УДК 621.391

АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ДЕКОДИРОВАНИЯ НЕДВОИЧНЫХ БЛОКОВЫХ КОДОВ

Е.Л. Онанченко, А.В. Лысенко
Сумский государственный университет, г. Сумы

В статье анализируются известные методы декодирования недвоичных блоковых кодов, исследуется возможность их использования для декодирования алгеброгеометрических кодов.

ВВЕДЕНИЕ

Развитие информационно-телекоммуникационных сетей (ИТС) тесно связано с повышением скорости и достоверности обработки и передачи информации. Решение этой проблемы за счет повышения энергетических ресурсов системы практически себя исчерпало. Одно из направлений, которое получило мировое развитие, связывают с разработкой теории и практики построения избыточных кодов с заданными характеристиками.

В этой отрасли науки получены фундаментальные теоретические результаты, разработаны и внедрены практические методы кодирования и декодирования помехоустойчивых кодов.

Целью статьи является проведение анализа известных методов декодирования недвоичных блоковых кодов.

РЕЗУЛЬТАТЫ АНАЛИЗА

В основе большинства известных методов декодирования недвоичных блоковых кодов лежат различные модификации отдельных этапов декодера Питерсона-Горенштейна-Цирлера [1-4, 5-6, 8, 9, 10], представленного на рис. 1.

Схема декодирования Питерсона-Горенштейна-Цирлера ориентирована на декодирование кодов БЧХ (кодов Рида-Соломона в том числе). Рассмотрим каждый этап представленной на рис. 1 схемы декодирования, проанализируем возможность их использования для декодирования алгеброгеометрических кодов.

Рассмотрим линейный блоковый (n, k, d) код над полем GF(q). Предположим, что при передаче по каналу с ошибками кодовое слово $c = (c_0, c_1, \ldots, c_{n-1})$ исказилось. Вектор ошибок обозначим как $e = (e_0, e_1, \ldots, e_{n-1})$. Принятое слово c^* после передачи по каналу с ошибками запишется в виде $c^* = c + e = (e_0 + c_0, e_1 + c_1, \ldots, e_{n-1} + c_{n-1})$. Задача декодера состоит в восстановлении кодового слова с по принятому слову c^*.

На первом этапе вычисляется синдромный вектор $S = (S_0, S_1, \ldots, S_{r-1})$. Если линейный блоковый код задан проверочной матрицей H,

$$H = \begin{pmatrix} h_{00} & h_{10} & \ldots & h_{n-1\,0} \\ h_{01} & h_{11} & \ldots & h_{n-1\,2} \\ \ldots & \ldots & \ldots & \ldots \\ h_{0\,r-1} & h_{1\,r-1} & \ldots & h_{n-1\,r-1} \end{pmatrix} = \left\| h_{ij} \right\|_{n,r},$$

вычисление синдрома осуществляется по следующему выражению:

$$S_j = \sum_{i=0}^{n-1} c_i^* h_{ij} = \sum_{i=0}^{n-1} e_i h_{ij},\ j = 0,\ \ldots,\ r-1.$$

Рисунок 1 – Декодер Питерсона-Горенштейна-Цирлера

или в матричной форме

$$\|S\|_r = \|h_{ij}\|_{n,r} \|e_i\|_n^T .$$

Применительно к декодированию кодов БЧХ элементы синдромной последовательности вычисляются как

$$S_l = \sum_{i=0}^{n-1} e_i X_i^l , \qquad (1)$$

где $X \in GF(q^m)$ и однозначно указывает положение ошибки, n - делитель q^m-1. Если матричное описание циклического кода заменить

полиномиальным, то вычисление компонент синдромного вектора по выражению (1) эквивалентно вычислению значения проверочного многочлена в точке X. Для этих целей на практике применяют быстрые алгоритмы вычисления значения многочленов такие, например, как схема Горнера, алгоритм Винограда, основанный на использовании результатов китайской теоремы об остатках [1-4, 5-6, 8, 9, 10].

Вычисление синдрома по схеме Горнера требует r(n - 1) операций сложения и столько же операций умножения в поле *GF(q)*. Если длина кода является составным числом, применение алгоритма Винограда позволяет уменьшить суммарное количество операций.

Теоретические подходы к алгоритмическому решению задачи декодирования основаны на алгебраических методах решения систем нелинейных уравнений над конечным полем.

Для решения этой задачи используют искусственный прием, заключающийся во введении в рассмотрение многочлена локаторов ошибок, решения которого однозначно локализуют (указывают местоположение) возникших ошибок [1-4, 5-6, 8, 9, 10]. В традиционных алгоритмах декодирования под многочленом локаторов ошибок понимают многочлен степени $\le t$ от одной переменной

$$a_0 + a_1 x + \ldots + x^t = 0, \qquad (2)$$

где t – число ошибок, которое может исправить код.

Умножив обе части многочлена (2) на e_i и просуммировав по всем $i = 0 \,..\, n - 1$ значениям в точке $(x = X_i)$, получим рекуррентное выражение

$$a_0 S_l + a_1 S_{l+1} + \ldots + S_{l+t} = 0, \qquad (3)$$

которое задает систему линейных уравнений относительно неизвестных коэффициентов многочлена локаторов ошибок. В матричной форме система запишется в виде

$$\begin{pmatrix} S_0 & S_1 & \ldots & S_{t-1} \\ S_1 & S_2 & \ldots & S_t \\ \ldots & \ldots & \ldots & \ldots \\ S_{t-1} & S_t & \ldots & S_{2t-2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} -S_t \\ -S_{t+1} \\ \ldots \\ -S_{2t-1} \end{pmatrix}. \qquad (4)$$

Ранг квадратной матрицы в левой части (4) задает истинное число произошедших ошибок. Решение системы (4) даст значения коэффициентов многочлена локаторов ошибок, однозначно указывающего на местоположение ошибок.

Для решения системы (4) используют алгоритмы, представленные на рис. 1. Так, определительный метод состоит в нахождении ранга матрицы и решении системы (1) по правилу Крамера. По оценкам [3, 7, 8, 10] этот алгоритм требует выполнения t^3 операций.

Использование метода исключения неизвестных по методу Гаусса и его модификаций состоит в приведении матрицы к диагональному виду и требует порядка t^3 операций [3, 7, 8, 10].

Суть алгоритма Берлекемпа состоит в синтезе регистра сдвига наименьшей длины с линейной обратной связью, генерирующего последовательность синдромов (синдромный вектор). Реализация второго этапа декодирования при использовании алгоритма Берлекемпа требует порядка t^2 операций [3, 7, 8, 10].

Сейчас разработаны модифицированные алгоритмы Берлекемпа, позволяющие снизить сложность декодирования, ускорить быстродействие (алгоритм Берлекемпа–Месси и его модификации) [3, 7, 8, 10].

Алгоритм Евклида состоит в нахождении наибольшего общего делителя двух многочленов при решении ключевого уравнения. Алгоритм Евклида по числу операций сравним с алгоритмом Берлекемпа. Подробное решение задачи декодирования кодов БЧХ с помощью введенного в рассмотрение многочлена локаторов ошибок см. в [1-4, 5-6, 7, 8, 9, 10].

На следующем этапе алгебраического декодирования вычисляются локаторы, однозначно указывающие на положение ошибок. Суть прямого и гибридного методов состоит в приведении многочлена локаторов к нормальному виду, что легко реализуемо при небольшом числе ошибок.

В процедуре Ченя не накладывается ограничений на число ошибок. Суть такого алгоритма состоит в подстановке всех возможных локаторов и выборе тех из них, которые обращают в нуль многочлен локаторов ошибок. Применительно к декодированию кодов БЧХ в многочлен локаторов ошибок подставляются все элементы поля $X \in GF(q^m)$. Количество операций при реализации процедуры Ченя составляет $2t \cdot (q^m - 1)$.

На последнем этапе алгебраического декодирования вычисляются значения e_i и формируется вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$. Подставив найденные локаторы в (1), получим систему линейных уравнений относительно неизвестных значений e_i. Для решения полученной системы используют различные алгоритмы, в том числе методы второго этапа декодирования (см. рис. 1). При решении дополнительно вводимого ключевого уравнения используют также метод Форни, который позволяет находить очередное значение e_i в момент соответствующего локатора. Сложность реализации алгоритма Форни порядка $2t \cdot (t - 1)$ [3, 7, 8, 10].

Исправление ошибок осуществляется по правилу

$$c = c^* - e = (c_0^* - e_0, c_1^* - e_1, \ldots, c_{n-1}^* - e_{n-1}).$$

Для некоторых низкоскоростных блоковых кодов для формирования вектора ошибок целесообразно использовать процедуры спектрального декодирования. Суть спектрального декодирования состоит в рекуррентном вычислении компонент синдрома и формировании вектора $S = (S_0, S_1, ..., S_{n-1})$. Эту задачу решают различными способами: генерацией синдромов через регистры сдвига, методом цепных дробей, непосредственно через рекуррентное выражение (3). Сложность формирования полного вектора $S = (S_0, S_1, ..., S_{n-1})$ через рекуррентное выражение составляет $(n - 2t)(2t - 1)$ операций. Обратное преобразование Фурье, которое является частным случаем интерполяционной формулы Лагранжа [3, 7, 8, 10], позволяет сформировать вектор ошибок. Сложность обратного преобразования Фурье составляет $2n^2$ операций. Переходя к быстрым методам преобразования Фурье, удается достичь уменьшения числа операций.

Декодирование линейных блоковых кодов существенно упрощается, если удается применить эффективные неалгебраические методы декодирования. На рис. 1. представлены наиболее распространенные из них. Кратко проанализируем возможность применения этих алгоритмов для декодирования длинных недвоичных кодов.

Декодер Меггита является простейшим алгоритмом декодирования циклических кодов. Этот алгоритм является разновидностью табличного декодера, суть которого состоит в хранении таблицы синдромов в

запоминающем устройстве. Для декодирования недвоичных кодов алгоритм используется мало по причине значительного объема запоминающего устройства [3, 7, 8]. Для декодирования алгеброгеометрических кодов этот алгоритм неприемлем по причине высоких системотехнических затрат, необходимых для его реализации.

Метод проб и ошибок основан на поочередном изменении символов кодового слова и определении момента уменьшения вектора ошибок. Такой алгоритм является разновидностью метода полного перебора и требует значительных временных затрат [3, 7, 8, 10]. Для декодирования алгеброгеометрических кодов этот алгоритм неприемлем по причине высоких вычислительных затрат, необходимых для его реализации.

Идея метода вылавливания ошибок состоит в преобразовании кодового слова с целью выведения комбинации из t ошибок в проверочную часть. В [3, 7, 8, 10] показано, что необходимым и достаточным условием исправления t ошибок методом вылавливания является $t < n/k$, что существенно сужает область применения этого алгоритма.

Перестановочное декодирование представляет собой последовательное применение к принятому слову метода вылавливания ошибок и перестановки символов, инвариантной относительно кода. Этот процесс продолжается до момента вывода всех ошибок в проверочную часть. Применение перестановочного декодера сдерживается неопределенностью в правиле выбора совокупности перестановок. В то же время для некоторых алгеброгеометрических кодов (небольшой длины) может быть успешно реализован перестановочный алгоритм декодирования.

Мажоритарный алгоритм декодирования привлекателен высоким быстродействием и низкой сложностью [1-4, 5-6, 7, 8, 9, 10]. Суть этого алгоритма состоит в мажоритарном оценивании веса ошибки для каждого символа отдельно. Алгоритм реализуем только для кодов, допускающих полную ортогонализацию. Если алгоритмический код допускает полную ортогонализацию, то для его декодирования можно использовать мажоритарный алгоритм.

ВЫВОДЫ

Проведенный в статье анализ методов декодирования недвоичных блоковых кодов позволяет ознакомиться с существующими методами и алгоритмами декодирования.

Показана возможность применения того или иного метода декодирования применительно к различным недвоичным блоковым кодам. Проанализированы систематические затраты при применении неалгебраических и алгебраических методов декодирования.

Проведенный анализ известных процедур декодирования недвоичных блоковых кодов позволяет сделать вывод о целесообразности разработки алгебраического декодера алгеброгеометрических кодов.

SUMMARY

THE ANALYSIS OF KNOWN METHODS OF DECODING OF NOT BINARY BLOCK CODES

E.L. Onanchenko, A.V. Lysenko
Sumy State University

In the article known methods of decoding not binary block codes are analyzed, possibility of their use for decoding algebraic codes is investigated.

СПИСОК ЛИТЕРАТУРЫ

1. Берлекэмп Э.Р. Алгебраическая теория кодирования: Пер. с англ.– М.: Мир, 1971.– 477 с.
2. Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. — 1104 с.

3. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
4. Блох Э.Д., Зяблов В.В. Обобщенные каскадные коды. – М.: Связь, 1976. – 240 с.
5. Кларк Дж.-мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Под ред. Б.С. Цыбакова. - М.: Радио и связь, 1987. - 392 с.
6. Ключко В.И. Защита информации от ошибок в АСУ. – МО СССР, 1980. – 256 с.
7. Коррекция ошибок в оптических накопителях информации // Типикин А.П., Петров В.В., Бабанин А.Г.; Отв. hед. Додонов А.Г.; АН УССР. Ин-т проблем регистрации информации. – К.: Наукова думка, 1990. – 172 с.
8. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки.- М.: Связь, 1979. - 744 с.
9. Мутер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1990. – 288 с.
10. Теория кодирования: Пер. с япон. / Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки /Под ред. Б.С. Цыбакова и С.И. Гельфанда. – М.: Мир, 1978. - 576 с.

Онанченко Е.Л., канд. техн. наук, доцент, СумГУ, г. Сумы;
Лысенко А.В., студент, СумГУ, г. Сумы

Поступила в редакцию 4 июля 2008 г.