$. Тогда $res(C, \mathbf{g})$ и $res(C, \mathbf{g} + \mathbf{1})$ являются самодополнительными.*

Доказательство. По определению, $res(C, \mathbf{g})$ – код длины $n - \mathrm{wt}(\mathbf{g})$. Так как код C – СД-код, то $\mathbf{g} + \mathbf{1}_n \in C$, причем $\mathrm{wt}(\mathbf{g} + \mathbf{1}_n) = n - \mathrm{wt}(\mathbf{g})$. По построению остаточного кода $res(C, \mathbf{g})$, вектор, получаемый из $\mathbf{g} + \mathbf{1}_n$ удалением координат с номерами из $\{1, 2, ..., n\} \setminus \mathrm{supp}(\mathbf{g})$, принадлежит $res(C, \mathbf{g})$. Следовательно, это СД-код. Аналогично показывается, что $res(C, \mathbf{g} + \mathbf{1}_n)$ — СД-код. □

Утверждение 4. *Пусть $G = [E_k|P]$ – порождающая матрица $[n, k]$-кода C. Код C является СД-кодом тогда и только тогда, когда в каждом столбце матрицы P нечётное число единиц.*

Доказательство. Если в каждом столбце матрицы P нечётное число единиц, то C – СД-код, так как сумма всех строк матрицы G дает вектор $\mathbf{1}_n$. Теперь докажем, что если C – СД-код, то в каждом столбце матрицы P нечётное число единиц. Предположим, что существует столбец с чётным числом единиц. Так как код самодополнительный, то в нём по определению существует вектор из всех единиц. Такой вектор может получиться только при суммировании всех строк матрицы $G = [E_k|P]$. Однако, в силу предположения, одна из координат вектора суммы будет нулевая. Таким образом, вектор $\mathbf{1}_n$ не принадлежит коду C, что противоречит предположению. □

Утверждение 5. *Пусть C — самодополнительный $[n, k, d]$-код, $k \geqslant 2$, $p \leqslant n - k$. Тогда существуют самодополнительные $[n, k' < k, d' \geqslant d]$-код, $[n - p, k, \max\{1, d - p\}]$-код и $[n' > n, k, d' \geqslant d]$-код.*

Доказательство. Пусть G – порождающая матрица СД-кода C, первая строка которой равна $\mathbf{1}_n$. Тогда первые $k' < k$ строк этой матрицы порождают самодополнительный $[n, k', d']$-код C', причем $d' \geqslant d$, так как $C' \subseteq C$. Пусть теперь матрица G записана в систематическом виде $G = [E_k|P]$. Удаление в этой матрице последних p столбцов не меняет размерность кода, при этом в силу утверждения 4, новый код будет СД-кодом. Заметим, что при удалении столбцов кодовое расстояние

может уменьшится на p, а так как кодовое расстояние не меньше единицы, то получаем, что существует $[n-p, k, \max\{1, d-p\}]$-код. Если же к матрице G в систематическом виде добавить $n' - n > 0$ столбцов нечетного веса, то получим, в силу утверждения 4, СД-код с параметрами $[n' > n, k, d' \geqslant d]$. □

Из утверждения 5 вытекает, что для фиксированного n последовательность $d(k, n)$ не возрастает с ростом k, а при фиксированном k последовательность $d(k, n)$ не убывает с ростом n.

Утверждение 6. *Пусть C — самодополнительный $[n, k, d]$-код, $k > 1$. Тогда существует линейный $[n-1, k-1, d' \geqslant d]$-код.*

Доказательство. Такой код можно получить укорочением на одну координату кода C, например, путем натягивания линейной оболочки на матрицу $[E_{k-1}|P']$, получающуюся из порождающей матрицы $G = [E_k|P]$ кода C путем выбрасывания первого столбца и первой строки. Известно (см., например, [10]), что такой код имеет параметры $[n-1, k-1, d' \geqslant d]$. □

Отметим, что в случае $d > 1$ укорочение самодополнительного $[n, k, d]$-кода, как следует из утверждения 4, не является СД-кодом, так как выбрасывание любой строки из P приводит к тому, что в P' найдется хотя бы один столбец четного веса.

Утверждение 7. *Пусть C — $[n, k]$-код, $G = [E_k|P]$ — его порождающая матрица в систематическом виде. Если*

1) сумма любых $i = 1, ..., k$ строк матрицы P дает строку веса не менее $d - i$,

2) вес каждого столбца матрицы P нечетный,

то C – самодополнительный $[n, k, d' \geqslant d]$-код.

Доказательство. Условие 1) гарантирует, что любая ненулевая линейная комбинацию строк G дает вектор веса не менее d, а условие 2), в соответствии с утверждением 4, гарантирует, что C – СД-код. □

Следствие 1. *Пусть C — самодополнительный $[n, n-1, d]$-код. Тогда*

$$d = \begin{cases} 1, \text{ если } n - \text{нечетное}, \\ 2, \text{ если } n - \text{четное}. \end{cases}$$

Доказательство. Пусть n – нечетное, тогда в порождающей матрице СД-кода в систематическом виде $G = [E_{n-1}|P]$ матрица P состоит из одного столбца четной высоты. Поэтому нечетный вес этого столбца (необходимое условие для СД-кода, в соответствии с утверждением 4) приводит к тому, что в G будет, как минимум, один вектор единичного веса. В случае четного n получаем, что для матрицы $G = [E_{n-1}|P]$, где единственный столбец матрицы P состоит из единиц, выполняются условия утверждения 7. □

2. Нижние оценки $d(k, n)$

Заметим, что оценка Грея-Рэнкина (1) для длин $n = 13, 14, 15$ не дает много информации о $d(k, n)$. В частности, можно получить только верхние оценки $d(6, 13) \leqslant 5$, $d(4, 13) \leqslant 6$, $d(5, 14) \leqslant 6$, $d(6, 15) \leqslant 6$, $d(5, 15) \leqslant 7$, а также вытекающие из них верхние оценки для меньших размерностей. Больший интерес представляют нижние оценки, для получения которых в настоящей работе предлагается использовать четыре подхода: на основе циклических кодов, на основе остаточных кодов, на основе $(u|u+v)$-конструкции и на основе тензорного произведения.

2.1. На основе циклических кодов

Одним из хорошо изученных классов линейных кодов является класс циклических кодов. Эти коды привлекательны тем, что многие их свойства, такие как кодовое расстояние, вид порождающей и проверочной матрицы могут быть описаны в алгебраических терминах колец и их идеалов. Для хранения порождающей матрицы циклического кода достаточно хранить её первую строку, из которой остальные строки порождающей матрицы получаются циклическим сдвигом. Для некоторых циклических кодов также существуют быстрые декодеры, а для циклических кодов небольшой длины известны способы нахождения минимального кодового расстояния (см., например, [12]). Поэтому в рамках задачи нахождения нижней оценки для $d(k, n)$ естественно возникает задача исследования циклических СД-кодов.

Пусть $\mathbb{F}_2[x]$ — кольцо полиномов над $\mathbb{F}_2$. Рассмотрим фактор-кольцо

$$\mathbb{F}_2[x]/(x^n + 1) = \{f(x) = f_0 + f_1 x + ... + f_{n-1}x^{n-1} \ : \ f_0, ..., f_{n-1} \in \mathbb{F}_2\},$$

в котором операция сложения элементов кольца $f(x)$ и $g(x)$ выполняется как операция сложения полиномов, а операция умножения этих элементов выполняется по модулю $x^n + 1$. Пусть $L : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2[x]/(x^n + 1)$ — преобразование Лорана, ставящее в соответствие вектору $(a_0, ..., a_{n-1}) \in \mathbb{F}_2^n$ полином $a(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1} \in \mathbb{F}_2[x]/(x^n+1)$. Любой идеал I кольца $\mathbb{F}_2[x]/(x^n+1)$ называется циклическим кодом. Так как $\mathbb{F}_2[x]/(x^n + 1)$ — кольцо главных идеалов (см., например, Теорему 3.4 в [13]), то для каждого I существует полином $g(x)$ такой, что $g(x)|x^n + 1$ и $I = (g(x))$. Полином $g(x)$ называется порождающим полиномом кода I, и $g(x)|c(x)$ для всех $c(x) \in I$. Размерность кода I равна $n - \deg(g(x))$.

Пусть $e(x) = L(\mathbf{1}_n)$. Следующее утверждение является очевидным.

Утверждение 8. *Циклический код $I = (g(x))$ является СД-кодом тогда, и только тогда, когда $g(x)|e(x)$.*

Следствие 2. *Пусть $e(x) = (e_1(x))^{\alpha_1} \cdot ... \cdot (e_s(x))^{\alpha_s}$, где $e_i(x)$ — неприводимые полиномы, $\alpha_i \in \mathbb{N}$ — кратность полинома $e_i(x)$, $i = 1, ..., s$. Тогда порождающий полином циклического СД-кода $I = (g(x))$ имеет вид*

$$g(x) = (e_{i_1}(x))^{\beta_{i_1}} \cdot ... \cdot (e_{i_t}(x))^{\beta_{i_t}}, t \leqslant s, \beta_{i_j} \leqslant \alpha_{i_j}, j = 1, ..., t.$$

Напомним, что любой идеал I фактор-кольца $\mathbb{F}_2[x]/(f(x))$, где $f(x)$ — нормированный полином степени n, называется псевдоциклическим кодом. Кольцо $\mathbb{F}_2[x]/(f(x))$ является кольцом главных идеалов, поэтому для I существует порождающий полином $g(x)$ такой, что $g(x)|f(x)$ и $I = (g(x))$. Тогда псевдоциклический код будет СД-кодом, если $g(x)|e(x)$.

Утверждение 9. *Двоичный псевдоциклический СД-код является циклическим той же длины.*

Доказательство. Пусть $f(x)$ — нормированный полином степени n, а $g(x)$ — такой полином, что $g(x)|f(x)$ и $g(x)|e(x)$. Тогда по определению идеал $I = (g(x))$ является псевдоциклическим СД-кодом длины n. С другой стороны, полином $x^n + 1$ раскладывается в произведение $x^n + 1 = (x + 1) \cdot (1 + x + x^2 + ... + x^{n-1}) = (x + 1) \cdot e(x)$. Следовательно, $g(x)|(x^n + 1)$. Отсюда, I является идеалом фактор-кольца $\mathbb{F}_2[x]/(x^n + 1)$, то есть является просто циклическим кодом. □

Таким образом, все циклические СД-коды длины n могут быть найдены путем перебора полиномов, делящих $e(x) = L(\mathbf{1}_n)$. Отметим, что отсюда, в частности, вытекает, что не для каждого k существует циклический СД-код. Кодовые расстояния для циклических СД-кодов могут быть найдены, например, с помощью алгоритма К. Циммермана [12], стр. 118. Тогда нижняя оценка на $d(k, n)$ получается путем нахождения максимального кодового расстояния среди циклических СД-кодов для заданных k и n (если для этих k и n такой код существует).

Table 1. Maximum code distance for a cyclic self-complementary code

Таблица 1. Максимальное кодовое расстояние для циклического самодополнительного кода

d		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	–	–	–	–	–	–	–	–	–	–	–	–		
	14	14	7	–	6	6	–	4	3	–	2	2	–	2	–	
	15	15	–	5	–	7	–	5	–	4	–	2	–	2	–	–

В таблице 1 приведено максимальное кодовое расстояние d самодополнительного $[n, k]$-кода при $n = 13, 14, 15$, причем символом «–» обозначено отсутствие соответствующего циклического СД-кода, пустые ячейки соответствуют случаю $k > n$. С помощью утверждения 5 по таблице 1 может быть построена нижняя оценка $d^c(k, n)$ на $d(k, n)$, которая приводится в таблице 2.

Table 2. Lower bound on $d(k, n)$ based on cyclic codes, $n = 13, 14, 15$

Таблица 2. Оценка снизу на $d(k, n)$ на основе циклических кодов, $n = 13, 14, 15$

$d^c(k, n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	5	5	5	3	3	2	1	1	1	1	1		
	14	14	7	6	6	6	4	4	3	2	2	2	2	2	1	
	15	15	7	7	7	7	5	5	4	4	2	2	2	2	1	1

2.2. На основе $(u|u+v)$-конструкции

В основе конструкции $(u|u+v)$ лежит использование двух кодов: $[n_1, k_1, d_1]_q$-кода C_1 и $[n_2, k_2, d_2]_q$-кода C_2, причем $n_1 = n_2$. Порождающая и проверочная матрицы получающегося кода, который будем обозначать $UV(C_1, C_2)$, имеют вид:

$$G = \begin{pmatrix} G_1 & G_1 \\ O_G & G_2 \end{pmatrix}, \; H = \begin{pmatrix} H_2 & -H_2 \\ H_1 & O_H \end{pmatrix}, \tag{3}$$

где O_G и O_H – нулевые $k_2 \times n_1$- и $(n_1 - k_1) \times n_2$-матрицы, G_1 и G_2 – порождающие матрицы кодов C_1 и C_2 соответственно. Из вида порождающей и проверочной матриц вытекает, что $[n_1 + n_2, k_1 + k_2, d]$-код $UV(C_1, C_2)$ и дуальный к нему $[n_1 + n_2, n_1 + n_2 - (k_1 + k_2), d^\perp]$-код $(UV(C_1, C_2))^\perp$ имеют четную длину, причём

$$d = \min\{2d_1, d_2\}, \; d^\perp = \min\{2d_2^\perp, d_1^\perp\}, \tag{4}$$

где $d_i^\perp$ — кодовое расстояние кода $C_i^\perp$, $i = 1, 2$. Напомним, что коды C и D длины n и одинаковой размерности называются перестановочно эквивалентными, если в симметрической группе S_n, действующей на множестве $\{1, ..., n\}$, найдется перестановка σ, что $D = \{(c_{\sigma^{-1}(1)}, ..., c_{\sigma^{-1}(n)}) \mid (c_1, ..., c_n) \in C\}$. Перестановочную эквивалентность кодов C и D будем обозначать $D \sim C$.

Утверждение 10. *Пусть $q = 2$, тогда $(UV(C_1, C_2))^\perp \sim UV(C_2^\perp, C_1^\perp)$.*

Доказательство. Вытекает из вида (3) проверочной матрицы $UV(C_1, C_2)$ и того, что $-H_2 = H_2$. □

Утверждение 11. *Пусть $q = 2$. Код $UV(C_1, C_2)$ является СД-кодом, тогда, и только тогда, когда C_1 – СД-код, а код $(UV(C_1, C_2))^\perp$ является СД-кодом, тогда, и только тогда, когда $C_2^\perp$ – СД-код.*

Доказательство. Вытекает из вида (3) порождающей матрицы $UV(C_1, C_2)$ и утверждения 10. □

Из утверждения 11 получаем способ построения СД-кода, который заключается в выборе самодополнительного $[n_1, k_1, d_1]$-кода C_1, линейного (необязательно СД-кода) $[n_2, k_2, d_2]$-кода C_2 и построении $UV(C_1, C_2)$. При этом, согласно (4), чем больше d_1 и d_2, тем больше кодовое расстояние кода $UV(C_1, C_2)$. Этим способом могут быть построены СД-коды четной длины и любой размерности. Для получения нижней оценки на $d(k, n)$ следует: 1) для каждой пары кодов (C_1, C_2), где C_1 – самодополнительный $[n/2, k_1, d_1]$-код с максимальным для k_1 кодовым расстоянием d_1, C_2 – $[n/2, k_2, d_2]$-код с максимальным для k_2 кодовым расстоянием d_2, такие, что $k_1 + k_2 = k$, найти d в соответствии с (4), 2) среди рассмотренных пар выбрать пару с максимальным значением d, которое будет нижней оценкой $D^u(k, n)$ для $d(k, n)$. Для длины $n = 14$ описанным способом найдена нижняя оценка $D^u(k, 14)$. С помощью утверждения 5 и найденных значений $D^u(k, 14)$ может быть построена нижняя оценка $d^u(k, n)$ на $d(k, n)$ при $n = 13, 14, 15$. В частности $d^u(k, 13) = \max\{D^u(k, 14) - 1, 1\}$ для $k = 1, ..., 13$, $d^u(k, 14) = D^u(k, 14)$ и $d^u(k, 15) = D^u(k, 14)$ при $k = 2, ..., 14$, $d^u(1, 15) = 15$, $d^u(15, 15) = 1$. Полученная нижняя оценка для $n = 13, 14, 15$ показана в таблице 3.

Table 3. Lower bound on $d(k, n)$ a self-complementary code based on the $(u|u + v)$-construction

Таблица 3. Нижняя оценка на $d(k, n)$ на основе $(u|u + v)$-конструкции

$d^u(k, n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	5	5	5	3	3	3	2	1	1	1	1		
	14	14	7	6	6	6	4	4	4	3	2	2	2	2	1	
	15	15	7	6	6	6	4	4	4	3	2	2	2	2	1	1

Заметим, что этот способ нахождения нижней оценки величины $d(k, n)$ предполагает перебор по тройкам $(n/2, k_1, d_1)$ и $(n/2, k_2, d_2)$ параметров СД-кодов и линейных кодов соответственно, имеющих максимальное кодовое расстояние при заданных размерностях. В случае СД-кодов для $n/2 \leqslant 12$ эти параметры можно найти, например, в [9]. Для линейных кодов при $n/2 \leqslant 21$ соответствующие параметры приведены, например, в [14].

2.3. На основе остаточных кодов

Из утверждения 3 вытекает, что по СД-коду могут быть построены два СД-кода меньшей размерности. Справедливо и обратное утверждение: по двум СД-кодам одинаковой размерности может быть построен СД-код большей размерности. Именно, справедливо следующее утверждение.

Утверждение 12. *Пусть C_i — самодополнительный $[n_i, k, d_i]$-код, G_i — его порождающая матрица вида*

$$G_i = \begin{pmatrix} \mathbf{1}_{n_i} \\ G_i^0 \end{pmatrix}, \; G_i^0 = \begin{pmatrix} \mathbf{g}_{i,1} \\ \dots \\ \mathbf{g}_{i,k-1} \end{pmatrix}, \; i = 1, 2.$$

Тогда код C с порождающей матрицей

$$G_C = \begin{pmatrix} \mathbf{1}_{n_1} & \mathbf{0}_{n_2} \\ \mathbf{0}_{n_1} & \mathbf{1}_{n_2} \\ G_1^0 & G_2^0 \end{pmatrix} \tag{5}$$

является самодополнительным $[n_1 + n_2, k + 1, d]$-кодом, где

$$d \geqslant \min\{n_1, n_2, d_1 + d_2\}. \tag{6}$$

Доказательство. Очевидно, что код C – СД-код, так как сумма первых двух строк его порождающей матрицы (5) даёт вектор $\mathbf{1}_{n_1+n_2}$. Из вида G_C также вытекает, что $d \geqslant \min\{n_1, n_2\}$. Так как кодовое расстояние кода $\mathcal{L}(G_1^0)$ не меньше d_1, а кодовое расстояние кода $\mathcal{L}(G_2^0)$ не меньше d_2, то кодовое расстояние кода $\mathcal{L}(G_1^0|G_2^0)$ не меньше $d_1 + d_2$. Отсюда и из вида (5) получаем оценку (6). □

Способ построения самодополнительного $[n, k]$-кода C заключается в выборе самодополнительных $[n_1, k-1, d_1]$- и $[n_2, k-1, d_2]$-кодов C_1 и C_2 и построении порождающей матрицы вида (5). Используя этот способ, можно строить СД-коды любой длины n и размерности не более $\lfloor n/2 \rfloor + 1$.

Для получения нижней оценки величины $d(k, n)$ следует: 1) для каждой пары кодов (C_1, C_2) найти нижнюю оценку на d в соответствии с (6), где C_i – самодополнительный $[n_i, k-1, d_i]$-код с максимально возможным кодовым расстоянием для заданных длины и размерности, $i = 1, 2$, $n = n_1 + n_2$, 2) выбрать пару с максимальным значением $\min\{n_1, n_2, d_1 + d_2\}$, которое будет нижней оценкой $D^r(k, n)$ для $d(k, n)$ (см. таблицу 4, где ячейки с «–» соответствуют случаю $k > \lfloor n/2 \rfloor + 1$). В этом способе, как и в способе на основе $(u|u+v)$-конструкции, предполагается перебор по параметрам самодополнительных кодов с максимально возможным кодовым расстоянием для заданных длины и размерности. Соответствующие параметры для $n_i \leqslant 12$ можно найти в [9].

Table 4. Bound on d for self-complementary code based on residual codes

Таблица 4. Оценка на d для СД-кода на основе остаточных кодов

$D^r(k,n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	6	5	5	4	–	–	–	–	–	–	–		
	14	14	7	6	6	6	4	3	2	–	–	–	–	–	–	
	15	15	7	7	7	7	5	3	3	–	–	–	–	–	–	–

На основе утверждения 5 и таблицы 4 получена нижняя оценка $d^r(k, n)$ (см. таблицу 5).

Table 5. Bound on $d(k, n)$ for self-complementary code based on residual codes

Таблица 5. Оценка на $d(k, n)$ для СД-кода на основе остаточных кодов

$d^r(k,n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	6	5	5	4	3	2	1	1	1	1	1		
	14	14	7	6	6	6	4	3	2	1	1	1	1	1	1	
	15	15	7	7	7	7	5	3	3	1	1	1	1	1	1	1

2.4. На основе тензорного произведения кодов

Напомним, что тензорным произведением $[n_1, k_1, d_1]_q$-кода C_1 и $[n_2, k_2, d_2]_q$-кода C_2 называется $[n_1 n_2, k_1 k_2, d_1 d_2]_q$-код вида $C_1 \otimes C_2 = \mathcal{L}(\{\mathbf{c}^1 \otimes \mathbf{c}^2 : \mathbf{c}^i \in C_i, i = 1, 2\})$, где $\mathbf{c}^1 \otimes \mathbf{c}^2 = (c_1^1 \mathbf{c}^2, ..., c_{n_1}^1 \mathbf{c}^2)$ [10].

Утверждение 13. *Если C_1 и C_2 – СД-коды, то $C_1 \otimes C_2$ – СД-код.*

Доказательство. Из определения тензорного произведения и условия утверждения вытекает, что $\mathbf{1}_{n_1} \otimes \mathbf{1}_{n_2} = \mathbf{1}_{n_1 n_2} \in C_1 \otimes C_2$, следовательно $C_1 \otimes C_2$ – СД-код. □

Способ получения нижней оценки $d^t(k, n)$ для $d(k, n)$ на основе тензорного произведения состоит в выполнении следующих шагов: 1) для каждой пары кодов (C_1, C_2), где C_i – самодополнительный

$[n_i, k_i, d(k_i, n_i)]$-код, $i = 1, 2$, $n_1 \cdot n_2 = n$, $k_1 \cdot k_2 = k$, вычислить $d = d(k_1, n_1) \cdot d(k_2, n_2)$, 2) среди этих пар выбрать пару с максимальным значением d, которое будет нижней оценкой $D^t(k, n)$.

Отметим, что для простого числа n найти нижнюю оценку $D^t(k, n)$ описанным выше способом не удается. В таблице 6 найдено $D^t(k, n)$ для СД-кодов длины $n = 14, 15$, получающихся тензорным произведением СД-кодов.

Table 6. The maximum code distance for self-complementary codes of length $n = 14, 15$ obtained by the tensor product of self-complementary codes

Таблица 6. Максимальное кодовое расстояние для СД-кодов длины $n = 14, 15$, получающихся тензорным произведением СД-кодов

$D^t(k, n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	14	14	7	6	6	4	3	2	3	–	2	–	1	–	1	
	15	15	6	6	3	3	2	–	1	2	1	–	1	–	–	1

Снова, применяя утверждение 5 и учитывая неравенство $d(k, n) > 0$, на основе найденных $D^t(k, n)$ получим нижнюю оценку $d^t(k, n)$ для $d(k, n)$ при $n = 13, 14, 15$ (см. таблицу 7).

Table 7. Lower bound on $d(k, n)$ for an self-complementary code based on the tensor product of codes

Таблица 7. Оценка на $d(k, n)$ для СД-кода на основе тензорного произведения кодов

$d^t(k, n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	5	5	3	2	2	2	1	1	1	1	1		
	14	14	7	6	6	4	3	3	3	2	2	1	1	1	1	
	15	15	7	6	6	4	3	3	3	2	2	1	1	1	1	1

В таблице 8 приведена оценка $d^{curt}(k, n)$, построенная на основе $d^c(k, n)$, $d^u(k, n)$, $d^r(k, n)$, $d^t(k, n)$:

$$d^{curt}(k, n) = \max\{d^c(k, n), d^u(k, n), d^r(k, n), d^t(k, n)\}.$$

Верхний индекс показывает, с помощью какой из трех оценок получена итоговая оценка. В частности, индекс i, ij или ijl, где $i, j, l \in \{c, u, r, t\}$, указывает на то, что эта оценка получена соответственно только с помощью одной оценки $d^i(k, n)$, с помощью одной из двух оценок: $d^i(k, n)$ и $d^j(k, n)$, – или может быть получена с помощью одной из трех оценок: $d^i(k, n)$, $d^j(k, n)$ или $d^l(k, n)$. Значения без верхнего индекса могут быть получены с помощью всех четырех оценок. Как видно из таблицы 8, для $n = 13, 14, 15$ нет значений, которые могли бы быть получены только с помощью $d^t(k, n)$.

Table 8. Bound on $d(k, n)$ based on $d^c(k, n)$, $d^u(k, n)$, $d^r(k, n)$, $d^l(k, n)$

Таблица 8. Нижняя оценка $d(k, n)$ для СД-кода на основе оценок $d^c(k, n)$, $d^u(k, n)$, $d^r(k, n)$, $d^l(k, n)$

$d^{curt}(k, n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	6^r	5	5^{cur}	4^r	3^{cur}	3^u	2^u	1	1	1	1		
	14	14	7	6	6	6^{cur}	4^{cur}	4^{cu}	4^u	3^u	2^{cu}	2^{cu}	2^{cu}	2^{cu}	1	
	15	15	7	7^{cr}	7^{cr}	7^{cr}	5^{cr}	5^c	4^{cu}	4^c	2^{cu}	2^{cu}	2^{cu}	2^{cu}	1	1

3. Построение СД-кодов с параметрами $[n, k, d(k, n)]$, $n = 13, 14, 15$

В таблице 9 приведены найденные в работе значения $d(k, n)$ для $n = 13, 14, 15$. Звездочкой помечены значения $d(k, n) \neq d^{curt}(k, n)$; отметим, что в этих случаях $d(k, n) = d^{curt}(k, n) + 1$. Примеры порождающих матриц соответствующих СД-кодов приведены в приложении.

Table 9. $d(k, n)$ for self-complementary code, $n = 13, 14, 15$

Таблица 9. $d(k, n)$ для СД-кода при $n = 13, 14, 15$

$d(k, n)$		k														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
n	13	13	6	6	5	5	4	4^*	3	2	2^*	2^*	1	1		
	14	14	7	6	6	6	5^*	4	4	3	2	2	2	2	1	
	15	15	7	7	7	7	5	5	4	4	3^*	3^*	2	2	1	1

Отметим, что случаи $k = 1, 2, n$ являются тривиальными с точки зрения нахождения $d(k, n)$ и построения порождающих матриц. Значения $d(k, n)$ для $k > 2$ находятся последовательно. Сначала рассмотрим случай $n = 13$. Отметим, что $d(3, 13) \leqslant 6$, при этом $d^{curt}(3, 13) = 6$ (см. таблицу 8), следовательно самодополнительный $[13, 3, 6]$-код может быть построен с помощью одного из рассмотренных методов (именно с помощью метода на основе остаточных классов). Покажем, что не существует самодополнительного $[13, 4, 6]$-кода. Пусть такой код C существует. Рассмотрим вектор $\mathbf{g} \in C$, $\mathrm{wt}(\mathbf{g}) = 6$, тогда в соответствии с теоремой 1 и утверждением 3, код $res(C, \mathbf{g} + \mathbf{1}_{13})$ является самодополнительным $[6, 3, 3]$-кодом. Однако такого СД-кода, как следует из [9], не существует. Следовательно $d(4, 13) \leqslant 5$, и код с расстоянием 5 может быть построен любым из рассмотренных способов. Более того, любым из рассмотренных способом, кроме способа на основе тензорного произведения, может быть построен самодополнительный $[13, 5, 5]$-код. Покажем, что не существует самодополнительного $[13, 6, 5]$-кода. Если бы такой код C существовал, то существовал бы линейный $[12, 5, d' \geqslant 5]$-код, получаемый из C укорочением на единицу (см. [10]). Однако такого кода не существует, как следует из [14]. Самодополнительный $[13, 6, 4]$-код может быть получен с помощью метода на основе остаточных кодов. В [9] показано существование самодополнительного $[12, 7, 4]$-кода. Тогда в соответствии с утверждением 4, может быть построен самодополнительный $[13, 7, 4]$-код, путем приписывания к порождающей матрице $[12, 7, 4]$-кода в систематическом виде столбца с нечетным числом единиц. Отметим, что ни один из рассмотренных способов не позволяет построить самодополнительный $[13, 7, 4]$-код. Путем проверки условий утверждения 7 доказано, что самодополнительных $[13, 8, 4]$-кода и $[13, 9, 3]$-кода не существует. При этом самодополнительные $[13, 8, 3]$-код и $[13, 9, 2]$-код могут быть получены с помощью $(u|u + v)$-конструкции. В [9] приведены примеры самодополнительных $[12, 10, 2]$-кода и $[12, 11, 2]$-кода, поэтому на их основе построены самодополнительные $[13, 10, 2]$-код и $[13, 11, 2]$-код. Снова отметим, что коды с такими параметрами не удалось построить с помощью рассмотренных методов. Из следствия 1 вытекает, что СД-кода с параметрами $[13, 12, 2]$ не существует.

Теперь рассмотрим случай $n = 14$. Для доказательства того, что не существует $[14, 3, 7]$-кода воспользуемся следующим свойством веса Хэмминга в пространстве над полем $\mathbb{F}_2$: $\mathrm{wt}(\mathbf{a} + \mathbf{b}) = \mathrm{wt}(\mathbf{a}) + \mathrm{wt}(\mathbf{b}) - 2|\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{b})|$. В коде $[14, 3, 7]$-коде все ненулевые векторы, кроме $\mathbf{1}_{14}$, должны иметь вес 7. Из приведенного свойства вытекает, что сумма любых векторов веса 7 должна давать вектор четного веса. Следовательно, любая пара векторов веса 7 должна в сумме давать вектор $\mathbf{1}_{14}$. Однако в предполагаемом коде должно быть 6 векторов веса 7, поэтому среди них найдется пара, сумма которых не равна $\mathbf{1}_{14}$. Следовательно, в коде должен быть вектор четного веса, отличающийся от $\mathbf{1}_{14}$. Пришли к противоречию, поэтому самодополнительного $[14, 3, 7]$-кода не существует. В то

же время $[14, 3, 6]$-код, $[14, 4, 6]$-код и $[14, 5, 6]$-код могут быть построены любым одним из рассмотренных способов. СД-кода с параметрами $[14, 6, 6]$ не существует, так как не выполняется граница Грея-Рэнкина (1), а существование СД-кода с параметрами $[14, 6, 5]$ доказывается путем построения порождающей матрицы, для которой выполняются условия утверждения 7 (в то время, как ни один из рассмотренных способов не позволяет построить код с такими параметрами). С помощью конструктивной проверки условий утверждения 7 показано, что не существует СД-кодов с параметрами $[14, 6, 5]$, $[14, 9, 4]$ и $[14, 10, 3]$. При этом СД-коды с параметрами $[14, 7, 4]$, $[14, 8, 4]$, $[14, 9, 3]$, $[14, 10, 2]$, $[14, 11, 2]$, $[14, 12, 2]$ и $[14, 13, 2]$ получены с помощью одного из рассмотренных способов.

Рассмотрим случай $n = 15$. Так как $d(k, 15) \leqslant 7$, то для $k = 3, 4, 5$ некоторые из рассмотренных конструкций (см. таблицу 8) позволяют построить СД-коды с максимально возможным кодовым расстоянием. СД-кода с параметрами $[15, 6, 7]$ не существует, так как не выполняется граница (1).

Утверждение 14. *Не существует самодополнительного* $[15, 6, 6]$*-кода.*

Доказательство. Предположим, что такой код C существует. Возможны два варианта: 1) ненулевые векторы имеют вес 6, 7, 8, 9, 15; 2) ненулевые векторы имеют вес 6, 9, 15. Сначала покажем, что кода с весами из первого варианта не существует. Пусть $\mathbf{g} \in C$ и $\mathrm{wt}(\mathbf{g}) = 7$. Тогда, в соответствии с теоремой 1 и утверждением 3 код $res(C, \mathbf{g})$ — СД-код с параметрами $[8, 5, d' \geqslant 3]$. Однако такого СД-кода, как вытекает из результатов работы [9], не существует.

Теперь покажем, что не существует СД-кода с весами из второго варианта. Отметим, что для доказательства не удается применить теорему 1 и утверждение 3, так как получающиеся параметры остаточных СД-кодов не противоречат весам из второго варианта. Для предполагаемого кода с весами из второго варианта нумератор весов, учитывая утверждение 1, будет иметь вид: $W_C(x, y) = y^{15} + 31x^6y^9 + 31x^9y^6 + x^{15}$. Пусть B_i — количество векторов веса i в коде $C^{\perp}$. Воспользовавшись тождеством Мак-Вильямс (2) и учитывая, что в коде, дуальном к СД-коду, все ненулевые векторы имеют четный вес (см. утверждение 2), получим:

$$\begin{aligned} y^{15} + 31x^6y^9 + 31x^9y^6 + x^{15} &= 512^{-1}\Sigma_{i=0}^{15} B_i(y-x)^i(x+y)^{15-i} = \\ &= 512^{-1}\big((x+y)^{15} + B_2(y-x)^2(x+y)^{13} + B_4(y-x)^4(x+y)^{11} + B_6(y-x)^6(x+y)^9 + \\ &+ B_8(y-x)^8(x+y)^7 + B_{10}(y-x)^{10}(x+y)^5 + B_{12}(y-x)^{12}(x+y)^3 + B_{14}(y-x)^{14}(x+y)\big). \end{aligned}$$

Приравнивая в левой и правой частях коэффициенты при одинаковых термах x^iy^j, $i, j = 0, ..., 15$, получим систему уравнений, которая не имеет решения относительно $B_2, B_4, ..., B_{14} \in \mathbb{N} \cup \{0\}$. Следовательно, СД-кода с параметрами $[15, 6, 6]$ не существует. □

СД-коды с параметрами $[15, 6, 5]$ и $[15, 7, 5]$ могут быть построены с помощью одного из рассмотренных способов. Из таблицы на стр. 47 работы [14] вытекает, что не существует линейного $[15, 8, 5]$-кода, следовательно, и СД-кода не существует. Самодополнительные коды $[15, 8, 4]$ и $[15, 9, 4]$ найдены с помощью одного из рассмотренных методов. С помощью проверки условий утверждения 3 показано, что не существует $[15, 10, 4]$-кода, при этом показано существование самодополнительных $[15, 10, 3]$-кода и $[15, 11, 3]$-кода (применение рассмотренных методов не позволило построить коды с такими параметрами). Так как не существует линейного $[15, 12, 3]$-кода (см. стр. 47 в [14]), поэтому не существует и СД-кода с такими параметрами. СД-коды с параметрами $[15, 12, 2]$ и $[15, 13, 2]$ найдены с помощью одного из рассмотренных методов. СД-кода с параметрами $[15, 14, 2]$ не существует в соответствии со следствием 1.

В общем случае, при нахождении $d(k, n)$ может использоваться следующая последовательность проверок, которая в ряде случаев позволяет доказать отсутствие самодополнительного $[n, k, d]$-кода:

1. *Проверка на основе границы Грея-Рэнкина (см. формула (1)).* Если для (n, k, d) не выполняется граница Грея-Рэнкина (1), то СД-кода с параметрами $[n, k, d]$ не существует.

2. *Проверка на основе известных результатов для СД-кодов (см. утверждения 3,5 и следствие 1).* Если $d(k,n)$ известно и $d(k,n) < d$, или $d(k,n-1) < d-1$, или $d(k-1,n) < d$, то СД-кода с параметрами $[n,k,d]$ не существует; если не существует СД-кода с параметрами $[n-d, k-1, d' \geqslant d - \lfloor d/2 \rfloor]$ или СД-кода с параметрами $[d, k-1, d' \geqslant d - \lfloor (n-d)/2 \rfloor]$, то СД-кода с параметрами $[n,k,d]$ не существует (значения $d(k,n)$ для $n \leqslant 12$ можно найти в [9], а значения при $n = 13, 14, 15$ — в настоящей работе).
3. *Проверка на основе известных результатов для линейных кодов (см. утверждение 6).* Если не существует линейного $[n,k,d]$-кода, то СД-кода с параметрами $[n,k,d]$ не существует; если не существует линейного $[n-1, k-1, d' \geqslant d]$-кода, то СД-кода с параметрами $[n,k,d]$ не существует (такие проверки могут выполняться на основе известных результатов для линейных кодов, например, взятых из [14]).
4. *Проверка на основе тождества Мак-Вильямс (см. утверждение 2 и способ доказательства утверждения 14).* Если для $w = d+1, ..., n-(d+1)$ не существует самодополнительного $[n-w, k-1, d-\lfloor w/2 \rfloor]$-кода, при этом система уравнений, составленная по тождеству

$$y^n + (2^{k-1}-1)(x^d y^{n-d} + x^{n-d} y^d) + x^n = 2^{k-n} \Sigma_{i=0}^{n} B_i (y-x)^i (x+y)^{n-i}$$

относительно неизвестных B_i, где $B_i = 0$ для нечетных i, не имеет решения во множестве целых неотрицательных чисел, то СД-кода с параметрами $[n,k,d]$ не существует.

В настоящей работе, если ни одна из указанных проверок не позволяла отвергнуть существование СД-кода с параметрами $[n,k,d]$, предпринималась попытка построения $k \times (n-k)$-матрицы P, удовлетворяющей условиям утверждения 7. В ряде случаев удавалось такую матрицу построить, что доказывало существование СД-кода с параметрами $[n,k,d]$, а в других случаях такую матрицу построить было невозможно, что доказывало обратное. Однако заметим, что построение матрицы P, удовлетворяющей условиям утверждения 7 имеет неполиномиальную сложность по k, что ограничивает применение этого способа при больших k.

4. Новая стегоконструкция на основе СД-кодов

В комбинаторной стеганографии задача сокрытия сообщения $\mathbf{m} \in \mathbb{F}_2^L$ в векторе $X \in \mathbb{F}_2^N$, $L \leqslant N$, заключается в построении таких преобразований (E, D), $E : \mathbb{F}_2^L \times \mathbb{F}_2^N \longrightarrow \mathbb{F}_2^N$, $D : \mathbb{F}_2^N \longrightarrow \mathbb{F}_2^L$, что, с одной стороны, $D(E(\mathbf{m}, X)) = \mathbf{m}$, а с другой стороны, расстояние Хэмминга $\rho(X, Z)$ между X и $Z = E(\mathbf{m}, X)$ было как можно меньше. Величина $e = L/\rho(X,Z)$ называется эффективностью сокрытия, а векторы X и Z — контейнером и стегоконтейнером соответственно. В [4] строится стегосистема, устойчивая к ошибкам в стегоконтейнере. В настоящей работе рассматривается одна модификация этой системы. Для ее описания рассмотрим контейнер $X (\in \mathbb{F}_2^N)$, $N = n2^r$, представимый в виде матрицы:

$$\begin{bmatrix} x_{1,1} & x_{2,1} & \dots & x_{n,1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,2^r-1} & x_{2,2^r-1} & \dots & x_{n,2^r-1} \\ x_{1,2^r} & x_{2,2^r} & \dots & x_{n,2^r} \end{bmatrix} = \begin{bmatrix} \mathbf{x}_1^T & \mathbf{x}_2^T & \dots & \mathbf{x}_n^T \\ x_{1,2^r} & x_{2,2^r} & \dots & x_{n,2^r} \end{bmatrix}. \tag{7}$$

Для контейнера вида (7) предлагается образовать два стегоканала, а информационное сообщение $\mathbf{m}$ разбить на две части: $\mathbf{m}_1 \in \mathbb{F}_2^k$ и $\mathbf{m}_2 \in \mathbb{F}_{2^r}^K$, $K = \lceil (L-k)/r \rceil$. В первый стегоканал вкладывается вектор $\mathbf{c}_1 \in \mathbb{F}_2^m$, представляющий собой закодированную часть $\mathbf{m}_1$, а во второй – вектор $\mathbf{c}_2 \in \mathbb{F}_{2^r}^M$, представляющий закодированную часть $\mathbf{m}_2$, $M = \lceil \frac{n}{2} \rceil$.

Первый стегоканал для удобства назовем *каналом сумм.* Он представляет собой вектор $\mathbf{y} = (y_1, \dots, y_n)$, $y_i = \oplus_{j=1}^{2^r} x_{i,j}$ для всех $i = 1, ..., n$. Вложение $\mathbf{c}_1 = (c_{1,1}, ..., c_{1,n})$ в канал сумм осуществляется путем инвертирования одного любого бита в i-ом столбце матрицы (7), если $c_{1,i} \neq y_i$. Обозначим через τ множество номеров координат y_i, которые необходимо изменить для вложения $\mathbf{c}_1$ в $\mathbf{y}$:

$\tau = \{i \in \{1, \dots, n\} : c_{1,i} \neq y_i\}$, $|\tau| = \mu$. Информационное сообщение $\mathbf{m}_1 = (m_{1,1}, \dots, m_{1,k})$ может быть вложено в канал сумм следующим образом. Рассмотрим самодополнительный $[n, k+1, d]$-код C_{sum}. Порождающая матрица кода C_{sum} может быть представлена в следующем виде: $G = [\tilde{G}^T | \mathbf{1}_n^T]^T$. Для вложения $\mathbf{m}_1$ необходимо сформировать кодовый вектор $\mathbf{c}_1 = \mathbf{m}_1 \tilde{G}$ и определить величину μ. В том случае, если $\mu \geqslant M$, в канал сумм вкладывается вектор $\mathbf{c}_1$. В противном случае в канал сумм вкладывается вектор $\mathbf{c}_1 + \mathbf{1}_n$. Конкретные биты, которые нужно изменить для вложения информации в канал сумм, определяются при дальнейшем процессе вложения. Множество τ и величина M также используются в дальнейшем процессе вложения.

Второй стегоканал, в точности как в [4], образуется из векторов $\mathbf{x}_1$,...,$\mathbf{x}_n$ с помощью проверочной матрицы H для $[2^r - 1, 2^r - r - 1, 3]_2$-кода Хэмминга. Так как радиус покрытия кода Хэмминга равен единице, то для любого вектора $\mathbf{s}_i (\in \mathbb{F}_2^r)$ найдется такой вектор $\mathbf{e}_i$ веса Хэмминга не более 1, что $H(\mathbf{x}_i + \mathbf{e}_i)^T = \mathbf{s}_i^T$. Иными словами, изменив значение не более чем одного бита в векторе $\mathbf{x}_i$, можно получить любой наперед заданный синдром $\mathbf{s}_i$. Это используется для вложения сообщения во второй стегоканал, называемый далее *каналом векторов*. Контейнером во втором канале является последовательность синдромов $\mathbf{s}_i$, рассматриваемых как элементы поля $\mathbb{F}_{2^r}$. Для получения нужного синдрома достаточно внести одно изменение в исходный вектор $\mathbf{x}_i$. При этом допускается изменение только тех $\mathbf{x}_i$, для которых $i \in \tau$. В случае, если $i \in \tau$, но вектор $\mathbf{x}_i$ требуется оставить без изменений, поскольку его синдром уже имеет необходимое значение, производится инверсия бита $x_{i,2^r}$ в контейнере вида (7). Для вложения информационного сообщения $\mathbf{m}_2 = (m_{2,1}, \dots, m_{2,l})$ стороны согласовывают (например, с помощью генератора псевдослучайных чисел) $(M \times n)$-матрицу Вандермонда D с элементами из поля $\mathbb{F}_{2^r}$ и порождающую матрицу G_{vec} $[M, l]_{2^r}$-кода C_{vec} в проективной метрике, порожденной матрицей D. После этого вычисляется стегоконтейнер $\mathbf{z}$, который должен удовлетворять соотношению: $D\mathbf{z}^T = (\mathbf{m}_2 G_{\text{vec}})^T$. На этом процесс вложения завершается.

Величины d и l выбираются из соображений помехоустойчивости стегосистемы: для исправления t ошибок и v стираний в стегоконтейнере необходимо, чтобы выполнялись условия: $v + 2t < d$, $v + t \leqslant M - l$. Также для построения кода в проективной метрике должно выполняться соотношение $n + l \leqslant 2^r$. Объем вкладываемой в контейнер вида (7) информации составляет $L = k + (\lceil n/2 \rceil - (t+v))r$ битов, а количество изменяемых бит равно $T \approx n/2(1 + \sqrt{2(\pi n)^{-1}})$ (см. формулу (12) в [4]). Эффективность сокрытия при этом составляет

$$e = \frac{L}{T} \approx \frac{k + (\lceil n/2 \rceil - (t+v))r}{n/2 + \sqrt{(n/2\pi)}} \approx \left(\frac{2k}{n} + r\right) \cdot \left(1 - \sqrt{\frac{2}{\pi n}} + \frac{2}{\pi n}\right) - \frac{2r(t+v)}{n}.$$

Число исправляемых ошибок t в стегоконтейнере, расчетная эффективность сокрытия e, размер N контейнера (в битах) и размер L вкладываемого сообщения (в битах) для стегосистемы с использованием параметров СД-кодов из таблицы 9 приведены в таблице 10. Для всех стегосистем полагается $r = 5$, $v = 0$. Серым выделены те наборы параметров, при которых достигается наибольший объем L вкладываемой информации (и соответственно наибольшая эффективность e сокрытия) для фиксированных t и N. Для $t = 2$ и $N = 480$ разработанная в [4] конструкция обеспечивает эффективность $e \approx 3,75$ при $L = 34$ (см. таблицу 1 в [4]). Из таблицы 10 видно, что предложенная в настоящей работе модификация при тех же (t, N) обеспечит бóльшую эффективность с помощью СД-кодов с параметрами $[15, 6, 5]$ и $[15, 7, 5]$.

Table 10. Characteristics of the (t, e, N, L) stegoconstruction from [4] based on the self-complementary code C_{sum} with parameters $[n, k+1, d(k+1, n)]$, $t = \lfloor (d-1)/2 \rfloor$

n	$k+1$	t	e	N	L
13	6	1	4,3935	416	35
13	7	1	4,5190	416	36
13	8	1	4,6446	416	37
14	7	1	4,2521	448	36
14	8	1	4,3703	448	37
14	9	1	4,4884	448	38
15	8	1	4,6301	480	42
15	9	1	4,7404	480	43
15	10	1	4,8506	480	44
15	11	1	4,9608	480	45
13	2	2	3,2637	416	26
13	3	2	3,3893	416	27
13	4	2	3,5148	416	28
13	5	2	3,6403	416	29
14	3	2	3,1891	448	27
14	4	2	3,3072	448	28
14	5	2	3,4253	448	29
14	6	2	3,5435	448	30
15	6	2	3,8584	480	35
15	7	2	3,9687	480	36
14	2	3	2,4804	448	21
15	2	3	2,8663	480	26
15	3	3	2,9765	480	27
15	4	3	3,0867	480	28
15	5	3	3,1970	480	29

Таблица 10. Характеристики (t, e, N, L) стегоконструкции из [4] на основе СД-кода C_{sum} с параметрами $[n, k+1, d(k+1, n)]$, $t = \lfloor (d-1)/2 \rfloor$

Приложение. Примеры порождающих матриц самодополнительных $[n, k, d(k, n)]$-кодов, $n = 13, 14, 15$

Ниже приводятся примеры порождающих матриц СД-кодов, для которых кодовое расстояние равно $d(k, n)$ при $n = 13, 14, 15$, $k = 3, \ldots, n$. Порождающие матрицы для $k = 1, 2$ не приводятся в силу их тривиальности. Выше каждой матрицы указана размерность порождаемого ею СД-кода, а соответствующие кодовые расстояния указаны в таблице 9.

Случай $n = 13$:

$k = 3$

$$\begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&0&0&0&0&0&0&0\\1&1&1&0&0&0&1&1&1&0&0&0&0\end{matrix},$$

$k = 4$

$$\begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&0&0&0&0&0&0\\1&1&1&0&0&0&1&1&1&0&0&0&0\\1&1&0&0&1&1&0&0&1&1&0&0&1\end{matrix},$$

$k = 5$

$$\begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&0&0&0&0&0&0&0\\1&1&1&0&0&0&1&1&1&0&0&0&0\\1&1&0&0&1&1&0&0&1&1&0&0&1\\1&0&0&1&1&0&1&0&0&1&0&1&0\end{matrix},$$

$k = 6$

$$\begin{matrix}1&0&0&1&0&0&0&0&0&1&1&0&0\\0&1&0&1&0&0&0&0&0&1&0&1&1\\0&0&1&1&0&0&0&0&0&0&1&1&0\\0&0&0&0&1&0&0&1&0&1&1&0&1\\0&0&0&0&0&1&0&1&0&1&0&1&0\\0&0&0&0&0&0&1&1&1&1&0&0&1\end{matrix},$$

$k = 7$

$$\begin{matrix}1&0&0&1&0&0&0&0&0&1&1&0&0\\0&1&0&1&0&0&0&0&0&1&0&1&1\\0&0&1&1&0&0&0&0&0&0&1&1&0\\0&0&0&0&1&0&0&1&0&1&1&0&1\\0&0&0&0&0&1&0&1&0&1&0&1&0\\0&0&0&0&0&0&1&1&1&0&0&1&1\\0&0&0&0&0&0&0&0&1&1&1&1&0\end{matrix},$$

$k = 8$

$$\begin{matrix}1&0&0&0&0&0&0&0&0&1&1&1&1\\0&1&0&0&0&0&0&0&1&0&1&0&0\\0&0&1&0&0&0&0&0&0&1&1&0&0\\0&0&0&1&0&0&0&0&1&1&1&1&1\\0&0&0&0&1&0&0&0&1&0&0&1&0\\0&0&0&0&0&1&0&0&0&1&0&1&1\\0&0&0&0&0&0&1&0&0&0&1&1&0\\0&0&0&0&0&0&0&1&1&1&1&0&0\end{matrix},$$

$k = 9$

$$\begin{matrix}1&0&0&0&0&0&0&0&0&0&0&1&1\\0&1&0&0&0&0&0&0&0&0&0&1&1\\0&0&1&0&0&0&0&0&0&1&0&0&1\\0&0&0&1&0&0&0&0&0&0&1&0&1\\0&0&0&0&1&0&0&0&0&0&1&0&1\\0&0&0&0&0&1&0&0&0&0&1&0&1\\0&0&0&0&0&0&1&0&0&0&1&0&1\\0&0&0&0&0&0&0&1&0&0&1&0&1\\0&0&0&0&0&0&0&0&1&0&0&1&1\end{matrix},$$

$k = 10$

$$\begin{matrix}1&0&0&0&0&0&0&0&0&0&0&1&1\\0&1&0&0&0&0&0&0&0&0&0&1&1\\0&0&1&0&0&0&0&0&0&0&1&0&0\\0&0&0&1&0&0&0&0&0&0&1&0&1\\0&0&0&0&1&0&0&0&0&0&1&0&1\\0&0&0&0&0&1&0&0&0&1&0&0&0\\0&0&0&0&0&0&1&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0&0&1&0&1\\0&0&0&0&0&0&0&0&1&0&1&0&1\\0&0&0&0&0&0&0&0&0&1&0&1&1\end{matrix},$$

$k = 11$

$$\begin{matrix}1&0&0&0&0&0&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&0&0&0&0&1&0\\0&0&1&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&1&1\\0&0&0&0&0&0&0&0&0&1&1&1&1\end{matrix},$$

$k = 12$

$$\begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&0&0&1&0&1\\0&0&0&0&0&0&0&0&0&0&0&1&1\end{matrix}.$$

Случай $n = 14$:

$$k = 3:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&0&0&0&0&0&0&0&1\\1&1&1&0&0&0&1&1&1&0&0&0&0&1\end{matrix},\quad k = 4:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&0&0&0&0&0&0&0\\1&1&1&0&0&0&1&1&1&0&0&0&0&0\\1&1&0&0&1&1&0&0&1&1&0&0&1&0\end{matrix},\quad k = 5:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&0&0&0&0&0&0&0\\1&1&1&0&0&0&1&1&1&0&0&0&0&0\\1&1&0&0&1&1&0&0&1&1&0&0&1&0\\1&0&0&1&1&0&1&1&1&0&1&1&0&0\end{matrix}$$

$$k = 6:\ \begin{matrix}1&0&0&0&0&0&1&1&1&1&1&1&1&0\\0&1&0&0&0&0&1&1&1&1&0&0&0&1\\0&0&1&0&0&0&1&0&1&1&0&0&1&0\\0&0&0&1&0&0&1&1&0&1&1&0&0&0\\0&0&0&0&1&0&1&0&0&0&1&1&0&1\\0&0&0&0&0&1&0&0&0&1&0&1&1&1\end{matrix},\quad k = 7:\ \begin{matrix}1&0&0&0&0&0&0&1&1&1&1&1&1&1\\0&1&0&0&0&0&0&1&1&1&1&1&0&0\\0&0&1&0&0&0&0&1&1&1&1&0&1&0\\0&0&0&1&0&0&0&1&1&1&0&1&1&0\\0&0&0&0&1&0&0&1&1&0&1&1&1&0\\0&0&0&0&0&1&0&0&1&1&0&0&1&1\\0&0&0&0&0&0&1&0&1&0&1&1&0&1\end{matrix},\quad k = 8:\ \begin{matrix}1&0&0&0&0&0&0&0&1&1&1&1&1&1\\0&1&0&0&0&0&0&0&1&1&1&1&0&0\\0&0&1&0&0&0&0&0&1&1&1&0&1&0\\0&0&0&1&0&0&0&0&1&1&0&1&1&0\\0&0&0&0&1&0&0&0&1&0&1&1&1&0\\0&0&0&0&0&1&0&0&1&0&0&1&1&1\\0&0&0&0&0&0&1&0&0&1&1&0&0&1\\0&0&0&0&0&0&0&1&1&1&0&0&1&0\end{matrix}$$

$$k = 9:\ \begin{matrix}1&0&0&0&0&0&0&0&0&1&1&0&0&0\\0&1&0&0&0&0&0&0&0&0&1&1&0&0\\0&0&1&0&0&0&0&0&0&0&0&1&1&0\\0&0&0&1&0&0&0&0&0&0&0&0&1&1\\0&0&0&0&1&0&0&0&0&1&1&1&0&0\\0&0&0&0&0&1&0&0&0&0&1&1&1&0\\0&0&0&0&0&0&1&0&0&0&0&1&1&1\\0&0&0&0&0&0&0&1&0&1&0&1&0&1\\0&0&0&0&0&0&0&0&1&0&1&1&1&0\end{matrix},\quad k = 1 0:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&0&1\\0&1&0&0&0&0&0&0&0&0&0&0&0&1\\0&0&1&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&1&1&1&0\end{matrix},\quad k = 1 1:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&0&1\\0&1&0&0&0&0&0&0&0&0&0&0&0&1\\0&0&1&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&0&0&0&1&1&1\end{matrix}$$

$$k = 1 2:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&0&1\\0&1&0&0&0&0&0&0&0&0&0&0&0&1\\0&0&1&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&0&0&0&1&0&1\\0&0&0&0&0&0&0&0&0&0&0&0&1&1\end{matrix},\quad k = 1 3:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&0&1\\0&1&0&0&0&0&0&0&0&0&0&0&0&1\\0&0&1&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&0&0&0&1&0&1\\0&0&0&0&0&0&0&0&0&0&0&0&1&1\end{matrix}.$$

Случай $n = 15$:

$$k = 3:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&1&1&1&1&1&1&1&1&0&0&0&0\end{matrix},\quad k = 4:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\0&0&0&1&1&1&1&1&1&1&1&0&0&0&0\\1&0&1&1&1&0&0&1&1&0&0&1&1&0&0\end{matrix},\quad k = 5:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\0&0&0&1&1&1&1&1&1&1&1&0&0&0&0\\1&0&1&1&1&0&0&1&1&0&0&1&1&0&0\\1&0&0&0&1&1&0&0&1&1&0&0&1&1&0\end{matrix}$$

$$k = 6:\ \begin{matrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\0&1&0&0&0&0&0&1&1&1&1&1&0&0&0\\0&0&1&0&0&0&0&1&1&1&0&0&0&1&1\\0&0&0&1&0&0&0&1&1&0&1&0&1&0&1\\0&0&0&0&1&0&0&1&0&0&1&1&0&1&1\\0&0&0&0&0&1&0&0&1&1&1&0&1&1&1\end{matrix},\quad k = 7:\ \begin{matrix}1&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&1&0&0&0&0&0&1&1&1&1&1&0&0&0\\0&0&1&0&0&0&0&1&1&1&0&0&0&1&1\\0&0&0&1&0&0&0&1&1&0&1&0&1&0&1\\0&0&0&0&1&0&0&1&0&0&1&1&0&1&1\\0&0&0&0&0&1&0&0&1&1&1&0&1&1&1\\0&0&0&0&0&0&1&0&0&1&1&1&0&1&1\end{matrix},\quad k = 8:\ \begin{matrix}1&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\0&1&0&0&0&0&0&0&1&1&1&1&0&0&0\\0&0&1&0&0&0&0&0&1&1&1&0&1&0&1\\0&0&0&1&0&0&0&0&1&1&0&1&1&1&1\\0&0&0&0&1&0&0&0&1&0&1&1&1&0&1\\0&0&0&0&0&1&0&0&1&0&0&1&1&1&1\\0&0&0&0&0&0&1&0&0&1&1&0&0&1&1\\0&0&0&0&0&0&0&1&1&1&0&0&1&0&1\end{matrix}$$

$$k = 9:\ \begin{matrix}1&0&0&0&0&0&0&0&0&1&1&1&0&0&0\\0&1&0&0&0&0&0&0&0&0&1&1&0&1&0&0\\0&0&1&0&0&0&0&0&0&1&0&0&1&1&0\\0&0&0&1&0&0&0&0&0&0&1&0&1&1&1\\0&0&0&0&1&0&0&0&0&0&0&1&1&1&1\\0&0&0&0&0&1&0&0&0&1&1&1&0&0&0\\0&0&0&0&0&0&1&0&0&0&1&0&0&1&1\\0&0&0&0&0&0&0&1&0&1&0&1&1&0&1\\0&0&0&0&0&0&0&0&1&0&1&1&1&1&1\end{matrix},\quad k = 1 0:\ \begin{matrix}1&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&1&0&1&0&0\\0&0&1&0&0&0&0&0&0&0&1&0&0&1&0\\0&0&0&1&0&0&0&0&0&0&0&1&0&0&1\\0&0&0&0&1&0&0&0&0&1&1&1&0&0&0\\0&0&0&0&0&1&0&0&0&1&1&0&0&1&1\\0&0&0&0&0&0&1&0&0&0&1&0&1&0&1\\0&0&0&0&0&0&0&1&0&1&0&1&1&1&1\\0&0&0&0&0&0&0&0&1&0&1&1&1&0&1\end{matrix},\quad k = 1 1:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0\\0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1\\0&0&0&0&1&0&0&0&0&0&1&1&1&0&1&0\\0&0&0&0&0&1&0&0&0&0&1&1&0&0&1&1\\0&0&0&0&0&0&1&0&0&0&1&0&1&0&1&0\\0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&1\\0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0\\0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&1\end{matrix}$$

$$k = 1 2:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\0&1&0&0&0&0&0&0&0&0&0&0&0&1&0\\0&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&0&0&1&0&0\\0&0&0&0&0&0&0&0&0&0&1&0&0&1&0\\0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\end{matrix},\quad k = 1 3:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\0&1&0&0&0&0&0&0&0&0&0&0&0&1&0\\0&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&0&0&1&0&0\\0&0&0&0&0&0&0&0&0&0&1&0&0&1&0\\0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\end{matrix},\quad k = 1 4:\ \begin{matrix}1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\end{matrix}$$

References

[1] D. Jungnickel and V. D. Tonchev, "The classification of antipodal two-weight linear codes", *Finite Fields and Their Applications*, vol. 50, pp. 372–381, 2018. DOI: https://doi.org/10.1016/j.ffa.2017.12.010.

[2] T. Klove and S. Yari, "Proper self-complementary codes", in *Proceedings of the 2010 International Symposium On Information Theory & Its Applications*, 2010, pp. 118–122. DOI: 10.1109/ISITA.2010.5649432.

[3] E. M. Gabidulin and M. Bossert, "Codes Resistant to the Phase Rotation", in *Proceedings of the 4-th Simposium on Communication and Applications*, 1997, pp. 65–84.

[4] Y. V. Kosolapov and F. S. Pevnev, "Error-tolerant ZZW-construction", *Siberian Electronic Mathematical Reports*, vol. 18, no. 2, pp. 1506–1516, 2021.

[5] L. D. Grey, "Some bounds for error-correcting codes", *IRE Transactions on Information Theory*, vol. 8, no. 3, pp. 200–202, 1962.

[6] G. McGuire, "Quasi-Symmetric Designs and Codes Meeting the Grey–Rankin Bound", *Journal of Combinatorial Theory, Series A*, vol. 78, no. 2, pp. 280–291, 1997. DOI: https://doi.org/10.1006/jcta.1997.2765.

[7] I. Bouyukliev, S. Bouyuklieva, and S. Dodunekov, "On binary self-complementary [120, 9, 56] codes having an automorphism of order 3 and associated SDP designs", *Problems of Information Transmission*, vol. 43, pp. 89–96, 2007. DOI: https://doi.org/10.1134/S0032946007010020.

[8] S. Dodunekov, S. Encheva, and S. Kapralov, "On the [28, 7, 12] binary self-complementary codes and their residuals", *Designs, Codes and Cryptography*, vol. 4, pp. 57–67, 1994. DOI: https://doi.org/10.1007/BF01388560.

[9] I. Asemota, *Binary Self-Complementary Codes*. B. Sc., Benson Idahosa University, Nigeri, 2016.

[10] R. H. Morelos-Zaragoza, *The Art of Error Correcting Coding, 2nd Edition*. Wiley, 2006.

[11] R. Hill and D. Newton, "Optimal ternary linear codes", in, vol. 2, 1992, pp. 137–157. DOI: https://doi.org/10.1007/BF00124893.

[12] M. Tomlinson, C. J. Tjhai, M. A. Ambroze, M. Ahmed, and M. Jibril, *Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications*. Springer Nature, 2017.

[13] V. M. Deundyak, A. E. Maevskij, and M. N. C., *Metody pomekhoustojchivoj zashchity dannyh*. Rostov-na-Donu: Izdatelstvo yuzhnogo federalnogo universiteta, 2014, in Russian.

[14] D. B. Jaffe, *Binary Linear Codes: New Results on Nonexistence*, 1996. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.44.628&rep=rep1&type=pdf.