ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391.1 : 519.725

© 2021 г. **В.А. Зиновьев, Д.В. Зиновьев**

ОБ ОБОБЩЕННОЙ КАСКАДНОЙ КОНСТРУКЦИИ КОДА НОРДСТРОМА – РОБИНСОНА И ДВОИЧНОГО КОДА ГОЛЕЯ[1]

Показано, что код Нордстрома – Робинсона и двоичный расширенный код Голея являются обобщенными каскадными кодами третьего порядка.

Ключевые слова: обобщенный каскадный код, код Нордстрома – Робинсона, двоичный расширенный код Голея.

DOI: 10.31857/S0555292321040033

§ 1. Введение

Пусть $E_q = \{0, 1, \ldots, q-1\}$ – алфавит размера q. Произвольное подмножество $C \subseteq E_q^n$ называется q-ичным кодом и обозначается через $(n, N, d)_q$, где n – длина кода, N – число его кодовых слов (или мощность), и d – его минимальное расстояние (Хэмминга). Линейный код C с параметрами $(n, N = q^k, d)_q$ обозначается через $[n, k, d]_q$. Для двоичных кодов приняты обозначения (n, N, d) и $[n, k, d]$ (т.е. q опускается). Пусть $J = \{1, 2, \ldots, n\}$ – координатное множество E_q^n. Для вектора $\boldsymbol{x} = (x_1, \ldots, x_n) \in E_q^n$ обозначим через $\operatorname{supp}(\boldsymbol{x})$ его носитель, т.е.

$$\operatorname{supp}(\boldsymbol{x}) = \{i \in J : \ x_i \neq 0\}.$$

Обозначим через $\operatorname{wt}(\boldsymbol{x})$ вес вектора $\boldsymbol{x}$, т.е. размер его носителя: $\operatorname{wt}(\boldsymbol{x}) = |\operatorname{supp}(\boldsymbol{x})|$. Для двоичного вектора $\boldsymbol{x}$ обозначим через $\bar{\boldsymbol{x}}$ дополнительный к нему вектор, т.е. вектор, полученный из $\boldsymbol{x}$ взаимной заменой элементов 0 и 1: $\bar{\boldsymbol{x}} = \boldsymbol{x} + (1, 1, \ldots, 1)$.

Нелинейный код Нордстрома – Робинсона с параметрами

$$n = 16, \quad N = 2^8, \quad d = 6$$

был построен в 1968 г. Нордстромом и Робинсоном [1] и независимо в [2]. Двоичный расширенный совершенный код Голея с параметрами

$$n = 24, \quad N = 2^{12}, \quad d = 8$$

был построен в 1949 г. Голеем [3]. По обоим кодам опубликовано очень много работ, значительная часть которых может быть найдена в монографии [4]. В частности, в [5] установлено, что код Нордстрома – Робинсона и двоичный код Голея единственны с точностью до эквивалентности. Это существенно упрощает нашу задачу (а именно достаточно построить ОК-коды с параметрами этих кодов). Мы только

[1] Работа выполнена в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364) и Национального научного фонда Болгарии (номер проекта 20-51-18002).

еще сошлемся на некоторые более поздние статьи, в основном по коду Нордстрома – Робинсона, в связи с полученными там интересными результатами (см. работы [6–12] и библиографию в них). Отметим, что в [13] (см. библиографию) было дано представление кода Голея как каскадного кода, полученного отображением из построенного в [13] кода длины 12 над $\mathbb{F}_4$ в двоичный код.

§ 2. Построение кода Нордстрома – Робинсона

Пусть B обозначает тривиальный $(4, 16, 1)$-код (т.е. все двоичные векторы длины 4). Этот код B разбивается на два тривиальных подкода: $(4, 8, 2)$-код B_1 с проверкой на четность и $(4, 8, 2)$-код B_2 с проверкой на нечетность, которые, в свою очередь, разбиваются на тривиальные $(4, 2, 4)$-коды $B_{i,j}$. Эти коды мы приводим вместе с нумерацией их слов (вектор с номером $\boldsymbol{b}(i, j, k)$, $k = 1, 2$, принадлежит коду $B_{i,j}$):

$$
\begin{aligned}
B_{1,1} &= \{\boldsymbol{b}(1,1,1) = (0\,0\,0\,0),\ \boldsymbol{b}(1,1,2) = (1\,1\,1\,1)\},\\
B_{1,2} &= \{\boldsymbol{b}(1,2,1) = (1\,1\,0\,0),\ \boldsymbol{b}(1,2,2) = (0\,0\,1\,1)\},\\
B_{1,3} &= \{\boldsymbol{b}(1,3,1) = (1\,0\,1\,0),\ \boldsymbol{b}(1,3,2) = (0\,1\,0\,1)\},\\
B_{1,4} &= \{\boldsymbol{b}(1,4,1) = (1\,0\,0\,1),\ \boldsymbol{b}(1,4,2) = (0\,1\,1\,0)\},\\
B_{2,1} &= \{\boldsymbol{b}(2,1,1) = (1\,0\,0\,0),\ \boldsymbol{b}(2,1,2) = (0\,1\,1\,1)\},\\
B_{2,2} &= \{\boldsymbol{b}(2,2,1) = (0\,1\,0\,0),\ \boldsymbol{b}(2,2,2) = (1\,0\,1\,1)\},\\
B_{2,3} &= \{\boldsymbol{b}(2,3,1) = (0\,0\,1\,0),\ \boldsymbol{b}(2,3,2) = (1\,1\,0\,1)\},\\
B_{2,4} &= \{\boldsymbol{b}(2,4,1) = (0\,0\,0\,1),\ \boldsymbol{b}(2,4,2) = (1\,1\,1\,0)\}.
\end{aligned}
$$

В качестве внешних выберем два МДР-кода A_1 и V_1 с параметрами $(4, 16, 3)_4$, которые разбиваются на подкоды $A_{1,i}$, $i = 1, 2, 3, 4$, и $V_{1,j}$, $j = 1, 2, 3, 4$, с расстоянием 4:

$$
A_{1,1} = \begin{bmatrix}(0\,0\,0\,0)\\(1\,1\,1\,1)\\(2\,2\,2\,2)\\(3\,3\,3\,3)\end{bmatrix},\quad
A_{1,2} = \begin{bmatrix}(0\,3\,2\,1)\\(3\,0\,1\,2)\\(2\,1\,0\,3)\\(1\,2\,3\,0)\end{bmatrix},\quad
A_{1,3} = \begin{bmatrix}(0\,2\,1\,3)\\(2\,0\,3\,1)\\(1\,3\,0\,2)\\(3\,1\,2\,0)\end{bmatrix},\quad
A_{1,4} = \begin{bmatrix}(0\,1\,3\,2)\\(1\,0\,2\,3)\\(3\,2\,0\,1)\\(2\,3\,1\,0)\end{bmatrix} \tag{1}
$$

и

$$
V_{1,1} = \begin{bmatrix}(0\,0\,0\,0)\\(1\,1\,1\,1)\\(2\,2\,2\,2)\\(3\,3\,3\,3)\end{bmatrix},\quad
V_{1,2} = \begin{bmatrix}(0\,1\,2\,3)\\(1\,0\,3\,2)\\(2\,3\,0\,1)\\(3\,2\,1\,0)\end{bmatrix},\quad
V_{1,3} = \begin{bmatrix}(0\,2\,3\,1)\\(2\,0\,1\,3)\\(3\,1\,0\,2)\\(1\,3\,2\,0)\end{bmatrix},\quad
V_{1,4} = \begin{bmatrix}(0\,3\,1\,2)\\(3\,0\,2\,1)\\(1\,2\,0\,3)\\(2\,1\,3\,0)\end{bmatrix}. \tag{2}
$$

Коды A_1 и V_1 пересекаются по подкодам $A_{1,1}$ и $V_{1,1}$, а все другие подкоды $A_{1,i}$, $i = 2, 3, 4$, и $V_{1,j}$, $j = 2, 3, 4$, находятся друг от друга на расстоянии 2 или 3, т.е.

$$
d(A_{1,i}, V_{1,j}) = \begin{cases} 0, & \text{если } i = j = 1,\\ 2, & \text{если } i, j \in \{2, 3, 4\},\\ 3, & \text{если } 1 \in \{i, j\},\ i \neq j. \end{cases} \tag{3}
$$

В качестве внешних кодов A_2 и V_2 возьмем два двоичных $(4, 8, 2)$-кода (т.е. внутренние коды B_1 и B_2): A_2 (с проверкой на четность) и V_2 (с проверкой на нечетность), которые разбиваются на подкоды $A_{2,i}$, где $i = 1, 2$, и $V_{2,j}$, где $j = 1, 2$, с расстоя-

нием 2:

$$A_{2,1} = \begin{bmatrix}(0\,0\,0\,0)\\(1\,1\,0\,0)\\(1\,0\,1\,0)\\(1\,0\,0\,1)\end{bmatrix}, \quad A_{2,2} = \begin{bmatrix}(1\,1\,1\,1)\\(0\,0\,1\,1)\\(0\,1\,0\,1)\\(0\,1\,1\,0)\end{bmatrix} \tag{4}$$

и

$$V_{2,1} = \begin{bmatrix}(1\,0\,0\,0)\\(0\,1\,0\,0)\\(0\,0\,1\,0)\\(0\,0\,0\,1)\end{bmatrix}, \quad V_{2,2} = \begin{bmatrix}(0\,1\,1\,1)\\(1\,0\,1\,1)\\(1\,1\,0\,1)\\(1\,1\,1\,0)\end{bmatrix}. \tag{5}$$

Построим следующие три ОКК-кода [14]:

- код C на основе внешних кодов $A = \{(0\,0\,0\,0), (1\,1\,1\,1)\}$, $A_1 \cup V_1$ (интерпретируя это как множество с повторениями), $A_2 \cup V_2$ и внутреннего кода $B = B_1 \cup B_2$;
- код C_1 на основе внешних кодов A_1 и A_2 и внутреннего кода B_1;
- код C_2 на основе внешних кодов V_1 и V_2 и внутреннего кода B_2.

Поясним построение кода C_1. Выберем два слова: $\boldsymbol{a} = (a_1, a_2, a_3, a_4)$ из кода A_1 и $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$ из кода A_2. Они индуцируют слово $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ кода C_1. В качестве i-го блока $\boldsymbol{c}_i$, $i = 1, 2, 3, 4$, возьмем слово $\boldsymbol{b}$ кода B_1 с номером $\boldsymbol{c}_i = \boldsymbol{b}(1, a_i + 1, x_i + 1)$ (сложение в действительном поле). Когда $\boldsymbol{a}$ и $\boldsymbol{x}$ пробегают все слова кодов A_1 и A_2, слово $\boldsymbol{c}$ пробегает все слова нового кода C_1. Из такой конструкции следует, что C_1 имеет параметры

$$n = 4 \cdot 4 = 16, \quad N = 16 \cdot 8 = 128, \quad d = \min\{2 \cdot 3, 4 \cdot 2\} = 6.$$

Код C_2 строится аналогично из внешних кодов V_1 и V_2 и внутреннего кода B_2 и имеет такие же параметры. Поясним построение C. При выборе слова $(0\,0\,0\,0)$ используются коды A_1 и A_2, а при выборе слова $(1\,1\,1\,1)$ используются V_1 и V_2.

Теперь наша цель доказать, что C_1 и C_2 находятся друг от друга на расстоянии 6. То, что они находятся на расстоянии 4, следует из того, что код C с кодовым расстоянием 4 (по каскадной конструкции) является объединением кодов C_1 и C_2.

Напомним, что все слова $\boldsymbol{c}$ кода C имеют блочный вид: $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$, где блоки $\boldsymbol{c}_i$ являются словами кода B. Так как кодовые слова внутренних кодов B_1 и B_2 не совпадают, то слова кодов C_1 и C_2 отличаются в каждом блоке, откуда, в частности, следует, что для любых слов $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ из кода C_1 и $\boldsymbol{c}' = (\boldsymbol{c}'_1 \,|\, \boldsymbol{c}'_2 \,|\, \boldsymbol{c}'_3 \,|\, \boldsymbol{c}'_4)$ из кода C_2 справедливо неравенство

$$d(\boldsymbol{c}_i, \boldsymbol{c}'_i) \geqslant 1 \quad \text{для каждого } i \in \{1, 2, 3, 4\}. \tag{6}$$

Разбиения (1), (2) и (4) кодов A_1 и V_1 на подкоды $A_{1,i}$, $i = 1, 2, 3, 4$, и $V_{1,j}$, $j = 1, 2, 3, 4$, соответственно, индуцируют разбиения кодов C_1 и C_2 на подкоды $C_{1,i}$ и $C_{2,j}$. Нужные нам свойства кодов C_1 и C_2 дает следующая

Лемма 1. *Пусть* $\boldsymbol{x} = (\boldsymbol{x}_1 \,|\, \boldsymbol{x}_2 \,|\, \boldsymbol{x}_3 \,|\, \boldsymbol{x}_4)$ – *произвольное слово кода* $C_1 \setminus C_{1,1}$, *а* $\boldsymbol{y} = (\boldsymbol{y}_1 \,|\, \boldsymbol{y}_2 \,|\, \boldsymbol{y}_3 \,|\, \boldsymbol{y}_4)$ – *произвольное слово кода* $C_2 \setminus C_{2,1}$. *Тогда* (*блочные*) *векторы* $\boldsymbol{x}_i$ *и* $\boldsymbol{y}_j$ *обладают следующими свойствами*:

(1) *Если* $\mathrm{wt}(\boldsymbol{x}) = 6$, *то имеется индекс* $i_0 \in \{1, 2, 3, 4\}$, *такой что* $i_0 \in \mathrm{supp}(\boldsymbol{x}_i)$ *для всех ненулевых* $\boldsymbol{x}_i$. *Если же индекс* s *отличен от* i_0, *то он покрыт носителем вектора* $\boldsymbol{x}_i$ *ровно один раз*, *т.е. только для одного* i;

(2) *Если* $\mathrm{wt}(\boldsymbol{x}) = 10$, *то имеется индекс* i_0, *такой что* $i_0 \in \mathrm{supp}(\boldsymbol{x}_i)$ *ровно один раз*, *т.е. только для одного* i. *Каждый индекс* i, *отличный от* i_0, *покрыт носителями* $\boldsymbol{x}_i$ *ровно три раза*;

(3) *Если* $\mathrm{wt}(\boldsymbol{y}) = 6$, *то имеется индекс* $j_0 \in \{1,2,3,4\}$, *который ни разу не покрыт ни одним из носителей* $\boldsymbol{y}_j$. *Все другие индексы* $j \neq j_0$ *покрыты два раза носителями* $\boldsymbol{y}_j$;

(4) *Если* $\mathrm{wt}(\boldsymbol{y}) = 10$, *то имеется индекс* j_0, *который покрыт носителями всех векторов* $\boldsymbol{y}_j$. *Все другие индексы* $j \neq j_0$ *покрыты два раза носителями* $\boldsymbol{y}_j$.

Доказательство непосредственно следует из описания приведенных выше внутренних кодов B_1 и B_2 и обоих внешних кодов A_i и V_i, $i = 1, 2$. ▲

Определим следующие три перестановки π_1, π_2 и π_3, действующие на множестве векторов длины 4: для любого вектора $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$ положим

$$\pi_1(\boldsymbol{x}) = (x_2, x_1, x_4, x_3), \quad \pi_2(\boldsymbol{x}) = (x_4, x_3, x_2, x_1), \quad \pi_3(\boldsymbol{x}) = (x_1, x_4, x_2, x_3).$$

Обозначим через $\mathcal{G}$ группу, порожденную перестановками π_1, π_2 и π_3.

Пусть $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ – произвольное слово кода C_1, построенного на основе кодовых слов $\boldsymbol{a} \in A_1$ и $\boldsymbol{x} \in A_2$, что можно записать в виде $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{x})$. Аналогично будем писать $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{v}, \boldsymbol{y})$ для слова $\boldsymbol{c} \in C_2$, построенного из слов $\boldsymbol{v} \in V_1$ и $\boldsymbol{y} \in V_2$.

Определим действие группы $\mathcal{G}$ на $\boldsymbol{c}$: для любого $g \in \mathcal{G}$ положим

$$g(\boldsymbol{c}) = \begin{cases} \boldsymbol{c}(g(\boldsymbol{a}), g(\boldsymbol{x})), & \text{если } \boldsymbol{c} \in C_1, \\ \boldsymbol{c}(g(\boldsymbol{v}), g(\boldsymbol{y})), & \text{если } \boldsymbol{c} \in C_2. \end{cases}$$

Лемма 2. *Справедливы следующие утверждения*:

(1) *Группа* $\mathcal{G}$ *стабилизирует коды* A_i *и* V_i *для* $i = 1, 2$ *и действует транзитивно на подкодах* $A_1 \setminus A_{1,1}$ *и* $V_1 \setminus V_{1,1}$;

(2) *Группа* $\mathcal{G}$ *стабилизирует коды* C_1 *и* C_2 *и действует транзитивно на подкодах* $C_1 \setminus C_{1,1}$ *и* $C_2 \setminus C_{2,1}$;

(3) *Для любых* $\boldsymbol{c} \in C_1$ *и* $\boldsymbol{c}' \in C_2$ *и для любого* $g \in \mathcal{G}$ *имеет место следующее равенство*:

$$d(g(\boldsymbol{c}), g(\boldsymbol{c}')) = d(\boldsymbol{c}, \boldsymbol{c}'); \tag{7}$$

(4) *Коды* C_1 *и* C_2 *инвариантны относительно сдвига на вектор из всех единиц, т.е.*

$$C_i + (1\,1\,\ldots\,1) = C_i, \quad i = 1, 2. \tag{8}$$

Доказательство. Первые два утверждения следуют непосредственно из таблиц кодовых слов (1), (2) и (4). Так как перестановки не меняют расстояния между векторами, а действие группы является автоморфизмом кодов C_1 и C_2, то получаем утверждение (3). Докажем утверждение (4) сначала для кода C_1. Пусть $\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$ – произвольное слово этого кода. По построению $\boldsymbol{c}_i = \boldsymbol{b}(1, a_i, x_i)$, где $(a_1\, a_2\, a_3\, a_4)$ – слово кода A_1, а $(x_1\, x_2\, x_3\, x_4)$ принадлежит A_2. Но, как легко видеть из всех его слов,

$$A_2 + (1\,1\,1\,1) = A_2.$$

По построению слово $\boldsymbol{x}$ пробегает весь код A_2. Поэтому для любого $\boldsymbol{x} = (x_1\, x_2\, x_3\, x_4)$ дополнительное к нему слово $\boldsymbol{x} + (1\,1\,1\,1)$ также принадлежит A_2. Следовательно, для любого слова

$$\boldsymbol{c} = (\boldsymbol{c}_1 \,|\, \boldsymbol{c}_2 \,|\, \boldsymbol{c}_3 \,|\, \boldsymbol{c}_4)$$

дополнительное к нему слово также принадлежит коду C_1. Для кода C_2 доказательство совершенно аналогично, так как код V_2 (участвующий в построении C_2) также инвариантен относительно сдвига на слово из всех единиц. ▲

Теорема 1. *Объединение кодов C_1 и C_2, т.е. код*

$$C = C_1 \cup C_2$$

представляет собой $(16, 256, 6)$-код, т.е. код Нордстрома – Робинсона C является ОКК-кодом третьего порядка.

Доказательство. Чтобы доказать утверждение теоремы, надо доказать, что для любых r и s выполнено следующее условие:

$$d(C_{1,r}, C_{2,s}) \geqslant 6, \quad r, s \in \{1, 2, 3, 4\}. \tag{9}$$

Пусть $\boldsymbol{x}$ и $\boldsymbol{y}$ – произвольные слова кодов $C_{1,r}$ и $C_{2,s}$ соответственно, которые можно представить в следующем блочном виде:

$$\boldsymbol{x} = (\boldsymbol{x}_1 \,|\, \boldsymbol{x}_2 \,|\, \boldsymbol{x}_3 \,|\, \boldsymbol{x}_4),$$
$$\boldsymbol{y} = (\boldsymbol{y}_1 \,|\, \boldsymbol{y}_2 \,|\, \boldsymbol{y}_3 \,|\, \boldsymbol{y}_4),$$

где $\boldsymbol{x}_i \in B_1$ и $\boldsymbol{y}_j \in B_2$. В силу леммы 2 для доказательства достаточно рассмотреть четыре разных случая в зависимости от условий $1 \in \{r, s\}$ или $1 \notin \{r, s\}$.

Случай $(r = 1,\ s = 1)$. В этом случае $\boldsymbol{x}_i$ – это одно слово $\boldsymbol{b}_1$ из подкода B_1 для всех $i \in \{1, 2, 3, 4\}$ или одно слово $\boldsymbol{b}_1$ из подкода B_1 и дополнительное к нему слово $\bar{\boldsymbol{b}}_1$, каждое повторенное два раза, а $\boldsymbol{y}_j$ – одно слово $\boldsymbol{b}_2$ из подкода B_2, повторенное три раза, и дополнительное к нему слово $\bar{\boldsymbol{b}}_2$. Предположим сначала, что $\mathrm{wt}(\boldsymbol{y}) = 6$. Если $\mathrm{supp}(\boldsymbol{b}_2) \not\subset \mathrm{supp}(\boldsymbol{b}_1)$, то и доказывать нечего. Поэтому рассмотрим случай $\mathrm{supp}(\boldsymbol{b}_2) \subset \mathrm{supp}(\boldsymbol{b}_1)$. Пусть сначала $\boldsymbol{b}_1$ встречается четыре раза. Тогда условие $\mathrm{supp}(\boldsymbol{b}_2) \subset \mathrm{supp}(\boldsymbol{b}_1)$ выполняется для трех блоковых векторов $\boldsymbol{y}_j$ веса 1 и не выполнено для четвертого блока, где $\boldsymbol{y}_j$ имеет вес 3, который и даст вклад 3 в расстояние между $\boldsymbol{x}$ и $\boldsymbol{y}$. Если же $\boldsymbol{b}_1$ и $\bar{\boldsymbol{b}}_1$ встречаются по два раза, то вклад 3 в расстояние между векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ даст третий блок веса 1. Пусть теперь $\mathrm{wt}(\boldsymbol{y}) = 10$ и $\mathrm{supp}(\boldsymbol{b}_1) \subset \mathrm{supp}(\boldsymbol{b}_2)$. В этом случае, аналогично предыдущему случаю, блок, в котором $\boldsymbol{y}_j$ имеет вес 1, даст вклад 3 в расстояние между $\boldsymbol{x}$ и $\boldsymbol{y}$. Случаи, когда один или более блоков $\boldsymbol{x}_i$ имеют вес 4, исключаются аналогично.

Случай $(r = 1,\ s = 2, 3, 4)$. В этом случае $\boldsymbol{y}_j$, $j = 1, 2, 3, 4$, – это четыре разных слова из кода B_2, а именно либо три слова веса 1 и слово веса 3, дополнительное к четвертому слову веса 1, либо три разных слова веса 3 и одно слово веса 1, дополнительное к четвертому слову веса 3. Ясно, что в случае, когда единица пробегает три разных позиции в трех блоках $\boldsymbol{y}_j$, а $\boldsymbol{x}_i$ – одно и то же слово $\boldsymbol{b}_1$, встречающееся во всех четырех блоках, то слова $\boldsymbol{x}_i$ и $\boldsymbol{y}_i$ по крайней мере в одном блоке будут на расстоянии 3 друг от друга. Пусть теперь слово $\boldsymbol{b}_1$ (веса 2) встречается в двух блоках $\boldsymbol{x}_i$, в которых оно покрывает два разных слова кода B_2 веса 1, скажем, $\boldsymbol{b}_2(i_1)$ и $\boldsymbol{b}_2(i_2)$. Ясно, что при этом $\bar{\boldsymbol{b}}_1$ покроет вектор $\boldsymbol{b}_2(i_3)$ веса 1 кода B_2 (три блока веса 1 кода B_2 имеют непересекающиеся единицы). Поэтому вклад в расстояние 3 даст четвертый блок (веса 3), где $\boldsymbol{y}$ содержит слово $\bar{\boldsymbol{b}}_2(i_4)$, дополнительное к четвертому слову $\boldsymbol{b}_2(i_4)$ кода B_2. Если же три блока $\boldsymbol{y}_j$ имеют вес 3, то те же аргументы остаются в силе с переходом к дополнительным словам.

Случай $(r = 2, 3, 4,\ s = 1)$. Этот случай совершенно аналогичен предыдущему, и поэтому мы не повторяем доказательство.

Случай $(r = 2, 3, 4, s = 2, 3, 4)$. В этом случае блоковые векторы $\boldsymbol{x}_i$ и $\boldsymbol{y}_j$ пробегают все различные слова кодов A_2 и V_2. Согласно лемме 1 для вектора $\boldsymbol{x}$ имеется индекс $i_0 \in \{1, 2, 3, 4\}$, который покрывается векторами из трех блоков $\boldsymbol{x}$, если $\mathrm{wt}(\boldsymbol{x}) = 6$, и покрывается только одним блоком, если $\mathrm{wt}(\boldsymbol{x}) = 10$. Для слова $\boldsymbol{y}_j$ также имеется индекс $j_0 \in \{1, 2, 3, 4\}$, который не покрывается ни одним из векторов всех четырех блоков $\boldsymbol{y}$, если $\mathrm{wt}(\boldsymbol{y}) = 6$, и покрывается четыре раза, если $\mathrm{wt}(\boldsymbol{y}) = 10$. Поэтому мы

проводим доказательство для двух разных случаев – когда индексы i_0 и j_0 равны и когда они не равны.

Предположим сначала, что для двух произвольных слов $\boldsymbol{x}$ и $\boldsymbol{y}$ индексы i_0 и j_0 совпадают, и пусть $\boldsymbol{x}$ и $\boldsymbol{y}$ имеют оба вес 6. В силу (6) в каждом блоке векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ находятся на расстоянии по крайней мере 1. Позиция с индексом $j_0 = i_0$ не покрыта ни одним блоком $\boldsymbol{y}_j$ веса 1. Нулевому блоку $\boldsymbol{x}_i$ будет соответствовать либо блок $\boldsymbol{y}_i$ веса 3 (и это даст вклад 3 в расстояние между $\boldsymbol{x}$ и $\boldsymbol{y}$), либо блок веса 1 (и тогда вклад 3 даст тот блок, в котором $\boldsymbol{y}_i$ имеет вес 3, так как он не может покрывать элемент 1 в позиции i_0 соответствующего блока $\boldsymbol{x}_i$).

Рассмотрим теперь случай, когда $\mathrm{wt}(\boldsymbol{x}) = 10$, а $\mathrm{wt}(\boldsymbol{y}) = 6$. Для этого случая нам понадобятся используемые нами внешние коды. Выберем произвольное слово $\boldsymbol{x}$ кода C_1, полученное, например, из пары $(0\,3\,2\,1)$ и $(1\,0\,0\,1)$:

$$\begin{array}{l}\boldsymbol{x} = (1\,1\,1\,1|\,1\,0\,0\,1|\,1\,0\,1\,0|\,0\,0\,1\,1),\\ \hline \boldsymbol{y} = (1\,0\,1\,1|\,0\,0\,0\,1|\,1\,0\,0\,0|\,0\,0\,1\,0),\\ \boldsymbol{y}' = (1\,0\,1\,1|\,1\,0\,0\,0|\,0\,0\,1\,0|\,0\,0\,0\,1).\end{array}$$

Легко выписать два единственно возможных вектора $\boldsymbol{y}$ и $\boldsymbol{y}'$ веса 6, которые по своей структуре могут быть кодовыми словами C_2 и которые покрываются кодовым словом $\boldsymbol{x}$, т.е. находятся от него на расстоянии 4. Используя таблицы кодов (1), (2) и (4), заключаем, что векторы $\boldsymbol{y}$ и $\boldsymbol{y}'$ получены из пар $(1\,3\,0\,2)$, $(1\,0\,0\,0)$ и $(1\,0\,2\,3)$, $(1\,0\,0\,0)$ соответственно. Но оба вектора $(1\,3\,0\,2)$ и $(1\,0\,2\,3)$ не принадлежат коду V_1, а значит, $\boldsymbol{y}$ и $\boldsymbol{y}'$ не принадлежат коду C_2.

Следующие два случая, когда $\mathrm{wt}(\boldsymbol{x}) = 6$, а $\mathrm{wt}(\boldsymbol{y}) = 10$, и когда $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 10$, доказывать не надо, так как они вытекают из двух предыдущих случаев ($\mathrm{wt}(\boldsymbol{x}) = 10$, $\mathrm{wt}(\boldsymbol{y}) = 6$ и $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 6$) в силу инвариантности обоих кодов C_1 и C_2 относительно сдвига на слово из всех единиц (лемма 2). Действительно, пусть, например, для случая $\mathrm{wt}(\boldsymbol{x}) = 6$, а $\mathrm{wt}(\boldsymbol{y}) = 10$ мы нашли два вектора $\boldsymbol{x}$ и $\boldsymbol{y}$ с меньшим расстоянием $d(\boldsymbol{x}, \boldsymbol{y}) \leqslant 5$. Тогда на этом же расстоянии будут находиться дополнительные к ним векторы $\boldsymbol{x} + (1\,1\,\ldots\,1)$ и $\boldsymbol{y} + (1\,1\,\ldots\,1)$, что противоречит уже доказанному случаю.

Рассмотрим теперь случай, когда индексы векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ не равны: $i_0 \neq j_0$. Доказательство проводится совершенно аналогично, и мы рассмотрим только два случая – когда $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 6$ и когда $\mathrm{wt}(\boldsymbol{x}) = 6$ и $\mathrm{wt}(\boldsymbol{y}) = 10$.

Пусть сначала $\mathrm{wt}(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{y}) = 6$. Выберем произвольное слово $\boldsymbol{x}$ кода C_1, например (индекс $\boldsymbol{x}$ равен $i_0 = 1$),

$$\begin{array}{l}\boldsymbol{x} = (0\,0\,0\,0|\,1\,0\,0\,1|\,1\,0\,1\,0|\,1\,1\,0\,0),\\ \hline \boldsymbol{y} = (0\,1\,0\,0|\,0\,0\,0\,1|\,1\,0\,0\,0|\,1\,1\,0\,1),\\ \boldsymbol{y}' = (0\,0\,0\,1|\,1\,1\,0\,1|\,1\,0\,0\,0|\,0\,1\,0\,0).\end{array}$$

Выпишем два единственно возможных вектора $\boldsymbol{y}$ и $\boldsymbol{y}'$ веса 6 с индексом $j_0 = 3$, которые могут быть кодовыми словами C_2 и которые находятся от $\boldsymbol{x}$ на расстоянии 4. На основе таблиц кодов снова выясняем, что векторы $\boldsymbol{y}$ и $\boldsymbol{y}'$ получены из пар $(1\,3\,0\,2)$, $(0\,0\,0\,1)$ и $(3\,2\,0\,1)$, $(0\,1\,0\,0)$ соответственно. Но $(1\,3\,0\,2)$ и $(3\,2\,0\,1)$ не принадлежат коду V_1, а значит, $\boldsymbol{y}$ и $\boldsymbol{y}'$ не принадлежат коду C_2. Оставшиеся два случая значения индекса $j_0 \in \{2, 4\}$ вектора $\boldsymbol{y}$ исключаются совершенно аналогично.

Пусть теперь $\mathrm{wt}(\boldsymbol{x}) = 6$ и $\mathrm{wt}(\boldsymbol{y}) = 10$. Выберем произвольное слово $\boldsymbol{x}$ кода C_1, например (индекс $\boldsymbol{x}$ равен $i_0 = 1$),

$$\begin{array}{l}\boldsymbol{x} = (0\,0\,0\,0|\,1\,0\,0\,1|\,1\,0\,1\,0|\,1\,1\,0\,0),\\ \hline \boldsymbol{y} = (0\,0\,0\,1|\,1 * \bar{*}1|\,1\,0\,1\,1|\,1\,1\,0\,1).\end{array}$$

Предположим, что индекс $\boldsymbol{y}$ равен $j_0 = 4$. Это означает, что каждый из трех блоков $\boldsymbol{y}_j$ веса 3 должен покрывать позицию с индексом $j_0 = 4$, и кроме того, две ненулевые позиции блоков $\boldsymbol{x}_i$. Легко убедиться, что это сделать невозможно. Действительно, в приведенном выше векторе $\boldsymbol{y}$ блок $\boldsymbol{y}_2$ не может быть достроен до веса 3 (в каждом из двух возможных случаев получим блоковый вектор $\boldsymbol{y}_2$, совпадающий с одним из блоковых векторов $\boldsymbol{y}_3$ или $\boldsymbol{y}_4$). Два оставшихся значения индекса $j_0 \in \{2, 3\}$ исключаются аналогично.

Чтобы завершить доказательство теоремы, напомним лемму 2, согласно которой коды инвариантны относительно действия группы $\mathcal{G}$. Это обосновывает наш выбор только одного вектора $\boldsymbol{x}$. Выбрав другой вектор $\boldsymbol{x}'$, мы получим такое же число возможных претендентов векторов на слова кода C_2, находящихся на расстоянии 4 от $\boldsymbol{x}$. Действительно, предположим, что для $\boldsymbol{x}'$ нашлось три претендента $\boldsymbol{y}$, $\boldsymbol{y}'$ и $\boldsymbol{y}''$ на слова кода C_2, находящихся на расстоянии 4 от $\boldsymbol{x}'$. Пусть $g \in \mathcal{G}_2$ переводит $\boldsymbol{x}'$ в $\boldsymbol{x}$, т.е. $g(\boldsymbol{x}') = \boldsymbol{x}$. При этом (по лемме 2) g переводит все векторы $\boldsymbol{y}$, $\boldsymbol{y}'$ и $\boldsymbol{y}''$ в векторы, находящиеся на расстоянии 4 от $\boldsymbol{x}$, которые также являются претендентами на слова кода C_2. Таким образом, приходим к противоречию, так как слову $\boldsymbol{x}$ соответствуют только два претендента. Это завершает доказательство теоремы. ▲

§ 3. Построение двоичного кода Голея

Построение двоичного расширенного $[24, 12, 8]$-кода Голея аналогично предыдущей конструкции кода Нордстрома – Робинсона. В качестве внутреннего кода берется тот же $[4, 4, 1]$-код B с таким же разбиением на $[4, 3, 2]$-подкоды: $[4, 3, 2]$-код B_0 (с проверкой на четность) и $(4, 8, 2)$-код B_1 (с проверкой на нечетность). При этом мы изменим следующим образом нумерацию их слов, чтобы линеаризовать отображение из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_0 (что нам нужно для доказательства линейности результирующего кода):

$$B_{0,0} = \{\boldsymbol{b}(0,0,0) = (0\,0\,0\,0),\ \boldsymbol{b}(0,0,1) = (1\,1\,1\,1)\},$$
$$B_{0,1} = \{\boldsymbol{b}(0,1,0) = (1\,1\,0\,0),\ \boldsymbol{b}(0,1,1) = (0\,0\,1\,1)\},$$
$$B_{0,2} = \{\boldsymbol{b}(0,2,0) = (1\,0\,1\,0),\ \boldsymbol{b}(0,2,1) = (0\,1\,0\,1)\},$$
$$B_{0,3} = \{\boldsymbol{b}(0,3,0) = (0\,1\,1\,0),\ \boldsymbol{b}(0,3,1) = (1\,0\,0\,1)\}.$$

Для кода B_1 нумерация имеет следующий вид:

$$B_{1,0} = \{\boldsymbol{b}(1,0,0) = (1\,0\,0\,0),\ \boldsymbol{b}(1,0,1) = (0\,1\,1\,1)\},$$
$$B_{1,1} = \{\boldsymbol{b}(1,1,0) = (0\,1\,0\,0),\ \boldsymbol{b}(1,1,1) = (1\,0\,1\,1)\},$$
$$B_{1,2} = \{\boldsymbol{b}(1,2,0) = (0\,0\,1\,0),\ \boldsymbol{b}(1,2,1) = (1\,1\,0\,1)\},$$
$$B_{1,3} = \{\boldsymbol{b}(1,3,0) = (0\,0\,0\,1),\ \boldsymbol{b}(1,3,1) = (1\,1\,1\,0)\}.$$

Определим внешние коды: $A = \{(0\,0\,0\,0\,0\,0),\ (1\,1\,1\,1\,1\,1)\}$ и $[6, 3, 4]_4$-код A_1 над $\mathbb{F}_4$, а также двоичные коды: $[6, 5, 2]$-код A_2 с проверкой на четность и $(6, 32, 2)$-код V_2 с проверкой на нечетность.

Поясним построение $[6, 3, 4]_4$-кода A_1 над $\mathbb{F}_4$. Пусть

$$\mathbb{F}_4 = \{0, 1, \xi, \xi^2\}, \quad \text{где } \xi^2 + \xi + 1 = 0,$$

и пусть $\mathbb{F}_{4^2}$ получено из $\mathbb{F}_4$ с помощью примитивного многочлена

$$f(x) = x^2 + x + \xi.$$

Пусть α – корень этого многочлена, т.е. примитивный элемент поля $\mathbb{F}_{4^2}$. Всюду далее в качестве элементов $0, 1, \xi, \xi^2$ поля $\mathbb{F}_4$ мы для удобства используем элементы

$0, 1, 2, 3$ соответственно, которыми нумеруются слова внутренних кодов. Обозначим через $m_i(x)$ минимальную функцию элемента α^i. Так как

$$x^5 + 1 = (x^2 + 3x + 1)(x^2 + 2x + 1)(x + 1), \tag{10}$$

то можно определить следующий циклический $[5, 3, 3]_4$-МДР-код C, имеющий порождающий многочлен

$$g_a(x) = m_3(x) = x^2 + 3x + 1.$$

Обозначим через A_1 код, полученный из C расширением, т.е. добавлением к каждому кодовому слову $\boldsymbol{a}' = (a_1, a_2, a_3, a_4, a_5)$ кода C еще одной позиции a_6 общей проверки:

$$a_6 = \sum_{i=1}^{5} a_i.$$

При этом получаем $[6, 3, 4]_4$-код A_1, образованный словами $\boldsymbol{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$. Этот код удобно описать с помощью следующих пяти кодовых слов (генераторов):

$$(1\,1\,1\,1\,1\,|\,1), \quad (2\,1\,2\,0\,0\,|\,1), \quad (3\,3\,0\,1\,0\,|\,1), \quad (1\,2\,2\,1\,0\,|\,0), \quad (1\,2\,3\,2\,1\,|\,3). \tag{11}$$

Первый генератор в (11) порождает, очевидно, три кодовых слова. Каждый из четырех остальных генераторов порождает 15 кодовых слов умножением на скаляр (т.е. на ξ и ξ^2) и пятью циклическими сдвигами. Если $\boldsymbol{a} = (a_1, a_2, a_3, a_4, a_5\,|\,a_6)$ – один из таких генераторов, то 15 соответствующих кодовых слов порождаются циклическими сдвигами (первых пяти позиций, позиция же a_6 остается неподвижной) трех векторов $\boldsymbol{a}$, $\xi\boldsymbol{a}$ и $\xi^2\boldsymbol{a}$.

Для удобства читателя приведем все слова кода A_1:

(000000)	(111111)	(222222)	(333333),
(212001)	(330101)	(122100)	(123213),
(021201)	(033011)	(012210)	(112323),
(002121)	(103301)	(101220)	(211233),
(200211)	(010331)	(210120)	(321123),
(120021)	(301031)	(221010)	(232113),
(323002)	(110202)	(233200)	(231321),
(032302)	(011022)	(023320)	(223131),
(003232)	(201102)	(202330)	(322311),
(300322)	(020112)	(320230)	(132231),
(230032)	(102012)	(332020)	(313221),
(131003)	(220303)	(311300)	(312132),
(013103)	(022033)	(031130)	(331212),
(001313)	(302203)	(303110)	(133122),
(100133)	(030223)	(130310)	(213312),
(310013)	(203023)	(113030)	(121332).

Строим три ОКК-кода:

- код G (порядка 3) на основе внутреннего кода B и внешних кодов A, A_1 и $A_2 \cup V_2$ (при выборе слова $(0\,0\,0\,0\,0\,0)$ используется A_2, а при выборе $(1\,1\,1\,1\,1\,1)$ используется V_2);
- код G_1 (порядка 2) на основе внутреннего кода B_0 и двух внешних кодов A_1 и A_2;
- код G_2 (порядка 2) на основе внутреннего кода B_1 и двух внешних кодов A_1 и V_2.

Отображение из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_0 обозначим через φ_0, а в слова кода B_1 – через φ_1:

$$\varphi_i(j,k) = \boldsymbol{b}(i,j,k), \quad i = 0,1.$$

Доопределим естественным образом эти отображения на векторы $\boldsymbol{x} = (x_1, \ldots, x_n)$ над $\mathbb{F}_4 \times \mathbb{F}_2$:

$$\varphi_i(\boldsymbol{x}) = (\varphi_i(x_1), \varphi_i(x_2), \ldots, \varphi_i(x_n)), \quad i = 0,1.$$

Лемма 3. *Справедливы следующие утверждения*:

(1) *Отображение φ_0 из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_0 линейно по обоим индексам, т.е. если $\boldsymbol{b}'$ и $\boldsymbol{b}''$ – слова кода B_0 с номерами $(0,j',k')$ и $(0,j'',k'')$ соответственно, то их сумма $\boldsymbol{b} = \boldsymbol{b}' + \boldsymbol{b}''$ имеет номер*

$$(i,j,k) = (0, j' + j'', k' + k''),$$

где индексы j' и j'' суммируются в поле $\mathbb{F}_4$ (с учетом введенных нами обозначений элементов поля $\mathbb{F}_4$), а индексы k' и k'' – в поле $\mathbb{F}_2$;

(2) *Отображение φ_1 из $\mathbb{F}_4 \times \mathbb{F}_2$ в слова кода B_1 линейно по первому индексу, а также линейно по второму с поправочным коэффициентом $k_3 \in \{0,1\}$ (в зависимости от четности числа появлений элемента 3 в множестве $\{j', j''\}$), т.е. если $\boldsymbol{b}'$ и $\boldsymbol{b}''$ – слова кода B_1 с номерами $(1,j',k')$ и $(1,j'',k'')$ соответственно, то их сумма $\boldsymbol{b} = \boldsymbol{b}' + \boldsymbol{b}''$ принадлежит коду B_0 и вектор $\boldsymbol{b}$ имеет номер*

$$(i,j,k) = (0, j' + j'', k' + k'' + k_3),$$

где k_3 – число появлений элемента 3 в множестве $\{j', j''\}$, взятое по модулю 2 и интерпретируемое как элемент поля $\mathbb{F}_2$.

Доказательство. Непосредственная проверка сложения номеров слов кодов B_0 и B_1, которое индуцируется сложением двоичных векторов длины 4. ▲

Лемма 4. *Справедливы следующие утверждения*:

(1) *Коды G_1 и G_2 имеют кодовое расстояние 8, причем $\mathrm{wt}(\boldsymbol{g}) \geqslant 8$ для любого слова $\boldsymbol{g}$ из G_2;*

(2) *Код G_1 является линейным кодом, т.е. $[24, 11, 8]$-кодом;*

(3) *Код G_2 инвариантен относительно сдвига на любое слово кода G_1.*

Доказательство. (1) Минимальные расстояния d_1 и d_2 кодов G_1 и G_2 следуют из обобщенной каскадной конструкции [14]:

$$d_1 = d_2 = \min\{2 \cdot 4, 4 \cdot 2\} = 8.$$

(2) Линейность кода G_1 следует из линейности кодов A_1 и A_2 и линейности отображения φ_0 (лемма 3).

(3) Заметим следующий очевидный факт: *множество всех двоичных векторов нечетного веса длины n инвариантно относительно сдвига на любой двоичный вектор четного веса длины n*. Поэтому код B_1 инвариантен относительно сдвига на любое слово кода B_0, а код V_2 инвариантен относительно сдвига на любое слово кода A_2. Следовательно, для любого слова $\boldsymbol{g} = \varphi_0(\boldsymbol{a}, \boldsymbol{b})$ кода G_1, $\boldsymbol{a} \in A_1$, $\boldsymbol{b} \in A_2$, получаем

$$\begin{aligned}
&\boldsymbol{g} + G_2 = \varphi_0(\boldsymbol{a}, \boldsymbol{b}) + \{\varphi_1(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \in A_1,\ \boldsymbol{y} \in V_2\} = \\
&= \{\varphi_1(\boldsymbol{x} + \boldsymbol{a}, \boldsymbol{y} + \boldsymbol{b}) : \boldsymbol{x} \in A_1,\ \boldsymbol{y} \in V_2\} = \\
&= \{\varphi_1(\boldsymbol{x}', \boldsymbol{y}') : \boldsymbol{x}' \in A_1,\ \boldsymbol{y}' \in V_2\} = G_2. \quad ▲
\end{aligned}$$

Лемма 5. *Коды G_1 и G_2 находятся друг от друга на расстоянии 8.*

Доказательство. Согласно лемме 4 код G_2 инвариантен относительно сдвига на любое слово кода G_1. Ясно, что условие $d(G_1, G_2) \leqslant 7$ означает, что $d(\boldsymbol{g}, G_2) \leqslant 7$ для некоторого слова $\boldsymbol{g} \in G_1$. Но это неравенство противоречит лемме 4, согласно которой код G_2 инвариантен относительно сдвига на любое слово кода G_1, и поэтому должно выполняться неравенство $d(\boldsymbol{g}, G_2) = 8$. ▲

На самом деле, мы уже доказали, что объединение кодов G_1 и G_2 является двоичным кодом Голея, так как известно [5], что любой двоичный код с параметрами $n = 24$, $N = 2^{12}$, $d = 8$ является кодом Голея. Тем не менее мы приведем второе доказательство этого факта через линейность кода.

Лемма 6. *Код G_2 является смежным классом кода G_1.*

Доказательство. Согласно лемме 4 имеем $\boldsymbol{g} + G_2 = G_2$ для любого $\boldsymbol{g} \in G_1$. Это равенство означает, что $\boldsymbol{g} + \boldsymbol{g}_1 = \boldsymbol{g}_2$ для любого $\boldsymbol{g}_1 \in G_2$, где $\boldsymbol{g}_2 \in G_2$, откуда и следует утверждение. ▲

Итак, доказана следующая

Теорема 2. *Объединение кодов G_1 и G_2, т.е. код*

$$G = G_1 \cup G_2$$

представляет собой $(24, 2^{12}, 8)$-код, т.е. ОКК-код третьего порядка G представляет собой двоичный расширенный совершенный $[24, 12, 8]$-код Голея.

Авторы благодарны Д. Кротову за стимулирующую беседу относительно ОКК-конструкции кода Нордстрома – Робинсона, результатом которой и является данная статья, а также рецензенту за полезные замечания, которыми мы воспользовались при подготовке окончательного варианта статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Nordstrom A.W., Robinson J.P.* An Optimum Nonlinear Code // Inform. Control. 1967. V. 11. № 5–6. P. 613–616. https://doi.org/10.1016/S0019-9958(67)90835-2
2. *Семаков Н.В., Зиновьев В.А.* Совершенные и квазисовершенные равновесные коды // Пробл. передачи информ. 1969. Т. 5. № 2. С. 14–18. http://mi.mathnet.ru/ppi1794
3. *Golay M.J.E.* Notes on Digital Coding // Proc. IRE. 1949. V. 37. P. 657. https://doi.org/10.1109/JRPROC.1949.233620
4. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. *Snover S.L.* The Uniqueness of the Nordstrom–Robinson and the Golay Binary Codes. Ph.D. Thesis. Dept. of Mathematics, Michigan State Univ., 1973. https://doi.org/10.25335/M56D5PM3R
6. *Preparata F.P.* A Class of Optimum Nonlinear Double-Error-Correcting Codes // Inform. Control. 1968. V. 13. № 4. P. 378–400. https://doi.org/10.1016/S0019-9958(68)90874-7
7. *Kerdock A.M.* A Class of Low-Rate Nonlinear Binary Codes // Inform. Control. 1972. V. 20. № 2. P. 182–187. https://doi.org/10.1016/S0019-9958(72)90376-2
8. *Vardy A.* The Nordstrom–Robinson Code: Representation over $GF(4)$ and Efficient Decoding // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 1686–1693. https://doi.org/10.1109/18.333895
9. *Forney G.D., Jr., Sloane N.J.A., Trott M.D.* The Nordstrom–Robinson Code Is the Binary Image of the Octacode // Coding and Quantization (Proc. DIMACS/IEEE Workshop. Princeton Univ., NJ, USA. Oct. 19–21, 1992). Providence, RI: Amer. Math. Soc., 1993. P. 19–26.
10. *Bierbrauer J.* Nordstrom–Robinson Code and A_7-Geometry // Finite Fields Appl. 2007. V. 13. № 1. P. 158–170. https://doi.org/10.1016/j.ffa.2005.05.004

11. *Могильных И.Ю.* О продолжении пропелинейных структур кода Нордстрома – Робинсона на код Хэмминга // Пробл. передачи информ. 2016. Т. 52. № 3. С. 97–107. http://mi.mathnet.ru/ppi2215
12. *Gillespie N.I., Praeger C.E.* New Characterisations of the Nordstrom–Robinson Codes // Bull. London Math. Soc. 2017. V. 49. № 2. P. 320–330. https://doi.org/10.1112/blms.12016
13. *Думер И.И., Зиновьев В.А.* Некоторые новые максимальные коды над полем Галуа $GF(4)$ // Пробл. передачи информ. 1978. Т. 14. № 3. С. 24–34. http://mi.mathnet.ru/ppi1543
14. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670

Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
20.12.2020
После доработки
17.11.2021
Принята к публикации
17.11.2021