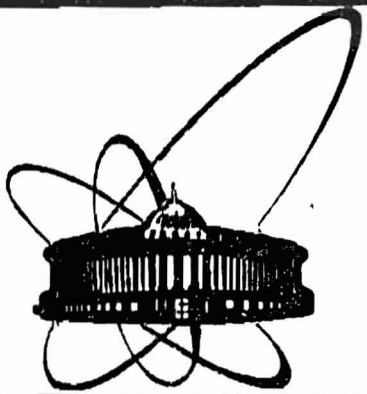

сообщения
объединенного
института
ядерных
исследований
дубна



Р10-88-853

Н.М.Никитюк

# БЫСТРЫЕ АЛГОРИТМЫ ДЛЯ КООРДИНАТНЫХ ПРОЦЕССОРОВ В ПОЛЕ ГАЛУА $F(2^m)$ ПРИ МНОЖЕСТВЕННОСТИ $1 \leq t \leq 3$

1988

## 1. ПОСТАНОВКА ЗАДАЧИ

В связи с широким развитием алгебраических методов обработки сигналов[1] возникает необходимость оптимизации как с точки зрения быстродействия, так и аппаратурных затрат алгоритмов для решений уравнений Ньютона и уравнений положения ошибок при декодирования БХЧ-кодов. В работах[2-8] показано, что алгебраическая теория кодирования может быть успешно использована для сжатия данных в электронных методах физики высоких энергий и создания различного рода устройств отбора событий по множественности t и координатных процессоров.

Координаты сработавших позиционно-чувствительных датчиков находятся из уравнения[9,11]

$$X^t + \sigma_1 X^{t-1} + \sigma_2 X^{t-2} + \dots \sigma_t = 0. \qquad /1/$$

В свою очередь, связь между симметрическими функциями $S_j$, которые по существу представляют собой код синдрома, содержащего в себе информацию как о количестве сработавших датчиков, так и об их координатах, и элементарными симметрическими функциями $\sigma_i$ описывается с помощью уравнений Ньютона[9,10]

$$\begin{bmatrix} S_1 & 1 & 0 & 0 & \dots & 0 \\ S_3 & S_2 & S_1 & 1 & & \\ \vdots & \vdots & & & \ddots & \\ S_{2t-3} & & & & & \\ S_{2t-1} & S_{2t-2} & & & & \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_1 \\ \sigma_2 \\ \\ \\ \sigma_t \end{bmatrix} = 0.$$

В настоящее время для выполнения различного рода операций над элементами поля $GF(2^m)$ используются модули ППЗУ[7, 9,11]. В работах[13-15] автором было показано, что, используя метод совмещенных операций, можно более эффективно использовать емкость ППЗУ и одновременно повысить быстродействие выполнения алгебраических операций. Суть метода заключается в том, что коли-

чество входов ППЗУ для переменных, необходимое для реализации сложного алгебраического выражения, зависит только от количества входящих в это выражение значений элементов поля и не зависит от того, под какой степенью они находятся. Например, для умножения двух элементов поля A и B и $A^3$ и $B^3$ требуется в обоих случаях ППЗУ, содержащее 2m входов. Как будет показано ниже, такой подход позволяет существенно упростить решение уравнения /1/.

В дальнейшем с целью упрощения изложения положим, что количество позиционно-чувствительных датчиков в детекторе $n=2^m-1=$ $= 2^6 - 1 = 63$. Это значит, что мы будем оперировать элементами поля $GF(2^6)$, образованного над неприводимым полиномом $X^6 + X + 1$ /3/. Таблица 63 ненулевых элементов поля $GF(2^6)$ имеется в приложении 1. Матрица проверочных соотношений $H^T_{63}$ в сокращенной записи при t = 4 имеет вид

$H^T_{63} =$

| | | | | | |
|---|---|---|---|---|---|
| * | 100000 | 100000 | 100000 | 100000 | 1 |
| | 010000 | 000100 | 000001 | 011000 | 2 |
| * | 001000 | 110000 | 000011 | 001010 | 3 |
| * | 000100 | 000110 | 000101 | 110111 | 4 |
| | 000010 | 101000 | 001111 | 001110 | 5 |
| * | 000001 | 000101 | 010001 | 110100 | 6 |
| | | | ⋮ | | ⋮ |
| | 100001 | 100111 | 111111 | 111110 | 63 |
| | ↓ | ↓ | ↓ | ↓ | |
| | $S_1$ | $S_3$ | $S_5$ | $S_7$ | |

Номер датчика

Символом * обозначены сработавшие датчики. Допустим, что в качестве элементной базы используются микросхемы 500-й серии. В работах /6,7,9/ было показано, что путем анализа значения определителей в поле $GF(2^m)$ можно довольно быстро определить величину множественности t регистрируемых сигналов в многоканальных детекторах заряженных частиц, а затем, решая уравнение /1/, определить координаты сработавших датчиков /3,5,10/.

В приложении 2 приведены формулы для вычисления определителей от первого до пятого порядков включительно и на рис.1 - блок-схема для аппаратной реализации определителей от первого до четвертого порядков. Следует отметить, что данная схема составлена таким образом, что для вычисления того или иного выражения достаточно использовать ППЗУ, содержащее не более 2 входов. Кроме того, ряд выражений, обозначенных для краткости буквами, можно использовать при вычислении значений t и уравнения /1/, что позволяет существенно сократить объем электронной аппаратуры при комплексном решении задачи, начиная от определения множественности и кончая нахождением координат событий.



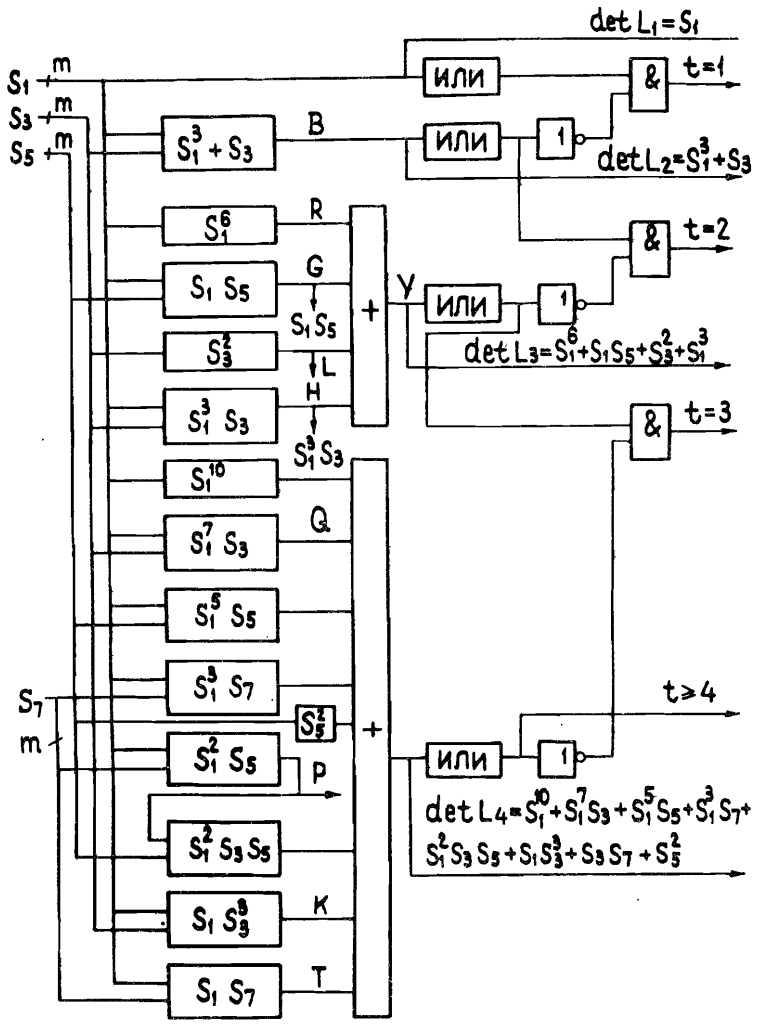


Рис.1. Блок-схема для вычисления определителей 1÷4-го порядков в поле $GF(2^m)$.

## 2. ПРОЦЕССОР ДЛЯ ОПРЕДЕЛЕНИЯ КООРДИНАТ ДВУХ СОБЫТИЙ

При t = 2 уравнение /1/ принимает вид

$$X^2 + \sigma_1 X + \sigma_2 = 0. \qquad /3/$$

Путем подстановки $X = \sigma_1 Y$ уравнение /3/ приводится к виду

$$Y^2 + Y = \gamma, \qquad /4/$$

где

$$\gamma = \sigma_2 / \sigma_1^2 = S_1^3 + S_3 / S_1^3 = 1 + S_3 (S_1^3)^{-1}.$$

Корни уравнения /3/ вычисляются из соотношений [3,11,17,20]

$$X_1 = \sigma_1 Y_1 \quad \text{и} \quad X_2 = \sigma_1 Y_2,$$

причем $Y_2 = Y_1 + 1$ в поле $GF(2^m)$, поэтому важно найти наиболее простой метод решения уравнения /4/.

Известная из алгебры формула для вычисления корней квадратного уравнения не подходит, поскольку дискриминант формулы равен нулю [21]. Известно несколько алгоритмов решения уравнения второй степени в поле $GF(2^m)$ [3,18-22]. Наиболее изящным, по мнению автора, остается алгоритм, предложенный Е.Берликэмпом [17], хотя после него появился ряд других работ [20-22].

В соответствии с методом Е.Берликэмпа уравнение /4/ имеет решение тогда и только тогда, когда оператор $Tr(\gamma) = 0$. Причем этот оператор /англ. Trace/ определяется из выражения

$$Tr(\gamma) = \sum_{i=0}^{m-1} \gamma^{2^i}, \quad Tr(\gamma) = 0,1. \qquad /5/$$

Далее, если $a^i$ - произвольный элемент поля $GF(2^m)$ и $a^k$ - элемент, для которого $Tr(a^k) = 1$, то для $i = 0,1,\ldots, m-1$ можно найти такое $y_i$, что

$$y_i^2 + y_i = \begin{cases} a^i, & \text{если } Tr(a^i) = 0, \\ a^i + a^k, & \text{если } Tr(a^i) = 1. \end{cases} \qquad /6/$$

Тогда при $Tr(\gamma) = 0$ решение уравнения имеет вид

$$Y_1 = \sum_{i=0}^{m-1} \gamma_i y_i, \qquad /7/$$

т.е. оно сводится к линейным операциям, где

$$Y_{10} = \gamma_0; \; Y_{11} = \gamma_0 + \gamma_1 + \gamma_5; \; Y_{12} = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_5, \; Y_{13} = \gamma_0, \qquad /8/$$
$$Y_{14} = \gamma_0 + \gamma_3 + \gamma_5, \; Y_{15} = \gamma_0 + \gamma_1 + \gamma_2 + \gamma_4 + \gamma_5.$$



На примере поля $GF(2^6)$ значения $y_0 - y_5$ вычисляются следующим образом. Путем несложных вычислений получаются значения $a^i$, для которых оператор $Tr(a^i) = 0$,

$$y_0 = a^\circ = 100000 \to a^i = 0,$$
$$y_1 = a^{11} = 110001 \to a^i = a^{36},$$
$$y_2 = a^{55} = 011101 \to a^i = a^{32}, \qquad /9/$$
$$y_3 = a^\circ = 100000 \to a^i = 0,$$
$$y_4 = a^{23} = 100101 \to a^i = a^{38},$$
$$y_5 = a^{43} = 111011 \to a^i = a^{19},$$

Например, оператор $Tr(a^{36}) = a^{36} a^{72} + a^{144} + a^{288} + a^{576} + a^{1152} + + = a^{36} a^9 + a^{18} + a^{36} + a^9 + a^{18} = 0$. Если теперь подставить значение $a^{55}$ в уравнения /6/, то получим

$$a^{110} + a^{55} = a^{32} = a^{47} + a^{55} = a^{32},$$

Из приложения 1 имеем

$$\begin{array}{r} 111001 \\ + \; 011101 \\ \hline 100100 = a^{32} \end{array}$$

Знак + обозначает "Сумма по модулю два".

С помощью вычисленных значений $y_0 \div y_5$ можно составить схему для решения уравнения /4/ в поле $GF(2^6)$, которая приведена на рис.2. Вначале с помощью ППЗУ вычисляется значение

$$\gamma = a^\circ \gamma_0 + a^1 \gamma_1 + a^2 \gamma_2 + a^3 \gamma_3 + a^4 \gamma_4 + a^5 \gamma_5,$$

где $a^1 \div a^5$ - базис поля $GF(2^6)$.

Выходы ППЗУ подключены к входам схем проверки на четность в соответствии с позициями единиц в решениях /9/, если их рассматривать как матрицу, состоящую из шести строк и стольких же столбцов. Так, например, на входы схемы 5 подаются значения $\gamma_0$, $\gamma_1$, $\gamma_2$, $\gamma_3$, $\gamma_4$ и $\gamma_5$, так как в решении $y_5 = 111011$ имеются единицы на соответствующих позициях. Этот же факт следует из равенств /8/.

Из схемы, приведенной на рис.2, видно, что время решения уравнения /3/ равно

Путем подстановки $X = \sigma_1 Y$ уравнение /3/ приводится к виду

$$Y^2 + Y = \gamma, \qquad /4/$$

где

$$\gamma = \sigma_2 / \sigma_1^2 = S_1^3 + S_3 / S_1^3 = 1 + S_3 (S_1^3)^{-1}.$$

Корни уравнения /3/ вычисляются из соотношений [3,11,17,20]

$$X_1 = \sigma_1 Y_1 \quad \text{и} \quad X_2 = \sigma_1 Y_2,$$

причем $Y_2 = Y_1 + 1$ в поле $GF(2^m)$, поэтому важно найти наиболее простой метод решения уравнения /4/.

Известная из алгебры формула для вычисления корней квадратного уравнения не подходит, поскольку дискриминант формулы равен нулю [21]. Известно несколько алгоритмов решения уравнения второй степени в поле $GF(2^m)$ [3,18-22]. Наиболее изящным, по мнению автора, остается алгоритм, предложенный Е.Берликэмпом [17], хотя после него появился ряд других работ [20-22].

В соответствии с методом Е.Берликэмпа уравнение /4/ имеет решение тогда и только тогда, когда оператор $Tr(\gamma) = 0$. Причем этот оператор /англ. Trace/ определяется из выражения

$$Tr(\gamma) = \sum_{i=0}^{m-1} \gamma^{2^i}, \quad Tr(\gamma) = 0,1. \qquad /5/$$

Далее, если $a^i$ - произвольный элемент поля $GF(2^m)$ и $a^k$ - элемент, для которого $Tr(a^k) = 1$, то для $i = 0,1,\ldots, m-1$ можно найти такое $y_i$, что

$$y_i^2 + y_i = \begin{cases} a^i, & \text{если } Tr(a^i) = 0, \\ a^i + a^k, & \text{если } Tr(a^i) = 1. \end{cases} \qquad /6/$$

Тогда при $Tr(\gamma) = 0$ решение уравнения имеет вид

$$Y_1 = \sum_{i=0}^{m-1} \gamma_i y_i, \qquad /7/$$

т.е. оно сводится к линейным операциям, где

$$Y_{10} = \gamma_0; \; Y_{11} = \gamma_0 + \gamma_1 + \gamma_5; \; Y_{12} = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_5, \; Y_{13} = \gamma_0, \qquad /8/$$
$$Y_{14} = \gamma_0 + \gamma_3 + \gamma_5, \; Y_{15} = \gamma_0 + \gamma_1 + \gamma_2 + \gamma_4 + \gamma_5.$$



На примере поля $GF(2^6)$ значения $y_0 - y_5$ вычисляются следующим образом. Путем несложных вычислений получаются значения $a^i$, для которых оператор $Tr(a^i) = 0$,

$$y_0 = a^\circ = 100000 \to a^i = 0,$$
$$y_1 = a^{11} = 110001 \to a^i = a^{36},$$
$$y_2 = a^{55} = 011101 \to a^i = a^{32}, \qquad /9/$$
$$y_3 = a^\circ = 100000 \to a^i = 0,$$
$$y_4 = a^{23} = 100101 \to a^i = a^{38},$$
$$y_5 = a^{43} = 111011 \to a^i = a^{19},$$

Например, оператор $Tr(a^{36}) = a^{36} a^{72} + a^{144} + a^{288} + a^{576} + a^{1152} + + = a^{36} a^9 + a^{18} + a^{36} + a^9 + a^{18} = 0$. Если теперь подставить значение $a^{55}$ в уравнения /6/, то получим

$$a^{110} + a^{55} = a^{32} = a^{47} + a^{55} = a^{32},$$

Из приложения 1 имеем

$$\begin{array}{r} 111001 \\ +\,011101 \\ \hline 100100 = a^{32} \end{array}$$

Знак + обозначает "Сумма по модулю два".

С помощью вычисленных значений $y_0 \div y_5$ можно составить схему для решения уравнения /4/ в поле $GF(2^6)$, которая приведена на рис.2. Вначале с помощью ППЗУ вычисляется значение

$$\gamma = a^\circ \gamma_0 + a^1 \gamma_1 + a^2 \gamma_2 + a^3 \gamma_3 + a^4 \gamma_4 + a^5 \gamma_5,$$

где $a^1 \div a^5$ - базис поля $GF(2^6)$.

Выходы ППЗУ подключены к входам схем проверки на четность в соответствии с позициями единиц в решениях /9/, если их рассматривать как матрицу, состоящую из шести строк и стольких же столбцов. Так, например, на входы схемы 5 подаются значения $\gamma_0$, $\gamma_1$, $\gamma_2$, $\gamma_3$, $\gamma_4$ и $\gamma_5$, так как в решении $y_5 = 111011$ имеются единицы на соответствующих позициях. Этот же факт следует из равенств /8/.

Из схемы, приведенной на рис.2, видно, что время решения уравнения /3/ равно

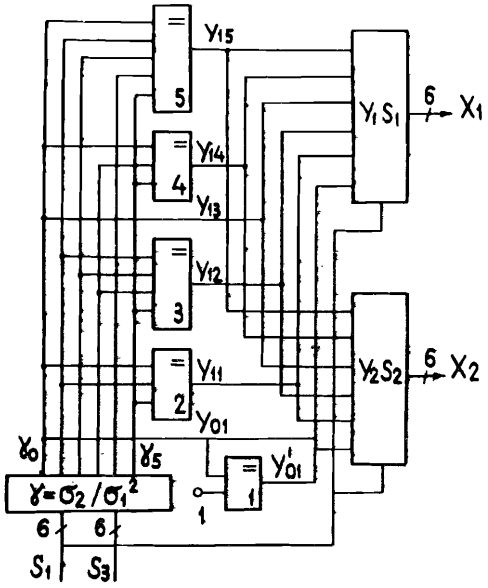


Рис.2. Блок-схема решения уравнения второго порядка в поле $GF(2^m)$ .

$$T_k = T_S + T_{ч} + T_4 + T_{ум} + T', \qquad /10/$$

где $T_S$, $T_{ч}$, $T_4$, $T_{ум}$, $T'$ - задержки в схемах для вычисления значения $S_j$ и $T_{ч}$ в схемах проверки на четность, в схеме умножения $T_{ум}$ и в сумматоре по модулю два.

Если требуется получение максимального быстродействия, то для вычисления значения $\gamma_i$ и для умножения двух элементов поля можно использовать микросхемы малой степени интеграции, такие, как К500ЛМ102 и К500ИЕ160, которые имеют задержки 2 и 6 нс соответственно /3/ . Тогда значение $\gamma_i$ можно вычислить за 8 нс, а в целом две координаты $X_1$ и $X_2$ можно определить не более чем за 35 нс.

Учитывая, что код $S_1S_3$ содержит 2m бит и что современные ПЛМ и ППЗУ имеют 18÷20 входов для переменных, при $m = 4 \div 9$ для вычисления двух координат можно использовать прямое декодирование синдрома $S_1S_3$ .

Рассмотрим численный пример. Допустим, что сработали те позиционно-чувствительные датчики, которые расположены на позициях $a^0 = X_1$ и $a^2 = X_2$. Имеем

$$S_1 = X_1 + X_2 = \begin{array}{r} 100000 \\ +\,001000 \\ \hline 101000 \end{array} = a^{12}, \quad S_3 = X_1 + X_3 = \begin{array}{r} 100000 \\ +\,110000 \\ \hline 010000 \end{array} = a^1.$$

Вычисляем $\sigma_1 = a^{12}$ и $\sigma_2 = a^{36} + a^1/a^{12} = a^2$ /см. приложение 1/. Далее имеем $\gamma = \sigma_2/\sigma_1^2 = a^2/a^{24} = a^2 a^{39} = a^{41} = 101110$. Здесь деление элемента $a^2$ на элемент $a^{24}$ заменено умножением $a^2$ на обратный к элементу $a^{24}$ ($a^{24} a^{39} = 1$) элемент $a^{39}$. Из соотношений /8/ имеем

$$y_0 = 1, y_1 = 1, \quad y_2 = 0, y_3 = 1, y_4 = 0, \quad y_5 = 1, \quad y_1 = 110111 = a^{51}$$

и $y_2 = a^{53}$ .



Координаты $X_1$ и $X_2$ равны

$$X_1 = Y_1 S_1 = a^{51} a^{12} = a^{63} = a^0 \qquad X_2 = a^{53} a^{12} = a^{65} = a^2.$$

Можно проверить, что координаты $a^0$ и $a^2$ удовлетворяют уравнению

$$X^2 + a^{12} X + a^2 = 0.$$

Если сравнить алгоритм Берликэмпа с другими известными методами решения уравнения второй степени, то получается, что как по быстродействию, так и с точки зрения аппаратурных затрат рассмотренный в данной работе способ более эффективен. Например, для вычисления константы $\gamma$ требуется только операция сложения. При этом предполагается, что для каждого $\gamma$ предварительно вычислены значения $a^i$ и $y_i$ . В работе /22/ для вычисления корня $Y_1$ предложена формула, для реализации которой требуется вычисление оператора $Tr(\gamma)$ .

## 3. РЕШЕНИЕ УРАВНЕНИЯ ТРЕТЬЕЙ СТЕПЕНИ

Для однозначной регистрации координат трех одновременно сработавших датчиков прежде всего требуется вычислить синдром $S_1S_3S_5$, разрядность которого равна 3m. С этим фактом приходится считаться при создании специализированных процессоров для $t \le 5$. В этом параграфе рассматривается такой алгоритм решения уравнения третьей степени, для реализации которого достаточно использовать ППЗУ или ПЛМ, содержащие не более 2m входов для переменных. Для нахождения координат $X_1$, $X_2$, и $X_3$ трех сработавших датчиков необходимо найти корни уравнения

$$X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3 = 0. \qquad /11/$$

Для нахождения корней /11/ табличным методом /19–22/ при помощи подстановок $X = Y + \sigma_1$ и $Y = Z(\sigma_1^2 + \sigma_2)^{1/2}$ оно приводится к виду

$$Z^3 + Z = C_1, \qquad /12/$$

где

$$C_1 = \frac{\sigma_1\sigma_2 + \sigma_3}{(\sigma_1^2+\sigma_2)(\sigma_1^2+\sigma_2)^{1/2}}. \qquad /13/$$

Уравнение /12/ имеет три различных корня только при определенном наборе значений $C_1$. Число таких констант равно 2,5 и 10 для m = 4,5, и 6 соответственно /20/. В таблице даны константы для m = 6 и t = 3, причем в памяти достаточно хранить по два значения корня для каждого $C_1$, а третий корень получается из формулы

$$X_3 = X_1 + X_2 + S_1.$$

Самым трудоемким при решении уравнения третьей степени является вычисление значения $C_1$. Так, для вычисления числителя выражения /13/ необходимо три ППЗУ на 3m входов, и при m = 6 его емкость должна составлять не менее 256К. С целью упрощения реализации формулы /13/ выразим константу $C_1$ непосредственно через $S_1$, $S_3$ и $S_5$,

$$C_1 = \frac{S_3^2 + S_1^6/S_1^3 + S_3}{S_1^5 + S_5/S_1^3 + S_3(S_1^5 + S_5/S_1^3 + S_3)^{1/2}} = \frac{D}{E \cdot E^{1/2}} = D(E \cdot E^{1/2})^{-1}.$$

*Таблица*

Решения для n = 63 и t = 3

| $C_1$ | $Z_{1j}$ | $C_1$ | $Z_{1j}$ |
|---|---|---|---|
| $C_1 = 1$ | $Z_{11} = a^{27}$ | $C_6 = a^{62}$ | $Z_{61} = a^{37}$ |
| | $Z_{12} = a^{45}$ | | $Z_{62} = a^{39}$ |
| $C_2 = a^{9}$ | $Z_{21} = a^{18}$ | $C_7 = a^{61}$ | $Z_{71} = a^{11}$ |
| | $Z_{22} = a^{55}$ | | $Z_{72} = a^{15}$ |
| $C_3 = a^{18}$ | $Z_{31} = a^{36}$ | $C_8 = a^{59}$ | $Z_{81} = a^{22}$ |
| | $Z_{32} = a^{47}$ | | $Z_{82} = a^{30}$ |
| $C_4 = a^{36}$ | $Z_{41} = a^{9}$ | $C_9 = a^{55}$ | $Z_{91} = a^{44}$ |
| | $Z_{42} = a^{31}$ | | $Z_{92} = a^{60}$ |
| $C_5 = a^{31}$ | $Z_{51} = a^{50}$ | $C_{10} = a^{47}$ | $Z_{101} = a^{25}$ |
| | $Z_{52} = a^{51}$ | | $Z_{102} = a^{57}$ |



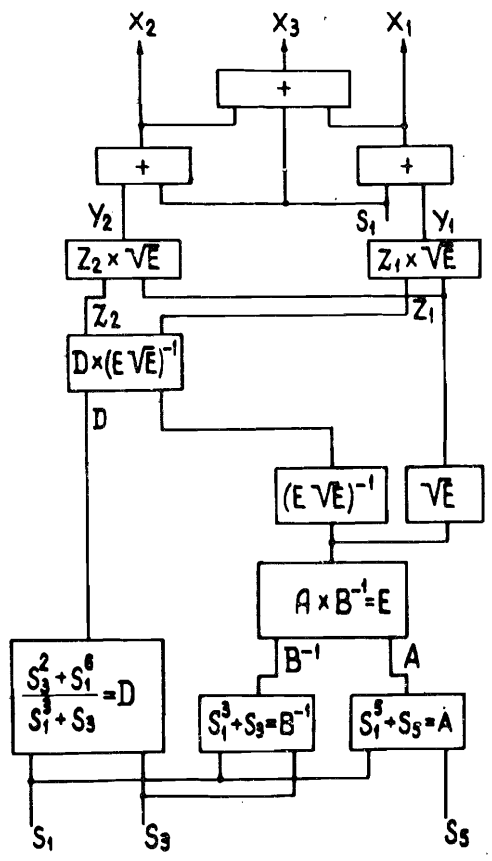


Рис.3. Блок-схема решения кубического уравнения в поле $GF(2^m)$.

Используя принцип выполнения совмещенных операций в поле $GF(2^m)$, константу $C_1$ можно вычислить с помощью ППЗУ, содержащего только 2m входов. На рис.3 приведена блок-схема решения уравнения /11/. Знаком "+" обозначены сумматоры по модулю два. Максимальное время нахождения трех координат равно

$$T_k = 5T_{ппзу} + 2T_s,$$

где $T_{ппзу}$ и $T_s$ - время задержки в ППЗУ и время суммирования по модулю два соответственно. Нетрудно заметить, что для вычисления $E^{1/2}$ достаточно использовать ППЗУ на m входов.

*Численный пример.* Положим, что сигналы поступили от первого, четвертого и шестого датчиков детектора заряженных частиц. Эти позиции обозначены символом * в матрице $H_{63}^T$. Имеем

$$S_1 = X_1 + X_2 + X_3, \; S_3 = X_1^3 + X_2^3 + X_3^3 \text{ и } S_5 = X_1^5 + X_2^5 + X_3^5.$$

Откуда

$$S_1 = a^0 + a^3 + a^5 = a^{23}, \; S_2 = a^{61} \text{ и } S_5 = a^0 + a^{15} + a^{25} = a^{35}.$$

При этих значениях $S_1$ $C_1 = a^{55}$, и в соответствии с таблицей имеем

$$Z_1 = a^{44} \text{ и } Z_2 = a^{60}. \quad Y_1 = a^{62}, \; Y_2 = a^{15}.$$

И, наконец,

$$X_1 = a^3, \; X_2 = a^0 \text{ и } X_3 = a^5.$$

Следует напомнить, что в методе синдромного кодирования позиции нумеруются степенями элементов поля Галуа $GF(2^m)$ .

## 4. МЕТОД ТРАНСФОРМАЦИИ ПЕРЕМЕННЫХ

При $t > 3$ существенно возрастает сложность вычислений элементарных симметрических функций $\sigma_i$ . С целью упрощения решения уравнений четвертой и пятой степеней автором был проанализирован малоизвестный алгоритм трансформации переменных /12,23/ для решения уравнений Ньютона в поле $GF(2^m)$, путем введения новой переменной $R_k$ , которая связана с $S_k$ следующим соотношением:

$R_k = \Sigma A_i \cdot S_{k-2}$ , где $A_o = S_o = 1$.

В результате уравнения /2/ приводятся к виду

$$\begin{bmatrix} R_1 & 1 & 0 & 0 \ldots\ldots 0 \\ R_3 & R_2 & R_1 & \ldots\ldots\ldots 0 \\ \vdots & & & \\ R_{2t-1} & R_{2t-1} & \ldots\ldots\ldots & R_t \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix} \qquad /14/$$

Или более кратко, $R_{2i-j-1}\,\sigma_j$ , $i = 1,2, \ldots t$ . Существенным в таком преобразовании является тот факт, что уравнения /14/ разделяются на две системы уравнений. Так, последние $\ell/2$ уравнений дают

$$\begin{bmatrix} R_{2t-5} & & \\ R_{2t-3} & R_{2t-5} & \\ R_{2t-1} & R_{2t-3} & R_{2t-5} \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_2 \\ \sigma_4 \\ \sigma_{[t/2]} \end{bmatrix},$$

где $[X]$ - целая часть $[X]$. В свою очередь, первые $(t - t/2)$ уравнений системы /14/ дают



$$\begin{bmatrix} \sigma_1 \\ \sigma_3 \\ \sigma_5 \\ \vdots \end{bmatrix} = \begin{bmatrix} R_1 & 0 & 0 \\ R_3 & R_1 & 0 \\ R_5 & R_3 & R_1 \\ R_{2t-1} & \cdots & \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_2 \\ \sigma_4 \\ \vdots \end{bmatrix} \qquad /15/$$

Причем в верхнем правом углу элемент матрицы равен $R_1$, если $t$ - четное и $R_3$, если $t$ - нечетное число. Для небольших $t$ имеют место следующие равенства :

$R_o = 1$,

$R_1 = S_1$,

$R_3 = S_3 + S_1^3 = B$,

$R_5 = S_5 + S_1^2 S_3$,

$R_7 = S_7 + S_1^2 S_5 + S_1 S_3^2 + S_1^7 = S_7 + P + K + S_1^7$,

$R_9 = S_9 + S_1^2 S_7 + S_3^3 + S_1^6 S_3$.

Например, при $t = 4$ получаются следующие матричные уравнения:

$$\begin{bmatrix} \sigma_1 \\ \sigma_3 \end{bmatrix} = \begin{bmatrix} R_1 & 0 \\ R_3 & R_1 \end{bmatrix} \begin{bmatrix} R_5 & R_3 & R_1 \\ R_7 & R_5 & R_3 \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_2 \\ \sigma_4 \end{bmatrix} = 0. \qquad /16/$$

Решения /16/ относительно $\sigma_1$ и $\sigma_3$ дают

$$\sigma_1 = R_1, \qquad /17/$$

$$\sigma_3 = R_3 + R_1\sigma_2. \qquad /18/$$

Аналогично из /17/ имеем

$$\begin{aligned} R_5 + R_3\sigma_2 + R_1\sigma_4 &= 0, \\ R_7 + R_5\sigma_2 + R_3\sigma_4 &= 0. \end{aligned} \qquad /19/$$

Первое из равенств /19/ не содержит значения $R_7$, и поэтому аппаратным методом решается проще,

$$\sigma_4 = \frac{R_5}{R_1} + \frac{R_3\sigma_2}{R_1}. \qquad /20/$$

Вычислив величину $\sigma_2$ /см. приложение 2/, затем, с определенной задержкой, можно по упрощенным выражениям получить $\sigma_3$ и $\sigma_4$. При t = 5 из /15/ /имеем /23//

$$\begin{bmatrix} R_5 & R_3 \\ R_7 & R_5 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_4 \end{bmatrix} = \begin{bmatrix} R_7 \\ R_9 \end{bmatrix}, \qquad /21/$$

$$\begin{bmatrix} \sigma_1 \\ \sigma_3 \\ \sigma_5 \end{bmatrix} = \begin{bmatrix} R_1 & 0 & 0 \\ R_3 & R_1 & 0 \\ R_5 & R_3 & R_1 \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_2 \\ \sigma_4 \end{bmatrix}. \qquad /22/$$

Уравнения /21/ и /22/ дают

$$\begin{aligned} R_7 &= R_5\sigma_2 + R_3\sigma_4, \\ R_9 &= R_7\sigma_2 + R_5\sigma_4, \\ \sigma_1 &= R_1, \qquad /23/ \\ \sigma_3 &= R_3 + R_1\sigma_2, \\ \sigma_5 &= R_5 + R_3\sigma_2 + R_1\sigma_4. \end{aligned}$$

Из уравнений /23/ следует, что, вычислив предварительно $\sigma_2$, $R_3$ и $R_7$, можно относительно просто получить значение $\sigma_4$, а затем и $\sigma_5$. В свою очередь, такая трансформация позволяет существенно упростить аппаратные средства для вычисления значений $\sigma_t$ за счет того, что эти значения определяются параллельно-последовательным методом. Поскольку в этом случае можно использовать быстродействующие ППЗУ с гораздо меньшим числом входов для переменных, то тем самым практически сохраняется такое же быстродействие, как и при вычислениях параллельным способом.



Приложение 1

Элементы поля Галуа $GF(2^m)$ по модулю многочлена $X^6 + X + 1$

| | | |
|---|---|---|
| $a^0 = 100000$ | $a^{21} = 110111$ | $a^{42} = 010111$ |
| $a = 010000$ | $a^{22} = 101011$ | $a^{43} = 111011$ |
| $a^2 = 001000$ | $a^{23} = 100101$ | $a^{44} = 101101$ |
| $a^3 = 000100$ | $a^{24} = 100010$ | $a^{45} = 100110$ |
| $a^4 = 000010$ | $a^{25} = 010001$ | $a^{46} = 010011$ |
| $a^5 = 000001$ | $a^{26} = 111000$ | $a^{47} = 111001$ |
| $a^6 = 110000$ | $a^{27} = 011100$ | $a^{48} = 101100$ |
| $a^7 = 011000$ | $a^{28} = 001110$ | $a^{49} = 010110$ |
| $a^8 = 001100$ | $a^{29} = 000111$ | $a^{50} = 001011$ |
| $a^9 = 000110$ | $a^{30} = 110011$ | $a^{51} = 110101$ |
| $a^{10} = 000011$ | $a^{31} = 101001$ | $a^{52} = 101010$ |
| $a^{11} = 110001$ | $a^{32} = 100100$ | $a^{53} = 010101$ |
| $a^{12} = 101000$ | $a^{33} = 010010$ | $a^{54} = 111010$ |
| $a^{13} = 010100$ | $a^{34} = 001001$ | $a^{55} = 011101$ |
| $a^{14} = 001010$ | $a^{35} = 110100$ | $a^{56} = 111110$ |
| $a^{15} = 000101$ | $a^{36} = 011010$ | $a^{57} = 011111$ |
| $a^{16} = 110010$ | $a^{37} = 001101$ | $a^{58} = 111111$ |
| $a^{17} = 011001$ | $a^{38} = 110110$ | $a^{59} = 101111$ |
| $a^{18} = 111100$ | $a^{39} = 011011$ | $a^{60} = 100111$ |
| $a^{19} = 011110$ | $a^{40} = 111101$ | $a^{61} = 100011$ |
| $a^{20} = 001111$ | $a^{41} = 101110$ | $a^{62} = 100001$ |
| | | $a^{63} = 100000$ |

Приложение 2

Координатные полиномы для специализированных процессоров

| t | Полиномы |
|---|---|
| 1 | $X + \sigma_1 = 0, \quad \sigma_1 = S_1$ |
| 2 | $X^2 + \sigma_1 X + \sigma_2 = 0; \ \sigma_1 = S_1; \ \sigma_2 = S_1^3 + S_3/S_1 = B/S_1$ |
| 3 | $X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3 = 0; \ \sigma_1 = S_1;$ |

Полиномы

$$\sigma_2 = \frac{S_1^2 S_3 + S_5}{B} = \frac{S_1^2}{B} + S_5/B$$

$$\sigma_3 = S_1^3 + S_3 + S_1(S_1^2 S_3 + S_5)/B = \frac{B+H}{B} + G \cdot B^{-1}$$

4 $X^4 + \sigma_1 X^3 + \sigma_2 X^2 + \sigma_3 X + \sigma_4 = 0, \quad \sigma_1 = S_1$

$$\sigma_2 = [S_1(S_1^7 + S_7) + S_3(S_1^5 + S_5)]/A = \frac{S_1^8 + T + S_1^5 S_3 + S_3 S_5}{R + G + H + L}$$

$$\sigma_3 = [S_1(S_1^3 S_5 + S_1 S_7) + S_3(S_1^6 + S_3^2)]/A = R_3 + R_1 \sigma_2 ;$$

$$\sigma_4 = [S_1^3(S_1^7 + S_7) + S_3(S_1^7 + S_1 S_3^2 + S_7) + S_5(S_1^5 + S_1^2 S_3 + S_5)]/A =$$

$$= R_5 + R_3 \sigma_2 / R_1 ;$$

$$A = S_1(S_1^5 + S_5) + S_3(S_1^3 + S_3) = R + G + H + L$$

ЛИТЕРАТУРА


1. Блейхат Р.Э. - ТИИР, 1985, т.73, № 5, с.30.
2. Nikityuk N.M., Radshabov R.S., Shafranov M.D. - Nucl.Instr. and Meth., 1978, v.155, No.1, p.485.
3. Никитюк Н.М. ОИЯИ, Р11-80-484, Дубна, 1980.
4. Nikityuk N.M. JINR, E11-87-10, Dubna, 1987.
5. Никитюк Н.М., Раджабов Р.С., Шафранов М.Д. - ПТЭ, 1978, № 4, с.95.
6. Гайдамака Р.И. и др. ОИЯИ, Р13-82-628, Дубна, 1982.
7. Nikityuk N.M. JINR, E10-88-28, Dubna, 1988, Доклад на первой Объединенной конференции ISSAC-80 and AAECC-6 Рим, июль, 1988.
8. Gustafson L. Hagberg. - Nucl. Instr. and Meth., 1988, v.A265, No.2, p.521.
9. Никитюк Н.М. ОИЯИ, Р10-87-254, Дубна.
10. Питерсон У., Уэлдон Э. - Коды, исправляющие ошибки, М.; Мир, 1976, с.302.
11. Оконо Н., Imai H. - IEEE Trans. on Comput., 1987, v. c-36, No.10, p.1165.
12. Berlekemp E.R. - IEEE Trans. on Inf. Theory, 1965, vol.IT-11, No.4, p.577.
13. Никитюк Н.М. Авт.свид. СССР № 1236457, - Опубликовано в ОИ, 1986, № 21, с.199.
14. Никитюк Н.М. Авт.свид. СССР № 1236458, - Опубликовано в ОИ, 1986, № 21, с.199.
    Никитюк Н.М., ОИЯИ, Р11-87-54, Дубна, 1987.
15. Gaidamaka R.I., Nikityuk N.M. JINR, E10-88-53, Dubna, 1988. Доклад на первой Объединенной конференции ISSAC-88 and AAECC-6, Рим, июль, 1988.
16. Никитюк Н.М. Авт.свид. СССР № 875408 - Опубликовано в ОИ, 1981, № 39, с.259.
17. Берликэмп Е.Р.- Алгебраическая теория кодирования. М.: "Мир", 1971, с.251.
18. Banerji R.B. - Proc. IEE, 1961, vol.49, No.10, p.1585.
19. Блох Э.Л. - Известия Академии наук СССР, Технич.кибернетика, 1964, № 3, с.20.
20. Polkingorn F. - IEEE Trans on Inf. Theory, 1966, v.12, No.4, p.480.
21. Chin-Long Chen. - IEEE Trans. on Information Theory, 1982, v.11-28, No.5, p.792.
22. Chien R.T., Cunningham - IEEE Trans. on Inf. Theory, 1969, v.IT-15, No.2, p.329.
23. Колесников В.Д., Мирончиков Е.Т. - Декодирование циклических кодов. М.: Связь , 1968, с.95.


Рукопись поступила в издательский отдел
12 декабря 1988 года.

## I. Введение

В связи с широким развитием алгебраических методов обработки цифровых сигналов /I,2/ и создаваемых для этих целей различного рода специализированных процессоров /4/ возникает необходимость в совершенствовании аппаратных методов выполнения операций в поле $GF(2^m)$. Это касается прежде всего таких операций, как умножение, деление и возведение в степень элементов поля $GF(2^m)$.
Выполнение подобных операций одновременно над двумя элементами не вызывает особых затруднений, и они довольно просто реализуются как на дискретных компонентах /3 - 6/, так и на основе ППЗУ /4,7,I0/.
В задачах, связанных с решением уравнения положения ошибок в процессе декодирования БЧХ-кодов и вычисления определителей приходится создовать схемы для вычисления сложных формул , содержащих большое количество сомножителей, находящихся под степенью. В работе /7/ операция умножения элемента А на сомножитель $(B)^2$ выполняется в два этапа . В начале вычисляется квадрат элемента В и затем с помощью схемы умножения получается произведение $A(B)^2$. В работах /5,6,8/ автором показано, что вычисление подобных и более сложных выражений в поле $GF(2^m)$ можно совместить в одном такте.
Например, в процессе решения уравнения третьей степени вычисляется формула /7/

$$Z = \frac{S_1^5 + S_5}{S_1^3 + S_3} \quad , \qquad (I)$$

где $S_1$ , $S_3$ , $S_5$ - синдром БЧХ-кода, исправляющего три ошибки. Поскольку в результате вычислений по формуле (I) должен получиться заведомо известный элемент поля, то ППЗУ можно запрограммировать таким образом, что при подаче на его входы значение синдрома можно получить правильный результат с задержкой, определяемой типом ППЗУ.
Другими словами, сложность вычислений алгебраических выражений в поле $GF(2^m)$ с использованием ППЗУ определяется количеством различных элементов, входящих в данную формулу. Причем отдельные члены выражения могут находиться под степенью.
Следует отметить, что для выполнения различного рода операций в поле $GF(2^m)$ нередко используются логарифмы /7,9/. В связи с появлением быстродействующих ППЗУ большой емкости методы вычислений над логарифмами элементов поля приобретают все более широкое применение в кодирующих и декодирующих устройствах БЧХ-кодов и в специализированных процессорах /I0/. Однако в этих работах используется такой алгоритм, в котором предусмотрено выполнение операций одно-

временно только над двумя элементами. В данной работе приводится описание быстрого алгоритма, с помощью которого можно выполнять операции одновременно над произвольным количеством сомножителей. Работа алгоритма поясняется с помощью предложенного автором устройства. Кроме того, рассмотрен вариант схемы умножения, построенной на основе ПЛМ.

## 2. Метод циклической компрессии

С целью наглядности и компактности изложения, а также учитывая, то, что алгебра Галуа носит модулярный характер, суть быстрого алгоритма рассмотрим на конкретном примере.

Рассмотрим поле $GF(2^4)$, образованное над неприводимым полиномом четвертой степени $X^4 \oplus^* X \oplus I$, ($m = 4$). При условии, что элемент a = 0I00 - корень этого полинома, пользуясь правилами выполнения операций над элементами в поле $GF(2^4)$ /9/, из уравнения $a^4 = a \oplus I$ получим I5 ненулевых элементов поля, которые приведены в таблице I слева. Здесь же справа даны их логарифмы по основанию a. Правила выполнения операций над логарифмами в поле $GF(2^m)$ мало чем отличаются (с учетом конечности поля) от операций над обычными числами.

Умножение двух элементов сводится к циклическому сложению их степеней по модулю $2^m - I$, а операция деления элемента A на элемент B эквивалентна сложению по модулю $2^m - I$ степени элемента A со степенью элемента $B^{-I}$, обратного к элементу B ($BB^{-I} = I$) с учетом обратного преобразования логарифмов в антилогарифмы.

Например, пусть элемент $A = a^7$ и элемент $B = a^{I0}$. Имеем

$\log_a a^7 = 0III$ и $\log_a a^{10} = I0I0$ (младший разряд справа). Складывая степени элементов A и B, получим

$$\begin{array}{r} 0III \\ +\ I0I0 \\ +\ \underset{\rightarrow}{\ \ I} \\ \hline 00I0 \end{array},$$

т.е. степень произведения $a^7 a^{I0}$ равна двум, так как $a^7 a^{I0} = a^{I5} a^2 = a^2$ в поле $GF(2^4)$.

Аналогично в случае деления имеем

$$\log_a A/B = \log_a A + \log_a (B^{-I}).$$

При ручных вычислениях удобно пользоваться правилом: для вычисления степени обратного элемента $B^{-I}$ к элементу B достаточно к величине $2^m - I$ прибавить по модулю два степень элемента B. Так, степень обратного элемента к элементу $a^{I0}$ равна пяти, так как $a^{10} \cdot a^5 = a^{15} = a^0$

*Знак $\oplus$ обозначает "Сумма" по модулю два.



$$\begin{array}{r} +\ IIII \\ +\ I0I0 \\ \hline 0I0I \end{array}.$$

Тогда $\log_a A/B$ равен

$$\begin{array}{r} +\ 0III \\ +\ 0I0I \\ \hline I\,I00 \end{array} = I2_{I0}.$$

Таблица I

| Элементы поля $GF(2^4)$ | Логарифмы по основанию a |
|---|---|
| $a^0 = I000$ | 0000 |
| $a^I = 0I00$ | 000I |
| $a^2 = 00I0$ | 00I0 |
| $a^3 = 000I$ | 00II |
| $a^4 = II00$ | 0I00 |
| $a^5 = 0II0$ | 0I0I |
| $a^6 = 00II$ | 0II0 |
| $a^7 = II0I$ | 0III |
| $a^8 = I0I0$ | I000 |
| $a^9 = 0I0I$ | I00I |
| $a^{I0} = III0$ | I0I0 |
| $a^{II} = 0III$ | I0II |
| $a^{I2} = IIII$ | I\,I00 |
| $a^{I3} = I0II$ | I\,I0I |
| $a^{I4} = I00I$ | IIII0 |
| $a^{I5} = a^0$ | IIII |

Чтобы существенно сократить время циклического суммирования степеней элементов поля при большом числе слагаемых автором предложены алгоритм циклической компрессии степеней и способ построения соответствующего устройства, которое является аналогом параллельного компрессора, применяемого в схемах ускоренного умножения обычных чисел /II,I2/. На рис. I приведены два примера, иллюстрирующие алгоритм работы циклического компрессора. Первый пример

слева соответствует одновременному умножению I5 элементов $a^0 = a^{I5}$ в поле $GF(2^4)$ или что то же самое, возведению в I5-ю степень элемента $a^0$. Процесс циклического суммирования (по модулю I5) четырехразрядных чисел можно условно разделить на пять этапов. На первом этапе в результате подсчета количества единиц в двоичном коде в каждом столбце I5 слагаемых сжимаются до четырех, Причем результат суммирования в нашем примере (IIII) записывается по диагонали, начиная с первого столбца справа. Вследствие этого старший разряд записывается под последним столбцом исходных чисел.

Аналогичная процедура выполняется на втором и третьем этапах суммирования. В конечном итоге из I5 слагаемых получается два, разделенных на две части. Причем вторая часть суммы (слево) представляет собой наибольшее число II0I0000, которое равно сумме переносов, возникающих в процессе циклической компрессии I5 слагаемых IIII. И, наконец, к значению 00I0 добавляется число II0I по модулю I5. На рис.I справа приведен пример для вычисления суммы степеней сомножителей

$$a^{I4}a^{I0}a^{9}a^{8}a^{7}a^{6}a^{5} = a^{59} = a^{45}a^{I4} = a^{I4}.$$

Рассмотренный пример сложения I5 элементов $a^0$ является одновременно диаграммой для построения принципиальной схемы соответствующего параллельного циклического компрессора. Под таким устройством будем понимать логическую схему комбинационного типа, с помощью которого $n$ слагаемых сжимаются до двух по правилам цмклического суммирования. Циклический компрессор имеет $m$ групп входов и $2m$ выходов, где $n = 2^m - I$. Он состоит из параллельных счетчиков и двух сумматоров по модулю 2 - I. Сокращенно такое устройство будем обозначать как

$[(2^m - I, 2m)]$ -компрессор.

На рис.2 приведена структурная схема $[(I5), 2\times4]$ -компрессора вместе с дополнительным сумматором и ППЗУ, с помощью которого получаются антилогарифмы. На этом рисунке не показаны схемы для вычичления логарифмов, которые, по существу, представляют собой ППЗУ, выходы которых имеют двоичные веса

$$2^0,\ 2^I,\ 2^2,\ \text{и}\ 2^3$$

и сгруппированы так, что шины с одинаковыми весами соединены со входами соответствующих им параллельных счетчиков. Как видно из рисунка, первый каскад компрессора состоит из четырех параллельных (I5,4)-счетчиков. Такие счетчики обычно используются в вычислительной технике /I3/ и в ядерной электронике /I4/.

Второй каскад компрессора состоит из группы (4,3)-, (3,2)- и (2,2)-счетчиков. Подобные счетчики проще всего создаются на основе полных сумматорах, которые представляют собой (3,2)-счетчики.



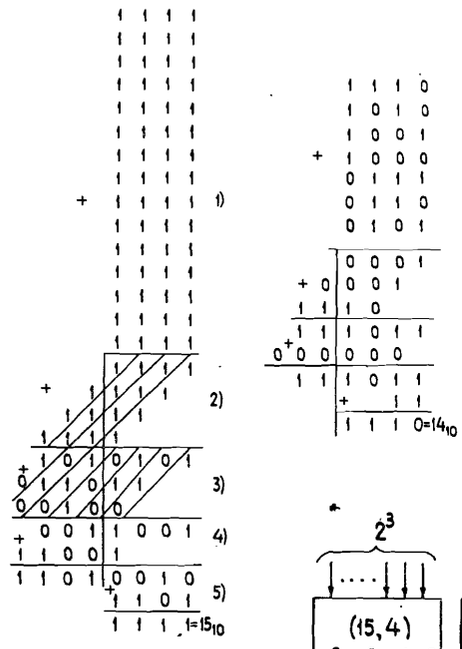


Рис.I. Пример для одновременного циклического суммирования I5 и 7 степеней элементов поля $GF(2^4)$.

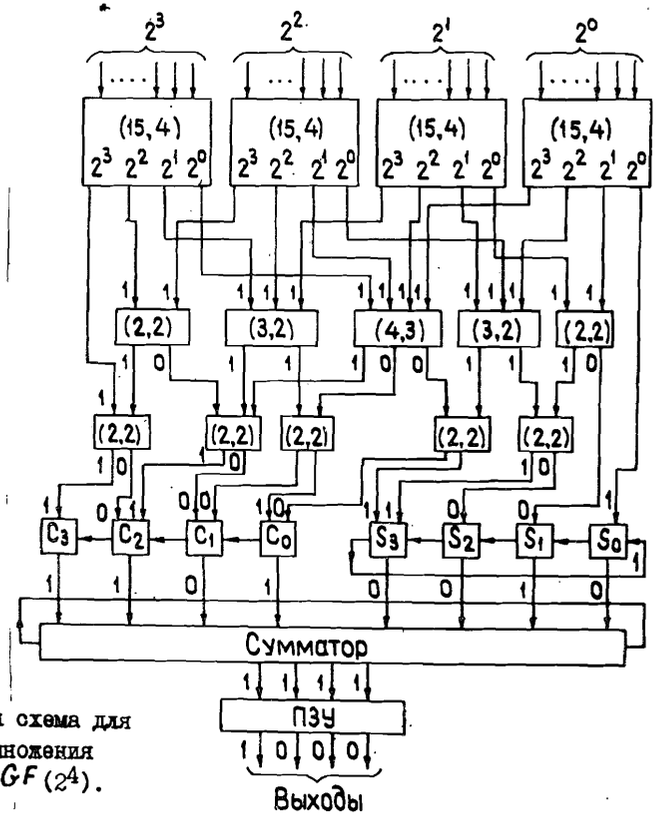


Рис.2.Структурная схема для одновременного умножения элементов в поле $GF(2^4)$.

Связи между входами данных счетчиков и выходами (I5,4)-счетчиков можно описать с помощью примера, приведенного на рис. I слева. Так, выход шины с весом $2^0$ первого (I5,4)-счетчика (крайний справа) подключен непосредственно к входу $S_0$ первого разряда циклического сумматора $S_0 - S_4$ по модулю I5. Далее, выход шины с весом $2^I$ этого же счетчика и выход с весом $2^0$ второго I(I5,4)-счетчика подключены к входам первого (справа) (2,2)-счетчика второго каскада, так как во втором столбце на второй позиции имеется две цифры, одна из которых получилась в результате суммирования цифр первого столбца, а вторая цифра получилась от суммирования второго столбца и т. д. Аналогично на третьем этапе суммирования выполняется сложение с переносом трех операндов.

Нетрудно заметить, что после третьего этапа получается всего два слагаемых, разделенных на две части, позиции и двоичные веса которых определяют связи между выходами (2,2)-счетчиков третьего каскада и входами двух сумматоров по модулю I5. С помощью сумматора $C_0 - C_3$ формируется общая сумма всевозможных циклических переносов (старшие четыре разряда). Вообще говоря, поскольку суммирование выполняется циклически, то количество слагаемых не имеет значения.

С помощью рассмотренного алгоритма можно эффективно вычислять относительно сложные выражения, например

$$\frac{A^p \cdot B^q \cdot C^z}{D^s \cdot E^t} = A^p \cdot B^q \cdot C^z (D^s)^{-1} \cdot (E^t)^{-1},$$

где A, B, C, D и E - произвольные элементы поля $GF(2^m)$. При этом предполагается, что для выполнения операции деления необходимо предварительно получить степени обратных элементов с помощью ППЗУ. Пользуясь соотношением для сложения двух элементов поля $a^i$ и $a^j$,

$$a^i + a^j = a^i (1 + a^{j-i}),$$

можно, не переходя обратно к антилогарифмам, выполнить сложение двух аналогичных выражений.

Следует отметить, что поскольку алгебра Галуа носит модулярный характер, то построение циклического компрессора при произвольных значениях $m$ можно выполнить по аналогии. Например, если $m = 5$, то следует составить диаграмму для циклического сложения 3I элемента поля $GF(2^5)$ и затем построить схему циклического компрессора. Для этих целей можно воспользоваться диаграммами, приведенными на рис. 3, которые являются аналогами примеров, приведенных на рис. I. С помощью таких диаграмм можно определить необходимое количество этапов суммирования M, состав и количество параллельных счетчиков, время суммирования и принципиальные схемы умножения для $m = 5 - 8$. Точками на рисунке обозначены двоичные цифры 0 или I.

Число каскадов параллельных счетчиков, необходимых для построения



циклического компрессора равно максимальному числу двоичных цифр в числе $m$. Так, при $m = 3 - 7$ M = 3, а при $m = 8 - I5$ M = 4.

Время $T_y$, необходимое для одновременного умножения 2 - I сомножителей, включая и время, требуемое для вычисления логарифмов и антилогарифмов, можно вычислить из выражения

$$T_y = 2T_п + (T_{CI} + T_{C2} + \dots + T_{CM}) + 2T_S, \qquad (2)$$

где $T_п$ - задержка в ППЗУ, используемом для преобразования кодов, $T_S$ - время суммирования по модулю $2^m - I$, и в скобках указаны задержки в параллельных счетчиках. Для определенности положим, что для построения схемы умножения используются микросхемы 500-й серии, в состав которой входят: микросхема К500ИМI80, содержащая два полных одноразрядных сумматора в одном корпусе, микросхема К500ИПI79 - схема ускоренного переноса с задержкой 2 нс и ППЗУ К500РЕI49, время преобразования кодов которого не превышает 20 нс. Причем время задержки сигналов на выходах "Сумма" и "Перенос" у микросхемы К500ИМI80 составляют 4,5 и 2,2 нс соответственно. В табл. 2 приведены данные о временах задержки и количество корпусов микросхем К500ИМI80, необходимых для построения параллельных счетчиков /I5/.

Таблица 2

Параметры некоторых параллельных счетчиков

| Счетчик / Параметр | 3,2 | 4,3 | 5,3 | 6,3 | 7,3 | I5,4 | 3I,5 | 63,6 | I27,7 |
|---|---|---|---|---|---|---|---|---|---|
| Число микросхем К500ИМI80 | 0,5 | I,5 | 2,0 | 2,0 | 2,0 | 5,5 | I3,0 | 28,5 | 60 |
| Задержка $T_{CM}$, нс | 4,5 | II,2 | II,2 | II,2 | II,2 | I7,9 | 24,6 | 3I,3 | 40 |

Допустим, что время циклического суммирования T с учетом переноса при $m = 4 - 8$ равно 6,5 8,5 8,5 8,5 8,5 нс соответственно.

В табл. 3 приведены параметры схем умножения для $m = 4 - 8$. Величина $T_y$ вычислена в соответствии с равенством (2).

Основная часть от общего количества сумматоров, необходимых для построения схемы умножения, приходится на первый каскад, состоящий из $(n, к)$-счетчиков (около 80%). Известно, что для построения $(n, к)$-счетчика требуется $S_{n,к}$ сумматоров /I3 -I5/:

$$S_{n,к} = (2^m - 1) - K.$$

Таблица 3

Параметры схем умножения для $m = 4 \div 8$

| Параметр \ $m$ | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|
| Количество корпусов К500ИМ180 | 34 | 8I,5 | I84 | 445 | II00 |
| $T_y$, нс | 86,6 | 97,3 | I04,0 | II4,0 | I26,0 |

| × | $a^0$ | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
|---|---|---|---|---|---|---|---|
| $a^0$ | $a^0$ | $a^2$ | $a^4$ | $a^6$ | $a^1$ | $a^3$ | $a^5$ |
| $a^1$ | $a^2$ | $a^4$ | $a^6$ | $a^1$ | $a^3$ | $a^5$ | $a^0$ |
| $a^2$ | $a^4$ | $a^6$ | $a^1$ | $a^3$ | $a^5$ | $a^0$ | $a^2$ |
| $a^3$ | $a^6$ | $a^1$ | $a^3$ | $a^5$ | $a^0$ | $a^2$ | $a^4$ |
| $a^4$ | $a^1$ | $a^3$ | $a^5$ | $a^0$ | $a^2$ | $a^4$ | $a^6$ |
| $a^5$ | $a^3$ | $a^5$ | $a^0$ | $a^2$ | $a^4$ | $a^6$ | $a^1$ |
| $a^6$ | $a^5$ | $a^0$ | $a^2$ | $a^4$ | $a^6$ | $a^1$ | $a^3$ |

| B \ A | $a^0$ | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
|---|---|---|---|---|---|---|---|
| $a^0$ | $a^0$ | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
| $a^1$ | $a^6$ | $a^0$ | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ |
| $a^2$ | $a^5$ | $a^6$ | $a^0$ | $a^1$ | $a^2$ | $a^3$ | $a^4$ |
| $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^0$ | $a^1$ | $a^2$ | $a^3$ |
| $a^4$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^0$ | $a^1$ | $a^2$ |
| $a^5$ | $a^2$ | $a^3$ | $a^7$ | $a^5$ | $a^6$ | $a^0$ | $a^1$ |
| $a^6$ | $a^1$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^0$ |

Рис. 3. Таблицы-диаграммы для расчета быстродействия и количества микросхем, необходимых для создания циклического компрессора при $m = 5 - 8$.

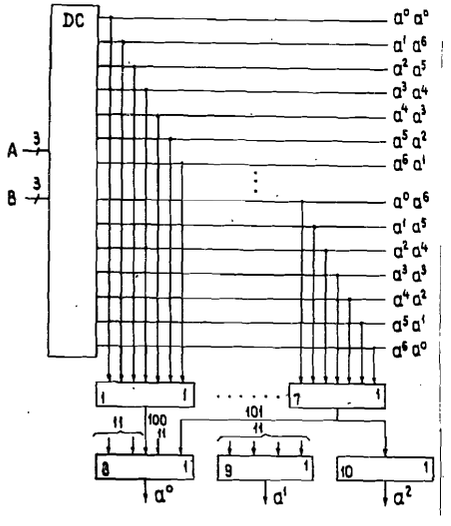


Рис. 4. Таблицы умножения и деления в поле $GF(2^3)$.



Тогда количество одноразрядных сумматоров, необходимых для создания первого каскада, равно

$$C = [(2^m - 1) - K]m .$$

Так, при $m = 7$ $C = 840$.

## 3. Применение программируемых логических матриц

Известно, что программируемые матрицы (ПЛМ), как правило, имеют большее число входов для переменных, нежели ППЗУ. Кроме того, в силу своей структуры ПЛМ потребляют сравнительно небольшую мощность и хорошо приспособлены для выполнения различного рода операций в поле $GF(2^m)$. На рис. 4 а и б приведены таблицы умножения и деления двух элементов в поле $GF(2^3)$. Это поле образовано над неприводимым полиномом

$$X^3 + X + I.$$

При условии, что элемент a = 0I0 - корень этого полинома и $a^0$ = I00, a = 0I0, - $a^2$ = 00I - базис поля, остальные четыре ненулевых элемента имеют следующие значения: $a^3$ = II0, $a^4$ = 0II, $a^5$ = III и $a^6$ = I0I.

Как и следовало ожидать, в силу конечности поля Галуа, таблицы, приведенные на рис. 4, идентичны с точностью до перестановки элементов. Более того, если составить такие таблицы для сложных выражений, содержащих сомножители под степенью, то получатся аналогичные таблицы. Другими словами, если для выполнения совмещенных операций использовать ПЛМ, то сложность логической структуры матрицы не будет зависеть от сложности реализуемого выражения.

На рис. 5 приведена блок-схема ПЛМ, запрограммированная для выполнения операции умножения двух элементов в поле $GF(2^3)$. Схема состоит из дешифратора, содержащего 49 выходов, которые сгруппированы по семь шин в группе, таких, что на них получаются одинаковые значения произведения двух элементов. Далее соответствующие группы шин объединены с помощью логических элементов ИЛИ I - 7. Вторая группа элементов ИЛИ 8- I0 образует шифратор элементов в поле $GF(2^3)$. Цифрой II обозначены те входы логических элементов, которые подключены к соответствующим выходам элементов ИЛИ I - 7.

Например, если результат операции равен $a^6 = a^0 + a^2$, то выход логического элемента ИЛИ 7 соединен со входами логических элементов 8 и I0. Поэтому на выходах логических элементов 8 - I0 формируется значение I0I. Если ПЛМ имеет I8 входов для переменных, то таким способом можно запрограммировать одновременное умножение до шести сомножителей, в том числе и таких, которые находятся под степенью.

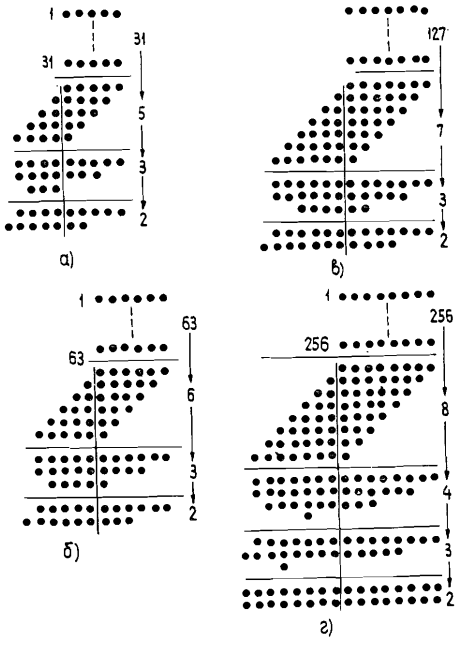


Рис.5. Структурная схема ПЛМ, запрограммированная для выполнения операции умножения двух элементов в поле $GF(2^3)$.

## Заключение

Имеют существенное преимущество предложенный автором алгоритм, а также устройство для выполнения одновременного умножения множества элементов поля $GF(2^m)$ по сравнению с известным /9/, при помощи которого такая процедура выполняется программно управляемым процессором. Циклический компрессор может найти применение в кодирующих и декодирующих устройствах /I6/, в вычислительной технике, а также в таком важном направлении в современном приборостроении, как сигнатурный анализ /I7/ и синтез переключательных функций, где в качестве переменных используются элементы в поле Галуа $GF(2^m)$ /I8 - 2I/.

## Литература


I. Блейхат Р.Э. Алгебраические поля, обработка сигналов, контроль ошибок. ТИИЭР, I985, т. 73. № 5, с. 30 - 53.

2. Вариченко Л.В., Лабунец В.Г., Раков М.А. Абстрактные алгебраические системы и цифровая обработка сигналов. "Наукова думка", Киев, I986, 247 с.





3. Bartee T..C., Schneider P.I. Computation with finite fields. Information and Control,1963, vol. 6., N 1, p.79.

4. Никитюк Н.М. Специализированный процессор с алгебраической структурой для быстрого отбора физических событий. Препринт ОИЯИ № PIO-87-254, Дубна, I987, I9.с.

5. Никитюк Н.М. Устройство для умножения и возведения в степень двух элементов в поле Галуа $GF(2^m)$. Авт. свид. СССР № I236457. Бюллетень ОИ, I986, № 2I, с. I99.

6. Никитюк Н.М. Устройство для выполнения операций возведения в степень, деления и умножения двух элементов в поле Галуа $GF(2^m)$. Авт. свид. СССР № I236458. Бюллетень ОИ, I986, № 2I, с. I99.

7. Okano H., Imai H. A Construction Method of high-speed decoders using ROM's for Bose-Chaudhuri-Hocquenghem and Reed-Solomon codes. IEEE Transaction on Computers., 1987, vol. C-36, No.10, p. 1165-1171.

8. Никитюк Н.М. Совмещенные операции в поле Галуа $GF(2^m)$. Препринт ОИЯИ № PII - 87 - 54, Дубна, I987, I4 с.

9. Берликэмп Э. Алгебраическая теория кодирования. "Мир", М.,I97I, С. 58.

I0. Устройство для обработки цифровых слов, являющихся элементами поля Галуа. Изобретения в СССР и за рубежом, I983, № 9, с. 62. Заявка № 006I345, ЕПВ кл. G 06 F II/I0.

II. Ho I.T., Chen T.C. A multiple addition by residue threshold functions and Their representation by array logic. IEEE on Comput., 1973, vol.C-22, No.8, 1973, p.762-767.

I2. Dormido S., Canto M.A. Parallel Compessors. IEEE Trans. on Computers, 1980, vol. C-30, No.5, p.393

I3 Swartzlander E. Parallel counters, IEEE Trans. on Computers, 1973, vol. C-22, No.11, p.1021.

I4. Гуськов Б.Н., Калинников В.А., Максимов А.Н., Крастев В.Р., Никитюк Н.М. Быстродействующий параллельный счетчик. ПТЭ, I984, № 6, с. 9I - 94.

I5. Никитюк Н.М. Быстрые и экономичные алгоритмы для специализированных процессоров. Регистрация суммарного сигнала в калориметрах. Препринт ОИЯИ, № PIO - 88 - 24I, Дубна, I988, I2 с.

I6. Shao H.M., Truong T.K., Deutch L.J et al. A VLSI design of a pipeline Reed-Solomon decoder. IEEE Transactions on Computers, 1985, vol. C-34, No.5, p.393-403.

17. Смирнов Н.И., Стручков А.А., Судовцев В.А. Диагностика неисправностей в цифровой радиоаппаратуре на БИС. Зарубежная радиоэлектроника, I979, № I, С.53-60.

18. Benjauthrit B., Reed I. Galois switching functions and their Applications. IEEE Transactions on Computers, 1976, vol.C-25, No.1, p.78-86.
19. Pradham D.K. A theory of Galois switching functions. IEEE Transactions on Computers, 1978, vol. C-27, No.3, p.239-248.
20. Александров И.Н., Гайдамака Р.И., Никитюк Н.М., Шириков В.П. Расчет переключательных функций, представленных элементами поля Галуа $GF(2^m)$. Препринт ОИЯИ № Р10-84-865, Дубна, 1984.
21. Gaidamaka R.I., Nikityuk N.M. Application of analytical transformations and calculations on coputers for synthesis of switching functions and solution of the problem of devising universal dynamically programmed logic modules. E10-88-53, 16p. Dubna, 1988, Доклад на I Объединенной конференции ААЕСС-6 и ISSAC-88, Рим, июнь, 1988.

Рукопись поступила в издательский отдел
12 декабря 1988 года.



Никитюк Н.М. P11-88-852

Быстрый алгоритм для выполнения операции умножения в поле Галуа $GF(2^m)$

Описан быстрый алгоритм выполнения операции умножения одновременно над многими элементами в поле Галуа $GF(2^m)$, представляемыми в виде логарифмов. Суть алгоритма основана на методе параллельной компрессии данных, который используется в схемах быстрого умножения обычных чисел. Эффективность алгоритма рассматривается на конкретном примере схемы для одновременного умножения 15 элементов в поле $GF(2^m)$. Предлагаемая схема умножения является базовой для выполнения таких операций, как деление и возведение в степень. В качестве элементной базы используются ППЗУ и ПЛМ.

Работа выполнена в Лаборатории высоких энергий ОИЯИ.

**Препринт Объединенного института ядерных исследований. Дубна 1988**

Перевод О.С.Виноградовой

Nikityuk N.M. P11-88-852

Fast Algorithms for Execution of Multiplication Over Galois Field $GF(2^m)$

A fast algorithm for execution of multiplication over Galois field $GF(2^m)$ elements simultaneously represented as algorithms is described. Essence of the algorithm is based on data parallel compression method which is used in schemes of fast multiplication of common numbers. Efficiency of the algorithm is considered on a concrete example of the scheme for simultaneous multiplication of 15 elements of the Galois field $GF(2^m)$ elements. The proposed multiplication scheme is a based for execution of such operations as division and raising of power PROM and PLA serve as element base.

The investigation has been performed at the Laboratory of High Energies, JINR.

**Preprint of the Joint Institute for Nuclear Research. Dubna 1988**