УДК 621.391

МЕТОД ПРЕОБРАЗОВАНИЯ СИСТЕМЫ ПРОВЕРОЧНЫХ УРАВНЕНИЙ В ЧАСТОТНОЙ ОБЛАСТИ ДЛЯ ДВОИЧНЫХ КОДОВ ГОППЫ

к.т.н. А.Д. Буханцов, к.т.н. Г.З. Халимов, к.т.н. А.И. Задонский
(представил д.т.н., проф. В.И. Долгов)

Предлагается метод преобразования системы уравнений, позволяющий существенно упростить ее решение, что необходимо для определения спектра кодовых слов кода Гоппы.

В работе [1] описывается метод определения информационных и проверочных частот применительно к двум частным случаям (8,2,5) и (32,17,7) кодов Гоппы с соответствующими многочленами Гоппы $\mathbf{G(x) = x^2 + x + 1}$ и $\mathbf{G(x) = x^3 + x + 1}$. При этом решается система проверочных уравнений вида

$$\begin{cases} \mathbf{c_+ = \sum_{j=0}^{n-1} H^*_{-j} C_j ;} \\ \mathbf{0 = \sum_{j=0}^{n-1} H^*_{-1-j} C_j ;} \\ \vdots \\ \mathbf{0 = \sum_{j=0}^{n-1} H^*_{-(2t-1)-j} C_j ,} \end{cases} \qquad (1)$$

где $\mathbf{C_j}$ - частотные компоненты спектра кода; $\mathbf{H^*_{-j},\ldots,H^*_{-(2t-1)-j}}$ - коэффициенты при переменных многочлена $\mathbf{H^*(x)}$, обратного квадрату многочлена Гоппы $\mathbf{G(x)}$ в поле $\mathbf{GF(2^m)}$; $\mathbf{c_+}$ - символ расширения кода; $\mathbf{n}$ - примитивная длина (нерасширенного) кода при $\mathbf{n = 2^m - 1}$; $\mathbf{t}$ - кратность исправляемых кодом ошибок.

Кроме того, имеются ограничения сопряженности

$$\mathbf{C_j^2 = C_{((2j))}} \ . \qquad (2)$$

Любой спектр, удовлетворяющий этим проверочным уравнениям и ограничениям сопряженности, является спектром кодового слова.

Трудность решения системы (1) заключается в том, что при замене сопряженных компонент $\mathbf{C_j}$ степенями одной из них в соответствии с (2), данная система уравнений становится нелинейной. Ниже предлагается преобразовать систему уравнений к такому виду, чтобы она стала линейной, что существенно упрощает ее решение.

Возведем каждое из уравнений системы (1) последовательно в степени $\mathbf{2},\ \mathbf{2^2,2^3,...,2^{m-1}}$. Получим систему уравнений

$$
\begin{cases}
\mathbf{c_+ = \sum_{j=0}^{n-1} H^{*}_{-j} C_j\ ;} \\
\mathbf{c_+ = \sum_{j=0}^{n-1} H^{*2}_{-j} C_j^2\ ;} \\
\quad \cdots \\
\mathbf{c_+ = \sum_{j=0}^{n-1} H^{*2^{m-1}}_{-j} C_j^{2^{m-1}}\ ;} \\
\mathbf{0 = \sum_{j=0}^{n-1} H^{*}_{-1-j} C_j\ ;} \\
\mathbf{0 = \sum_{j=0}^{n-1} H^{*2}_{-1-j} C_j^2\ ;} \\
\quad \cdots \\
\mathbf{0 = \sum_{j=0}^{n-1} H^{*2^{m-1}}_{-1-j} C_j^{2^{m-1}}\ ;} \\
\quad \vdots \\
\mathbf{0 = \sum_{j=0}^{n-1} H^{*}_{-(2t-1)-j} C_j\ ;} \\
\mathbf{0 = \sum_{j=0}^{n-1} H^{*2}_{-(2t-1)-j} C_j^2\ ;} \\
\quad \cdots \\
\mathbf{0 = \sum_{j=0}^{n-1} H^{*2^{m-1}}_{-(2t-1)-j} C_j^{2^{m-1}}\ .}
\end{cases}
\tag{3}
$$

Согласно [2] данная операция выполнима, поскольку обратные преобразования Фурье полученных уравнений линейно зависимы. При

этом учтено, что в поле Галуа характеристики 2 квадрат суммы элементов поля равен сумме квадратов, а символ расширения $\mathbf{c_+}$ принадлежит полю **GF(2)**. Выражение (3) представляет собой систему нелинейных уравнений. Для того, чтобы система стала линейной, воспользуемся ограничениями сопряженности (2) заменив степени компонент $\mathbf{C}_j$ соответствующими компонентами в первой степени. При этом система (3) преобразуется к виду

$$
\begin{cases}
\mathbf{c_+} = \sum_{j=0}^{n-1} \mathbf{H}^{*}_{-j}\mathbf{C}_j ; \\
\mathbf{c_+} = \sum_{j=0}^{n-1} \mathbf{H}^{*2}_{-j}\mathbf{C}_{((2j))} ; \\
\quad \cdots \\
\mathbf{c_+} = \sum_{j=0}^{n-1} \mathbf{H}^{*2^{m-1}}_{-j}\mathbf{C}_{((2^{m-1}j))} ; \\
\mathbf{0} = \sum_{j=0}^{n-1} \mathbf{H}^{*}_{-1-j}\mathbf{C}_j ; \\
\mathbf{0} = \sum_{j=0}^{n-1} \mathbf{H}^{*2}_{-1-j}\mathbf{C}_{((2j))} ; \\
\quad \cdots \\
\mathbf{0} = \sum_{j=0}^{n-1} \mathbf{H}^{*2^{m-1}}_{-1-j}\mathbf{C}_{((2^{m-1}j))} ; \\
\quad \vdots \\
\mathbf{0} = \sum_{j=0}^{n-1} \mathbf{H}^{*}_{-(2t-1)-j}\mathbf{C}_j ; \\
\mathbf{0} = \sum_{j=0}^{n-1} \mathbf{H}^{*2}_{-(2t-1)-j}\mathbf{C}_{((2j))} ; \\
\quad \cdots \\
\mathbf{0} = \sum_{j=0}^{n-1} \mathbf{H}^{*2^{m-1}}_{-(2t-1)-j}\mathbf{C}_{((2^{m-1}j))} .
\end{cases}
\qquad (4)
$$

Таким образом, получена система линейных уравнений (4) с **n+1** неизвестными, состоящая из **2tm** уравнений. Для решения данной системы можно воспользоваться любым известным методом, например,

методом Гаусса [3], позволяющим привести систему уравнений к так называемому ступенчатому виду. В результате решения получаем не более **2tm** зависимых (проверочных) компонент спектра. Остальные компоненты являются свободными (информационными).

В качестве примера выберем (8,2,5) - двоичный код Гоппы, применив для нахождения его спектра разработанный метод. Код задается многочленом Гоппы $\mathbf{G(x)= x^2 + x + 1.}$ Поскольку многочлен **G(x)** неприводим в поле **GF(8)**, код полностью определяется **t** уравнениями исходной системы (1) с коэффициентами многочлена $\mathbf{H(x) = x^6 + x^5 + x^3 + x^2 + 1}$, а, именно:

$$\begin{cases} c_+ = C_0 + C_1 + C_2 \quad + C_4 + C_5 \quad ; \\ 0 = C_0 + C_1 \quad + C_3 + C_4 \quad + C_6 \, . \end{cases}$$

Возведем каждое из уравнений в степени 2 и 4 и получим

$$\begin{cases} c_+ = C_0 + C_1 + C_2 \quad + C_4 + C_5 \quad ; \\ c_+ = C_0^2 + C_1^2 + C_2^2 \quad + C_4^2 + C_5^2 \quad ; \\ c_+ = C_0^4 + C_1^4 + C_2^4 \quad + C_4^4 + C_5^4 \quad ; \\ 0 = C_0 + C_1 \quad + C_3 + C_4 \quad + C_6 \, ; \\ 0 = C_0^2 + C_1^2 \quad + C_3^2 + C_4^2 \quad + C_6^2 \, ; \\ 0 = C_0^4 + C_1^4 \quad + C_3^4 + C_4^4 \quad + C_6^4 \, . \end{cases}$$

Используя условия сопряженности (2), имеем

$$\begin{cases} c_+ = C_0 + C_1 + C_2 \quad + C_4 + C_5 \quad ; \\ c_+ = C_0 + C_2 + C_4 \quad + C_1 + C_3 \quad ; \\ c_+ = C_0 + C_4 + C_1 \quad + C_2 + C_6 \quad ; \\ 0 = C_0 + C_1 \quad + C_3 + C_4 \quad + C_6 \, ; \\ 0 = C_0 + C_2 \quad + C_6 + C_1 \quad + C_5 \, ; \\ 0 = C_0 + C_4 \quad + C_5 + C_2 \quad + C_3 \, . \end{cases}$$

Представим систему уравнений в виде

$$\begin{cases} c_+ = C_0 + C_1 + C_2 + C_4 + C_5 ; \\ c_+ = C_0 + C_1 + C_2 + C_3 + C_4 ; \\ c_+ = C_0 + C_1 + C_2 + C_4 + C_6 ; \\ 0 = C_0 + C_1 + C_3 + C_4 + C_6 ; \\ 0 = C_0 + C_1 + C_2 + C_5 + C_6 ; \\ 0 = C_0 + C_2 + C_3 + C_4 + C_5 . \end{cases}$$

Легко показать, что данную систему уравнений путем последовательного исключения переменных можно привести к ступенчатому виду

$$\begin{cases} c_+ = C_1 + C_6 ; \\ c_+ = C_1 + C_5 ; \\ 0 = C_1 + C_4 ; \\ c_+ = C_1 + C_3 ; \\ 0 = C_1 + C_2 ; \\ 0 = C_0 . \end{cases}$$

Откуда окончательно имеем:

$$C_0 = 0 ; \; c_+ = C_1 + C_3 ; \; C_1 = C_2 = C_4 ; \; C_3 = C_5 = C_6 .$$

Таким образом, компоненты C_1 и C_3 являются произвольными информационными символами поля **GF(2)**. Символ расширения $c_+ = C_1 + C_3$ является зависимой компонентой, а символ $C_0 = 0$. В результате получили искомый двоичный (8,2,5) - код Гоппы.

ЛИТЕРАТУРА

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – С. 269 - 279.
2. Лидл Р., Нидеррайтер Г. Конечные поля. – М.: Мир, 1988. – 430 с.
3. Боревич З.И. Определители и матрицы. – М.: Наука, 1970. – 200 с.

Поступила в редколлегию 18.12.2000