

УДК 621.391

А. Ю. Бибов<sup>1</sup>, В. М. Деундяк<sup>2</sup>

## О распространении декодеров Сидельникова на класс кодов БЧХ

**Ключевые слова:** помехоустойчивое кодирование, списочный декодер, коды БЧХ, декодер Сидельникова.

Получено распространение декодеров В. М. Сидельникова на семейство кодов Боуза–Чоудхури–Хоквингема. Для построенных алгоритмов декодирования выполнена программная реализация.

**Keywords:** error-control coding, list decoder, BCH-codes, Sidelnikov's decoder.

We obtain the distribution of Sidelnikov's decoders for the family of BCH-codes. We have realized a program implemenetation of this algorithms.

### 1. Введение

В работе В. М. Сидельникова [4] рассмотрен вероятностный метод декодирования кодов Рида–Соломона, позволяющий исправлять ошибки в случае, когда их число превосходит половину кодового расстояния. Этот декодер в [3] обобщен А. Ю. Серебряковым на некоторый класс одноточечных алгебро-геометрических кодов на эллиптических кривых; программная реализация декодера Серебрякова рассмотрена в [2].

Цель настоящей работы — распространение метода Сидельникова на семейство кодов Боуза–Чоудхури–Хоквингема, построение алгоритмов декодирования и их программная реализация на основе библиотеки GFL, представленной в [1].

Раздел 2 содержит необходимые предварительные сведения. В разделе 3 построен детерминированный декодер для случая, когда число ошибок  $t$  не превосходит половины конструктивного кодового расстояния  $d$ , а в разделе 4 — списочный декодер, для случая, когда число ошибок превосходит  $d$ .

### 2. Предварительные сведения

Приведем необходимые сведения о БЧХ-кодах (см. [5], гл. 5). Пусть  $\mathbb{N}$  — множество натуральных чисел,  $R_{q,n}(\in \mathbb{F}_q[x])$  — кольцо многочленов над полем Галуа  $\mathbb{F}_q$  степени, не превосходящей  $n(\in \mathbb{N})$ , с умножением по модулю  $x^n - 1$ . Известно, что  $R_{q,n}$  является кольцом главных идеалов.

<sup>1</sup>Южный Федеральный Университет; E-mail: lexe42152@gmail.com.

<sup>2</sup>Южный Федеральный Университет; E-mail: vlade@math.rsu.ru.

Кольцо  $R_{q,n}$  естественно изоморфно как линейное пространство пространству Хемминга  $\mathbb{F}_q^n$ . Если  $a(x) \in R_{q,n}$ , то соответствующий вектор коэффициентов из  $\mathbb{F}_q^n$  будем обозначать  $\bar{a}$ . Идеалу кольца  $R_{q,n}$  соответствует инвариантное подпространство оператора правого циклического сдвига, которое называется циклическим кодом. Порождающий многочлен всякого идеала в  $R_{q,n}$  называется порождающим многочленом соответствующего циклического кода.

Пусть  $d \in \mathbb{N}$  и  $d \geq 3$ . Рассмотрим последовательность

$$N_{q^r}(\alpha, b, d) = \{\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+d-2}\},$$

где  $\alpha \in \mathbb{F}_{q^r}$ ,  $r \in \mathbb{N}$ , а все элементы различны. Циклический код, построенный по элементам  $N_{q^r}(\alpha, b, d)$  как по нулям, называется кодом БЧХ, а параметр  $d$  называется конструктивным кодовым расстоянием или расстоянием Боуза. Для его кодового расстояния  $D$  известна оценка:  $D \geq d$ , а длина  $n$  равна порядку элемента  $\alpha$ . Размерность  $k$  и порождающий многочлен  $g(x)$  определяются по формулам

$$k = n - \sum \deg(m_\alpha(x))$$

и

$$g(x) = \prod m_\alpha(x),$$

где  $m_\alpha$  — минимальный многочлен элемента  $\alpha$  над полем  $\mathbb{F}_q$ , а суммирование и произведение ведутся по всем попарно несопряженным элементам последовательности  $N_{q^r}(\alpha, b, d)$ .

### 3. Алгоритм декодирования при $t \leq \frac{d-1}{2}$

Рассмотрим следующие последовательности из  $\mathbb{F}_q$  и  $\mathbb{F}_{q^r}$  соответственно:

$$\chi = (k_1, k_2, \dots, k_u), \quad \mathfrak{R} = (\beta_1, \beta_2, \dots, \beta_u), \quad (1)$$

где  $u \leq q-1$  и  $\beta_i \neq \beta_j$  при  $i \neq j$ . Пусть  $b \in \mathbb{N} \cup \{0\}$ ,

$$m_i = \sum_{j=1}^u k_j \beta_j^i, \quad i = b, b+1, \dots \quad (2)$$

Элементы  $m_i$  называются моментами, порожденными тройкой  $(\mathfrak{R}, \chi, b)$  (см. [4]).

**Лемма 1.** Пусть  $W_{u-1}$  — определитель Вандермонда порядка  $u$ , построенный по элементам  $\beta_1, \beta_2, \dots, \beta_u$ ,

$$\Delta_l = \begin{vmatrix} m_b & m_{b+1} & \dots & m_{b+l} \\ m_{b+1} & m_{b+2} & \dots & m_{b+l+1} \\ \dots & \dots & \dots & \dots \\ m_{b+l} & m_{b+l+1} & \dots & m_{b+2l} \end{vmatrix}, \quad l \in \mathbb{N}. \quad (3)$$

Тогда справедливы следующие утверждения:

- 1)  $\Delta_{u-1} = (W_{u-1})^2 \prod_{j=1}^u \beta_j k_j \neq 0$ ;
- 2)  $\Delta_l = 0$ , если  $l \geq u$ ;
- 3) для симметрического многочлена от двух переменных

$$T_l(x, y) = (\Delta_{l-1})^{-1} \begin{vmatrix} 0 & x^b & x^{b+1} & \dots & x^{b+l-1} \\ y^b & m_b & m_{b+1} & \dots & m_{b+l-1} \\ y^{b+1} & m_{b+1} & m_{b+2} & \dots & m_{b+l} \\ \dots & \dots & \dots & \dots & \dots \\ y^{b+l-1} & m_{b+l-1} & m_{b+l} & \dots & m_{b+2l-2} \end{vmatrix} \quad (4)$$

выполняется равенство

$$T_u(\beta_i, \beta_j) = \begin{cases} 0, & i \neq j, \\ -\frac{1}{k_j}, & i = j; \end{cases}$$

- 4) определитель

$$O_u(y) = \begin{vmatrix} 1 & m_b & \dots & m_{b+u-1} \\ y & m_{b+1} & \dots & m_{b+u} \\ \dots & \dots & \dots & \dots \\ y^u & m_{b+u} & \dots & m_{b+2u-1} \end{vmatrix} \quad (5)$$

является многочленом степени  $u$ , а множество его корней над полем  $\mathbb{F}_{q^r}$  исчерпывается набром  $\mathfrak{A}$ .

Доказательство утверждений леммы проводится по схеме доказательств аналогичных утверждений из [4]. Заметим лишь, что при  $b = 0$  (3), (4), (5) совпадают с соответствующими конструкциями из [4]. Лемма 1 позволяет построить алгоритм декодирования кода БЧХ. В самом деле, рассмотрим БЧХ-код, построенный по набору

$$N_{q^r}(\alpha, b, d) = \{\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+d-2}\}.$$

Предположим, что в результате передачи по каналу с помехами вектора  $\bar{c}$ , был получен вектор  $\bar{h}$ . Тогда  $\bar{h} = \bar{c} + \bar{e}$ , когда  $\bar{e}$  — вектор ошибок. Синдромом вектора ошибок называется вектор (см. [5])

$$\bar{s} = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \dots & \alpha^{(n-1)(b+d-2)} \end{pmatrix} \bar{h}. \quad (6)$$

Обозначим

$$\beta_1 = 1, \beta_2 = \alpha, \beta_3 = \alpha^2, \dots, \beta_n = \alpha^{n-1}.$$

В соответствии со сказанным выше  $\text{ord}(\alpha) = n$ , поэтому в последнем наборе все элементы ненулевые и различные. Предположим теперь, что в

процессе передачи произошло  $u$  ошибок, т. е. вектор  $\bar{e} = (e_1, e_2, \dots, e_n)$  имеет  $u$  отличных от нуля коэффициентов; пусть  $i_1, i_2, \dots, i_u$  — индексы этих коэффициентов. Тогда

$$s = \left( \sum_{j=1}^u e_{i_j} \beta_{i_j}^b, \dots, \sum_{j=1}^u e_{i_j} \beta_{i_j}^{b+u-1} \right) = (m_b, \dots, m_{b+u-1}).$$

### Алгоритм 1

Вход:  $\bar{V}_N$  — вектор, искаженный  $u$  ошибками, где  $u \leq \frac{d-1}{2}$ .

Выход:  $\bar{V}_R$  — восстановленное закодированное сообщение.

1. Вычислить синдром  $\bar{s}$  по формуле (6):

$$\bar{s} = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \dots & \alpha^{(n-1)(b+d-2)} \end{pmatrix} \bar{V}_N.$$

2.  $i := \left\lfloor \frac{d-1}{2} \right\rfloor$ .

3. Вычислить определитель  $\Delta_i$  по формуле (3):

$$\Delta_i = \begin{vmatrix} m_b & m_{b+1} & \dots & m_{b+i} \\ m_{b+1} & m_{b+2} & \dots & m_{b+i+1} \\ \dots & \dots & \dots & \dots \\ m_{b+i} & m_{b+i+1} & \dots & m_{b+2i} \end{vmatrix}, \quad l \in \mathbb{N}.$$

4.  $i := i - 1$ . Если  $i < 0$ ,  $t := 0$ ,  $\bar{V}_R := \bar{V}_N$ , вернуть  $\bar{V}_R$ , выйти из алгоритма.

5. Сформировать определитель  $\Delta_i$ . Если  $\Delta_i \neq 0$ ,  $t := i + 1$  и переход на шаг 6. Иначе — переход на шаг 4.

6. Сформировать определитель  $O_t(y)$  в соответствии с (5):

$$O_t(y) = \begin{vmatrix} 1 & m_b & \dots & m_{b+t-1} \\ y & m_{b+1} & \dots & m_{b+t} \\ \dots & \dots & \dots & \dots \\ y^t & m_{b+t} & \dots & m_{b+2t-1} \end{vmatrix}.$$

7. Найти множество позиций ошибок  $\mathfrak{R}$ , состоящее из всех корней уравнения  $O_t(y) = 0$ .

8. Сформировать определитель  $T_t(x, y)$  в соответствии с (4):

$$T_t(x, y) = (\Delta_{t-1})^{-1} \begin{vmatrix} 0 & x^b & x^{b+1} & \dots & x^{b+t-1} \\ y^b & m_b & m_{b+1} & \dots & m_{b+t-1} \\ y^{b+1} & m_{b+1} & m_{b+2} & \dots & m_{b+t} \\ \dots & \dots & \dots & \dots & \dots \\ y^{b+t-1} & m_{b+t-1} & m_{b+t} & \dots & m_{b+2t-2} \end{vmatrix}.$$

9. Для каждого элемента  $\nu \in \mathfrak{X}$  вычислить значения ошибки

$$k_\nu := -\frac{1}{T_t(\nu, \nu)}.$$

10. С помощью  $\mathfrak{X}$  и  $\{k_\nu\}$  вычислить вектор ошибки  $\bar{e}$ .

11. Вычислить  $\bar{V}_R := \bar{V}_N - \bar{e}$ . Возвратить  $\bar{V}_R$  и выйти из алгоритма.

#### 4. Обобщение на случай $t > \frac{d-1}{2}$

Будем теперь предполагать, что элементы  $k_1, k_2, \dots, k_u$  из последовательности, определенной в (1), могут быть нулевыми, и введем новые конструкции. Как и в разделе 3, при  $b = 0$  они совпадают с соответствующими конструкциями из [4]. Введем обозначения:

$$\Delta_{n,r} = \begin{vmatrix} 1 & \dots & 1 & m_b & \dots & m_{b+n-r} \\ \beta_1 & \dots & \beta_r & m_{b+1} & \dots & m_{b+n-r+1} \\ \beta_1^2 & \dots & \beta_r^2 & m_{b+2} & \dots & m_{b+n-r+2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \beta_1^n & \dots & \beta_r^n & m_{b+n} & \dots & m_{b+2n-r} \end{vmatrix}, \quad (7)$$

где  $r \leq n$  и  $n \in \mathbb{N} \cup \{0\}$ ;

$$D_u(y_1, y_2, \dots, y_r) = \begin{vmatrix} 1 & \dots & 1 & m_b & \dots & m_{b+u-r} \\ y_1 & \dots & y_r & m_{b+1} & \dots & m_{b+u-r+1} \\ y_1^2 & \dots & y_r^2 & m_{b+2} & \dots & m_{b+u-r+2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ y_1^u & \dots & y_r^u & m_{b+n} & \dots & m_{b+2u-r} \end{vmatrix}; \quad (8)$$

$$O_u(y_1, y_2, \dots, y_r) = \left( \prod_{i>j} (y_i - y_j) \right)^{-1} D_u(y_1, y_2, \dots, y_r). \quad (9)$$

Следующие леммы являются обобщениями соответствующих утверждений из работы [4]. Отметим, что их доказательства нетрудно провести по схеме доказательств из [4].

**Лемма 2.** Если  $\Delta_{n,r}$  — детерминант, определенный в (7), а  $u \in \mathbb{N}$ , то

- 1)  $\Delta_{u-1,r} \neq 0$  и  $\Delta_{n,r} = 0$  при  $n \geq u$ ,
- 2) линейная оболочка строк определителя  $\Delta_{n,r}$  равна  $u$  при  $n \geq u - 1$ .

**Лемма 3.** Пусть  $\Omega' = \{\omega_1, \omega_2, \dots, \omega_{r-1}\} \subset \mathbb{F}_{q^r} \setminus \{0\}$ , причем  $r \leq u$ .

Тогда

- 1) рациональная функция  $O_u(y, \omega_1, \omega_2, \dots, \omega_{r-1})$  является многочленом,
- 2)  $O_u(y, \beta_1, \beta_2, \dots, \beta_{r-1}) = C \prod_{j=r}^u (y - \beta_j)$ .

**Лемма 4.** Пусть  $\Omega' = \{\omega_1, \omega_2, \dots, \omega_{r-1}\} \subset \mathbb{F}_{q^r} \setminus \{0\}$ , причем  $r \leq u$ . Тогда справедливы следующие утверждения.

1) Если  $O_u(y, \omega_1, \omega_2, \dots, \omega_{r-1})$  — ненулевой многочлен степени  $u-r+1$ , разложимый в поле  $\mathbb{F}_{q^r}$ ,  $\Omega'' = \{\omega_r, \omega_{r+1}, \dots, \omega_u\}$  — его корни, кроме того,  $\Omega' \cap \Omega'' = \emptyset$  и  $\Omega' \cup \Omega'' \subsetneq \mathbb{F}_{q^r}$ , то найдутся такие элементы  $h_j \in \mathbb{F}_{q^r}$ , что моменты вычисляются по формуле

$$m_{b+i} = \sum_{j=1}^u h_j \omega_j^{b+i}, \quad i = 0, 1, \dots, 2u - r,$$

причем  $h_j \neq 0$  когда  $j = r, \dots, u$ .

2) Многочлен  $O_u(y, \omega_1, \omega_2, \dots, \omega_{r-1})$  является нулевым тогда и только тогда, когда моменты могут быть представлены в виде

$$m_{b+i} = \sum_{j=1}^{\nu} h_j \omega_j^{b+i},$$

где  $i = 0, \dots, 2u - r$  и  $\nu < u$ .

3) Если ненулевой многочлен  $O_u(y, \omega_1, \omega_2, \dots, \omega_{r-1})$  имеет степень, меньшую  $u - r + 1$ , то моменты  $m_{b+i}$  не могут быть представлены в виде

$$m_{b+i} = \sum_{j=1}^u h_j \omega_j^{b+i}, \quad i = 0, \dots, 2u - r,$$

для  $\omega_r, \omega_{r+1}, \dots, \omega_u$  и  $h_1, h_2, \dots, h_u$  из произвольных расширений полей  $\mathbb{F}_{q^r}$  и  $\mathbb{F}_q$  соответственно.

Леммы 2, 3, 4 позволяют построить алгоритм декодирования в случае, когда число ошибок больше половины кодового расстояния Боуза.

## Алгоритм 2

Вход:  $t$  — верхний порог числа ошибок,  $\bar{V}_N$  — вектор, искаженный не более, чем  $t$  ошибками.

Выход:  $\bar{V}_R$  — кодовый вектор.

1. Вычислить синдром  $s$  по формуле (6):

$$\bar{s} = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \dots & \alpha^{(n-1)(b+d-2)} \end{pmatrix} \bar{V}_N.$$

2. Выбрать случайным образом  $r \leq u$  и  $r$ -элементное подмножество  $\Omega' = \{\omega_1, \omega_2, \dots, \omega_r\}$  множества  $N_{q^r}(\alpha, b, d)$ .

3. Сформировать определитель в соответствии с (8):

$$D_u(y_1, y_2, \dots, y_r) = \begin{vmatrix} 1 & \dots & 1 & m_b & \dots & m_{b+u-r} \\ y_1 & \dots & y_r & m_{b+1} & \dots & m_{b+u-r+1} \\ y_1^2 & \dots & y_r^2 & m_{b+2} & \dots & m_{b+u-r+2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ y_1^u & \dots & y_r^u & m_{b+n} & \dots & m_{b+2u-r} \end{vmatrix}.$$

4. Найти множество  $\Omega''$  корней многочлена  $O_u(y, \omega_1, \omega_2, \dots, \omega_r)$ , определяемого в соответствии с (9):

$$O_u(y_1, y_2, \dots, y_r) = \left( \prod_{i>j} (y_i - y_j) \right)^{-1} D_u(y_1, y_2, \dots, y_r).$$

5. Проверить, выполнены ли следующие условия:

- а)  $\Omega' \cap \Omega'' = \emptyset$ ,
- б)  $\Omega' \cup \Omega'' \subsetneq \mathbb{F}_{q^r}$ ,
- в)  $|\Omega''| = t - r$ .

Если эти условия выполнены, перейти на шаг 6, в противном случае перейти на шаг 2.

6. Решить следующую систему уравнений над полем  $\mathbb{F}_{q^r}$ :

$$\sum_{\nu \in \Omega' \cup \Omega''} k_\nu \nu^{b+i} = m_{b+i}, \quad i = 0, \dots, t-1.$$

Если решение принадлежит полю  $\mathbb{F}_q$ , перейти на шаг 6; иначе — на шаг 2.

7. С помощью множества позиций ошибок  $\Omega' \cup \Omega''$  и множества соответствующих им значений ошибок  $\{k_\nu\}$ , вычислить вектор ошибок  $\bar{e}$ .

8. Вычислить  $\bar{V}_R := \bar{V}_N - \bar{e}$ . Возвратить  $\bar{V}_R$  и выйти из алгоритма.

Отметим, что быстрота работы алгоритма существенно зависит от того, когда на шаге 6 появится решение соответствующей системы, принадлежащее полю  $\mathbb{F}_q$ . Число ошибок  $t$ , подаваемое на вход описанного алгоритма можно оценивать, применяя следующий эвристический алгоритм определения числа ошибок.

### Алгоритм 3

Вход:  $\bar{V}_N$  — вектор, искаженный ошибками,  $0 < \epsilon < 1$  — оценочный коэффициент, параметр  $Q$  определяет порог прерывания алгоритма.

Выход:  $t$  — оценка количества ошибок в векторе или ошибка закливания.

1. Вычислить синдром  $\bar{s}$  вектора  $\bar{V}_N$  по формуле (6).
2.  $r := 0$ ,  $K := 0$ ,  $C := 0$ ,  $n := \lfloor \frac{d-1+r}{2} \rfloor$ . Выбрать случайным путем  $r$ -элементное множество  $\{\beta_1, \beta_2, \dots, \beta_r\} \subset \mathfrak{A}$ .
3.  $C := C + 1$ . Сформировать определитель

$$\Delta_{n,r} = \begin{vmatrix} 1 & \dots & 1 & m_b & \dots & m_{b+n-r} \\ \beta_1 & \dots & \beta_r & m_{b+1} & \dots & m_{b+n-r+1} \\ \beta_1^2 & \dots & \beta_r^2 & m_{b+2} & \dots & m_{b+n-r+2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \beta_1^n & \dots & \beta_r^n & m_{b+n} & \dots & m_{b+2n-r} \end{vmatrix}.$$

4. Если  $\Delta_{n,r} = 0$  и  $n > r$ , то  $n := n - 1$  и перейти на шаг 3.
5. Если  $\Delta_{n,r} = 0$  и  $n = r$ , положить  $t := r$  и выйти из алгоритма.

6. Если  $\Delta_{n,r} \neq 0$  и  $n < \left\lfloor \frac{d-1+r}{2} \right\rfloor$ , положить  $t := n+1$  и выйти из алгоритма.
7. Если  $C > Q$ , выдать ошибку заикливания и выйти из алгоритма.
8. Если  $K > 0$ , перейти на шаг 11; если  $K = 0$ , перейти на шаг 9.
9. Если  $r = 0$ , то положить  $r := 0$ , если  $d-1$  нечетное число, или  $r := 2$ , если  $d-1$  четное число. В противном случае  $r := r+2$ .
10. Вычислить  $p := \frac{C_n^r}{C_{|\mathfrak{A}|}^r}$ ,  $K := \frac{\ln(1-\epsilon)}{\ln(1-p)}$ .
11. Выбрать любое  $\{\beta_1, \beta_2, \dots, \beta_r\} \subset \mathfrak{A}$ ,  $K := K+1$ . Перейти на шаг 3.

Описанные в настоящей работе алгоритмы реализованы с использованием библиотеки GFL, предназначенной для вычислений в конечных полях [1].

Коды БЧХ, вообще говоря, не являются MDS-кодами и поэтому уступают с точки зрения числа исправляемых ошибок кодам Рида–Соломона. Однако, благодаря конструктивному построению, БЧХ-коды не имеют столь жестких ограничений на длину и размерность. Ввиду этого, они находят применение в тех случаях, когда использование кодов Рида–Соломона оказывается затруднительным [5]. Таким образом, представленный в настоящей статье декодер имеет в некотором смысле более широкий спектр применения, нежели декодер Сидельникова.

## Список литературы

1. Бибов А. Ю. О новой библиотеке для вычислений в конечных полях и ее применении в реализации кодека Сидельникова // Материалы Международного Российско-Абхазского симпозиума “Уравнения смешанного типа и родственные проблемы анализа и информатики”. – Нальчик: Эльбрус, 2009. – С. 261–262.
2. Деундяк В. М., Харченко Д. В. О реализации помехоустойчивых кодеков на эллиптических кривых с использованием алгоритмов декодирования Серебрякова // Вестник ДГТУ. – 2005. – Т. 5. – № 1 (23). – С. 7–11.
3. Серебряков А. Ю. Декодирование кодов на эллиптических кривых при числе ошибок, большем половины конструктивного кодового расстояния // Проблемы передачи информации. – 1997. – Т. 3. – № 3. – С. 29–38.
4. Сидельников В. М. Декодирование кодов Рида–Соломона при числе ошибок, большем  $(d-1)/2$ , и нули многочленов нескольких переменных // Проблемы передачи информации. – 1994. – Т. 30. – № 1. – С. 51–69.
5. Сидельников В. М. Теория кодирования. – М.: Физматлит, 2008. – 322 с.

Поступила в редакцию 26.03.2010.