УДК 681.325.3:621.391.25:621.394.14

Кубицкий В.И.

ОРГАНИЗАЦИЯ МУЛЬТИПЛИКАТИВНОГО ОБРАЩЕНИЯ ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ

ГосНИИ «Аэронавигация» (Россия, Москва)

Рассмотрена организация мультипликативного обращения элементов конечного поля $GF(2^m)$. Предложен алгоритм вычисления их инверсных значений реализация которого возможна на комбинационных схемах

Во многих областях науки и техники используются вычисления в конечных полях. Наряду с другими операциями интерес представляет инвертирование элементов конечного поля. Распространение получила реализация инвертирования на регистрах сдвига [1 - 4]. Вычисления обратного элемента производятся также на комбинационных схемах [5], однако такие схемы не являются однородными и универсальными.

В [6] предложен метод, дающий возможность выполнять операцию инвертирования элементов конечных полей $GF(2^m)$ на универсальных комбинационных схемах. Приведём алгоритм инвертирования элементов конечных полей, основанный на этом методе.

Инвертирование элементов конечного поля GF(2^m)

Пусть

$a(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1 x + a_0$ – многочлен, представляющий элемент поля $GF(2^m)$, инверсное значение которого необходимо найти. Инверсией этого многочлена будет многочлен

$$b(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_1 x + b_0$$

такой, что $\left\langle a(x)\cdot b(x)\right|_{p(x)} = 1$ или

$$a(x)\cdot b(x) = p(x)\cdot q(x) + c(x), \qquad (1)$$

где $p(x) = p_m x^m + p_{m-1}x^{m-1} + \ldots + p_1 x + p_0$;

$q(x) = q_{m-2}x^{m-2} + q_{m-3}x^{m-3} + \ldots + q_1 x + q_0$;

$c(x) = c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \ldots + c_1 x + c_0$

(здесь $c_{m-1} = c_{m-2} = \ldots = c_1 = 0$, $c_0 = 1$).

Решение $b(x)$ может быть найдено по алгоритму Евклида. Но этот процесс сложно реализовать аппаратно, так как он имеет большое число промежуточных результатов, которые должны запоминаться.

Из выражения (1) видно, что при инвертировании используется операция умножения элементов конечного поля. Поэтому для определения процедур инвертирования используем положения, разработанные для операции умножения элементов поля [7].

Учитывая выражения для умножения многочленов над полем $GF(2)$ [8] и умножения элементов конечного поля $GF(2^m)$ [7], запишем:

$$A_1 \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = P_1 \otimes \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{m-3} \\ q_{m-2} \end{bmatrix} \oplus \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix}, \quad (2)$$

$$A_2 \otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = P_2 \otimes \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{m-3} \\ q_{m-2} \end{bmatrix}, \qquad (3)$$

где $A_1 = \begin{bmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ \vdots & \vdots & \ddots & & \\ a_{m-2} & a_{m-3} & \ldots & a_0 & \\ a_{m-1} & a_{m-2} & \ldots & a_1 & a_0 \end{bmatrix}$,

$$A_2 = \begin{bmatrix} a_{m-1} & a_{m-2} & \dots & a_2 & a_1 \\ & a_{m-1} & \dots & a_3 & a_2 \\ & & \ddots & \vdots & \vdots \\ & & & a_{m-1} & a_{m-2} \\ & & & & a_{m-1} \end{bmatrix},$$

$$P_1 = \begin{bmatrix} p_0 & & & \\ p_1 & p_0 & & \\ \vdots & \vdots & \ddots & \\ p_{m-2} & p_{m-3} & \cdots p_1 & p_0 \\ p_{m-1} & p_{m-2} & \cdots p_2 & p_1 \end{bmatrix},$$

$$P_2 = \begin{bmatrix} p_m & p_{m-1} & p_{m-2} & \cdots & p_3 & p_2 \\ & p_m & p_{m-1} & \cdots & p_4 & p_3 \\ & & \ddots & \dots & \vdots & \vdots \\ & & & & p_m & p_{m-1} \\ & & & & & p_m \end{bmatrix}.$$

Здесь матрица A_1 является квадратной матрицей порядка m; матрицы A_2 и P_2 – квадратные матицы порядка $(m-1)$; матрица P_1 – $(m, m-1)$ – матрица.

Найдем решения линейных уравнений, представленных выражениями (2) и (3). Неизвестными являются величины b_i и q_i, из которых необходимо определить b_i.

Умножим слева правую и левую часть выражения (3) на матрицу P_2^{-1}, обратную матрице P_2. Отметим, что матрица P_2^{-1} существует, так как при $p_m \neq 0 = 1$ определитель $\left|P_2\right| = p_m \cdot p_m \cdot \ldots \cdot p_m = 1 \neq 0$ [9]. Получим:

$$P_2^{-1} \otimes A_2 \otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = P_2^{-1} \otimes P_2 \otimes \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{m-3} \\ q_{m-2} \end{bmatrix} =$$

$$= E \otimes \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{m-3} \\ q_{m-2} \end{bmatrix} = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{m-3} \\ q_{m-2} \end{bmatrix}, \qquad (4)$$

где E – единичная квадратная матица порядка $(m-1)$.

Подставим (4) в (2):

$$A_1 \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} =$$

$$= P_1 \otimes P_2^{-1} \otimes A_2 \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} \oplus \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix} =$$

$$= P_1 \otimes P_2^{-1} \otimes A_2^* \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} \oplus \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix},$$

где

$$A_2^* = \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \dots & a_2 & a_1 \\ & 0 & a_{m-1} & \dots & a_3 & a_2 \\ & & \ddots & \vdots & \vdots & \\ & & & 0 & a_{m-1} & a_{m-2} \\ & & & & 0 & a_{m-1} \end{bmatrix}.$$

Тогда

$$(A_1 \oplus P_1 \otimes P_2^{-1} \otimes A_2^*) \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix} =$$

$$= A \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix}. \qquad (5)$$

Определим матрицу $A = (A_1 \oplus P_1 \otimes P_2^{-1} \otimes A_2^*)$. Для этого произведём некоторые вычисления.

Применяя способ Гаусса [9], находим обратную матрицу P_2^{-1}:

$$P_2^{-1} = \begin{bmatrix} \overline{p}_{11} & \overline{p}_{12} & \dots & \overline{p}_{1,\,m-2} & \overline{p}_{1,\,m-1} \\ & \overline{p}_{22} & \dots & \overline{p}_{2,\,m-2} & \overline{p}_{2,\,m-1} \\ & & \ddots\ \dots & \vdots & \vdots \\ & & & \overline{p}_{m-2,\,m-2} & \overline{p}_{m-2,\,m-1} \\ & & & & \overline{p}_{m-1,\,m-1} \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & \overline{p}_{m-1} & \overline{p}_{m-2} & \overline{p}_{m-3} & \dots & \overline{p}_3 & \overline{p}_2 \\ & 1 & \overline{p}_{m-1} & \overline{p}_{m-2} & \dots & \overline{p}_4 & \overline{p}_3 \\ & & \ddots & & \dots & \vdots & \vdots \\ & & & & & 1 & \overline{p}_{m-1} \\ & & & & & & 1 \end{bmatrix}.$$

где

$$\overline{p}_{11} = \overline{p}_{22} = \dots = \overline{p}_{m-2,\,m-2} = \overline{p}_{m-1,\,m-1} = p_m^{-1} = 1;$$

$$\overline{p}_{m-1} = \overline{p}_{12} = \overline{p}_{23} = \dots = \overline{p}_{m-2,\,m-1} = p_{m-1};$$

$$\overline{p}_{m-2} = \overline{p}_{13} = \overline{p}_{24} = \dots = \overline{p}_{m-4,\,m-2} = \overline{p}_{m-3,\,m-1} = p_{m-2} \oplus p_{m-1} \otimes \overline{p}_{m-1};$$

$$\overline{p}_{m-3} = \overline{p}_{14} = \overline{p}_{25} = \dots = \overline{p}_{m-5,\,m-2} = \overline{p}_{m-4,\,m-1} = p_{m-3} \oplus p_{m-2} \otimes \overline{p}_{m-1} \oplus p_{m-1} \otimes \overline{p}_{m-2};$$

$$\overline{p}_{m-4} = \overline{p}_{15} = \dots = \overline{p}_{m-5,\,m-1} = p_{m-4} \oplus p_{m-3} \otimes \otimes \overline{p}_{m-1} \oplus p_{m-2} \otimes \overline{p}_{m-2} \oplus p_{m-1} \otimes \overline{p}_{m-3};$$

$$\vdots$$

$$\overline{p}_4 = \overline{p}_{1,\,m-3} = \overline{p}_{2,\,m-2} = \overline{p}_{3,\,m-1} = p_4 \oplus p_5 \otimes \overline{p}_{m-1} \oplus p_6 \otimes \overline{p}_{m-2} \oplus \oplus p_7 \otimes \overline{p}_{m-3} \oplus \dots \oplus p_{m-1} \otimes \overline{p}_5;$$

$$\overline{p}_3 = \overline{p}_{1,\,m-2} = \overline{p}_{2,\,m-1} = p_3 \oplus p_4 \otimes \overline{p}_{m-1} \oplus p_5 \otimes \overline{p}_{m-2} \oplus \dots \oplus \oplus p_{m-2} \otimes \overline{p}_5 \oplus p_{m-1} \otimes \overline{p}_4;$$

$$\overline{p}_2 = \overline{p}_{1,\,m-1} = p_2 \oplus p_3 \otimes \overline{p}_{m-1} \oplus p_4 \otimes \overline{p}_{m-2} \oplus \dots \oplus \oplus p_{m-2} \otimes \overline{p}_4 \oplus p_{m-1} \otimes \overline{p}_3.$$

Умножая матрицы P_1 и P_2^{-1}, получим:

$$P = \begin{bmatrix} P_{11} & P_{12} & \dots P_{1,\,m-2} & P_{1,\,m-1} \\ P_{21} & P_{22} & \dots P_{2,\,m-2} & P_{2,\,m-1} \\ \vdots & \vdots & \dots \vdots & \vdots \\ P_{m-1,\,1} & P_{m-1,\,2} & \dots P_{m-1,\,m-2} & P_{m-1,\,m-1} \\ P_{m1} & P_{m2} & \dots P_{m,\,m-2} & P_{m,\,m-1} \end{bmatrix},$$

где для столбца 1:

$$P_{11} = p_0, \quad P_{21} = p_1, \quad P_{31} = p_2, \dots,$$

$$P_{m-1,\,1} = p_{m-2}, \quad P_{m1} = p_{m-1};$$

для столбца 2: $P_{12} = p_0 \otimes \overline{p}_{m-1}$,

$$P_{22} = p_1 \otimes \overline{p}_{m-1} \oplus p_0 = p_1 \otimes \overline{p}_{m-1} \oplus P_{11},$$

$$P_{32} = p_2 \otimes \overline{p}_{m-1} \oplus p_1 = p_2 \otimes \overline{p}_{m-1} \oplus P_{21}, \dots,$$

$$P_{m-1,\,2} = p_{m-2} \otimes \overline{p}_{m-1} \oplus p_{m-3} = p_{m-2} \otimes \overline{p}_{m-1} \oplus P_{m-2,\,1},$$

$$P_{m2} = p_{m-1} \otimes \overline{p}_{m-1} \oplus p_{m-2} = p_{m-1} \otimes \overline{p}_{m-1} \oplus P_{m-1,\,1};$$

для столбца 3: $P_{13} = p_0 \otimes \overline{p}_{m-2}$,

$$P_{23} = p_1 \otimes \overline{p}_{m-2} \oplus p_0 \otimes \overline{p}_{m-1} = p_1 \otimes \overline{p}_{m-2} \oplus P_{12},$$

$$P_{33} = p_2 \otimes \overline{p}_{m-2} \oplus p_1 \otimes \overline{p}_{m-1} \oplus p_0 = p_2 \otimes \overline{p}_{m-2} \oplus P_{22}, \dots,$$

$$P_{m-1,\,3} = p_{m-2} \otimes \overline{p}_{m-2} \oplus p_{m-3} \otimes \overline{p}_{m-1} \oplus \oplus p_{m-4} = p_{m-2} \otimes \overline{p}_{m-2} \oplus P_{m-2,\,2},$$

$$P_{m3} = p_{m-1} \otimes \overline{p}_{m-2} \oplus p_{m-2} \otimes \overline{p}_{m-1} \oplus p_{m-3} = p_{m-1} \otimes \overline{p}_{m-2} \oplus P_{m-1,\,2};$$

$$\vdots$$

для столбца $(m-2)$:

$$P_{1,m-2} = p_0 \otimes \overline{p}_3,$$

$$P_{2,m-2} = p_1 \otimes \overline{p}_3 \oplus p_0 \otimes \overline{p}_4 = \\ = p_1 \otimes \overline{p}_3 \oplus P_{1,m-3}$$

$$P_{3,m-2} = p_2 \otimes \overline{p}_3 \oplus p_1 \otimes \overline{p}_4 \oplus p_0 \otimes \overline{p}_5 = \\ = p_2 \otimes \overline{p}_3 \oplus P_{2,m-3}, \ldots,$$

$$P_{m-2,m-2} = p_{m-3} \otimes \overline{p}_3 \oplus p_{m-4} \otimes \overline{p}_4 \oplus \ldots \oplus \\ \oplus p_1 \otimes \overline{p}_{m-1} \oplus p_0 = p_{m-3} \otimes \overline{p}_3 \oplus P_{m-3,m-3},$$

$$P_{m-1,m-2} = p_{m-2} \otimes \overline{p}_3 \oplus p_{m-3} \otimes \overline{p}_4 \oplus \ldots \oplus \\ \oplus p_2 \otimes \overline{p}_{m-1} \oplus p_1 = p_{m-2} \otimes \overline{p}_3 \oplus P_{m-2,m-3},$$

$$P_{m,m-2} = p_{m-1} \otimes \overline{p}_3 \oplus p_{m-2} \otimes \overline{p}_4 \oplus \ldots \oplus \\ \oplus p_3 \otimes \overline{p}_{m-1} \oplus p_2 = p_{m-1} \otimes \overline{p}_3 \oplus P_{m-1,m-3};$$

для столбца $(m-1)$:

$$P_{1,m-1} = p_0 \otimes \overline{p}_2,$$

$$P_{2,m-1} = p_1 \otimes \overline{p}_2 \oplus p_0 \otimes \overline{p}_3 = \\ = p_1 \otimes \overline{p}_2 \oplus P_{1,m-2},$$

$$P_{3,m-1} = p_2 \otimes \overline{p}_2 \oplus p_1 \otimes \overline{p}_3 \oplus p_0 \otimes \overline{p}_4 = \\ = p_2 \otimes \overline{p}_2 \oplus P_{2,m-2}, \ldots,$$

$$P_{m-2,m-1} = p_{m-3} \otimes \overline{p}_2 \oplus p_{m-4} \otimes \overline{p}_3 \oplus \ldots \oplus \\ \oplus p_0 \otimes \overline{p}_{m-1} = p_{m-3} \otimes \overline{p}_2 \oplus P_{m-3,m-2},$$

$$P_{m-1,m-1} = p_{m-2} \otimes \overline{p}_2 \oplus p_{m-3} \otimes \overline{p}_3 \oplus \ldots \oplus \\ \oplus p_1 \otimes \overline{p}_{m-1} \oplus p_0 = p_{m-2} \otimes \overline{p}_2 \oplus P_{m-2,m-2},$$

$$P_{m,m-1} = p_{m-1} \otimes \overline{p}_2 \oplus p_{m-2} \otimes \overline{p}_3 \oplus \ldots \oplus \\ \oplus p_2 \otimes \overline{p}_{m-1} \oplus p_1 = p_{m-1} \otimes \overline{p}_2 \oplus P_{m-1,m-2}.$$

Матрица $P = P_1 \cdot P_2^{-1}$ является *операционной матрицей* конечного поля, а коэффициенты P_{kl} этой матрицы - *операционными коэффициентами* конечного поля. Следует отметить, что P_{kl} $\left(k = i+1,\ l = j+1,\ i = \overline{1,m},\ j = \overline{1,m-1}\right)$ равны коэффициентам $p_i^{(j)} = \sum_{i=1}^{j} p_{m-1}\, p_i^{(j-1)} + p_{i-j}$ (при $j = 0: p_i^{(0)} = p_i$; при $i < j: p_{i-j} = 0$) [10], вычисление которых приведено в [11].

Так как для многих значений m существуют неприводимые над полем $GF(2)$ примитивные многочлены $p(x) = p_m x^m + h(x)$, вес которых равен 3 и $\deg h(x) = k = 1$, то, с учётом того, что $p_0 = p_1 = 1$ и $p_2 = p_3 = \ldots = p_{m-1} = 0$, получим следующую операционную матрицу конечного поля:

$$P = P_1 \otimes P_2^{-1} = \begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ 0 & 1 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & \ldots 1 & 1 \\ 0 & 0 & \ldots 0 & 1 \end{bmatrix} \otimes$$

$$\otimes \begin{bmatrix} 1 & 0 & 0 & 0 & \ldots & 0 & 0 \\ & 1 & 0 & 0 & \ldots & 0 & 0 \\ & & 1 & 0 & \ldots & 0 & 0 \\ & & & \ddots & \ldots & \vdots & \vdots \\ & & & & & 1 & 0 \\ & & & & & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ 0 & 1 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & \ldots 1 & 1 \\ 0 & 0 & \ldots 0 & 1 \end{bmatrix}.$$

Для этого случая операционные коэффициенты конечного поля вычислять не требуется.

Умножим матрицы P и A_2^*. Получим:

$$\widetilde{A}_2^* = \begin{bmatrix} \widetilde{A}_{11} & \widetilde{A}_{12} & \ldots & \widetilde{A}_{1,m-1} & \widetilde{A}_{1m} \\ \widetilde{A}_{21} & \widetilde{A}_{22} & \ldots & \widetilde{A}_{2,m-1} & \widetilde{A}_{2m} \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ \widetilde{A}_{m-1,1} & \widetilde{A}_{m-1,2} & \ldots & \widetilde{A}_{m-1,m-1} & \widetilde{A}_{m-1,m} \\ \widetilde{A}_{m1} & \widetilde{A}_{m2} & \ldots & \widetilde{A}_{m,m-1} & \widetilde{A}_{mm} \end{bmatrix},$$

где для столбца 1:

$$\widetilde{A}_{11} = \widetilde{A}_{21} = \widetilde{A}_{31} = \ldots = \widetilde{A}_{m-1,1} = \widetilde{A}_{m1} = 0;$$

для столбца 2: $\widetilde{A}_{12} = P_{11} \otimes a_{m-1}$,

$$\widetilde{A}_{22} = P_{21} \otimes a_{m-1}, \quad \widetilde{A}_{32} = P_{31} \otimes a_{m-1}, \ldots,$$

$$\widetilde{A}_{m-1,2} = P_{m-1,1} \otimes a_{m-1}, \quad \widetilde{A}_{m2} = P_{m1} \otimes a_{m-1};$$

для столбца 3:

$$\widetilde{A}_{13} = P_{11} \otimes a_{m-2} \oplus P_{12} \otimes a_{m-1},$$

$$\widetilde{A}_{23} = P_{21} \otimes a_{m-2} \oplus P_{22} \otimes a_{m-1},$$

$$\widetilde{A}_{33} = P_{31} \otimes a_{m-2} \oplus P_{32} \otimes a_{m-1}, \ldots,$$

$$\widetilde{A}_{m-1,3} = P_{m-1,1} \otimes a_{m-2} \oplus P_{m-1,2} \otimes a_{m-1},$$

$$\widetilde{A}_{m3} P_{m1} \otimes a_{m-2} \oplus P_{m2} \otimes a_{m-1};$$

$$\vdots$$

для столбца $(m-1)$:

$$\widetilde{A}_{1,m-1} = P_{11} \otimes a_2 \oplus P_{12} \otimes a_3 \oplus \ldots \oplus \oplus P_{1,m-3} \otimes a_{m-2} \oplus P_{1,m-2} \otimes a_{m-1},$$

$$\widetilde{A}_{2,m-1} = P_{21} \otimes a_2 \oplus P_{22} \otimes a_3 \oplus \ldots \oplus \oplus P_{2,m-3} \otimes a_{m-2} \oplus P_{2,m-2} \otimes a_{m-1},$$

$$\widetilde{A}_{3,m-1} = P_{31} \otimes a_2 \oplus P_{32} \otimes a_3 \oplus \ldots \oplus \oplus P_{3,m-3} \otimes a_{m-2} \oplus P_{3,m-2} \otimes a_{m-1},$$

$$\ldots,$$

$$\widetilde{A}_{m-1,m-1} = P_{m-1,1} \otimes a_2 \oplus P_{m-1,2} \otimes a_3 \oplus \ldots \oplus \oplus P_{m-1,m-3} \otimes a_{m-2} \oplus P_{m-1,m-2} \otimes a_{m-1},$$

$$\widetilde{A}_{m,m-1} = P_{m1} \otimes a_2 \oplus P_{m2} \otimes a_3 \oplus \ldots \oplus \oplus P_{m,m-3} \otimes a_{m-2} \oplus P_{m,m-2} \otimes a_{m-1};$$

для столбца m:

$$\widetilde{A}_{1m} = P_{11} \otimes a_1 \oplus P_{12} \otimes a_2 \oplus \ldots \oplus \oplus P_{1,m-2} \otimes a_{m-2} \oplus P_{1,m-1} \otimes a_{m-1},$$

$$\widetilde{A}_{2m} = P_{21} \otimes a_1 \oplus P_{22} \otimes a_2 \oplus \ldots \oplus \oplus P_{2,m-2} \otimes a_{m-2} \oplus P_{2,m-1} \otimes a_{m-1},$$

$$\widetilde{A}_{3m} = P_{31} \otimes a_1 \oplus P_{32} \otimes a_2 \oplus \ldots \oplus \oplus P_{3,m-2} \otimes a_{m-2} \oplus P_{3,m-1} \otimes a_{m-1}, \ldots,$$

$$\widetilde{A}_{m-1,m} = P_{m-1,1} \otimes a_1 \oplus P_{m-1,2} \otimes a_2 \oplus \ldots \oplus \oplus P_{m-1,m-2} \otimes a_{m-2} \oplus P_{m-1,m-1} \otimes a_{m-1},$$

$$\widetilde{A}_{m,m} = P_{m1} \otimes a_1 \oplus P_{m2} \otimes a_2 \oplus \ldots \oplus \oplus P_{m,m-2} \otimes a_{m-2} \oplus P_{m,m-1} \otimes a_{m-1}.$$

Просуммируем матрицы A_1 и $\widetilde{A}_2^*$. Получим матрицу:

$$A = \begin{bmatrix} A_{11} & A_{12} & \ldots & A_{1,m-1} & A_{1m} \\ A_{21} & A_{22} & \ldots & A_{2,m-1} & A_{2m} \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ A_{m-1,1} & A_{m-1,2} & \ldots & A_{m-1,m-1} & A_{m-1,m} \\ A_{m1} & A_{m2} & \ldots & A_{m,m-1} & A_{mm} \end{bmatrix}, \quad (6)$$

где для столбца 1: $A_{11} = a_0 \oplus \widetilde{A}_{11} = a_0$;

$$A_{21} = a_1 \oplus \widetilde{A}_{21} = a_1,$$

$$A_{31} = a_2 \oplus \widetilde{A}_{31} = a_2, \ldots,$$

$$A_{m-1,1} = a_{m-2} \oplus \widetilde{A}_{m-1,1} = a_{m-2},$$

$$A_{m1} = a_{m-1} \oplus \widetilde{A}_{m1} = a_{m-1};$$

для столбца 2: $A_{12} = \widetilde{A}_{12}$;

$$A_{22} = a_0 \oplus \widetilde{A}_{22}, \quad A_{32} = a_1 \oplus \widetilde{A}_{32}, \ldots,$$

$$A_{m-1,2} = a_{m-3} \oplus \widetilde{A}_{m-1,2},$$

$$A_{m2} = a_{m-2} \oplus \widetilde{A}_{m2};$$

для столбца 3: $A_{13} = \widetilde{A}_{13}$;

$$A_{23} = \widetilde{A}_{23}, \quad A_{33} = a_0 \oplus \widetilde{A}_{33}, \ldots,$$

$$A_{m-1,3} = a_{m-4} \oplus \widetilde{A}_{m-1,3}, \quad A_{m3} = a_{m-3} \oplus \widetilde{A}_{m3};$$

$$\vdots$$

для столбца $(m-1)$: $A_{1,m-1} = \widetilde{A}_{1,m-1}$,

$$A_{2,m-1} = \widetilde{A}_{2,m-1}, \quad A_{3,m-1} = \widetilde{A}_{3,m-1}, \ldots,$$

$$A_{m-1,m-1} = a_0 \oplus \widetilde{A}_{m-1,m-1},$$

$$A_{m,m-1} = a_1 \oplus \widetilde{A}_{m,m-1};$$

для столбца m: $A_{1m} = \widetilde{A}_{1m}$,

$$A_{2m} = \widetilde{A}_{2m}, \quad A_{3m} = \widetilde{A}_{3m}, \ldots,$$

$$A_{m-1,m} = \widetilde{A}_{m-1,m}, \quad A_{mm} = a_0 \oplus \widetilde{A}_{mm}.$$

Подставим выражение матрицы A (6) в (5). В результате получим систему m линейных уравнений от m неизвестных, представленную в матричном виде:

$$\begin{bmatrix} A_{11} & A_{12} & \dots & A_{1,m-1} & A_{1m} \\ A_{21} & A_{22} & \dots & A_{2,m-1} & A_{2m} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ A_{m-1,1} & A_{m-1,2} & \dots & A_{m-1,m-1} & A_{m-1,m} \\ A_{m1} & A_{m2} & \dots & A_{m,m-1} & A_{mm} \end{bmatrix} \otimes$$

$$\otimes \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix}. \qquad (7)$$

Решением этой системы уравнений будет искомое инверсное значение элемента конечного поля. Решение существует, так как для каждого ненулевого элемента конечного поля есть обратное значение и притом единственное. Следовательно, если $a \neq 0$, то $|A| \neq 0$.

Так как операции при вычислении определителя $|A|$ производятся в поле GF(2), то $|A| = 1$.

Утверждение. Решением системы уравнений (7) для $c(x) = 1$ является соотношение

$$b_i = |A|_{1j},$$

где $|A|_{1j}$ – минор элемента A_{1j} матрицы A; $j = i+1$, $i = \overline{0, m-1}$.

Доказательство. Известно, что систему линейных уравнений можно решить по формуле Крамера [7]:

$$b_i = \frac{1}{|A|} \begin{vmatrix} A_{11} & \dots & A_{1,j-1} & c_0 & A_{1,j+1} & \dots & A_{1m} \\ A_{21} & \dots & A_{2,j-1} & c_1 & A_{2,j+1} & \dots & A_{1m} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ A_{m-1,1} & \dots & A_{m-1,j-1} & c_{m-2} & A_{m-1,j+1} & \dots & A_{1m} \\ A_{m1} & \dots & A_{m,j-1} & c_{m-1} & A_{m,j+1} & \dots & A_{mm} \end{vmatrix} =$$

$$= \frac{|A|_{1j} \cdot c_0 + |A|_{2j} \cdot c_1 + \dots + |A|_{mj} \cdot c_{m-1}}{|A|}.$$

Так как $c_{m-1} = c_{m-2} = \dots = c_1 = 0$, $c_0 = 1$ и $|A| = 1$, то получим $b_i = |A|_{1j}$.

Ч. т. д.

При выполнении деления имеем $\left\langle c(x) \cdot a^{-1}(x) \right|_{p(x)} = b(x)$ или $\left\langle a(x) \cdot b(x) \right|_{p(x)} = c(x)$, где многочлен $c(x)$ не обязательно соответствует 1. Тогда решением системы уравнений (7) будет соотношение:

$$b_i = |A|_{1j} \cdot c_0 + |A|_{2j} \cdot c_1 + \dots + |A|_{mj} \cdot c_{m-1}.$$

Алгоритм инвертирования элементов конечного поля GF(2^m)

На основании полученных результатов предлагается алгоритм определения инверсного значения элемента конечного поля (*алгоритм И1*):

1) вычисляются операционные коэффициенты $P_{kl} = p_i^{(j)}$ матрицы P;

2) выполняется умножение матрицы P и матрицы A_2^*, результат которого $\widetilde{A}_2^* = P \cdot A_2^*$ суммируется с матрицей A_1 – $A = A_1 + \widetilde{A}_2^*$;

3) определяется минор элемента A_{1j} матрицы A – вычисляется обратный элемент конечного поля $b_i = |A|_{1j}$.

Операционные коэффициенты матрицы P могут быть вычислены либо реализацией, предложенной в [11], либо с помощью следующей процедуры:

1) производится обращение матрицы P_2, элементами которой являются коэффициенты p_i неприводимого многочлена $p(x)$;

2) выполняется умножение матриц $P_1 \cdot P_2^{-1}$.

Выводы

Предложенный метод и разработанные математические выражения и алгоритм позволяют реализовать вычисление инверсных значений элементов конечного поля $GF(2^m)$ на быстродействующих комбинационных схемах, структура которых однородна и универсальна. Это делает их

перспективными для реализации в виде БИС. Этот метод также проще метода, описанного в [12], где необходимо решать систему $(2m-1)$ уравнений от $(2m-1)$ неизвестных.

Список литературы

1. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки: Пер. с англ. / Под ред. Р.Л. Добрушина и С.И. Самойленко. – М.: Мир, 1976. – 596 с.

2. *Гилл А.* Линейные последовательностные машины – М.: Наука, 1974. – 287 с.

3. *Блох Э. Л., Зяблов В. В.* Обобщенные каскадные коды – М.: Связь, 1976. – 240 с.

4. *Берлекэмп Э.* Алгебраическая теория кодирования – М.: Мир, 1971. – 477 с.

5. *Bartee T.C., Shneider D.I.* Computations with finite fields – Information and control, 1963, 6. – P. 79–98.

6. *Кубицкий В.И.* Метод инвертирования элементов конечного поля $GF(2^m)$. – Сбірник тез II Міжнародної науково-технічної конференції «Комп'ютерні системи та мережні технології» (CSNT). – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2009. – С. 57.

7. *Кубицкий В.И.* Умножение элементов конечного поля $GF(2^m)$. – Научный Вестник МГТУ ГА, № 145 (8). – М.: МГТУ ГА, 2009. – С. 105–112.

8. *Кубицкий В.И.* Операции над многочленами в поле GF(2). – Научный вестник ГосНИИ "Аэронавигация", серия «Проблемы организации воздушного движения. Безопасность полетов». №7. – М.: 2007. – С. 185–194.

9. *Мальцев А.И.* Основы линейной алгебры. – М.: Наука, 1975. – 400 с.

10. *Жуков И.А., Кубицкий В.И., Дрововозов В.И.* Алгоритмы выполнения операций над элементами конечного поля $GF(2^m)$ в вычислительных устройствах. – Матеріали VIII Міжнародної науково-технічної конференції "АВІА-2007". – Т.1. – К.: НАУ, 2007. – С. 13.5–13.8.

11. Патент №25491 Украины, МПК G06F 7/49 (2007/01). Пристрій для множення елементів скінченних полів $GF(2^n)$ / Жуков И.А., Кубицкий В.И., Синельников А.А.; заявл. 02.04.2007, № u 2007 03644; опубл. 10.08.2007. Бюл. № 12.

12. *Davida G. I.* Inverse of elements of a Galois field. – Electronics Letters, 1972, 8, №21, pp. 518–520.

Подано до редакції 22.03.10