УДК 621.391

АЛГОРИТМ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ КОДОВ ПО КРИВЫМ ЭРМИТА

к.т.н. А.А. Кузнецов, к.т.н. А.В. Северинов, В.Н. Лысенко, к.в.н. И.В. Науменко
(представил д.т.н., проф. Ю.В. Стасев)

Предлагается алгоритм алгеброгеометрического кодирования. Алгоритм допускает построение кодов по произвольной кривой в P^2 над GF(q). Получены конструктивные характеристики кодов, построенных по кривым Эрмита над GF(4), GF(16), GF(64).

Анализ последних исследований и публикаций. Алгеброгеометричекие коды как линейные системы на алгебраических кривых впервые предложены В.Д. Гоппой [1]. Дальнейшие работы были направлены на исследование асимптотических свойств таких кодов [2 – 4]. Известно, что коды, построенные по кривым с большим числом точек по сравнению с родом, лежат выше границы Варшамова-Гилберта [3 – 4]. В работах [5 – 6] показано, что их применение в недвоичных каналах позволяет получить существенный энергетический выигрыш, по сравнению с другими блоковыми кодами. Этот факт свидетельствует о высоких потенциальных возможностях таких кодов по исправляющей и обнаруживающей способности.

Выделим **нерешенную часть проблемы** использования алгеброгеометрических кодов для помехоустойчивой передачи информации, которая состоит в отсутствии регулярных алгоритмов помехоустойчивого кодирования, практических схем кодеров, реализующих эти алгоритмы, эффективных процедур декодирования.

Целью статьи является разработка алгоритма помехоустойчивого кодирования передаваемой информации с использованием кодов, построенным по алгебраическим кривым, оценка конструктивных характеристик кодов по кривым Эрмита.

Общая конструкция алгеброгеометрических кодов. Зафиксируем конечное поле GF(q). Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n над GF(q); g = g(X) – род кривой; X(GF(q)) – множество ее точек над конечным полем; N = X(GF(q)) – их число. Пусть C – класс дивизоров на X степени $\alpha > g - 1$. Тогда C определяет отображение $\varphi: X \to P^{k-1}$, где $k \geq \alpha - g + 1$. Набор $y_i = \varphi(x_i)$ задает

код. Число точек в пересечении $\varphi(X)$ с гиперплоскостью равно α, т.е. $n - d \le \alpha$. Эта конструкция позволяет строить коды с параметрами $k + d \ge n - g + 1$, длина n которых меньше либо равна числу точек на кривой X. При $2g < \alpha \le n$ алгеброгеометрический код имеет параметры $(n, \alpha - g + 1, d)$, $d \ge n - \alpha$. Двойственный к нему код также является алгеброгеометрическим и имеет параметры $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \ge \alpha - 2g + 2$ [1 – 4]. Дадим следующее определение алгеброгеометрического кода.

Определение. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q). Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным в P^n уравнениями F = 0, где F – однородные одночлены степени degF. Алгеброгеометрический код по кривой X над GF(q) – это линейный код, состоящий из всех слов $(c_1, c_2, \dots, c_n)$ длины $n \le N$, для которых выполняется равенство $d + g - 1$ уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0, \qquad (1)$$

где $c_i \in GF(q)$, $d \ge \alpha - 2g + 2$, $\alpha = degX \cdot degF$.

Это определение равносильно матричному представлению алгеброгеометрического кода

$$H\,(c_0, c_1, \dots, c_{n-1})^T = 0,$$

где H – проверочная матрица кода размерности $r \times n$, $r = n - k = d + g - 2$:

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

Алгоритм систематического кодирования. Пусть I – множество k информационных позиций кодового слова (т.е. множество номеров позиций, входящих в заданный информационный набор кода) и h – множество $r = n - k$ проверочных позиций. Объединение множеств $I \cup h$ содержит все целые числа (номера) от 0 до $n - 1$. На информационных позициях разместим k символов сообщения, а на проверочных нули. Вычислим суммы

$$S_j = \sum_{i \in I} c_i F_j(P_i),\ j = \overline{0, r-1},$$

или в матричной форме

$$\left\| S_j \right\|_r = \left\| F_j(P_i) \right\|_{k,r} \left\| c_i \right\|_k^T. \qquad (2)$$

Задача состоит в том, чтобы вычислить и записать на проверочных позициях такие символы c_i, $i \in h$, которые удовлетворяют уравнениям (1). Из определения алгеброгеометрического кода следует, что значения $r = n - k$ проверочных символов могут быть найдены из системы линейных уравнений

$$\sum_{i \in h} c_i F_j(P_i) = -S_j, \quad j = \overline{0, r-1}.$$

В матричном представлении последняя запись эквивалентна выражению

$$\left\| F_j(P_i) \right\|_{r,r} \left\| c_i \right\|_r^T = \left\| -S_j \right\|_r.$$

Для нахождения значений r = n – k проверочных символов используем методы обращения матриц. Запишем в матричной форме

$$\left\| c_i \right\|_r = \left\| F_j(P_i) \right\|_{r,r}^{-1} \left\| -S_j \right\|_r^T. \qquad (3)$$

Поскольку размещение проверочных позиций обычно известно и фиксировано, то заранее можно найти обратную матрицу для системы уравнений (1) и получить все проверочные символы умножением вектора $(S_0, S_1, \ldots, S_{r-1})$ на матрицу $\left\| F_j(P_i) \right\|_{r,r}^{-1}$. В качестве информационных могут быть выбраны любые k позиций кодового слова. Следовательно, всегда можно выбрать такое множество проверочных (и информационных) позиций, для которого данная матрица наиболее удобна для вычислений.

Алгоритм систематического кодирования определим как последовательность следующих шагов.

ШАГ 1. На заранее определенные информационные позиции кодового слова поместим k символов сообщения.

ШАГ 2. Вычислим по выражению (2) матрицу-строку $\left\| S_j \right\|_r$.

ШАГ 3. Вычислим по выражению (3) матрицу-строку $\left\| c_i \right\|_r$.

ШАГ 4. Поместим элементы матрицы $\left\| c_i \right\|_r$ на проверочные позиции кодового слова.

Оценка конструктивных характеристик кодов по кривым Эрмита. Рассмотрим кривую Эрмита X в P^2 над GF(q), как совокупность решений уравнения $x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0$. Зафиксируем конечное поле $GF(2^2)$. Кривая Эрмита над $GF(2^2)$ как совокупность решений однородного алгебраического уравнения $x^3 + y^3 + z^3 = 0$ имеет род g = 1, число точек N = 9. Зафиксируем конечное поле $GF(2^4)$. Кривая Эрмита над $GF(2^4)$ как совокупность решений однородного алгебраического уравнения $x^5 + y^5 + z^5 = 0$ имеет род g = 6, число точек N = 65. Конструктивные характеристики кодов по кривой Эрмита над $GF(2^2)$ и $GF(2^4)$ сведены в табл. 1. Зафиксируем конечное поле $GF(2^6)$. Кривая Эрмита над $GF(2^6)$ как совокупность решений однородно-

го алгебраического уравнения $x^9 + y^9 + z^9 = 0$ имеет род $g = 28$, число точек $N = 513$. Конструктивные характеристики кодов по кривой Эрмита над $GF(2^6)$ сведены в табл. 2.

Таблица 1

Конструктивные характеристики кодов по кривой Эрмита над $GF(2^2)$ и $GF(2^4)$

α	n, k, d	n, n – k, $d_\perp$		α	n, k, d	n, n – k, $d_\perp$
Кривая Эрмита над $GF(2^2)$				30	65, 25, 35	65, 40, 20
3	9,3,6	9,6,3		35	65, 30, 30	65, 35, 25
6	9,6,3	9,3,6		40	65, 35, 25	65, 30, 30
Кривая Эрмита над $GF(2^4)$				45	65, 40, 20	65, 25, 35
10	65, 5, 55			50	65, 45, 15	65, 20, 40
15	65, 10, 50	65, 55, 5		55	65, 50, 10	65, 15, 45
20	65, 15, 45	65, 50, 10		60	65, 55, 5	65, 10, 50
25	65, 20, 40	65, 45, 15		65		65, 5, 55

Таблица 2

Конструктивные характеристики кодов по кривой Эрмита над $GF(2^6)$

α	n, k, d	n, n – k, $d_\perp$		α	n, k, d	n, n – k, $d_\perp$
1	2	3		5	6	7
36	513, 9, 477			297	513, 270, 216	513, 243, 243
45	513, 18, 468			288	513, 261, 225	513, 252, 234
54	513, 27, 459			306	513, 279, 207	513, 234, 252
63	513, 36, 450	513, 477, 9		315	513, 288, 198	513, 225, 261
72	513, 45, 441	513, 468, 18		324	513, 297, 189	513, 216, 270
81	513, 54, 432	513, 459, 27		333	513, 306, 180	513, 207, 279
90	513, 63, 423	513, 450, 36		342	513, 315, 171	513, 198, 288
99	513, 72, 414	513, 441, 45		351	513, 324, 162	513, 189, 297
108	513, 81, 405	513, 432, 54		360	513, 333, 153	513, 180, 306
117	513, 90, 396	513, 423, 63		369	513, 342, 144	513, 171, 315
126	513, 99, 387	513, 414, 72		378	513, 351, 135	513, 162, 324
135	513, 108, 378	513, 405, 81		387	513, 360, 126	513, 153, 333
144	513, 117, 369	513, 396, 90		396	513, 369, 117	513, 144, 342
153	513, 126, 360	513, 387, 99		405	513, 378, 108	513, 135, 351
162	513, 135, 351	513, 378, 108		414	513, 387, 99	513, 126, 360
171	513, 144, 342	513, 369, 117		423	513, 396, 90	513, 117, 369
180	513, 153, 333	513, 360, 126		432	513, 405, 81	513, 108, 378
189	513, 162, 324	513, 351, 135		441	513, 414, 72	513, 99, 387
198	513, 171, 315	513, 342, 144		450	513, 423, 63	513, 90, 396
207	513, 180, 306	513, 333, 153		459	513, 432, 54	513, 81, 405
216	513, 189, 297	513, 324, 162		468	513, 441, 45	513, 72, 414
225	513, 198, 288	513, 315, 171		477	513, 450, 36	513, 63, 423
234	513, 207, 279	513, 306, 180		486	513, 459, 27	513, 54, 432
243	513, 216, 270	513, 297, 189		495	513, 468, 18	513, 45, 441
252	513, 225, 261	513, 288, 198		504	513, 477, 9	513, 36, 450
261	513, 234, 252	513, 279, 207		513		513, 27, 459
270	513, 243, 243	513, 270, 216		522		513, 18, 468

279	513, 252, 234	513, 261, 225		531		513, 9, 477

Выводы. Разработанный алгоритм алгеброгеометрического кодирования позволяет формировать кодовые слова для произвольных k символов сообщения размещенных на любых k позициях кодового слова. Алгоритм допускает построение кодов по произвольной кривой в P^2 над GF(q). Получены конструктивные характеристики кодов, построенных по кривым Эрмита над GF(4), GF(16), GF(64).

Дальнейшие исследования могут быть направлены на разработку практических схем кодеров, реализующих предложенный алгоритм алгеброгеометрического кодирования.

ЛИТЕРАТУРА

1. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 – 1290.*
2. *Влэдуц С.Г., Манин Ю.И. Линейные коды и модулярные кривые // Современные проблемы математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209 – 257.*
3. *Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова-Гилберта // Проблемы передачи информации. – 1982. – № 3. – С. 3 – 6.*
4. *Ian Blake, Chris Heegard, Tom Hoholdt, Victor K. W. Wei; Algebraic-Geometry Codes, IEEE Trans. Info. Theory, vol. IT-44, P. 2596 – 2618, October 1998.*
5. *Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2003. – Вып. 133. – С. 76 – 82.*
6. *Кузнецов А.А. Каскадное кодирование с алгеброгеометрическим кодом внешней ступени // Інформаційно-керуючі системи на залізничному транспорті. – 2002. – № 2. – С. 39 –43.*

Поступила 18.09.2003

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, начальник научно-исследовательской лаборатории Харьковского военного университета. В 1996 году окончил ХВУ. Область научных интересов – теория аутентификации, алгебраическая теория кодов.*

***СЕВЕРИНОВ Александр Васильевич**, канд. техн. наук, зам. нач. кафедры Харьковского военного университета. В 1992 году окончил ХВВКИУ РВ. Область научных интересов – применение помехоустойчивого кодирования в системах передачи данных.*

***ЛЫСЕНКО Валерий Николаевич**, старший научный сотрудник Научного центра. В 1985 году окончил ХВВКИУ РВ. Область научных интересов – применение помехоустойчивого кодирования в системах передачи данных.*

***НАУМЕНКО Игорь Викторович**, канд. воен. наук, начальник управления Научного центра. В 1996 году окончил НАВС. Область научных интересов – обработка и передача информации в системах управления.*