УДК 621.391

РАЗРАБОТКА АЛГОРИТМА ДЕКОДИРОВАНИЯ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ

к.т.н. А.В. Северинов, к.т.н. А.А. Кузнецов, В.В. Куриш
(представил д.т.н., проф. В.И. Долгов)

Предложен алгоритм декодирования алгеброгеометрических кодов, построенных по точкам гладких проективных кривых. Его отличительная особенность – декодирование кодов с квазициклической структурой.

Опыт практического использования телекоммуникационных систем подтверждает целесообразность применения каскадных схем помехоустойчивого кодирования. В качестве кода внешнего каскада используются, как правило, **q**-ичные кодовые конструкции. Перспективными в этом направлении являются алгеброгеометрические коды, так как для фиксированной длины и кратности кода они дают наибольшее кодовое расстояние.

Алгеброгеометрические коды – линейные блочные алгебраические коды, соответствующие линейному пространству, построенному на рациональном отображении гладкой проективной кривой. Возможность построения таких кодов теоретически обоснована [1].

Асимптотические свойства алгеброгеометрических кодов подтверждают целесообразность их практического использования. Доказано, что при больших **q** (**q ≥ 49**) существуют алгеброгеометрические коды, лежащие выше границы Варшамова - Гилберта [2]. Алгоритмы построения алгеброгеометрических кодов подробно изложены в [3, 4]. Эффективные алгоритмы декодирования алгеброгеометрических кодов в отечественной литературе не изложены.

На существующие алгоритмы декодирования **q** - ичных кодов накладываются определенные ограничения. Они разработаны для циклических кодов и применимы при различных допущениях. Так, например, синдромный декодер требует больших объемов памяти (при больших **n - k** и **t**). Этот факт свидетельствует о нецелесообразности их применения для кодов большой длины. Алгоритмы порогового декодирования разработаны для **q** - ичных кодов только определенной структуры (например, коды Рида - Соломона).

Задачей работы является изложение разработанного алгоритма декодирования **q**-ичных кодов с циклической и квазициклической структурой. Особенность алгоритма состоит в декодировании алгеброгеометрических кодов, определение которых в общем виде не предполагает цикличность структуры. В основе разработанного алгоритма лежит модифицированный алгоритм декодирования 2-ичных кодов Омуры [5].

Предложенный алгоритм для **q**-ичных систем кодирования учитывает кратность возникающей ошибки одного символа кодового слова.

Пусть задан код **C** – алгеброгеометрический код с конструктивными характеристиками (**n**, **k**, **d**):

$$\begin{cases} \mathbf{n} \le \mathbf{N}; \\ \mathbf{k} \ge \alpha - \mathbf{g} + \mathbf{1}; \\ \mathbf{d} \ge \mathbf{n} - \alpha, \end{cases}$$

где **N** - число рациональных точек кривой, на отображении которых построен код; **g** - род кривой; **α** - степень класса дивизоров.

Его дуальный код **C'** – алгеброгеометрический код с конструктивными характеристиками (**n**, **k**, **d**):

$$\begin{cases} \mathbf{n} \le \mathbf{N}; \\ \mathbf{k} \ge \mathbf{n} - \alpha + \mathbf{g} - \mathbf{1}; \\ \mathbf{d} \ge \alpha - \mathbf{2g} + \mathbf{2}. \end{cases}$$

Пусть проверочная матрица алгеброгеометрического кода $\mathbf{H} = \{\mathbf{h_1}, \mathbf{h_2}, \ldots, \mathbf{h_n}\}$ задана в каноническом виде **[Y:I]**, где $\mathbf{h_i}$ - **i**-й столбец матрицы **H**, **Y** - информационное множество, **I** - единичная матрица, соответствующая проверочному множеству.

Последовательность операций алгоритма приведена ниже.

1. Выбирается проверочное множество и соответствующая ему проверочная матрица (для однозначного определения начальных условий берется матрица **H**).

2. Вычисляется синдром $\mathbf{S_i}$ по матрице $\mathbf{H_i}$ и формируется вектор ошибок $\mathbf{e_i}$, причем если $\mathbf{S^T}=\{\mathbf{S_0}, \mathbf{S_1},\ldots,\mathbf{S_{n-k}}\}$, то $\mathbf{e^T}=\{\mathbf{0,0},\ldots,\mathbf{0}, \mathbf{S_0},\mathbf{S_1},\ldots,\mathbf{S_{n-k}}\}$.

3. Если вес $\mathbf{We_i} \le \mathbf{t}$, то решение найдено: возникшая ошибка имеет вид $\mathbf{e^T}= \{\mathbf{0,0},\ldots,\mathbf{0}, \mathbf{S_0},\mathbf{S_1},\ldots,\mathbf{S_{n-k}}\}$.

4. Если $\mathbf{We_i} > \mathbf{t}$, то определяется такая ошибка информационного множества, которая в совокупности с **e** уменьшает вес $\mathbf{We_i}$. Эта процедура осуществляется путем выбора столбца $\mathbf{h_i}$ информационного множества и сложения с синдромом $\mathbf{S_i}$ над полем **GF(q)**. Отличительная особенность алгоритма состоит в необходимости учитывать кратность ошибки l на одной позиции, $l \in \mathbf{GF(q)}$.

5. По выбранной сумме столбца $\mathbf{h_i}$ и $\mathbf{S_i}$ формируется вектор $\mathbf{e^T_i}=\{\mathbf{0,0},\ldots\mathbf{l},\ldots,\mathbf{0}, \mathbf{S_0},\mathbf{S_1},\ldots,\mathbf{S_{n-k}}\}$. Он равен $\mathbf{S_i}$ на проверочных позициях и равен кратности ошибки на информационных.

6. Если $\mathbf{We_i} \le \mathbf{t}$ то решение найдено, и вектор ошибки имеет вид $\mathbf{e^T_i}=\{\mathbf{0,0},\ldots\mathbf{l},\ldots,\mathbf{0}, \mathbf{S_0},\mathbf{S_1},\ldots,\mathbf{S_{n-k}}\}$.

7. Если $\mathbf{We_i} > \mathbf{t}$, то выбирается элемент информационного множества и переставляется с элементом проверочного путем выполнения элементарных операций над строками. Перестановка столбцов возможна в случае отличия

от нуля элементов одной строки. Если $\mathbf{Ws_i > Ws_{i-1}}$, то такое множество не рассматривается. Если $\mathbf{Ws_i < Ws_{i-1}}$, то это множество принимается для рассмотрения по критерию **minWs**. Формируется новая матрица $\mathbf{H_i}$.

8. Вычисляется синдром $\mathbf{S_{i+1}}$. Если $\mathbf{Ws_{i+1} \le t}$, то вектор ошибки имеет вид $\mathbf{e^T_i = \{0,0,\ldots,0, S_0,S_1,\ldots,S_{n-k}\}}$. Если $\mathbf{Ws_{i+1} > t}$, то происходит возврат к шагу 4 при условиях $\mathbf{S_i = S_{i+1}}$, $\mathbf{H_i = H_{i+1}}$.

Алгоритм позволяет на первой итерации определить место нахождения ошибки: информационное или проверочное множество. Показателем предпочтения при выборе проверочного множества является **We**. Критерием выбора является минимизация этого показателя.

Задача процедуры декодирования состоит в нахождении вектора ошибки. Вероятность нахождения решения за **m** шагов для перестановочного декодирования двоичных кодов оценена в [5]. В случае превышения веса возникнувшей ошибки алгоритм переберет все возможные множества, и не найдет решения (решения для данного кода не существует). Для ограничения числа итераций возможен вариант предопределения их максимального числа. Выбор числа итераций предлагается осуществлять на основе анализа зависимости вероятностного обнаружения ошибки за конечное число шагов с учетом требований к быстродействию алгоритма декодирования.

Достоинство алгоритма состоит в декодировании широкого класса **q** - ичных кодов. Особенностью является декодирование кодов квазициклической структуры – алгеброгеометрических кодов. Алгоритм может быть применен для декодирования кодов выходного каскада.

ЛИТЕРАТУРА

1. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289 - 1290.*
2. *Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова – Гилберта. // Проблемы передачи информации. – 1982. – Т. 18. – С. 3 - 6.*
3. *Кузнецов А.А. Построение кодов по гладким проективным кривым // Сб. научн. тр. НТУ "ХПИ". – Харьков: НТУ "ХПИ". – 2001. – С. 56 - 61.*
4. *Johan P. Hansen; Codes on the Klein quartic, ideals, and decoding (Corresp.) // IEEE Trans. Info. Theory. – Vol IT – 33, November 1987. – P. 923 - 925.*
5. *Кларк Дж., Клейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. – М.: Радио и связь, 1987. – 392 с.*

Поступила 16.01.2002

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

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, зам. нач. НИЛ ХВУ. В 1996 году закончил ХВУ. Область научных интересов - теория аутентификации, алгебраическая теория кодов и их применение в системах передачи данных.*

E - mail : spider@ skynet.kharkov.com

***КУРИШ Вячеслав Викторович**, инженер кафедры ХВУ. Область научных интересов - применение помехоустойчивого кодирования в системах передачи данных.*