УДК 621.391

В.И. Грабчак[1], И.В. Пасько[1], Р.В. Королев[2], И.Е. Кужель[2]

[1]*Военный институт ракетных войск и артиллерии им. Б. Хмельницкого Сумского государственного университета*
[2]*Харьковский университет Воздушных Сил им. И. Кожедуба*

# АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ АЛГЕБРОГЕОМЕТРИЧЕСКИМИ КОДАМИ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ

*Рассматриваются алгеброгеометрические коды построенные на пространственных кривых. Предлагается алгебраический алгоритм кодирования кодов на пространственных кривых в систематическом и несистематическом виде.*

***алгеброгеометрические коды, пространственные кривые***

## Введение

**Постановка проблемы в общем виде, анализ литературы**. Одним из эффективных средств повышения достоверности передачи данных и защиты информации от ошибок в телекоммуникационных системах является помехоустойчивое кодирование информации [1 – 3]. Основными требованиями к помехоустойчивому кодированию являются высокая обнаруживающая и исправляющая способность кода, низкая вносимая избыточность, высокое быстродействие и низкая сложность реализации процедур кодирования-декодирования [4 – 7]. Перспективным направлением развития помехоустойчивого кодирования являются коды, возникающие на алгебраических кривых (алгеброгеометрические коды) [8, 9]. Использование этих кодов в каналах позволяет значительно снизить вероятность ошибочного приема дискретных сообщений и получить энергетический выигрыш от кодирования [10]. Однако, методы построения алгеброгеометрических кодов исследованы для кривых, заданных в проективном пространстве $P^2$ неприводимым однородным уравнением от трех переменных [9, 11]. Этот подход позволяет строить простые схемы кодирования и декодирования алгеброгеометрических кодов, длина которых над конечным полем GF(q) не превышает $q^2$ [11]. Перспективным направлением дальнейших исследований является разработка методов и алгоритмов построения алгеброгеометрических кодов на пространственных кривых, задаваемых в проективном пространстве $P^3$ совместными решениями совокупности двух однородных уравнений от четырех переменных.

**Целью статьи** является разработка практических алгоритмов помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых, оценка сложности их реализации.

## Основной материал

**Алгебраический метод помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых в $P^3$.**

Зафиксируем гладкую проективную алгебраическую кривую X в проективном пространстве $P^3$ над полем $GF(q)$ как это совокупность решений двух однородных неприводимых алгебраических уравнений от 4-х переменных с коэффициентами из $GF(q)$:

$$\begin{cases} f_1(x_0,x_1,x_2,x_3)=0; \\ f_2(x_0,x_1,x_2,x_3)=0. \end{cases} \quad (1)$$

Пусть $p_0(x_0,x_1,x_2,x_3)$, $p_1(x_0,x_1,x_2,x_3)$, …, $p_{N-1}(x_0,x_1,x_2,x_3)$ – N совместных решений системы уравнений (1) – точек пространственной кривой X.

Зафиксируем дивизор D кривой X и множество рациональных функций, ассоциированных с дивизором D, т.е. множество, состоящее из нуля и функций $f \neq 0$, для которых $(f)+D \geq 0$. Это эквивалентно набору генераторных функций:

$$F_0(x_0,x_1,x_2,x_3);\ F_1(x_0,x_1,x_2,x_3);$$
$$F_2(x_0,x_1,x_2,x_3);\ \ldots;\ F_m(x_0,x_1,x_2,x_3),$$

где $F_0,F_1,\ldots,F_m$ – формы одинаковой степени и $F_0(x_0,x_1,x_2,x_3)\neq 0$.

Иначе говоря,

$$\varphi(x)=(F_0(x),F_1(x),\ldots,F_m(x)),$$

как точка в $P^m$.

Пусть $\alpha$ – степень класса дивизоров, $\alpha > g-1$, тогда отображение $\varphi: X \to P^m$ задает порождающую матрицу

$$G=\begin{pmatrix} F_0(p_0(x_0,x_1,x_2,x_3)) & F_0(p_1(x_0,x_1,x_2,x_3)) & \ldots & F_0(p_{n-1}(x_0,x_1,x_2,x_3)) \\ F_1(p_0(x_0,x_1,x_2,x_3)) & F_1(p_1(x_0,x_1,x_2,x_3)) & \ldots & F_1(p_{n-1}(x_0,x_1,x_2,x_3)) \\ \ldots & \ldots & \ldots & \ldots \\ F_m(p_0(x_0,x_1,x_2,x_3)) & F_m(p_1(x_0,x_1,x_2,x_3)) & \ldots & F_N(p_{n-1}(x_0,x_1,x_2,x_3)) \end{pmatrix} \quad (2)$$

 

алгеброгеометрического кода, с конструктивными характеристиками

$$(n \le N, k \ge \alpha - g + 1, d \ge n - \alpha).$$

Алгеброгеометрический код на пространственной кривой X над GF(q) построенный через порождающую матрицу G – это линейный код, все кодовые слова ($c_0$, $c_1$, …, $c_{n-1}$) которого задаются равенством

$$\sum_{i=0}^{m-1} I_i F_i\left(p_j\left(x_0, x_1, x_2, x_3\right)\right) = c_j, \ j = 0, \ldots, n-1.$$

Для формирования кодового слова

$$\left(c_0, c_1, \ldots c_{n-1}\right)$$

алгеброгеометрического кода на пространственных кривых, заданного через порождающую матрицу достаточно умножить информационный вектор

$$\left(I_0, I_1, \ldots I_{k-1}\right)$$

на матрицу (2), т.е. для всех $j = 0, \ldots, n-1$ выполнить следующее преобразование:

$$c_j = \sum_{i=0}^{m-1} I_i F_i\left(p_j\left(x_0, x_1, x_2, x_3\right)\right). \qquad (3)$$

Пусть $\alpha > 2g - 2$, тогда отображение $\varphi : X \to P^{m-1}$ задает проверочную матрицу

$$H = \begin{pmatrix} F_0\left(p_0\left(x_0, x_1, x_2, x_3\right)\right) & F_0\left(p_1\left(x_0, x_1, x_2, x_3\right)\right) & \ldots & F_0\left(p_{n-1}\left(x_0, x_1, x_2, x_3\right)\right) \\ F_1\left(p_0\left(x_0, x_1, x_2, x_3\right)\right) & F_1\left(p_1\left(x_0, x_1, x_2, x_3\right)\right) & \ldots & F_1\left(p_{n-1}\left(x_0, x_1, x_2, x_3\right)\right) \\ \ldots & \ldots & \ldots & \ldots \\ F_m\left(p_0\left(x_0, x_1, x_2, x_3\right)\right) & F_m\left(p_1\left(x_0, x_1, x_2, x_3\right)\right) & \ldots & F_N\left(p_{n-1}\left(x_0, x_1, x_2, x_3\right)\right) \end{pmatrix} \qquad (4)$$

алгеброгеометрического кода, с конструктивными характеристиками

$$\left(n \le N, k \ge n - \alpha + g - 1, d \ge \alpha - 2g + 2\right).$$

Алгеброгеометрический код по кривой X над GF(q) построенный через проверочную матрицу H – это линейный код, состоящий из всех слов ($c_0$, $c_1$, …, $c_{n-1}$) длины $n \le N$, для которых выполняется равенство d + g – 1 уравнений

$$\sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right) = 0, \quad j = 0, \ldots, m. \qquad (5)$$

Для формирования кодовых слов заданного таким образом алгеброгеометрического кода на пространственных кривых воспользуемся приемами обращения матриц.

Разобьем кодовое слово

$$\left(c_0, c_1, \ldots c_{n-1}\right)$$

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∪W 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

$$\left(I_0, I_1, \ldots I_{k-1}\right),$$

а на проверочных позициях множества W разместим r нулевых символов.

Вычислим суммы

$$S_j = \sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right), \ j = \overline{0, r-1},$$

или в матричной форме

$$\left\|S_j\right\|_r = \left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{k,r} \left\|c_i\right\|_k^T. \qquad (6)$$

Задача формирования кодового слова состоит в том, чтобы вычислить и записать на r проверочных позициях такие символы $c_i$, $i \in W$, которые удовлетворяют уравнениям (5).

Из определения 2 алгеброгеометрического кода следует, что значения r = n – k проверочных символов могут быть найдены из системы линейных уравнений

$$\sum_{i \in W} c_i F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right) = -S_j, \ j = \overline{0, r-1}.$$

В матричном представлении последняя запись эквивалентна выражению

$$\left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{r,r} \left\|c_i\right\|_r^T = \left\|-S_j\right\|_r.$$

Для нахождения значений r = n – k проверочных символов, используя методы обращения матриц, запишем

$$\left\|c_i\right\|_r = \left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{r,r}^{-1} \left\|-S_j\right\|_r, \qquad (7)$$

где $\left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{r,r}^{-1}$ – матрица, обратная матрице $\left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{r,r}$.

Поскольку размещение проверочных позиций обычно известно и фиксировано, то заранее можно найти обратную матрицу для системы уравнений (6) и получить все проверочные символы умножением вектора $\left(S_0, S_1, \ldots S_{r-1}\right)$ на матрицу $\left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{r,r}^{-1}$.

В качестве информационных могут быть выбраны любые k позиций кодового слова. Следовательно, всегда можно выбрать такое множество проверочных (и информационных) позиций, для которого матрица

$$\left\|F_j\left(p_i\left(x_0, x_1, x_2, x_3\right)\right)\right\|_{r,r}^{-1}$$

наиболее удобна для вычислений.

Таким образом, рассмотренные операции позволяют формировать кодовые слова алгеброгеометрических кодов на пространственных кривых, заданных как через порождающую, так и через проверочную матрицы.

**Пример помехоустойчивого кодирования алгеброгеометрическиих кодов на пространственных кривых.**

Зафиксируем два алгебраических уравнения $xy^2 + x^2z + yz^2 = 0$ и $yz^2 + y^2v + zv^2 = 0$ над полем $GF(2^2)$, множество совокупных решений которых задает пространственную кривую. После подстановки элементов поля $GF(2^2)$ в уравнения получим их решения (табл. 1 и 2).

Совместные решения уравнений $xy^2 + x^2z + yz^2 = 0$ и $yz^2 + y^2v + zv^2 = 0$ представлены в табл. 3.

Таблица 1

Решения уравнения $xy^2 + x^2z + yz^2 = 0$ над полем $GF(2^2)$

| x | y | z | v | x | y | z | v | x | y | z | v | x | y | z | v |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 2 | 2 | 1 | 1 | 0 | 0 | 3 | 1 |
| 0 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | 1 | 3 | 1 | 1 | 1 | 1 | 3 | 1 |
| 0 | 0 | 1 | 0 | 3 | 0 | 0 | 1 | 3 | 3 | 1 | 1 | 3 | 1 | 3 | 1 |
| 2 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 2 | 1 | 2 | 2 | 3 | 1 |
| 3 | 1 | 1 | 0 | 0 | 2 | 0 | 1 | 1 | 1 | 2 | 1 | 3 | 2 | 3 | 1 |
| 1 | 2 | 1 | 0 | 0 | 3 | 0 | 1 | 2 | 1 | 2 | 1 | 1 | 3 | 3 | 1 |
| 2 | 2 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 3 | 3 | 1 |
| 1 | 3 | 1 | 0 | 2 | 1 | 1 | 1 | 3 | 2 | 2 | 1 | | | | |
| 3 | 3 | 1 | 0 | 3 | 1 | 1 | 1 | 2 | 3 | 2 | 1 | | | | |
| 0 | 0 | 0 | 1 | 1 | 2 | 1 | 1 | 3 | 3 | 2 | 1 | | | | |

Таблица 2

Решения уравнения $yz^2 + y^2v + zv^2 = 0$ над полем $GF(2^2)$

| x | y | z | v | x | y | z | v | x | y | z | v | x | y | z | v |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 3 | 3 | 1 | 1 | 1 | 1 | 3 | 1 |
| 0 | 1 | 0 | 0 | 2 | 0 | 0 | 1 | 0 | 1 | 2 | 1 | 2 | 1 | 3 | 1 |
| 1 | 1 | 0 | 0 | 3 | 0 | 0 | 1 | 1 | 1 | 2 | 1 | 3 | 1 | 3 | 1 |
| 2 | 1 | 0 | 0 | 0 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 0 | 3 | 3 | 1 |
| 3 | 1 | 0 | 0 | 1 | 2 | 1 | 1 | 3 | 1 | 2 | 1 | 1 | 3 | 3 | 1 |
| 0 | 0 | 1 | 0 | 2 | 2 | 1 | 1 | 0 | 2 | 2 | 1 | 2 | 3 | 3 | 1 |
| 1 | 0 | 1 | 0 | 3 | 2 | 1 | 1 | 1 | 2 | 2 | 1 | 3 | 3 | 3 | 1 |
| 2 | 0 | 1 | 0 | 0 | 3 | 1 | 1 | 2 | 2 | 2 | 1 | | | | |
| 3 | 0 | 1 | 0 | 1 | 3 | 1 | 1 | 3 | 2 | 2 | 1 | | | | |
| 0 | 0 | 0 | 1 | 2 | 3 | 1 | 1 | 0 | 1 | 3 | 1 | | | | |

Таблица 3

Совместные решения уравнений $xy^2 + x^2z + yz^2 = 0$ и $yz^2 + y^2v + zv^2 = 0$ над полем $GF(2^2)$

| | $P_0$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ | $P_7$ | $P_8$ | $P_9$ | $P_{10}$ | $P_{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 3 | 1 | 3 | 1 | 2 |
| Y | 2 | 2 | 3 | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 3 | 3 |
| Z | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 |
| v | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Таблица 4

Значения генераторных функций в точках пространственной кривой

| | $P_0$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ | $P_7$ | $P_8$ | $P_9$ | $P_{10}$ | $P_{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $x^2$ | 1 | 3 | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 2 | 1 | 3 |
| xy | 2 | 3 | 3 | 2 | 1 | 2 | 2 | 1 | 1 | 3 | 3 | 1 |
| $y^2$ | 3 | 3 | 2 | 2 | 1 | 1 | 3 | 3 | 1 | 1 | 2 | 2 |
| xz | 1 | 2 | 1 | 3 | 2 | 3 | 2 | 1 | 3 | 2 | 3 | 1 |
| yz | 2 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 2 | 2 |
| $z^2$ | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 2 |
| xv | 1 | 2 | 1 | 3 | 1 | 2 | 1 | 3 | 1 | 3 | 1 | 2 |
| yv | 2 | 2 | 3 | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 3 | 3 |
| zv | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 |

На множестве точек $\{P_0, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{11}\}$ построим алгеброгеометрический код. Зафиксируем множество генераторных функций в виде одночленов степени deg = 2: $\{ x^2, y^2, z^2, v^2, xy, xz, xv, yz, yv, zv \}$. Вычислим значения генераторных функций в точках кривой и сформируем проверочную матрицу кода (табл. 4).

Следовательно, проверочная матрица

$$H = \begin{pmatrix} 1 & 3 & 1 & 2 & 1 & 3 & 1 & 2 & 1 & 2 & 1 & 3 \\ 3 & 3 & 2 & 2 & 1 & 1 & 3 & 3 & 1 & 1 & 2 & 2 \\ 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 2 & 2 & 2 & 2 \\ 2 & 3 & 3 & 2 & 1 & 2 & 2 & 1 & 1 & 3 & 3 & 1 \\ 1 & 2 & 1 & 3 & 2 & 3 & 2 & 1 & 3 & 2 & 3 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 3 & 1 & 3 & 1 & 2 \\ 2 & 2 & 3 & 3 & 2 & 2 & 3 & 3 & 3 & 3 & 2 & 2 \\ 2 & 2 & 3 & 3 & 1 & 1 & 2 & 2 & 1 & 1 & 3 & 3 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

задает (12, 3, 8) код, который исправляет любую конфигурацию из трех ошибок.

Соответствующая порождающая матрица равна

$$G = \begin{pmatrix} 3 & 0 & 2 & 0 & 0 & 3 & 1 & 3 & 0 & 2 & 1 & 2 \\ 3 & 0 & 3 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 3 & 0 \\ 3 & 1 & 1 & 0 & 0 & 2 & 0 & 1 & 3 & 2 & 2 & 0 \end{pmatrix}.$$

*Рассмотрим пример несистематического способа кодирования.*

Пусть информационный вектор I = (2, 1, 3), тогда для формирования кодового слова

$$(c_0, c_1, \dots c_{n-1})$$

достаточно умножить информационный вектор на порождающую матрицу G.

После выполнения умножения (по правилу умножения матриц) кодовое слово запишется в виде:

C = (0 3 3 1 2 1 2 0 2 0 0 3).

Легко проверить, что решение истинно. Так как при умножении полученного кодового слова на проверочную матрицу, получается нулевая матрица.

*Рассмотрим пример систематического способа кодирования.*

В соответствии с вышеизложенным материалом разобьем кодовое слово

$$(c_0, c_1, \dots c_{n-1})$$

на множества информационных и проверочных позиций.

На k информационных позициях кодового слова, разместим k символов сообщения i = (2 1 3), а на проверочных позициях разместим *r* нулевых символов

C = (0 2 0 1 0 0 3 0 0 0 0 0).

Задача формирования кодового слова состоит в том, чтобы вычислить и записать на r проверочных позициях такие символы $c_i$, которые удовлетворяют уравнениям (6).

Тогда вектор $\|S_j\|_{rk}$ равен:

$$\|S_j\|_{rk} = (0\ 1\ 1\ 2\ 1\ 3\ 2\ 1\ 2).$$

Вычислим матрицу $\|H\|_{r,r}^{-1}$ обратную матрице $\|H\|_{r,r}$ по методу Жордана – Гаусса:

$$\|H\|_{r,r}^{-1} = \begin{pmatrix} 3 & 3 & 1 & 2 & 3 & 1 & 2 & 2 & 0 \\ 2 & 0 & 3 & 1 & 2 & 3 & 3 & 3 & 2 \\ 3 & 3 & 1 & 2 & 1 & 2 & 1 & 2 & 2 \\ 0 & 2 & 2 & 0 & 2 & 1 & 3 & 1 & 3 \\ 2 & 2 & 2 & 1 & 2 & 3 & 3 & 0 & 3 \\ 2 & 2 & 1 & 3 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 3 & 3 & 2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 3 & 1 & 1 & 3 & 3 & 0 & 2 & 0 & 0 \end{pmatrix}.$$

Найдем значения r = n – k проверочных символов, используя уравнение (7)

$$\|c_i\|_r = (0\ 0\ 2\ 0\ 2\ 1\ 0\ 3\ 1).$$

Объединение множеств k информационных позиций кодового слова и r = n – k проверочных позиций дает кодовое слово:

C = (0 2 0 1 2 0 3 2 1 0 3 1).

Таким образом, в результате проведенных исследований получено практическое решение задачи формирования кодового слова алгеброгеометрических кодов на пространственных кривых, как систематическим, так и несистематическим способами.

**Оценка алгоритмической сложности разработанных алгоритмов.**

Для алгоритма кодирования через порождающую матрицу, при известных (заранее сформированных) элементов матрицы

$$\|F_j(p_i(x_0, x_1, x_2, x_3))\|_{n,k}$$

необходимо выполнить $k \times n$ операций сложения и умножения.

Таким образом, $S_E$ – емкостная сложность алгоритма $S_E = kn = 3 \times 12 = 36$;

$S_B$ – временная сложность алгоритма $S_B = kn = 3 \times 12 = 36$ элементарных операций.

Формально, емкостная и временная сложность алгоритма кодирования через порождающую матрицу запишется как асимптотическая (в пределе при увеличении размера задачи) функция $O(r \times n)$.

Для алгоритма кодирования через порождающую матрицу, если заранее сформированы матрицы

$$\|F_j(p_i(x_0, x_1, x_2, x_3))\|_{k,r}$$

$$\text{и } \|F_j(p_i(x_0, x_1, x_2, x_3))\|_{r,r}^{-1},$$

то при формировании кодового слова через проверочную матрицу, необходимо $k \times r$ операций сложения и умножения для вычисления вектора синдромов и $r \times r$ операций сложения и умножения для вычисления вектора проверочных символов.

Таким образом, при затратах

$$S_E = kr + rr = rn = 9 \times 12 = 108$$

ячеек памяти для работы алгоритма необходимо выполнить

$$S_B = kr + rr = rn = 9 \times 12 = 108$$

элементарных операций.

Формально, емкостная и временная сложность алгоритма кодирования через проверочную матрицу запишется как асимптотическая (в пределе при увеличении размера задачи) функция $O(r \times n)$.

Для реализации рассмотренных алгоритмов без значительных затрат элементов памяти формирование кодовых слов следует реализовать посредством последовательного вычисления значений генераторных функций в точках пространственной кривой. Основной вычислительной операцией в этом случае является нахождение значения генераторной функции

$$F_j(p_i(x_0, x_1, x_2, x_3)).$$

Для вычисления

$$F_j(p_i(x_0, x_1, x_2, x_3))$$

потребуется, в общем случае, четыре операции возведения в степень и три операции умножения.

При выполнении аналогичных операций над однородными координатами точек кривой потребуется реализовать три операции возведения в степень и две операции умножения.

Если принять равными вычислительную сложность операций умножения и возведения в степень, тогда имеем:

$$S_E = 3n = 9$$

ячеек памяти для хранения точек кривой (трех значений в однородных координатах для каждой точки) и

$$S_B = 5kn = 180$$

операций при кодировании через порождающую матрицу и

$$S_B = 5rn = 540$$

операций при кодировании через проверочную матрицу.

Формально, асимптотическая емкостная сложность оценивается как $O(n)$, асимптотическая временная сложность оценивается как $O(kn)$ и $O(rn)$, соответственно.

## Выводы

Разработан практический алгоритм кодирования алгеброгеометрическими кодами на пространственных кривых, заданными в проективном пространстве $P^3$ совместными решениями совокупности двух однородных уравнений от четырех переменных. Сложность его реализации растет полиномиально от параметров кода.

**Перспективным направлением дальнейших исследований** является оценка энергетического выигрыша от кодирования в каналах с независимыми и группирующимися ошибками.

## Список литературы


1. *Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.*
2. *Гоппа В.Д. Коды и информация. // Успехи математических наук. – 1984. – Т. 30, вып. 1 (235). – С. 77-120.*
3. *Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые //Современные проблемы маттематики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209-257.*
4. *Бэрлэкэмп Э. Алгебраическая теория кодирования: Пер. с англ. – М.: Мир, 1971. – 477 с.*
5. *Sakata S., Justesen J., Madelung Y., Jensen H.E., Hoholdt T. Fast Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance // IEEE Trans. Inform. Theory. – 1995. – Vol. 41, N 5. – P. 1672-1677.*
6. *Ruud Pellikaan. Asymptotically good sequences of curves and codes. // Proc. 34th Allerton Conf. on Communication, Control, and Computing, Urbana-Champaign, October 2-4, 1996. – 1996. – P. 276-285.*
7. *Feng G.L., Rao T.R.N. Decoding algebraic geometric codes up to the designed minimum distance // IEEE Trans. Inform. Theory. – 1993. – Vol. 39, N 1. – P. 37-46.*
8. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289-1290.*
9. *Кузнецов А.А. Алгеброгеометрические коды // Электроника и системы управления. – К.: НАУ. – 2005. – № 2 (4). – С. 25-34.*
10. *Кузнецов А.А. Линейные блоковые коды на алгебраических кривых // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – 2005. – № 1-2. – С. 52-58.*
11. *Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов. //Электронное моделирование: Международный научно-теоретический журнал. – К: НАНУ, РАН. – 2004. – №2. – С. 27-38.*
12. *Науменко М.І., Стасєв Ю.В., Кузнєцов О.О. Теоретичні основи побудови алгебраїчних кодів: Монографія. – Х.: ХУ ПС, 2005. – 267 с.*


*Поступила в редколлегию 30.07.2007*

**Рецензент:** д-р физ.-мат. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.