УДК 621.391

АЛГОРИТМ МАЖОРИТАРНОГО ДЕКОДИРОВАНИЯ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ

к.т.н. А.А. Кузнецов, к.т.н А.В. Северинов, В.Н. Лысенко
(представил д.ф.-м.н., проф. Н.Н. Горобец)

Предлагается мажоритарный алгоритм декодирования алгеброгеометрических кодов в один шаг. Получены верхние границы мощности множества ортогональных уравнений одношагового мажоритарного декодирования линейных нециклических блоковых кодов. Рассмотрен пример мажоритарного декодирования кода по кривой Эрмита.

Введение. Мажоритарное декодирование является одним из наиболее простых и удобных в реализации методов декодирования алгебраических блоковых кодов. Практическая реализация таких декодеров привлекательна высоким быстродействием и низкой сложностью [1 – 2].

Суть мажоритарного декодирования состоит в мажоритарном оценивании веса ошибки, произошедшей в i-м символе кодового слова. Подобная оценка проводится над ортогональными относительно i-го кодового символа проверочными уравнениями. Ортогональное относительно i-й координаты подмножество проверочных уравнений состоит из всех уравнений, в каждое из которых входит i-я компонента, а остальные компоненты входят не более чем в одно уравнение. Для циклических кодов такое подмножество совпадает для всех координат, декодирование состоит в оценивании веса ошибки, произошедшей в i-м символе циклически сдвинутого кодового слова. Если структура кода такова, что множество проверочных уравнений ортогонально относительно нескольких координат, то мажоритарное решение применимо для локализации ошибки в подмножестве этих компонент. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), обладают высокой исправляющей способностью при небольшой доле вносимой избыточности [3 – 6]. В работах [5 – 6] показано, что их применение в недвоичных каналах позволяет получить существенный энергетический выигрыш, по сравнению с другими блоковыми кодами.

Актуальной ***научно-технической проблемой*** является разработка эффективных, с точки зрения простоты технической реализации и низкой системотехнической сложности, методов их декодирования. Это

связано с важным ***практическим заданием*** – практическая реализация алгеброгеометрического кодирования (декодирования) для повышения достоверности передачи данных в сетях управления.

Цель статьи – разработка мажоритарного алгоритма декодирования линейных нециклических блоковых кодов, допускающего декодирование алгеброгеометрических кодов, с минимальным числом ортогональных проверок.

Алгеброгеометрические коды, в общем виде, не обладают цикличной структурой, ортогональные подмножества относительно каждой координаты различны. ***Анализ литературы*** [1 – 3] показал, что применение стандартного алгоритма мажоритарного декодирования для нециклических кодов требует выполнения 2t ортогональных проверок для каждой из n компонент (n, k, d) кода. Разработка таких декодеров усложняется также поиском ортогональных подмножеств (систем проверочных уравнений) для каждой из n координат. Задача поиска минимального набора ортогональных проверок мажоритарного декодирования нециклических кодов, оценка мощности этого набора – ***нерешенная часть проблемы***.

В статье предлагается алгоритм формирования таких подмножеств с верхней оценкой мощности множества ортогональных уравнений, позволяющих осуществить ортогонализацию нециклического (n, k, d) кода в один шаг (если такая ортогонализация возможна).

Алгоритм формирования системы проверочных уравнений. Пусть задан алгебраический блоковый нециклический (n, k, d) код, t – число ошибок, исправляемых при мажоритарном декодировании кода в один шаг, $t \le$ $\le (n-1)/(2d_{\perp}-2)$, $(n, n-k, d_{\perp})$ – дуальный код. Предлагаемый алгоритм формирования системы проверочных уравнений состоит из следующих шагов.

1. С помощью элементарных преобразований над проверочной матрицей кода найдем 2t проверочных уравнений, ортогональных по первой координате. Каждое из полученных уравнений содержит, как минимум, $d_{\perp}$ слагаемых и, соответственно, может быть использовано для ортогонализации по $d_{\perp} - 1$ другим координатам.

2. Найдем 2t проверочных уравнений, ортогональных по второй координате. На этом шаге используем уже найденные уравнения, в состав которых входит слагаемое со второй компонентой. Остальные уравнения находим путем элементарных преобразований над проверочной матрицей кода.

3. Повторив шаг № 2 для каждой координаты, получим систему проверочных уравнений, позволяющих осуществить ортогонализацию (n, k, d) кода в один шаг.

Утверждение о минимальном наборе ортогональных уравнений одношаговой ортогонализации нециклического кода. Минимальный набор уравнений для одношаговой ортогонализации нециклического (n, k, d) кода содержит не более $2tn/d_{\perp}$ уравнений (t – число ошибок, исправляемое одношаговым мажоритарным декодером; $d_{\perp}$ – минимальное расстояние дуального кода).

Доказательство. Для мажоритарного декодирования (n, k, d) кода в один шаг, по определению, необходимо выполнить 2tn проверок. Пусть M – число уравнений, полученных в результате выполнения предлагаемого алгоритма. Каждое из проверочных уравнений используется, как минимум, в $d_{\perp}$ проверках, следовательно, $Md_{\perp} \le 2tn$. Равенство выполняется всегда, если дуальный код эквидистантен. В общем случае полученная в результате выполнения предлагаемого алгоритма система уравнений содержит $M \le 2tn/d_{\perp}$ уравнений. *Утверждение доказано.*

Если нециклический (n, k, d) код допускает одношаговую ортогонализацию, применение результата последнего утверждения позволяет упростить процедуру одношагового мажоритарного декодирования. Достаточно записать систему $M \le 2tn/d_{\perp}$ проверочных уравнений в виде матрицы коэффициентов уравнений размерности $n \times M$ и осуществлять декодирование в виде последовательности следующих шагов.

Алгоритм мажоритарного декодирования нециклических кодов в один шаг. 1. Систему из $M \le 2tn/d_{\perp}$ проверочных уравнений запишем в виде матрицы $n \times M$, значения элементов матрицы – коэффициенты проверочных уравнений. Каждый столбец матрицы содержит 2t ненулевых элемента. Строки с ненулевыми элементами в i-м столбце соответствуют проверочным уравнениям, ортогональным по i-й координате.

2. Выполняем M проверок. Мажоритарно оцениваем вес ошибки в каждом символе. Локализуем ошибку.

3. Вычисляем кратность ошибки в локализованных ошибочных символах. Используем те проверочные уравнения, в которые входит только одна из ошибочных компонент.

Пример. Рассмотрим алгеброгеометрический код (9, 3, 6) по кривой Эрмита над GF(4), задаваемой совокупностью решений однородного алгебраического уравнения $x^3 + y^3 + z^3 = 0$. Род кривой g(X) = 1, число точек N = 9. Точки P_i, i = 1 ... 9 кривой Эрмита над GF(4) приведены в табл. 1.

Таблица 1

Решения уравнения $x^3 + y^3 + z^3 = 0$ над GF(4)

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
x	1	2	3	1	2	3	0	0	0
y	1	1	1	0	0	0	1	2	3
z	0	0	0	1	1	1	1	1	1

Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным в P^2 уравнениями F = 0, где F – однородные одночлены первой степени. Пусть C – класс дивизоров на X степени $\alpha = \deg F \cdot \deg X = 3 > g - 1$. Тогда C задает отображение $\varphi : X \to P^{k-1}$, набор генераторных функций $y_i = \varphi(x_i)$ задает порождающую матрицу кода, причем $n \le N$, $k \ge \alpha - g + 1 = 3$, $d \ge n - \alpha = 6$. Порождающая матрица примет вид

$$G = \begin{Vmatrix} f_1(P_i) \\ f_2(P_i) \\ f_3(P_i) \end{Vmatrix}, \quad i = \overline{1,9},$$

где $f_1(x,y,z) = x$, $f_2(x,y,z) = y$, $f_3(x,y,z) = z$ – генераторные функции, задающие код. Порождающая и проверочная матрица кода в каноническом виде

$$G = \begin{vmatrix} 1 & 0 & 0 & 2 & 3 & 1 & 2 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 & 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 2 & 0 & 3 & 1 & 3 & 3 \end{vmatrix}; \quad H = \begin{vmatrix} 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Число ошибок, которые код может исправить, t = 2. Дуальный к рассматриваемому коду – код с параметрами (9, 6, 3). Сформируем систему проверочных уравнений в соответствии с предложенным алгоритмом. Всего необходимо выполнить 36 проверок. Для рассматриваемого примера минимальное число проверочных уравнений, в соответствии с доказанным утверждением, M = 36/3 = 12. В табл. 2 представлена матрица коэффициентов проверочных уравнений.

Таблица 2

Матрица коэффициентов проверочных уравнений
для мажоритарного декодироваия кода (9, 3, 6) в один шаг

1	1	0	0	2	0	0	0	0
1	0	1	3	0	0	0	0	0
1	0	0	0	0	1	0	0	1
1	0	0	0	0	0	2	3	0
0	1	2	0	0	0	0	0	3
0	1	0	1	0	0	0	1	0
0	1	0	0	0	2	1	0	0
0	0	1	0	3	0	1	0	0
0	0	1	0	0	3	0	1	0
0	0	0	1	1	2	0	0	0
0	0	0	1	0	0	1	0	1
0	0	0	0	1	0	0	1	1

Каждый столбец матрицы содержит 2t = 4 ненулевых элементов. Строки с ненулевыми элементами в i-м столбце соответствуют проверочным уравнениям, ортогональным по i-й координате. Пусть c – кодовое слово рассматриваемого (9, 3, 6) кода, c = {102130021}. Пусть e – вектор ошибок, e = {300000100}. Принятая с ошибками кодовая последовательность c* = {202130121}. Для первой компоненты кодовой последовательности коэффициенты ортогональных уравнений записаны в первых четырех строках табл. 1. Для второй компоненты коэффициенты уравнений записаны в первой, пятой, шестой и седьмой строке, и т.д. для всех компонент. Результат ортогональных проверок, для удобства, запишем в виде матрицы n × M (табл. 3).

Таблица 3

Результат выполнения ортогональных проверок
при декодировании алгеброгеометрического кода (9, 3, 6) в один шаг

False	*False*	0	0	*False*	0	0	0	0
False	0	*False*	*False*	0	0	0	0	0
False	0	0	0	0	*False*	0	0	*False*
True	0	0	0	0	0	*True*	*True*	0
0	*True*	*True*	0	0	0	0	0	*True*
0	*True*	0	*True*	0	0	0	*True*	0
0	*False*	0	0	0	*False*	*False*	0	0
0	0	*False*	0	*False*	0	*False*	0	0
0	0	*True*	0	0	*True*	0	*True*	0
0	0	0	*True*	*True*	*True*	0	0	0
0	0	0	*False*	0	0	*False*	0	*False*
0	0	0	0	*True*	0	0	*True*	*True*
False	***True***	***True***	***True***	***True***	***True***	***False***	***True***	***True***

Значения ячеек табл. 3 заполняем символами истинности: «*True*» – если результат проверки положителен, «*False*» – в противном случае. Арифметические операции выполняем над конечным полем из четырех элементов. Значение «0» соответствует нулевому коэффициенту в проверочном уравнении (в проверке не участвует). Последняя строка табл. 3 содержит результат мажоритарного оценивания веса ошибки в каждой компоненте кодовой последовательности (мажоритарный порог – «≥ 2»). Результат мажоритарного оценивания позволил локализовать ошибку – ошибка произошла в первом и седьмом символе. Исправить ошибку можно с помощью любого проверочного уравнения, в которое входит только одна из ошибочных компонент. Для первого символа – это первое, второе или третье уравнение, для седьмого символа – это седьмое,

восьмое или одиннадцатое уравнение. В результате получим:

$c_1 = c_2 + 2 \times c_5 = 0 + 2 \times 3 = 1;$ $\quad c_7 = c_2 + 2 \times c_6 = 0 + 2 \times 0 = 0;$

$c_1 = c_3 + 3 \times c_4 = 2 + 3 \times 1 = 1;$ $\quad c_7 = c_3 + 3 \times c_5 = 2 + 3 \times 3 = 0;$

$c_1 = c_6 + c_9 = 0 + 1 = 1;$ $\quad c_7 = c_4 + c_9 = 1 + 1 = 0.$

Ошибка локализована и исправлена.

Выводы. Предложенный алгоритм формирования системы проверочных уравнений позволяет получить минимальный набор ортогональных проверок. Использование минимального набора проверок позволяет существенно сократить объем запоминающего устройства для хранения коэффициентов ортогональных уравнений мажоритарного декодера нециклического кода. Так, в рассмотренном примере использование набора из 12 проверочных уравнений (вместо 36) позволяет сократить в три раза объем необходимой памяти (ячеек матрицы коэффициентов уравнений). На рассмотренном примере продемонстрирована конструктивность мажоритарного декодирования алгеброгеометрических кодов.

ЛИТЕРАТУРА

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.*
2. *Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.*
3. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259. – № 6. – С. 1289 – 1290.*
4. *Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы математики. – М.: ВИНИТИ, 1984. – Т. 25. – С. 209 – 257.*
5. *Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2003. – Вып. 133.*
6. *Кузнецов А.А. Каскадное кодирование с алгеброгеометрическим кодом внешнего каскада // Информационно-управляющие системы на железнодорожном транспорте. – 2002. – С. 39 – 45.*

Поступила 26.05.2003

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, зам. нач. НИЛ ХВУ. В 1996 году окончил ХВУ. Область научных интересов – теория аутентификации, алгебраическая теория кодов и их применение в системах передачи данных. E - mail : kuznetsov@sky.net.ua .*

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

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