УДК 621.391

И.В. Пасько

*Военный институт ракетных войск и артиллерии им. Б. Хмельницкого Сумского государственного университета*

# АЛГЕБРАИЧЕСКОЕ ДЕКОДИРОВАНИЕ КОДОВ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ

*Рассматриваются алгеброгеометрические коды, построенные на пространственных кривых. Предлагается алгебраический алгоритм декодирования кодов на пространственных кривых.*

***алгеброгеометрические коды, пространственные кривые***

## Введение

**Постановка проблемы в общем виде, анализ литературы**. Одним из эффективных средств защиты информации от ошибок в телекоммуникационных системах является помехоустойчивое кодирование информации [1, 2]. Основными требованиями к помехоустойчивому кодированию являются высокая обнаруживающая и исправляющая способность кода, низкая вносимая избыточность, высокое быстродействие и низкая сложность реализации процедур кодирования-декодирования [8 – 12]. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым, обладают высокой исправляющей способностью при небольшой доле вносимой избыточности [1 – 7]. В тоже время методы декодирования алгеброгеометрических кодов ориентированы на узкий класс кодов и, строго говоря, не позволяют реализовать их потенциальные свойства. В работе [13] предложен метод декодирования кодов на пространственных кривых ($P^3$). **Целью настоящей статьи** является разработка практического алгоритма декодирования алгеброгеометрических кодов, оценка сложности его реализации.

## Алгебраический метод декодирования кодов на пространственных кривых

Зафиксируем конечное поле GF(q).

Пусть X гладкая проективная алгебраическая кривая в проективном пространстве $P^n$ над полем $GF(q)$, т.е. совокупность решений системы однородных неприводимых алгебраических уравнений от $(n+1)$ переменной с коэффициентами из $GF(q)$. $g = g(X)$ – род кривой, $X(GF(q))$ – множество ее точек над конечным полем, $N = |X(GF(q))|$ – их число. Рациональное отображение $\varphi : X \to Y \subset P^m$ задает алгеброгеометрический код с характеристиками $k + d \ge n - g + 1$, длина n которых меньше либо равна числу точек кривой X.

При $2g < \alpha \le n$, $\alpha > g - 1$ алгеброгеометрический код имеет параметры:

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

Двойственный к нему код также является алгеброгеометрическим и имеет параметры:

$$(n,\ n - \alpha + g - 1,\ d^{\perp}),\ d^{\perp} \ge \alpha - 2g + 2.$$

Алгебраическая кривая в $P^3$ (пространственная кривая) задается множеством совместных решений двух однородных не приводимых уравнений. Предположим, что это множество состоит из точек:

$$P_0(X_0,Y_0,Z_0),\ P_1(X_1,Y_1,Z_1),\ \ldots,\ P_n(X_n,Y_n,Z_n), \quad (1)$$

Тогда алгеброгеометрический код задается проверочной матрицей H [11]:

$$H = \begin{pmatrix} F_{0,0,0}(X_0,Y_0,Z_0) & \ldots & F_{0,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) \\ F_{1,0,0}(X_0,Y_0,Z_0) & \ldots & F_{1,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) \\ \ldots & \ldots & \ldots \\ F_{0,0,\deg F}(X_0,Y_0,Z_0) & \ldots & F_{0,0,\deg F}(X_{n-1},Y_{n-1},Z_{n-1}) \end{pmatrix}, \quad (2)$$

где $F_{i_x,i_y,i_z}$ – одночлен степени $i_x + i_y + i_z \le \deg F$,

т.е. $F_{i_x,i_y,i_z} = x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$, $i = 0,\ldots,M-1$,

$$M = C^0_{\deg F} + C^1_{1+\deg F} + C^2_{2+\deg F} + C^3_{3+\deg F}.$$

Синдромная последовательность

$$s = \left(s_{0,0,0}, s_{1,0,0}, \ldots, s_{0,0,\deg F}\right), \quad (3)$$

вычисляется по правилу:

$$s_{i_x,i_y,i_z} = \sum_{j=0}^{n-1} e_j \cdot F_{i_x,i_y,i_z}(X_j,Y_j,Z_j),$$

$$i = 0,\ldots,M-1, \quad (4)$$

В работе [13] задача алгебраического декодирования, т.е. задача нахождения вектора ошибок

$$e = (e_0,\ e_1,\ \ldots,\ e_{n-1})$$

по известной синдромной последовательности (3) сведена к решению системы линейных уравнений

$$\begin{cases} s_{u-2,0,0} + a_{u-3,1,0} \cdot s_{u-3,1,0} + \ldots + a_{1,0,0} \cdot s_{1,0,0} + \\ + a_{0,1,0} \cdot s_{0,1,0} + a_{0,0,1} \cdot s_{0,0,1} + a_{0,0,0} \cdot s_{0,0,0} = 0; \\ s_{u-1,0,0} + a_{u-3,1,0} \cdot s_{u-2,1,0} + \ldots + a_{1,0,0} \cdot s_{2,0,0} + \\ + a_{0,1,0} \cdot s_{1,1,0} + a_{0,0,1} \cdot s_{1,0,1} + a_{0,0,0} \cdot s_{1,0,0} = 0; \\ \ldots \\ s_{2 \cdot u-4,0,0} + a_{u-3,1,0} \cdot s_{2 \cdot u-5,1,0} + \ldots + a_{1,0,0} \cdot s_{u-1,0,0} + \\ a_{0,1,0} \cdot s_{u-2,1,0} + a_{0,0,1} \cdot s_{u-2,0,1} + a_{0,0,0} \cdot s_{u-2,0,0} = 0, \end{cases} \quad (5)$$

которые дают значения неизвестных коэффициентов многочлена локаторов ошибок

$$\Lambda(x,y,z) = x^{u-2} + a_{t-3,1,0}\cdot x^{u-3}\cdot y + a_{1,0,0}\cdot x + \\ + a_{0,1,0}\cdot y + a_{0,0,1}\cdot z + a_{0,0,0}. \quad (6)$$

Корнями $\Lambda(x,y,z)$ являются наборы $(X_\xi, Y_\xi, Z_\xi)$, которые локализуют ошибку в кодовом слове. Нахождение значения ошибок производится с помощью условия $c\cdot H = 0$.

Для практических приложений предлагается алгебраический алгоритм декодирования, практически реализующий рассмотренные теоретические положения.

## Предлагаемый алгоритм алгебраического декодирования

Алгоритм декодирования алгеброгеометрических кодов определим как последовательность следующих шагов (рис. 1).

ШАГ 1. По выражению (4) вычислим элементы синдромной последовательности.

ШАГ 2. Решим систему линейных уравнений (5). Получим коэффициенты многочлена локаторов ошибок.

ШАГ 3. Воспользуемся процедурой Ченя. Применительно к декодированию алгеброгеометрических кодов на пространственных кривых она состоит в подстановке всех пар ($X_i$, $Y_i$, $Z_i$), соответствующих проективным точкам (1) пространственной кривой, в многочлен локаторов ошибок (6). 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 $c\cdot H = 0$. Решение системы линейных уравнений даст значения (кратность) произошедших ошибок. Локализация ошибок и найденные их значения позволяют сформировать вектор ошибок $e = (e_0, e_1, \ldots, e_{n-1})$.

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

Оценим сложность реализации предложенного алгоритма декодирования. Основные этапы разработанного алгебраического алгоритма состоят в решении системы линейных уравнений (шаги 2 и 4) и выполнении процедуры Ченя (шаг 3). Эти стандартные процедуры, а также процедура вычисления вектора синдромов могут быть реализованы любым из известных на сегодняшний день алгоритмов. Сложность решения системы линейных уравнений методом Гаусса $O(n^2)$, где n – число переменных. В системе (6) число уравнений соответствует числу одночленов от трех неизвестных степени (t – 2), следовательно, число уравнений можно выразить выражением:

$$\frac{(t+1)!}{(t-2)!(t+1-(t-2))!} = \frac{(t+1)(t)(t-1)}{3} = \frac{t^3-t}{3}.$$

Таким образом, сложность реализации 2-го шага алгоритма составляет

$$\left(\left(t^3-t\right)/3\right)^2 = \left(t^6-2t^4+t^2\right)/9.$$

Сложность реализации процедуры Ченя составляет $6(t-2)$. Общая сложность алгоритма $\left(t^6-2t^4+t^2+54t-108\right)/9$, асимптотическая сложность (в пределе как функция размера задачи) $O(t) = t^6 - t^4 + t^2 + t$.

**Пример алгебраического декодирования 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. Род кривой g(x) = 1. 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.

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

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

задает (12, 2, 8) код, который исправляет любую конфигурацию из трех ошибок.

Определим синдромную последовательность как вектор

$$s = \begin{pmatrix} s_{0,0,0}, s_{1,0,0}, s_{0,1,0}, s_{0,0,1}, s_{1,1,0}, s_{1,0,1}, \\ s_{0,1,1}, s_{2,0,0}, s_{0,2,0}, s_{0,0,2} \end{pmatrix},$$

вычисленный по правилу:

$$s_{0,0,0} = \sum_{j=0}^{11} e_j;\ s_{1,0,0} = \sum_{j=0}^{11} e_j\cdot X_j;\ s_{0,1,0} = \sum_{j=0}^{11} e_j\cdot Y_j;$$

$$s_{0,0,1} = \sum_{j=0}^{11} e_j\cdot Z_j;\ s_{1,1,0} = \sum_{j=0}^{11} e_j\cdot X_j\cdot Y_j;$$

$$s_{1,0,1} = \sum_{j=0}^{11} e_j\cdot X_j\cdot Z_j;\ s_{0,1,1} = \sum_{j=0}^{11} e_j\cdot Y_j\cdot Z_j;$$

$$s_{2,0,0} = \sum_{j=0}^{11} e_j\cdot X_j^2;\ s_{0,2,0} = \sum_{j=0}^{11} e_j\cdot Y_j^2;\ s_{0,0,2} = \sum_{j=0}^{11} e_j\cdot Z_j^2.$$

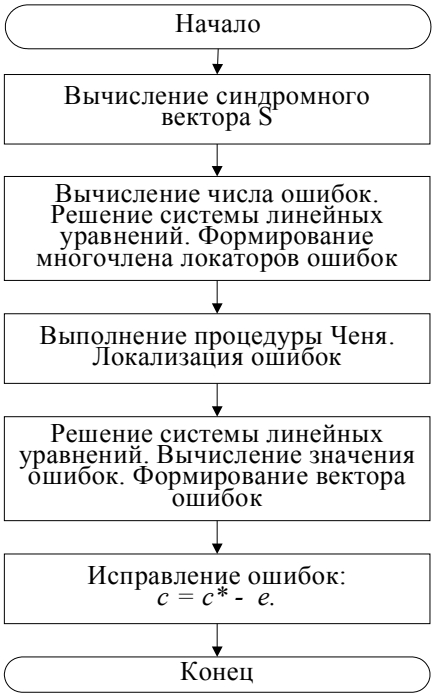


Рис. 1. Схема алгебраического алгоритма декодирования

Таблица 1

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

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

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

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

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

Таблица 2

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

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

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

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

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

Предположим, что в переданном кодовом слове произошла ошибка:

$(e_0 = 0, e_1 = 0, e_2 = 3, e_3 = 0, e_4 = 1, e_5 = 0, e_6 = 0, e_7 = 0, e_8 = 0, e_9 = 0, e_{10} = 0, e_{11} = 2)$.

Тогда синдромный вектор равен:

$$s_{0,0,0} = 3+1+2 = 0;\ s_{1,0,0} = 3\cdot1+1\cdot1+2\cdot2 = 1;$$

$$s_{0,1,0} = 3\cdot3+1\cdot1+2\cdot3 = 2;\ s_{0,0,1} = 3\cdot1+1\cdot2+2\cdot3 = 0;$$

$$s_{1,1,0} = 3\cdot1\cdot3+1\cdot1\cdot1+2\cdot2\cdot3 = 1;$$

$$s_{1,0,1} = 3\cdot1\cdot1+1\cdot1\cdot2+2\cdot2\cdot3 = 3;$$

$$s_{0,1,1} = 3\cdot3\cdot1+1\cdot1\cdot2+2\cdot3\cdot3 = 3;$$

$$s_{2,0,0} = 3\cdot1^2+1\cdot1^2+2\cdot2^2 = 3;$$

$$s_{0,2,0} = 3\cdot3^2+1\cdot1^2+2\cdot3^2 = 3;$$

$$s_{0,0,2} = 3\cdot1^2+1\cdot2^2+2\cdot3^2 = 3.$$

Обозначим множество $ej \neq 0$ символом E. Для однозначного нахождения вектора ошибок воспользуемся искусственным приемом, состоящем в ведении многочлена локаторов ошибок. Количество ошибок, которое может исправить код, t = 3, многочлен локаторов ошибок в общем виде примет вид:

$$\Lambda(x, y, z) = x + a_{0,1,0}\cdot y + a_{0,0,1}\cdot z + a_{0,0,0},$$

решениями которого являются локаторы – такие наборы $(X_\xi, Y_\xi, Z_\xi)$, которые обращают в нуль многочлен локаторов ошибок, причем все $e_\xi \in E$.

Сформируем систему линейных уравнений:

$$\begin{cases} s_{1,0,0} + a_{0,1,0} \cdot s_{0,1,0} + a_{0,0,1} \cdot s_{0,0,1} + a_{0,0,0} \cdot s_{0,0,0} = 0; \\ s_{2,0,0} + a_{0,1,0} \cdot s_{1,1,0} + a_{0,0,1} \cdot s_{1,0,1} + a_{0,0,0} \cdot s_{1,0,0} = 0; \\ s_{1,1,0} + a_{0,1,0} \cdot s_{0,2,0} + a_{0,0,1} \cdot s_{0,1,1} + a_{0,0,0} \cdot s_{0,1,0} = 0; \\ s_{1,0,1} + a_{0,1,0} \cdot s_{0,1,1} + a_{0,0,1} \cdot s_{0,0,2} + a_{0,0,0} \cdot s_{0,0,1} = 0. \end{cases}$$

Получим

$$\begin{cases} 1 + a_{0,1,0} \cdot 2 = 0; \\ 3 + a_{0,1,0} + a_{0,0,1} \cdot 3 + a_{0,0,0} = 0; \\ 1 + a_{0,1,0} \cdot 3 + a_{0,0,1} \cdot 3 + a_{0,0,0} \cdot 2 = 0; \\ 3 + a_{0,1,0} \cdot 3 + a_{0,0,1} \cdot 3 = 0. \end{cases}$$

Система разрешима, ее решения:

$$a_{0,1,0} = 3; \quad a_{0,0,0} = 1; \quad a_{0,0,1} = 2.$$

Подставив найденные коэффициенты в многочлен локаторов ошибок, получим

$$\Lambda(x, y, z) = x + 3 \cdot y + 2 \cdot z + 1 .$$

Подставим в полученный многочлен поочередно все точки пространственной кривой, имеем:

$$P_0: \ \Lambda(1,2,1) = 1 + 3 \cdot 2 + 2 \cdot 1 + 1 = 3 \neq 0 ;$$

$$P_1: \ \Lambda(2,2,1) = 2 + 3 \cdot 2 + 2 \cdot 1 + 1 = 0 ;$$

$$P_2: \ \Lambda(1,3,1) = 1 + 3 \cdot 3 + 2 \cdot 1 + 1 = 0 ;$$

$$P_3: \ \Lambda(3,3,1) = 3 + 3 \cdot 3 + 2 \cdot 1 + 1 = 2 \neq 0 ;$$

$$P_4: \ \Lambda(1,1,2) = 1 + 3 \cdot 1 + 2 \cdot 2 + 1 = 0 ;$$

$$P_5: \ \Lambda(2,1,2) = 2 + 3 \cdot 1 + 2 \cdot 2 + 1 = 3 \neq 0 ;$$

$$P_6: \ \Lambda(1,2,2) = 1 + 3 \cdot 2 + 2 \cdot 2 + 1 = 2 \neq 0 ;$$

$$P_7: \ \Lambda(3,2,2) = 3 + 3 \cdot 2 + 2 \cdot 2 + 1 = 0 ;$$

$$P_8: \ \Lambda(1,1,3) = 1 + 3 \cdot 1 + 2 \cdot 3 + 1 = 2 \neq 0 ;$$

$$P_9: \ \Lambda(3,1,3) = 3 + 3 \cdot 1 + 2 \cdot 3 + 1 = 0 ;$$

$$P_{10}: \ \Lambda(1,3,3) = 1 + 3 \cdot 3 + 2 \cdot 3 + 1 = 3 \neq 0 ;$$

$$P_{11}: \ \Lambda(2,3,3) = 2 + 3 \cdot 3 + 2 \cdot 3 + 1 = 0 .$$

Как следует из полученных результатов, ошибка локализована в следующих символах:

$$(e_0 = 0, e_1, e_2, e_3 = 0, e_4, e_5 = 0, e_6 = 0,$$
$$e_7, e_8 = 0, e_9, e_{10} = 0, e_{11}),$$

соответствующих следующим точкам пространственной кривой (табл. 5):

Таблица 5

Точки пространственной кривой, соответствующие символам в которых локализована ошибка

| | P1 | P2 | P4 | P7 | P9 | P11 |
|---|---|---|---|---|---|---|
| X | 2 | 1 | 1 | 3 | 3 | 2 |
| Y | 2 | 3 | 1 | 2 | 1 | 3 |
| Z | 1 | 1 | 2 | 2 | 3 | 3 |
| V | 1 | 1 | 1 | 1 | 1 | 1 |

Подставим полученный вектор ошибок в систему синдромных уравнений (4), получим:

$$s_{0,0,0} = e_1 + e_2 + e_4 + e_7 + e_9 + e_{11} = 0 ;$$

$$s_{1,0,0} = e_1 \cdot 2 + e_2 \cdot 1 + e_4 \cdot 1 + e_7 \cdot 3 + e_9 \cdot 3 + e_{11} \cdot 2 = 1 ;$$

$$s_{0,1,0} = e_1 \cdot 2 + e_2 \cdot 3 + e_4 \cdot 1 + e_7 \cdot 2 + e_9 \cdot 1 + e_{11} \cdot 3 = 2 ;$$

$$s_{0,0,1} = e_1 \cdot 1 + e_2 \cdot 1 + e_4 \cdot 2 + e_7 \cdot 2 + e_9 \cdot 3 + e_{11} \cdot 3 = 0 ;$$

$$s_{1,1,0} = e_1 \cdot 2 \cdot 2 + e_2 \cdot 1 \cdot 3 + e_4 \cdot 1 \cdot 1 + e_7 \cdot 3 \cdot 2 + e_9 \cdot 3 \cdot 1 + e_{11} \cdot 2 \cdot 3 = 1;$$

$$s_{1,0,1} = e_1 \cdot 2 \cdot 1 + e_2 \cdot 1 \cdot 1 + e_4 \cdot 1 \cdot 2 + e_7 \cdot 3 \cdot 2 + e_9 \cdot 3 \cdot 3 + e_{11} \cdot 2 \cdot 3 = 3;$$

$$s_{0,1,1} = e_1 \cdot 2 \cdot 1 + e_2 \cdot 3 \cdot 1 + e_4 \cdot 1 \cdot 2 + e_7 \cdot 2 \cdot 2 + e_9 \cdot 1 \cdot 3 + e_{11} \cdot 3 \cdot 3 = 3;$$

$$s_{2,0,0} = e_1 \cdot 2^2 + e_2 \cdot 1^2 + e_4 \cdot 1^2 + e_7 \cdot 3^2 + e_9 \cdot 3^2 + e_{11} \cdot 2^2 = 3;$$

$$s_{0,2,0} = e_1 \cdot 2^2 + e_2 \cdot 3^2 + e_4 \cdot 1^2 + e_7 \cdot 2^2 + e_9 \cdot 1^2 + e_{11} \cdot 3^2 = 3;$$

$$s_{0,0,2} = e_1 \cdot 1^2 + e_2 \cdot 1^2 + e_4 \cdot 2^2 + e_7 \cdot 2^2 + e_9 \cdot 3^2 + e_{11} \cdot 3^2 = 3.$$

Решая данную систему, получим:

$$e_1 = 0 ; \ e_2 = 3 ; \ e_4 = 1 ; \ e_7 = 0 ; \ e_9 = 0 ; \ e_{11} = 2 .$$

Сформируем вектор ошибок:

$$e = (0\ 0\ 3\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 2).$$

Восстановим кодовое слово с по известной последовательности $c^*$ и найденному вектору ошибок:

$$c = c^* - e = (c_0^* - e_0, c_1^* - e_1, ..., c_{11}^* - e_{11}) .$$

Ошибка локализована и исправлена, задача декодирования решена. Сложность реализации алгоритма декодирования 64 групповых операций.

Таким образом, в результате проведенных исследований получено практическое решение задачи декодирования алгеброгеометрических кодов построенных по кривым в $P^3$.

## Выводы

Впервые разработан практический алгоритм декодирования алгеброгеометрических кодов на пространственных кривых, основанный на сведении задачи декодирования к решению систем линейных уравнений. Сложность его реализации растет полиномиально от параметров кода.

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

## Список литературы

*1. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289-1290.*

*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 математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209-257.*

*4. 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.*

*5. Voss, Tom Hoholdt. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps. //IEEE Trans. Info. Theory. – 1997. – Vol. IT-43. – P. 128-135.*

*6. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Радиотехника. – Х.: ХТУРЭ. – 2003. – Вып. 134. – С. 218-222.*

*7. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов // Электронное моделирование. – К: НАНУ, РАН. – 2004. – № 2. – С. 27-38.*

*8. Кузнецов А.А., Северинов А.В., Лысенко В.Н. Алгоритм мажоритарного декодирования алгеброгеометрических кодов // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2003. – Вип. 4 (26). – С. 61-66.*

*9. Северинов А.В., Кузнецов А.А., Куриш В.В. Разработка алгоритма декодирования алгеброгеометрических кодов // Системи обробки інформації. – Х.: НАНУ, ПАНИ, ХВУ. – 2002. – Вип. 1 (17). – С. 161-163.*

*10. Кузнецов А.А., Северинов А.В., Задворный Д.А. Лысенко В.Н. Алгебраическое декодирование кодов по кривым Эрмита // Вісник ХПІ. – Х.: НТУ "ХПІ" – 2003. – № 26. – С. 95-102.*

*11. 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.*

*12. 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.*

*13. Кузнецов О.О., Пасько І.В. Алгебраїчний метод декодування лінійних блокових кодів на алгебраїчних кривих у $P^3$ // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2006. – № 3 (7). – С. 69-72.*

*Поступила в редколлегию 19.12.2006*

**Рецензент:** д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.