УДК 621.391

А.А. Кузнецов[1], И.В. Пасько[2], Р.В. Королёв[1]

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

АЛГЕБРАИЧЕСКИЙ МЕТОД ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ АЛГЕБРОГЕОМЕТРИЧЕСКИМИ КОДАМИ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ

Исследуется общая конструкция алгеброгеометрических кодов, как линейных систем, возникающих на проективных алгебраических кривых. Разрабатывается метод и алгоритмы помехоустойчивого кодирования алгеброгеометрическими кодами, заданными на пространственных кривых.

алгеброгеометрические коды, помехоустойчивое кодирование

Введение

Постановка проблемы в общем виде, анализ литературы. Эффективным средством повышения достоверности передачи данных в телекоммуникационных системах и сетях является помехоустойчивое кодирование [1, 3, 8]. Перспективным направлением его развития являются коды, возникающие на алгебраических кривых (алгеброгеометрические коды). Использование алгеброгеометрических кодов в каналах с независимыми и группирующимися ошибками позволяет получить энергетический выигрыш от кодирования и значительно снизить вероятность ошибочного приема дискретных сообщений [2, 4, 8]. В тоже время, методы построения алгеброгеометрических кодов исследованы для кривых, заданных в проективном пространстве P^2 неприводимым однородным уравнением от трех переменных [6, 7, 10]. Этот подход позволяет строить простые схемы кодирования и декодирования алгеброгеометрических кодов, длина которых над конечным полем GF(q) не превышает мощности множества точек плоской кривой [4, 6, 8, 9]. Перспективным направлением дальнейших исследований является разработка методов построения алгеброгеометрических кодов большой длины, т.е. кодов на пространственных кривых, задаваемых, например, в проективном пространстве P^3 совместными решениями совокупности двух однородных уравнений от четырех переменных.

Целью статьи является изложение основных результатов, полученных при разработке алгебраического метода помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых.

Основной материал

1. Разработка метода кодирования алгеброгеометрическими кодами на пространственных кривых. 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 α – 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

$$(n \leq N, k \geq \alpha - g + 1, d \geq n - \alpha).$$

Определение 1. 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

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

Для формирования кодового слова

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

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

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

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

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

Пусть $\alpha > 2g-2$, тогда отображение

$$\varphi: X \to P^{m-1}$$

задает проверочную матрицу

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

алгеброгеометрического кода, с конструктивными характеристиками

$$(n \leq N, k \geq n - \alpha + g - 1, d \geq \alpha - 2g + 2).$$

Определение 2. 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 $n \leq N$, для которых выполняется равенство d + g – 1 уравнений

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

Для формирования кодовых слов заданного таким образом алгеброгеометрического кода на пространственных кривых воспользуемся приемами обращения матриц [1].

Разобьем кодовое слово

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

на множества информационных и проверочных позиций (рис. 1).

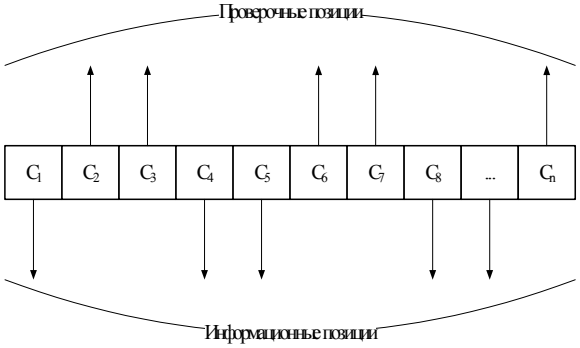

Рис. 1. Разбиение кодового слова на информационные и проверочные позиции

Пусть U – множество k информационных позиций кодового слова (т.е. множество номеров позиций, входящих в заданный информационный набор кода) и W – множество r = n – k проверочных позиций. Объединение множеств $U \cup W$ 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

$$(I_0, I_1, ...I_{k-1}),$$

а на проверочных позициях множества W разместим r нулевых символов.

Для примера, приведенного на рис. 1, имеем:

$$c = (I_0, 0, 0, I_1, I_2, 0, 0, I_3, ...0).$$

Вычислим суммы

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

или в матричной форме

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

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

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

В матричном представлении последняя запись эквивалентна выражению

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

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

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

где

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

матрица, обратная матрице

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

т.е.

$$\left\|\|F_j(p_i(x_0, x_1, x_2, x_3))\|_{r,r}\right\|_{r,r}^{-1} = \left\|\frac{A\left[\|F_j(p_i(x_0, x_1, x_2, x_3))\|_{r,r}\right]}{\Delta}\right\|_{r,r},$$

где

$$A\left[\|F_j(p_i(x_0, x_1, x_2, x_3))\|_{r,r}\right] -$$

алгебраическое дополнение элемента

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

Δ – определитель матрицы

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

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

$$(S_0, S_1, ...S_{r-1})$$

на матрицу

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

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

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

наиболее удобна для вычислений.

Таким образом, для формирования кодового слова алгеброгеометрического кода на пространственных кривых, заданного через проверочную матрицу достаточно хранить элементы матриц

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

и

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

либо поочередно вычислять

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

как значения генераторных функций в точках пространственной кривой.

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

2. Разработка алгоритмов помехоустойчового кодирования алгеброгеометрическими кодами на пространственных кривых. Введенные выше определения 1, 2 алгеброгеометрических кодов на пространственных кривых и функциональные соответствия (3), (6), (7) позволяют формировать кодовые слова как через порождающую так и через проверочную матрицы. В первом случае алгоритм помехоустойчового кодирования задается последовательностью шагов, представленных на рис. 2. Очевидно, формирование кодового слова осуществляется итеративной процедурой, позволяющей на каждом шаге работы алгоритмы формировать соответствующий кодовый символ.

При формировании кодового слова алгеброгеометрических кодов на пространственных кривых через проверочную матрицу алгоритм помехоустойчивого кодирования задается последовательностью шагов, представленных на рис. 3.

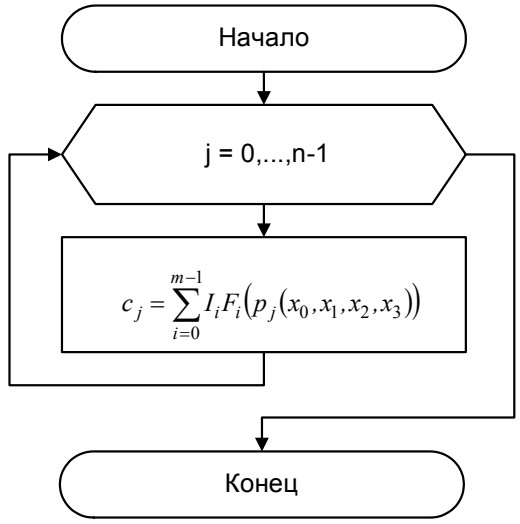

Рис. 2. Схема алгоритма помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых через порождающую матрицу

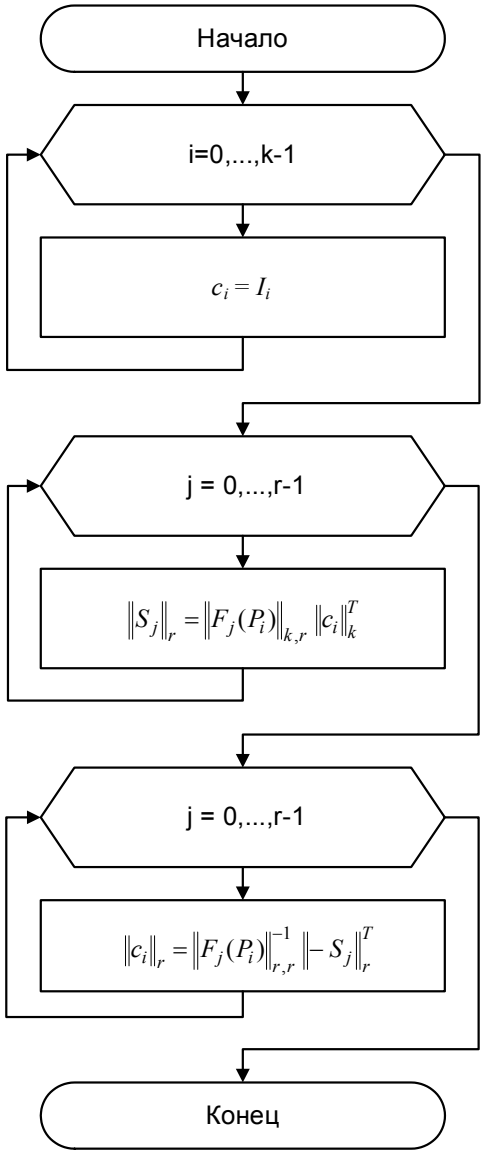

Рис. 3. Схема алгоритма помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых через проверочную матрицу

В этом случае процедура формирования кодового слова реализует операции обращения подматриц проверочной матрицы (4) алгеброгеометрического кода на пространственных кривых:

– на первом этапе информационные символы помещаются на информационные позиции кодового слова;

– на втором этапе с помощью выражения (6) осуществляется вычисление элементов вектора $(S_0, S_1, ..S_{r-1})$;

– на третьем этапе с помощью выражения (7) осуществляется вычисление проверочных символов кодового слова.

Таким образом, разработанные алгоритмы позволяют за конечное число шагов формировать кодовые слова алгеброгеометрических кодов на пространственных кривых, заданных как через порождающую, так и через проверочную матрицы.

Оценим сложность разработанных алгоритмов. Обозначим символом S_E – емкостную сложность алгоритма, т.е. количество необходимых для работы алгоритма ячеек памяти как функцию размера задачи и символом S_B – временную сложность алгоритма, т.е. количество необходимых для работы алгоритма элементарных операций как функцию размера задачи.

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

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

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

Таким образом, при затратах

$$S_E = kn$$

ячеек памяти для работы алгоритма необходимо выполнить

$$S_B = kn$$

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

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

и

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

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

$$S_E = kr + rr = rn$$

ячеек памяти для работы алгоритма необходимо выполнить

$$S_B = kr + rr = rn$$

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:

$$S_E = 3n$$

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

$$S_B = 5kn$$

операций при кодировании через порождающую матрицу и

$$S_B = 5rn$$

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

Впервые предложен метод кодирования алгеброгеометрическими кодами на пространственных кривых, заданными в проективном пространстве P^3 совместными решениями совокупности двух однородных уравнений от четырех переменных. Данный метод развивает отдельное направление теории помехоустойчивого кодирования и является дальнейшим развитием известных методов кодирования кодами на кривых, заданными в проективном пространстве P^2 решениями однородного уравнений от трех переменных (кодами на плоских кривых).

Проведенная оценка сложности реализации разработанных алгоритмов кодирования алгеброгеометрическими кодами на пространственных кривых показала, что формирование кодовых слов реализуется с использованием элементарных арифметических операций над элементами конечного поля и может быть выполнено алгоритмами полиномиальной сложности от параметров кода.

Перспективным направлением дальнейших исследований является разработка практических алгоритмов помехоустойчивого кодирования алгеброгеометрическими кодами на пространственных кривых с использованием предложенного метода, исследование их временной и емкостной сложности реализации.

Список литературы

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.

2. Бэрлэкэмп Э. Алгебраическая теория кодирования. Пер. с англ. / Под ред. С.Д. Бермана. – М.: Мир, 1971. – 477 с.

3. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые //Современные проблемы маттематики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209-257.

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

5. Гоппа В.Д. Коды и информация. // Успехи математических наук. – 1984. – Т. 30, вып. 1 (235). – С. 77-120.

6. Кузнецов А.А. Алгеброгеометрические коды // Электроника и системы управления. – К.: НАУ. – 2005. – № 2 (4). – С. 25-34.

7. Кузнецов А.А. Линейные блоковые коды на алгебраических кривых // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – 2005. – № 1-2. – С. 52-58.

8. Науменко М.І., Стасєв Ю.В., Кузнєцов О.О. Теоретичні основи побудови алгебраїчних кодів: Монографія. – Х.: ХУ ПС, 2005. – 267 с.

9. 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.

10. 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.

11. 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.

12. 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.

Поступила в редколлегию 10.04.2007

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