

**ПОСТРОЕНИЕ ОБОБЩЕННЫХ КАСКАДНЫХ КОДОВ
С АЛГЕБРОГЕОМЕТРИЧЕСКИМИ КОДАМИ НА ВНЕШНÉЙ СТУПЕНИ**

В.И. Грабчак, канд. техн. наук;
А.П. Мельник*

*Львовский институт Сухопутных войск Национального университета
“Львовская политехника”, г. Львов*

**Научный центр боевого применения РВиА Сумского государственного
университета, г. Сумы*

В статье исследуются вопросы построения обобщенных каскадных кодов с алгебрографетическими кодами на внешней ступени. Рассматривается процедура кодирования и декодирования алгебрографетическими кодами на внешней ступени обобщенного каскадного кода.

У статті досліджуються питання побудови узагальнених каскадних кодів з алгебрографетичними кодами на зовнішньому ступені. Розглядається процедура кодування та декодування алгебрографетичними кодами на зовнішньому ступені узагальненого каскадного коду.

**ПОСТАНОВКА ПРОБЛЕМЫ В ОБЩЕМ ВИДЕ
И АНАЛИЗ ЛИТЕРАТУРЫ**

Каскадные (составные) коды впервые были предложены Форни в качестве метода практической реализации кода с большой длиной и весьма высокой корректирующей способностью. Эти цели достигаются при наличии нескольких уровней кодирования многими различными способами. При применении таких кодов хорошие характеристики получаются путем увеличения общей длины блока при одновременном уменьшении практической сложности реализации [1- 3].

Наиболее распространенной схемой построения каскадных кодов, является схема с двумя уровнями кодирования. В качестве внешнего кода, как правило, используются коды Рида-Соломона. Эти коды наиболее широко распространены, поскольку являются кодами с максимально достижимым расстоянием ($d = n - k + 1$) и относительно просто реализуются. В качестве внутреннего кода можно выбрать один из многих различных кодов [1, 2].

Общим классом каскадных кодов, которые имеют более двух уровней кодирования, являются обобщенные каскадные коды. Алгебраической теории построения обобщенных каскадных кодов, исследованию сложности их реализации посвящена монография [4]. Обобщенные каскадные коды являются одним из наиболее общих схем каскадного кодирования и являются, в теоретическом плане, обобщением большинства известных каскадных кодовых конструкций (итерированные коды, каскадные коды и коды для локализации ошибок).

Одним из перспективных направлений в развитии теории помехоустойчивого кодирования являются методы алгебрографетического кодирования, которые обобщают (содержат как подкласс) коды Рида-Соломона. Алгебрографетические коды как линейные системы, построенные по точкам алгебраических кривых, впервые были предложены в работах Гоппы В.Д. [5, 6]. Они принадлежат подклассу линейных блоковых кодов и являются обобщением хорошо известных кодов Рида-Соломона и кодов Гоппы. Основное достоинство методов алгебрографетического кодирования состоит в построении длинных недвоичных блоковых кодов, обладающих хорошими асимптотическими

свойствами. Их практическое использование позволяет исправлять сложные комбинации коррелированных ошибок [7].

Целью статьи являются построение обобщенных каскадных кодов с алгебро-геометрическими кодами на внешней ступени, разработка процедуры кодирования и декодирования алгебро-геометрическими кодами на внешней ступени обобщенного каскадного кода.

ОСНОВНАЯ ЧАСТЬ

Обобщенные каскадные коды. Исходными данными для описания обобщенного каскадного кода являются [4]:

– двоичное слово c длины $n = n_1 n_2$, которое представляется в виде последовательности двоичных векторов C_j , $j = \overline{1, n_2}$, длины n_1 , т.е.

$$c = (c_1, c_2, \dots, c_{n_1}, c_{n_1+1}, \dots, c_{2n_1}, c_{2n_1+1}, \dots, c_{n_2 n_1}) = ((c_1, c_2, \dots, c_{n_1}), (c_{n_1+1}, \dots, c_{2n_1}), \dots, (c_{2n_1+1}, \dots, c_{n_2 n_1})) = (C_1, C_2, \dots, C_{n_2}), C_j = (c_{(j-1)n_1+1}, \dots, c_{jn_1}); \quad (1)$$

– n_2 квадратных двоичных матриц H_0^j , $j = \overline{1, n_2}$, порядка n_1 ;

– $m + 1$ групповых над $GF(2^{a_i})$, $i = \overline{1, m + 1}$, кодов (кодов внешней ступени) с параметрами (n_2, b_i, d_{2i}) . При этом выполняется

равенство $\sum_{i=1}^{m+1} a_i = n_1$.

В основном варианте построения обобщенных каскадных кодов в качестве матриц H_0^j для всех $j = \overline{1, n_2}$ выбирается одна и та же треугольная матрица H_0 порядка n_1 , которая в клеточной форме имеет вид

$$H_0 = \begin{vmatrix} I_{a_1} & & & & & & \\ P_{11} & I_{a_2} & & & & & 0 \\ P_{21} & P_{22} & I_{a_3} & & & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ P_{m1} & P_{m2} & P_{m3} & \dots & P_{mm} & I_{a_{m+1}} & \end{vmatrix} = \begin{vmatrix} \tilde{H}_0 \\ \tilde{H}_1 \\ \tilde{H}_2 \\ \vdots \\ \tilde{H}_m \end{vmatrix}, \quad (2)$$

где

$$\tilde{H}_i = \begin{vmatrix} P_{i_1} & P_{i_2} & \dots & P_{i_i} & I_{a_1} & 0 & \dots & 0 \end{vmatrix}, i = \overline{1, m}, \quad (3)$$

клетки P_{i_s} – двоичные матрицы размеров $a_{i+1} \times a_s$, I_{a_s} – единичная матрица порядка a_s .

Проверочная матрица H_i , вида

$$H_i = \begin{vmatrix} \tilde{H}_i \\ \tilde{H}_{i+1} \\ \vdots \\ \tilde{H}_m \end{vmatrix} = \begin{vmatrix} P_{i_1} & P_{i_2} & \dots & P_{i_i} & I_{a_{i+1}} & 0 \\ P_{i+1_1} & P_{i+1_2} & \dots & P_{i+1_i} & P_{i+1_{i+1}} & I_{a_{i+2}} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ P_{m_1} & P_{m_2} & \dots & P_{m_i} & P_{m_{i+1}} & \dots & P_{m_m} & I_{a_{m+1}} \end{vmatrix}, i = \overline{1, m}, \quad (4)$$

полностью определяемая матрицей H_0 (состоит из $m-i+1$ клеточных строк матрицы H_0) задает i -й код внутренней ступени с параметрами (n_1, k_i, d_{1i}) . При этом для числа информационных символов i -го кода выполняется соотношение $k_i = a_1 + a_2 + \dots + a_i$.

Зафиксируем линейное отображение векторов C_j :

$$C_j H_0^T = (\gamma_{1j}, \gamma_{2j}, \dots, \gamma_{m+1j}), \quad j = \overline{1, n_2}, \quad (5)$$

где γ_{ij} – двоичный вектор длины a_i .

Трактуя векторы γ_{ij} как элементы поля $GF(2^{a_i})$, составим из этих элементов, полученных в результате отображения (5) (для каждого слова c), векторы $\gamma_i = (\gamma_{i1}, \gamma_{i2}, \dots, \gamma_{in_i})$, $i = \overline{1, m+1}$.

По определению [4] двоичное слово c длины $n = n_1 n_2$ является кодовым словом обобщенного каскадного кода порядка m тогда и только тогда, когда все связанные со словом c векторы γ_i , $i = \overline{1, m+1}$, представляют собой кодовые слова соответствующих (i -х) кодов внешней ступени.

Во многих случаях удобна следующая геометрическая трактовка обобщенного каскадного кода (рис.1).

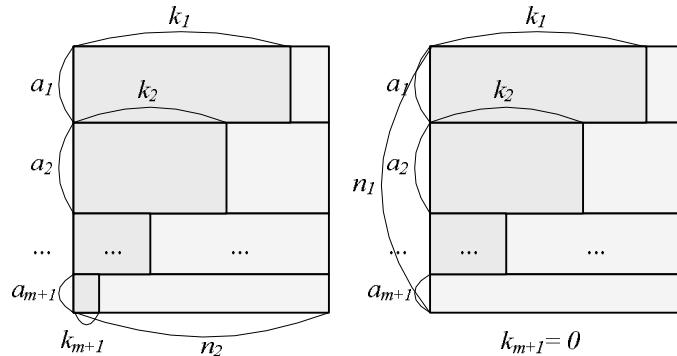


Рисунок 1 – Геометрическая трактовка обобщенного каскадного кода

Величины $a_i > 0$ и $b_i \geq 0$, определяющие внутреннюю структуру обобщенного каскадного (n, k, d) кода, выбираются произвольно, при этом (n, k, d) параметры удовлетворяют следующим соотношениям [4]:

$$n = n_1 n_2; \quad k = \sum_{i=1}^{m+1} a_i b_i; \quad d \geq \begin{cases} \min \{ d_{1i} d_{2i} : i = \overline{1, m} \} & \text{при } b_{m+1} = 0, \\ \min \{ d_{2m+1}, d_{1i} d_{2i} : i = \overline{1, m} \} & \text{при } b_{m+1} \neq 0. \end{cases}$$

АЛГЕБРОГЕОМЕТРИЧЕСКИЕ КОДЫ

АГК как линейные системы на алгебраических кривых впервые были предложены Гоппой В.Д. [5,6]. Коды, построенные по кривым с большим числом точек по сравнению с родом, лежат выше границы Варшамова-Гилberta. Рассмотрим общую схему построения АГК [5,8].

Пусть $X(GF(q))$ - множество точек кривой X над конечным полем $GF(q)$, $N = |X(GF(q))|$ - их число. Число N точек кривой X над $GF(q)$ ограничено сверху выражением Хассе-Вейля [5, 7]

$$N \leq 2\sqrt{q} \cdot g + q + 1,$$

где $g = g(X)$ - род кривой.

Пусть C - класс дивизоров на X степени α . Тогда C задает отображение $\varphi : X \rightarrow P^m$, набор генераторных функций $y_i = \varphi(x_i)$ задает АГК длины $n \leq N$.

Кодовые характеристики (n, k, d) связаны соотношением [5, 7]: $k + d \geq n - g + 1$.

Если $2g - 2 < \alpha \leq n$, код связан характеристиками $(n, \alpha - g + 1, d)$, $d \geq n - \alpha$. Дуальный к нему код также является алгеброгеометрическим с характеристиками

$$(n, n - \alpha + g - 1, d_{\perp}), \quad d_{\perp} \geq \alpha - 2g + 2.$$

Кодирование алгеброгеометрическими кодами. Рассмотрим вариант построения АГК, заданного через порождающую матрицу [8].

АГК над $GF(q)$ построенный через отображение кривой X вида $\varphi : EC \rightarrow P^{k-1}$ это линейный код длины $n \leq N$, кодовые слова $C(c_1, c_2, \dots, c_{n-1})$ которого задаются равенством

$$\sum_{j=0}^{k-1} I_j F_j(P_i) = c_i, \quad (6)$$

где $P_i(X_i, Y_i, Z_i)$ - проективные точки кривой X , т.е. (X_i, Y_i, Z_i) - решения однородного алгебраического уравнения, задающие кривую X , $i = \overline{1, n}$; $F_j(P_i)$ - значения генераторных функций в точках кривой.

Это определение равносильно матричному представлению АГК:

$$G (i_0, i_1, \dots, i_{k-1})^T = (c_0, c_1, \dots, c_{n-1}),$$

где G - порождающая матрица размерности $k \times n$, $k = \alpha \cdot g + 1$, $\alpha = \deg X \cdot \deg F$.

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,k}. \quad (7)$$

Кодовое слово, в этом случае, может быть сформировано (в матричной форме) как произведение информационного вектора-строки на порождающую матрицу

$$\|c_j\|_n = G \|I_i\|_k^T = \|F_i(P_j)\|_{n,k} \|I_i\|_k^T.$$

АГК над $GF(q)$ построенный через отображение кривой X вида $\varphi: EC \rightarrow P^{r-1}$ это линейный код длины $n \leq N$, кодовые слова $C(c_1, c_2, \dots, c_{n-1})$ которого задаются равенством

$$\sum_{j=0}^{n-1} c_i F_j(P_i) = 0, \quad (8)$$

где $c_i \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = \deg X \cdot \deg F$.

Это определение равносильно матричному представлению АГК: $H (c_0, c_1, \dots, c_{n-1})^T = 0$, где H – проверочная матрица размерности $r \times n$, $r = n - k = d + g - 2$.

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \dots & F_{r-1}(P_{n-1}) \end{pmatrix} = \|F_j(P_i)\|_{n,r}. \quad (9)$$

Для формирования кодовых слов заданного таким образом АГК воспользуемся приемами обращения матриц [8, 9, 10].

Разобьем кодовое слово $(c_0, c_1, \dots, c_{n-1})$ на множества информационных и проверочных позиций. Пусть U – множество k информационных позиций кодового слова и W – множество $r = n - k$ проверочных позиций. Объединение множеств $U \cup V$ содержит все целые числа (номера) от 0 до $n - 1$. На k информационных позициях кодового слова, т.е. на позициях множества U разместим k символов сообщения $(I_0, I_1, \dots, I_{k-1})$, а на проверочных позициях множества W разместим r нулевых символов.

Вычислим суммы $S_j = \sum_{i=0}^{n-1} c_i F_j(P_i)$, $j = \overline{0, r-1}$, или в матричной форме

$$\|S_j\|_r = \|F_j(P_i)\|_{k,r} \|c_i\|_k^T. \quad (10)$$

Задача формирования кодового слова АГК, заданного через проверочную матрицу, состоит в том, чтобы вычислить и записать на r проверочных позициях такие символы c_i $i \in W$, которые удовлетворяют уравнениям (8). Значения $r = n - k$ проверочных символов могут быть

найдены из системы линейных уравнений $\sum_{i \in W}^{n-1} c_i F_j(P_i) = -S_j$, $j = \overline{0, r-1}$.

В матричном представлении последняя запись эквивалентна выражению $\|F_j(P_i)\|_{r,r} \|c_i\|_r^T = \|-S_j\|_r$. Для нахождения значений $r = n - k$ проверочных символов используем методы обращения матриц [10], запишем $\|c_i\|_r = \|F_j(P_i)\|_{r,r}^{-1} \|-S_j\|_r^T$, где $\|F_j(P_i)\|_{r,r}^{-1}$, матрица, обратная матрице $\|F_j(P_i)\|_{r,r}$. Поскольку размещение проверочных позиций обычно известно и фиксировано, то заранее можно найти обратную матрицу для системы

уравнений (10) и получить все проверочные символы умножением вектора $(S_0, S_1, \dots, S_{r-1})$ на матрицу $\|F_j(P_i)\|_{r,r}^{-1}$.

Рассмотренный алгоритм построения АГК может быть эффективно использован при реализации процедуры кодирования во внешнем каскаде обобщенных каскадных кодов.

Декодирование алгебрографетическими кодами. Предположим, что при передаче по каналу с ошибками кодовое слово алгебрографетического кода исказилось, вектор ошибок обозначим как $e = (e_0, e_1, \dots, e_{n-1})$. Принятое слово c^* , после передачи по каналу с ошибками запишется в виде

$$c^* = c + e = (e_0 + c_0, e_1 + c_1, \dots, e_{n-1} + c_{n-1}).$$

Определим синдромную последовательность как вектор $S = (S_1, S_2, \dots, S_r)$, вычисленный по следующему правилу

$$S_j = \sum_{i=0}^{n-1} c^* \cdot F_j(P_i), \quad j = \overline{1, r},$$

или в матричной форме $\|S_j\|_r = \|F_j(P_i)\|_{n,r} \|c^*\|_n^T$. Очевидно, что

$$S_j = \sum_{i=0}^{n-1} [c_i \cdot F_j(P_i) + e_i \cdot F_j(P_i)] = \sum_{i=0}^{n-1} e_i \cdot F_j(P_i), \quad j = \overline{1, r},$$

или в матричной форме $\|S_j\|_r = \|F_j(P_i)\|_{n,r} \cdot \|e_i\|_n^T = H \|e_i\|_n^T$, значение синдрома зависит только от вектора ошибок и не зависит от кодового слова.

Задача декодирования алгебрографетического кода состоит в нахождении вектора ошибок $e = (e_0, e_1, \dots, e_{n-1})$ по известной синдромной последовательности $S = (S_0, S_1, \dots, S_{r-1})$.

Рассмотрим в качестве генераторных функций однородные одночлены степени $\deg F$. Каждый такой одночлен запишем в виде $f_{lmp} = x^l y^m z^p$, $l + m + p = \deg F$.

На множестве проективных точек кривой X , представимых в однородных координатах в виде $P(X, Y, 1)$, значения генераторных функций примут вид $f_{lm} = X_i^l Y_i^m$, $i = \overline{0, n-1}$, $1 + m \leq \deg F$. Проверочная матрица H запишется в виде

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ X_0 & X_1 & \dots & X_{n-1} \\ \dots & \dots & \dots & \dots \\ Y_0^{\deg F} & Y_1^{\deg F} & \dots & Y_{n-1}^{\deg F} \end{pmatrix}.$$

Элементы синдромной последовательности, как элементы вектора $\|S_{lm}\|_r$, вычислим по правилу $S_{lm} = \sum_{i=0}^{n-1} c_i^* X_i^l Y_i^m = \sum_{i=0}^{n-1} e_i X_i^l Y_i^m$, $1 + m \leq \deg F$, или, в матричной форме

$$\|S_{lm}\|_r = H \left\| c_n^* \right\|_n^T = \left\| X_i^l Y_i^m \right\|_{n,r} \left\| e_i \right\|_n^T. \quad (11)$$

Таким образом, задача декодирования алгебрографетического кода, построенного через отображение проективных точек $P(X, Y, 1)$ кривой однородными одночленами степени $\deg F$, эквивалентна задаче решения системы из $r = d + g - 1$ нелинейных уравнений от $3t$ переменных.

Для решения этой задачи воспользуемся искусственным приемом, заключающимся во введении в рассмотрение многочлена локаторов ошибок, решения которого однозначно локализуют (указывают местоположение) возникших ошибок. Задача декодирования алгебрографетического кода осложняется тем, что для локализации ошибок в алгебрографетическом кодовом слове необходимо указать как минимум две координаты X и Y , которые однозначно укажут на положение возникшей ошибки, т.е. укажут на точку $P(X, Y, 1)$ алгебраической кривой, образ которой соответствует кодовому символу, искаженному в результате воздействия помех.

Определим многочлен локаторов ошибок алгебрографетического кода как многочлен от двух переменных степени $\leq (t - 1)$:

$$a_{00} + a_{10}x + \dots + y^{t-1} = 0, \quad (12)$$

где t – число ошибок, которое может исправить алгебрографетический код.

Умножив обе части многочлена (12) на e_i и просуммировав по всем $i = \overline{0, n-1}$ значениям в точке ($x = X_i, y = Y_i$), получим рекуррентное выражение $a_{i,j}S_{i,j} + a_{i+1,j}S_{i+1,j} + \dots + S_{i,t-1} = 0$, которое задает систему линейных уравнений относительно неизвестных коэффициентов многочлена локаторов ошибок. В матричном виде система линейных уравнений запишется в виде

$$\begin{pmatrix} S_{00} & S_{10} & \dots & S_{1,t-2} \\ S_{10} & S_{20} & \dots & S_{2,t-2} \\ \dots & \dots & \dots & \dots \\ S_{1,t-2} & S_{0,t-2} & \dots & S_{2,2t-4} \end{pmatrix} \cdot \begin{pmatrix} a_{00} \\ a_{10} \\ \dots \\ a_{1,t-2} \end{pmatrix} = \begin{pmatrix} -S_{0,t-1} \\ -S_{1,t-1} \\ \dots \\ -S_{1,2t-3} \end{pmatrix}. \quad (13)$$

После нахождения коэффициентов многочлена локаторов ошибок процедура локализации ошибок состоит в подстановке всех возможных локаторов и выборе тех из них, которые обращают в нуль многочлен локаторов ошибок. После нахождения локаторов ошибок, указывающих на расположение возникшей ошибки, процедура нахождения кратности ошибки (значение всех $e_i \neq 0$) состоит в подстановке локаторов в систему (11), которая вырождается в систему $\leq r$ линейных уравнений относительно $\leq t$ неизвестных. Алгоритм декодирования алгебрографетических кодов представим в виде последовательности следующих шагов.

Шаг 1. По выражению (11) вычислим элементы синдромной последовательности.

Шаг 2. Решим систему линейных уравнений (13). Получим коэффициенты многочлена локаторов ошибок.

Шаг 3. Воспользуемся процедурой Ченя. Применительно к декодированию алгебрографетических кодов она состоит в подстановке всех пар (X, Y) , соответствующих проективным точкам кривой, в

многочлен локаторов ошибок. Те пары, которые при подстановке в этот многочлен обращают его в нуль, локализуют ошибки, т.е. указывают на их искомое расположение.

Шаг 4. Подставляем полученные локаторы ошибок в систему уравнений (8). Решение системы линейных уравнений даст значения (кратность) произошедших ошибок. Локализация ошибок и найденные их значения позволяют сформировать вектор ошибок $e = (e_0, e_1, \dots, e_{n-1})$.

Шаг 5. Исправим ошибки: $c = c^* - e$.

Рассмотренный алгоритм декодирования АГК может быть эффективно использован при реализации процедуры декодирования во внешнем каскаде обобщенных каскадных кодов.

ВЫВОДЫ

Для практической реализации кода с большой длиной и высокой корректирующей способностью в статье рассматривается вариант построения каскадных кодов, общим классом которых, являются обобщенные каскадные коды с алгебро-геометрическими кодами на внешней ступени.

Рассмотрена процедура кодирования и декодирования алгебро-геометрических кодов, которая может быть эффективно использована при реализации процедуры кодирования и декодирования во внешнем каскаде обобщенных каскадных кодов.

SUMMARY

THE CONSTRUCTION OF GENERALIZED CASCADE CODES WITH ALGEBROGEOMETRICAL CODES ON THE EXTERNAL LEVEL

*V.I. Grabchak, A.P. Melnyk**

L'viv Institute of Land Forces at The National University "L'vivska Politehnika;

**Sumy State University*

The questions of construction of generalized cascade codes with algebrogeometrical codes on the external level are investigated in the article. The procedure of encoding and decoding with algebrogeometrical codes on the external level of generalized cascade code.

СПИСОК ЛИТЕРАТУРЫ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
2. Бернард Склар. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.
3. Злотник Б. М. Помехоустойчивые коды в системах связи. – М.: Радио и связь, 1989. – 232 с.
4. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. – М.: Связь, 1976. – 240с.
5. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т.259, № 6. – С. 1289-1290.
6. Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. – Т.30, Вып. 1(235). – С. 77-120.
7. Кузнецов А.А. Энергетический выигрыш алгебро-геометрического кодирования. // Всеукр. меж вед. науч.-техн. сб. – Харьков: ХТУРЭ, 2003. – Вып.184. – С. 218-222.
8. Науменко М.І., Стасев Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів. Монографія. – Х.: ХУ ПС, 2005. – 267 с.
9. Гантмахер Ф.Р. Теория матриц. - М.: Наука, 1988. – 552 с.
10. Грабчак В.И., Паслько И.В., Королев Р.В., Кужель И.Е. Алгебро-геометрическое кодирование алгебро-геометрическими кодами на пространственных кривых // Системи обробки інформації. – Харків: ХУПС, 2007. – Вип. 8 (66). – С. 134-138.

Поступила в редакцию 24 марта 2009 г.