УДК 519.711/.72

ПРЕОБРАЗОВАНИЯ ГРЕЯ В ПОЛЯХ ГАЛУА ПО МОДУЛЮ НЕПРИВОДИМОГО МНОГОЧЛЕНА

А.Я. Белецкий
Национальный авиационный университет, г. Киев

Вводится новый класс обратимых кодов Грея, основанных на преобразованиях над конечными полями Галуа.

ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

Теория кодирования, криптография и ряд других разделов дискретной математики в значительной мере связаны с мощными и изящными структурами современной алгебры. Многие важные коды основаны на структурах колец многочленов и полей Галуа. Кроме того, эти понятия и методы являются необходимым рабочим инструментом для конструирования кодеров и декодеров в системах приемо-передачи дискретной информации, шифраторов и дешифраторов в криптографических системах и в других приложениях.

В данной статье ставится задача синтеза грееподобных кодов [1] над совокупностью полиномов, состоящей из l в общем случае m-ичных n-разрядных чисел в расширенных полях Галуа $GF(2^k)$, $k \geq 1$, и построения алгебраических преобразований полиномов, подобных преобразованиям чисел составными кодами Грея [2].

ПРОСТЫЕ КОДЫ ГРЕЯ НАД ПОЛЕМ $GF(2^k)$

Классическое прямое преобразование Грея m-ичных n-разрядных чисел $\boldsymbol{x} = \{x_{n-1},\ x_{n-2},\ \ldots, x_1,\ x_0\}$ определяется системой линейных модульных уравнений:

$$\begin{aligned} & y_{n-1} = x_{n-1}\ ; \\ & y_{n-2} = x_{n-1} \overset{m}{\oplus} x_{n-2}\ ; \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & y_0 = x_1 \overset{m}{\oplus} x_0\ , \end{aligned} \qquad (1)$$

в которых $\overset{m}{\oplus}$ – оператор сложения по mod m.

Решая (1) относительно переменных x_i $(i = \overline{0,\ n-1})$, приходим к системе рекуррентных соотношений:

$$\begin{aligned} & x_{n-1} = y_{n-1}\ ; \\ & x_{n-2} = (y_{n-2} - x_{n-1})_m\ ; \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & x_0 = (y_1 - x_1)_m\ , \end{aligned} \qquad (2)$$

где $(a)_m$ – основной оператор модульной арифметики, вычисляющий остаток от деления a на m, т.е. $(a)_m = \mathrm{mod}\ (a,\ m)$.

Перейдем к построению кодов Грея над полями Галуа $GF(2^k)$. Элементами поля являются полиномы

$$\pi(x) = \alpha_{k-1}x^{k-1} + \alpha_{k-2}x^{k-2} + \ldots + \alpha_1 x + \alpha_0$$

с коэффициентами разложения $\alpha_i \in [0,\ 1] = GF(2)$. Все преобразования выполняются по модулю неприводимого многочлена, в качестве которого используем полином

$$\varphi(x) = x^8 + x^4 + x^3 + x + 1\ ,$$

двоичный цифровой эквивалент которого имеет вид

$$\varphi = 100011011\ . \qquad (3)$$

Полином (3) принят в качестве неприводимого в симметричном блочном криптографическом алгоритме Rijndael, введенного в 2000 г. в качестве стандарта США [3].

В полях Галуа $GF(2^k)$ арифметические операции сложения и вычитания двух произвольных полиномов $\pi_1(x)$ и $\pi_2(x)$ сводятся к поразрядному сложению $\oplus$ или вычитанию $\ominus$ по модулю p. Из этого следует, что операции

$$\pi_1(x) \overset{p}{\oplus} \pi_2(x) \ \text{ и } \ \pi_1(x) \overset{p}{\ominus} \pi_2(x) \qquad (4)$$

не подходят для построения преобразований Грея по модулю неприводимого полинома, так как результат поразрядного сложения или вычитания (4) есть многочлен, порядок которого не превосходит порядка полинома, используемого в качестве модуля преобразования.

Выберем в качестве бинарной операции прямого преобразования Грея в полях Галуа операцию умножения, т.е. заменим оператор $\overset{m}{\oplus}$ на оператор $\overset{\varphi}{\otimes}$. Умножение двух полиномов $\pi_1(x)$ и $\pi_2(x)$, порядок которых равен k_1 и k_2 соответственно, приводит в полях Галуа к полиному π порядка

$$k_+ = k_1 + k_2 - 1\ .$$

В том случае, когда k_+ оказывается не меньшим, чем k, возникает необходимость (в преобразованиях Грея) в приведении полинома $\pi(x)$ к остатку по $\mathrm{mod}\ \varphi(x)$. Исходя из вышеизложенных рассуждений, составим структурную схема (рис. 1) алгоритма формирования четырехразрядного прямого левостороннего кода Грея над полем $GF(2^8)$ по модулю неприводимого полинома (3).

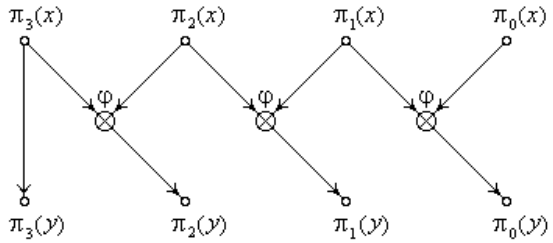

Рисунок 1

Систему уравнений, отвечающих преобразованиям в схеме на рис. 1, представим в виде:

$$\begin{aligned} \pi_3(y) &= \pi_3(x)\ ; \\ \pi_2(y) &= \pi_3(x) \overset{\varphi}{\otimes} \pi_2(x)\ ; \\ \pi_1(y) &= \pi_2(x) \overset{\varphi}{\otimes} \pi_1(x)\ ; \\ \pi_0(y) &= \pi_1(x) \overset{\varphi}{\otimes} \pi_0(x)\ . \end{aligned} \qquad (5)$$

Выберем для примера такие числовые значения полиномов (табл. 1).

Таблица 1

$\pi_3(x)$	$\pi_2(x)$	$\pi_1(x)$	$\pi_0(x)$
1001101	11011	111001	101010

Вычислим произведение $\pi_2'(x)$ полиномов $\pi_3(x)$ и $\pi_2(x)$. Имеем

$$\begin{array}{rcccccccccc} \pi_3(x) = & & & & & \times & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ \pi_2(x) = & & & & & & & & 1 & 1 & 0 & 1 & 1 \\ \hline & & & & & & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ & & & & \oplus & & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ & & & 1 & 0 & 0 & 1 & 1 & 0 & 1 & & & \\ & 1 & 0 & 0 & 1 & 1 & 0 & 1 & & & & & \\ \hline \pi_2'(x) = & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1. \end{array}$$

Промежуточный полином $\pi_2'(x)$ получен как поразрядная сумма по mod 2 результата произведения полиномов $\pi_3(x)$ и $\pi_2(x)$. Порядок многочлена $\pi_2'(x)$ равен 10 и превосходит порядок, равный восьми, неприводимого полинома φ, заданного соотношением (3).

Определим остаток $\pi_2(y)$ полинома $\pi_2'(x)$ по модулю φ. Поскольку преобразования выполняются в двоичном пространстве, т.е. над коэффициентами в поле $GF(2)$, то операция поразрядного вычитания по mod 2 совпадает с операцией сложения. Полином $\pi_2(y)$ находим по обычным правилам деления двоичных кодовых комбинаций. При этом следует помнить, что операцию вычитания, возникающую при делении,

следует заменить на операцию поразрядного сложения по mod 2. Получим

$$\pi_2'(x) = 1\,1\,0\,0\,1\,1\,0\,1\,1\,1\,1 \;\big|\; 1\,0\,0\,0\,1\,1\,0\,1\,1 = \varphi$$
$$\oplus\; 1\,0\,0\,0\,1\,1\,0\,1\,1 \qquad\qquad 1\,1\,0$$
$$1\,0\,0\,0\,0\,0\,0\,0\,1$$
$$\oplus\; 1\,0\,0\,0\,1\,1\,0\,1\,1$$
$$1\,1\,0\,1\,0\,1$$
$$\oplus\; 0\,0\,0\,0\,0\,0$$
$$1\,1\,0\,1\,0\,1 = \pi_2(y)$$

Таким образом, остаток от деления полинома $\pi_2'(x)$ на модуль φ составляет величину

$$\pi_2(y) = 110101 \ .$$

Аналогичным образом определяем оставшиеся полиномы $\pi_i(y)$, полная совокупность которых представлена в табл. 2.

Таблица 2

$\pi_3(y)$	$\pi_2(y)$	$\pi_1(y)$	$\pi_0(y)$
1001101	110101	100101	11000000

Решая формально системы уравнений (5) относительно переменных $\pi_i(x)$, приходим к обратному преобразованию Грея по модулю неприводимого полинома φ. Имеем

$$\begin{aligned}
&\pi_3(x) = \pi_3(y)\ ;\\
&\pi_2(x) = \pi_2(y) \overset{\varphi}{\otimes} \pi_3^{-1}(x)\ ;\\
&\pi_1(x) = \pi_1(y) \overset{\varphi}{\otimes} \pi_2^{-1}(x)\ ;\\
&\pi_0(x) = \pi_0(y) \overset{\varphi}{\otimes} \pi_1^{-1}(x)\ .
\end{aligned} \qquad (6)$$

Полиномы $\pi_i^{-1}(x)$ являются мультипликативно обратными к полиномам $\pi_i(x)$ и сведены в табл. 3.

Таблица 3

$\pi_3^{-1}(x)$	$\pi_2^{-1}(x)$	$\pi_1^{-1}(x)$
100101	11001100	110101

Воспользовавшись системой (6), составим схему обратного преобразования Грея по модулю неприводимого полинома (рис. 2).

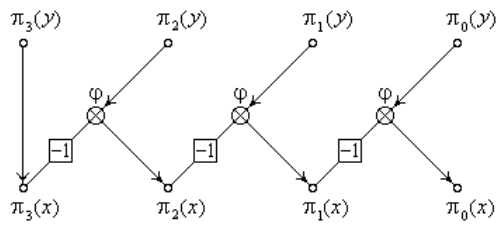

Рисунок 2

На рис. 2 элемент –1 вычисляет мультипликативное обратное входному полиному над заданным неприводимым полиномом φ.

Проведем, для примера, вычисление в системе (6) полинома $\pi_2(x)$. С этой целью на первом этапе следует рассчитать произведение двоичных полиномов $\pi_2(y)$ из табл. 2 и $\pi_3^{-1}(x)$ из табл. 3. Имеем

$$
\begin{array}{rl}
\pi_2(y) = & \quad 1\ 1\ 0\ 1\ 0\ 1 \\
\pi_3^{-1}(x) = & \times \quad \underline{1\ 0\ 0\ 1\ 0\ 1} \\
 & \quad\ 1\ 1\ 0\ 1\ 0\ 1 \\
\oplus & \quad 1\ 1\ 0\ 1\ 0\ 1 \\
 & \underline{1\ 1\ 0\ 1\ 0\ 1} \\
 & 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1 = (\pi_2(y)\cdot\pi_3^{-1}(x))_2 \ .
\end{array}
$$

На втором этапе преобразований полученное произведение необходимо привести к остатку по mod φ. Получим

$$
\begin{array}{l}
\oplus\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1 \ \big|\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1 = \varphi \\
\quad\ \underline{1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1}\ \big\downarrow\ \big|\ \underline{1\ 1} \\
\quad\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0 \\
\oplus\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\big\downarrow \\
\quad\ \underline{\qquad\qquad 1\ 1\ 0\ 1\ 1} = \pi_2(x)
\end{array}
$$

Как следует из полученных соотношений, обратное преобразование возвращает полином $\pi_2(x)$. Аналогичным образом можно проверить корректность восстановления полиномов $\pi_1(x)$ и $\pi_0(x)$.

СОСТАВНЫЕ КОДЫ ГРЕЯ НАД ПОЛЕМ $GF(2^k)$

Системам линейных модульных уравнений (1) и (2) можно придать матричные формы

$$\boldsymbol{y} = \boldsymbol{x}\ \ \boldsymbol{M}\ ;\ \boldsymbol{x} = \boldsymbol{y}\ \ \bar{\boldsymbol{M}}\ , \qquad (7)$$

в которых $\boldsymbol{x}$ и $\boldsymbol{y}$ – входной и выходной операнды, а $\boldsymbol{M}$ и $\bar{\boldsymbol{M}}$ – матрицы прямого и обратного преобразования Грея левостороннего. Здесь термин *левосторонний* означает направление преобразования, развивающееся (согласно рис. 1 и 2) слева направо.

Для $n = 4$ канонические, т.е. независящие от основания системы счисления (модуля) m, матрицы преобразования $\boldsymbol{M}$ и $\bar{\boldsymbol{M}}$, которым для удобства мы придадим цифровые обозначения 2 и 3 соответственно, имеют вид:

$$
2 := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \qquad 3 := \begin{bmatrix} 1 & -1 & 1 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \qquad (8)
$$

К матрице 3 в (8) легко приходим, освободившись в правых частях уравнений системы (2) от переменных x_i.

Если в обычных преобразованиях Грея вычисления (7) выполняются по классическим правилам матричного исчисления, то применительно к преобразованиям Грея над полями Галуа не следует забывать такие особенности. Во-первых, в качестве компонент входного и выходного операндов в полях Галуа $GF(2^k)$ выступают n-компонентные векторы $\boldsymbol{\pi}(x) = \{\pi_{n-1}(x),\ \ldots,\ \pi_0(x)\}$ и $\boldsymbol{\pi}(y) = \{\pi_{n-1}(y),\ \ldots,\ \pi_0(y)\}$, в которых $\pi_i(\circ)$ – полиномы не более чем $(k-1)$-го порядка с коэффициентами над $GF(2)$. Во-вторых, операция сложения $\overset{m}{\oplus}$ при вычислении кодов Грея в полях Галуа заменяется операцией умножения $\overset{\varphi}{\otimes}$. И, наконец, в третьих, элемент -1 в матрицах преобразования для полей Галуа означает, что при вычислениях вместо элемента $\pi_i(\circ)$ необходимо использовать $\pi_i^{-1}(\circ)$, мультипликативно обратный к $\pi_i(\circ)$ по модулю неприводимого многочлена $\varphi(x)$. В частности, согласно второму преобразованию в (7), в котором $\bar{M}$ замещается матрицей 3 из (8), имеем

$$\begin{aligned}
&\pi_3(x) = \pi_3(y)\ ;\\
&\pi_2(x) = (\pi_3^{-1}(y)\cdot\pi_2(y))_\varphi\ ;\\
&\pi_1(x) = (\pi_3(y)\cdot\pi_2^{-1}(y)\cdot\pi_1(y))_\varphi\ ;\\
&\pi_0(x) = (\pi_3^{-1}(y)\cdot\pi_2(y)\cdot\pi_1^{-1}(y)\cdot\pi_0(y))_\varphi\ .
\end{aligned} \qquad (9)$$

К соотношениям (9) легко приходим из системы уравнений (6), освободившись в правых частях последних от полиномов $\pi_i^{-1}(x)$.

В монографии [1] введен так называемый класс *правосторонних* кодов Грея, матрицы преобразования которых образуются транспонированием матриц преобразования левосторонних кодов Грея. Для прямого и обратного правостороннего преобразований Грея (придадим им цифровые обозначения 4 и 5 соответственно) из соотношений (8) получим

$$4 := \begin{bmatrix} 1 & 0 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 1 \end{bmatrix};\qquad 5 : \begin{bmatrix} 1 & 0 & 0 & 0\\ -1 & 1 & 0 & 0\\ 1 & -1 & 1 & 0\\ -1 & 1 & -1 & 1 \end{bmatrix}. \qquad (10)$$

Дополним систему матриц преобразований Грея (8) и (10) матрицей эквивалентных преобразований e, являющейся единичной матрицей n-го порядка, и матрицей инверсной перестановки с цифровым обозначением 1. Для $n = 4$

$$e := \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix};\qquad 1 := \begin{bmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Легко проверить, что $(2\cdot 3)_m = (3\cdot 2)_m = e$, а также $(4\cdot 5)_m = (5\cdot 4)_m = e$, как и должно быть по определению.

К *составным кодам Грея* будем относить коды, образованные различными комбинациями лево- и правостороннего преобразований Грея (как прямого, так и обратного), дополненные в отдельных случаях операцией инверсной перестановки. Таким образом, составной код Грея (СКГ) есть некоторая последовательность простых операторов Грея. Например, СКГ $G = 212$ означает, что некоторый входной вектор $\boldsymbol{x}$ сначала подвергается прямому преобразованию Грея левостороннему, затем вектор, сформированный на первом этапе преобразования, подвергается инверсной перестановке, после чего снова выполняется прямое левостороннее преобразование Грея.

На простом примере проиллюстрируем методику вычисления прямых и обратных составных кодов Грея над полем Галуа $GF(2^k)$ по модулю неприводимого многочлена φ, полагая $n = 4$ и $G = 252$. СКГ 252 отвечает матрица прямого преобразования

$$252 \Rightarrow \boldsymbol{M} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix}, \qquad (11)$$

к которой приходим обычными приемами матричных произведений, при этом каждый элемент вычислений должен быть приведен к остатку по mod 2. Матрице прямого преобразования (11) соответствует система линейных уравнений:

$$\begin{aligned} \pi_3(y) &= \pi_0^{-1}(x)\ ; \\ \pi_2(y) &= \pi_3(x)\ ; \\ \pi_1(y) &= (\pi_3(x) \cdot \pi_2(x))_\varphi\ ; \\ \pi_0(y) &= (\pi_2(x) \cdot \pi_1(x))_\varphi\ , \end{aligned}$$

решая которую относительно входных полиномов $\pi_i(x)$, получим систему обратных преобразований

$$\begin{aligned} \pi_3(x) &= \pi_2(y)\ ; \\ \pi_2(x) &= (\pi_2^{-1}(y) \cdot \pi_1(y))_\varphi\ ; \\ \pi_1(x) &= (\pi_2(y) \cdot \pi_1^{-1}(y) \cdot \pi_0(y))_\varphi\ ; \\ \pi_0(x) &= \pi_3^{-1}(y)\ . \end{aligned} \qquad (12)$$

Матрицу обратного преобразования, отвечающую СКГ $\bar{G} = 343$, легко определим или из системы (12), или на основании матричного произведения $(343)_2$. В обоих случаях приходим к одинаковому результату

$$343 \Rightarrow \bar{\boldsymbol{M}} = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad (13)$$

Матричные формы СКГ дают возможность составить структурные схемы алгоритмов параллельных вычислений кодов Грея над $GF(2^k)$ по mod φ. На рис. 3 приведена в качестве примера структурная форма алгоритма, отвечающая матрице обратного преобразования (13).

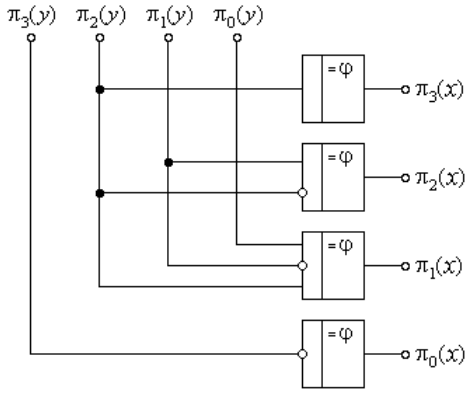

Рисунок 3

Кружочки на входе операторов, осуществляющих вычисление произведения полиномов $\pi_i(y)$ по mod φ, означают формирование мультипликативно обратной соответствующей переменной.

ЗАКЛЮЧЕНИЕ

В системах прямого (5) и обратного (6) преобразований Грея, в равной степени как и в соответствующих структурных схемах на рис. 1 и 2, в явном виде отсутствует информация относительно порядков преобразуемых полиномов и неприводимого многочлена. Отмеченное обстоятельство означает, что полученные результаты легко обобщаются на произвольные значения порядка k неприводимого многочлена φ и величины основания p поля Галуа $GF(p^k)$, где p – простое число. Однако не следует забывать при этом, что порядок преобразуемых полиномов $\pi(x)$ не должен превышать величину, на единицу меньшую порядка неприводимого многочлена.

SUMMARY

We introduce the new class of reverse Grey's codes which are based on the finite Galya's fields transformations.

СПИСОК ЛИТЕРАТУРЫ

1. Gray F. Pulse code communication. – Pat USA, № 2632058, 1953.
2. Белецкий А. Я. Комбинаторика кодов Грея. – Киев: КВІЦ, 2003. – 506 с.
3. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard". Nov.2001. Available at http://csrc.nist.gov/publications/fips/

А.Я. Белецкий, проф.
Национальный авиационный университет, г. Киев

Поступила в редакцию 11 апреля 2007 г.