УДК 621.391.25

АЛГЕБРАИЧЕСКОЕ ДЕКОДИРОВАНИЕ АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВ НА ПРОСТРАНСТВЕННЫХ КРИВЫХ

А.А.Кузнецов
доктор технических наук, с.н.с.
Начальник информационно-вычислительного центра
Харьковский университет Воздушных Сил им. Ивана Кожедуба.
ул. Сумская 77/79, г. Харьков, Украина, 61123.
Контактный телефон: (057) 752-64-15.
e-mail: kyznetsov_alex@rambler.ru

И.В.Пасько
Научный сотрудник центра боевого применения РВиА
Сумской государственный университет
Контактный телефон: (050) 307-71-72
e-mail: pasko-p@rambler.ru

С.П.Евсеев
кандидат технических наук
Доцент кафедры информационных систем*
e-mail:Evseev_serg@inbox.ru.

О.Г.Король
Преподаватель кафедры информационных систем*
e-mail: Korol_o@mail.ru
*Харьковский национальный экономический университет
проспект Ленина 9-а, г. Харьков, Украина, 61001.
Контактный телефон: (057) 702-18-31

Рассматриваются избыточные коды, возникающие на алгебраических кривых (алгеброгеометрические коды), исследуются эффективные методы их декодирования. Предложена аппаратная реализация алгоритма декодирования алгеброгеометрических кодов на пространственных кривых, задаваемых в проективном пространстве P^3. Показано, что разработанная структурная схема позволяет практически реализовать алгоритм алгебраического декодирования алгеброгеометрических кодов на пространственных как в программном, так и в аппаратном виде.

1. Введение

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 [3-5]. Перспективным направлением в этом смысле являются коды, возникающие на алгебраических кривых [5-7]. В [8, 9] показано, что кодовые характеристики этих кодов при большой длине лежат выше границы Варшамова-Гилберта. В тоже время методы декодирования алгеброгеометрических кодов ориентированы на узкий класс кодов и, строго говоря, не позволяют реализовать их потенциальные свойства. В работах [10, 11] предложен метод декодирования кодов на пространственных кривых (P3).

2. Цель работы

Целью данной статьи является исследование эффективных методов декодирования алгеброгеометрических кодов, разработка предложений по реализации устройств декодирования кодов на пространственных кривых.

3. Исследование методов декодирования алгеброгеометрических кодов.

Рассмотрим кодовое слово алгеброгеометрического (n, k, d) кода над GF(q), построенного по пространственным кривым (алгебраическим кривым в P3). Предположим, что алгеброгеометрический код задан через проверочную матрицу

$$H=\begin{pmatrix} F_{0,0,0}(X_0,Y_0,Z_0) & F_{0,0,0}(X_1,Y_1,Z_1) & \dots \\ \dots & F_{0,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) & \\ F_{1,0,0}(X_0,Y_0,Z_0) & F_{1,0,0}(X_1,Y_1,Z_1) & \dots \\ \dots & F_{1,0,0}(X_{n-1}Y_{n-1}Z_{n-1}) & \\ \dots & \dots & \dots \\ F_{0,0,\deg F}(X_0,Y_0,Z_0) & F_{0,0,\deg F}(X_1,Y_1,Z_1) & \dots \\ \dots & F_{0,0,\deg F}(X_{n-1},Y_{n-1},Z_{n-1}) & \end{pmatrix}$$

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

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

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

Справедливо равенство: $C\cdot H^T=0$,

откуда следует равенство:

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

для всех $i=0,...,M-1$.

Предположим, что при передаче по каналу с ошибками кодовое слово исказилось, вектор ошибок обозначим, как e = (e0, e1, ..., en-1), а принятое с ошибками слово как

$C^* = (C^*_0, C^*_1, ..., C^*_{n-1}) = C + e =$

$= (C_0 + e_0, C_1 + e_1, ..., C_{n-1} + e_{n-1})$.

Определим синдромную последовательность как вектор

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

вычисленный по правилу [10, 11]:

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

По определению значение синдромной последовательности s зависит только от вектора ошибок e и не зависит от кодового слова C. Действительно, вычислим произведение

$$C^*\cdot H^T=0,$$

получим: $(C+e)\cdot H=C\cdot H+e\cdot H=e\cdot H$,

откуда следует справедливость $i=0,...,M-1$ равенств:

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

Задача алгебраического декодирования кодового слова алгеброгеометрического кода, построенного по кривой в P3 состоит в нахождении вектора e = (e_0, e_1, ..., e_{n-1})по известной синдромной последовательности

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

Нахождение вектора e позволяет в свою очередь восстановить кодовое слово C по известной последовательности C*:

$$C=C^*-e=(C^*_0-e_0,C^*_1-e_1,...,C^*_{n-1}-e_{n-1}).$$

Для однозначного нахождения вектора ошибок воспользуемся искусственным приемом, состоящем в ведении многочлена локаторов ошибок [10, 11]:

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

решениями которого являются локаторы – такие наборы (X_ξ,Y_ξ,Z_ξ), которые обращают в нуль многочлен (2).Многочлен (2) однозначно задает расположение ошибок в векторе e = (e_0, e_1, ..., e_{n-1}),
так как однозначно указывает на его ненулевые компоненты.

Умножим многочлен (2) на ej и вычислим в точке (X_j,Y_j,Z_j), получим:

$$e_j\cdot X_j^{u-2}+a_{t-3,1,0}\cdot e_j\cdot X_j^{u-3}\cdot Y_j+...+a_{1,0,0}\cdot e_j\cdot X_j+$$
$$+a_{0,1,0}\cdot e_j\cdot Y_i+a_{0,0,1}\cdot e_j\cdot Z_j+a_{0,0,0}\cdot e_j. \quad (3)$$

Просуммируем по всем j = 0,...,n-1, получим:

$$\sum_{j=0}^{n-1}e_j\cdot X_j^{u-2}+\sum_{j=0}^{n-1}a_{t-3,1,0}\cdot e_j\cdot X_j^{u-3}\cdot Y_j+...$$
$$+\sum_{j=0}^{n-1}a_{1,0,0}\cdot e_j\cdot X_j+\sum_{j=0}^{n-1}a_{0,1,0}\cdot e_j\cdot Y_j+$$
$$+\sum_{j=0}^{n-1}a_{0,0,1}\cdot e_j\cdot Z_j+\sum_{j=0}^{n-1}a_{0,0,0}\cdot e_j=0. \quad (4)$$

С учетом введенных выше обозначений, значение одночлена $F_{i_x,i_y,i_z}=x^{i_x}\cdot y^{i_y}\cdot z^{i_z}$

в точке (X_j,Y_j,Z_j) примет вид

$$F_{i_x,i_y,i_z}(X_j,Y_j,Z_j)=X_j^{i_x}\cdot Y_j^{i_y}\cdot Z_j^{i_z}$$

Но по введенному выше определению

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

Следовательно, имеем:

$$s_{u-2,0,0}+a_{t-3,1,0}\cdot s_{u-3,1,0}+...+a_{1,0,0}\cdot s_{1,0,0}+$$
$$+a_{0,1,0}\cdot s_{0,1,0}+a_{0,0,1}\cdot s_{0,0,1}+a_{0,0,0}\cdot s_{0,0,0}=0.$$

Вернемся теперь к рассмотрению многочлена (2). Умножим его на произвольный одночлен $x^{i_x}\cdot y^{i_y}\cdot z^{i_z}$ и проведем аналогичные рассуждения. После суммирования по всем j = 0,...,n-1 и выполнении очевидных подстановок получим:

$$s_{i_x+u-2,i_y,i_z}+a_{t-3,1,0}\cdot s_{i_x+u-3,i_y+1,i_z}+...+a_{1,0,0}\cdot s_{i_x+1,i_y,i_z}+$$
$$+a_{0,1,0}\cdot s_{i_x,i_y+1,i_z}+a_{0,0,1}\cdot s_{i_x,i_y,i_z+1}+a_{0,0,0}\cdot s_{i_x,i_y,i_z}=0.$$

Выполнив соответствующие преобразования для всех $i = 0,...,M-1$ получим систему линейных уравнений:

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

Решения системы (5) дают значения неизвестных коэффициентов многочлена локаторов ошибок $\Lambda(x,y,z)$ (2), который в свою очередь однозначно задает значения локаторов – таких наборов (X_ξ, Y_ξ, Z_ξ), которые обращают в нуль многочлен (2).

Поиск искомых (X_ξ, Y_ξ, Z_ξ) может быть выполнен, например, поочередной подстановкой всех (X_j, Y_j, Z_j), $j = 0,...,n-1$ в многочлен $\Lambda(x,y,z)$ и проверкой на равенство нулю.

Найденные (X_ξ, Y_ξ, Z_ξ) локализуют ошибку в кодовом слове.

Таким образом, рассмотренные операции позволяют получить общее решение задачи декодирования алгеброгеометрических кодов, построенных по пространственным кривым, заданных в проективном пространстве P3 совместными решениями совокупности двух однородных уравнений от четырех переменных.

4. Результаты исследований и их интерпретация

В результате проведенных исследований показано, что задачу декодирования алгеброгеометрических кодов можно свести к решению совокупности линейных уравнений, что легко реализуется как в программном, так и в аппаратном виде. На рис. 1. представлена схема алгоритма декодирования алгеброгеометрических кодов на пространственных кривых.

Анализ соотношений (1) – (5) и структурной схемы алгоритма, приведенного на рис. 1 показывает, что операции алгебраического декодирования алгеброгеометрических кодов на пространственных кривых можно реализовать с использованием элементарных арифметических операций над элементами конечного поля. На рис. 2 приведена схему устройства декодирования алгеброгеометрических кодов на пространственных кривых. На рис. 2 обозначены: БВКС – блок ввода кодового слова с ошибкой; БФСП – блок формирования синдромной последовательности; БФГМ – блок формирования генераторной матрицы; БХФ – блок хранения генераторных функций; БХТ – блок хранения точек пространственной кривой; РБ1 – 1-й решающий блок (вычисление коэффициентов многочлена локаторов ошибок); БФЛ – блок формирования локаторов ошибок; РБ2 – 2-й решающий блок (вычисление значений кратности ошибок); БФВО – блок формирования вектора ошибок; БС – блок согласования; БИО – блок исправления ошибок в кодовом слове.

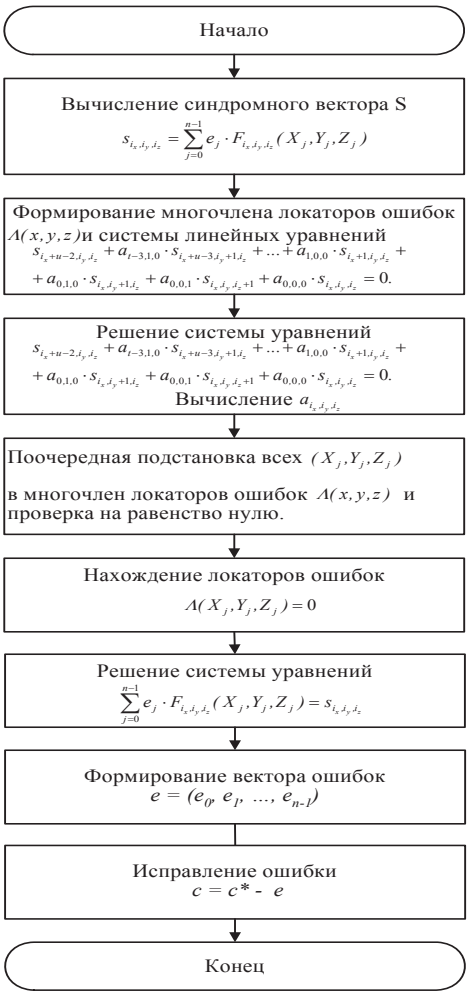

Рис. 1. Схема алгебраического алгоритма декодирования

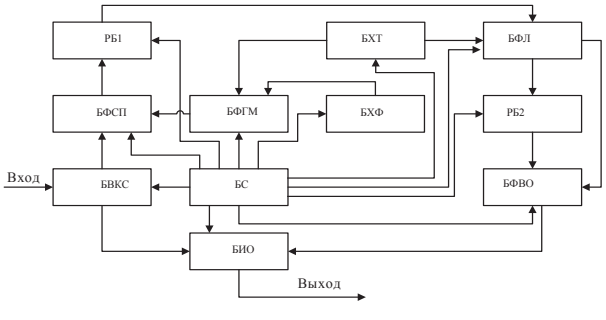

Рис. 2. Структурная схема устройства декодирования алгеброгеометрических кодов на пространственных кривых

Устройства функционирует следующим образом. Кодовое слово с ошибкой поступает на блок ввода кодового слова, откуда оно поступает в блок формирования синдромной последовательности и на блок исправления ошибок в кодовом слове. В блоке формирования синдромной последовательности с использованием элементов генераторной матрицы, вычисленных в блоке формирования генераторной матрицы с использованием параметров генераторных функций и точек пространственной кривой, считанных с блоков

хранения генераторных функций и хранения точек пространственной кривой соответственно, формируется синдромная последовательность, которая поступает на вход 1-го решающего блока. В 1-м решающем блоке производится вычисление коэффициентов многочлена локаторов ошибок, которые поступают на вход блока формирования локаторов ошибок. В блоке формирования локаторов ошибок с использованием считанных с блока БХТ точек пространственной кривой и поступивших на его вход коэффициентов многочлена локаторов ошибок производится вычисление локаторов. Найденные локаторы ошибок поступают на вход 2-го решающего блока и на вход блока формирования вектора ошибок. В 2-м решающем блоке производится вычисление значений кратности произошедших ошибок. С их помощью в блоке формирования вектора ошибок, с учетом локаторов поступивших с выхода блока формирования локаторов ошибок, формируется вектор ошибок. Найденный вектор ошибок поступает на вход блока исправления ошибок в кодовом слове. В блоке исправления ошибок кодовое слово с ошибками с использованием сформированного вектора ошибок преобразуется в кодовое слово алгеброгеометрического кода, в результате чего процесс декодирования завершается. Сформированное кодовое слов поступает на выход устройства декодирования. Блок согласования предназначен для согласования работы отдельных блоков устройства декодирования.

5. Выводы

Таким образом, в результате проведенных исследований получено общее решение задачи декодирования алгеброгеометрических кодов, построенных по пространственным кривым. Разработанная структурная схема устройства декодирования позволяют практически реализовать разработанный алгебраический метод как в программном, так и в аппаратном виде.

Литература

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. Северинов А.В., Кузнецов А.А., Куриш В.В. Разработка алгоритма декодирования алгеброгеометрических кодов // Системи обробки інформації. – Харків: НАНУ, ПАНИ, ХВУ. – №1(17). – 2002. – С. 161-163.
4. 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.
5. 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.
6. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые //Современные проблемы маттематики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209-257.
7. Влэдуц С. Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. – М.: МЦИМО, 2003. – 504 с.
8. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЭ. – 2003. – Вып. 134. – С. 218-222.
9. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов. //Электронное моделирование: Международный научно-теоретический журнал. – К: НАНУ, РАН. – 2004. – №2. – С. 27-38.
10. Кузнецов О.О., Пасько І.В. Алгебраїчний метод декодування лінійних блокових кодів на алгебраїчних кривих у Р3. // Системи озброєння і військова техніка. – Х.: ХУПС. - 2006. –№ 3(7). – С – 69-72.
11. Пасько И.В. Алгебраическое декодирование кодов на пространственных кривых // Системи обробки інформації: Збірник наукових праць.– Х.: ХУПС, 2007. – Вип. 1 (59). – С. 121 - 125.