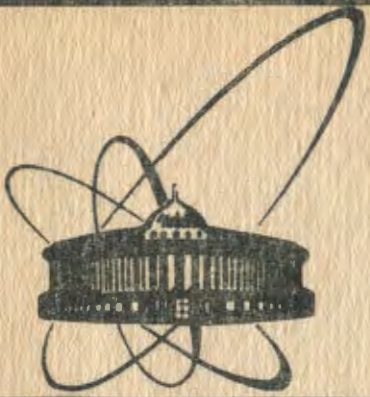


сообщения
объединенного
института
ядерных
исследований
дубна

Р10-89-16

Н.М.Никитюк

БЫСТРЫЕ АЛГОРИТМЫ ДЛЯ КООРДИНАТНЫХ ПРОЦЕССОРОВ В ПОЛЕ ГАЛУА ДЛЯ МНОЖЕСТВЕННОСТИ $t = 4,5$ И $t > 5$

1989

1. ПОСТАНОВКА ЗАДАЧИ

В работе[1] были описаны быстрые методы решения определителей 1 ÷ 4-го порядков и координатных уравнений второй и третьей степени в поле Галуа $GF(2^m)$, используемые для построения мажоритарных схем совпадений и специализированных процессоров для спектрометров физики высоких энергий.

При этом рассматривались методы решения при множественности $1 < t \leq 3$. Как это следует из ряда работ по теории алгебраического кодирования[2,3], методы табличного решения уравнений второй и третьей степени являются базовыми для аппаратного решения уравнений четвертой и пятой степени. В данной работе алгоритмы для решения уравнений для $t = 4$ и 5 представлены таким образом, что для запоминания таблиц решений достаточно использовать быстродействующие ППЗУ и ПЛМ, содержащие $2m$ входов для переменных.

Координаты сработавших позиционно-чувствительных датчиков многоканального детектора заряженных частиц находятся из уравнений

$$\sigma(X) = X^t + \sigma_1 X^{t-1} + \sigma_2 X^{t-2} + \ldots \sigma_t . \qquad (1)$$

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 описывается с помощью уравнений Ньютона[4,5]

$$\begin{bmatrix} S_1 & 1 & 0 & 0 & \ldots\ldots & 0 \\ S_3 & S_2 & S_1 & 1 & & \\ \vdots & & & & \ddots & \\ S_{2t-3} & & & & & \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix} \qquad (2)$$

С использованием метода трансформации переменных[4] в работе[1] получены следующие соотношения для множественности $t = 4$ регистрируемых сигналов:

$$\sigma_3 = R_3 + R_1\sigma_2, \qquad (3)$$

$$\sigma_4 = \frac{R_7 + R_5\sigma_2}{R_3},$$

причем значения $R_1 - R_{11}$ равны[5]

$$R_1 = S_1,$$

$$R_3 = S_3 + S_1^2 S_1,$$

$$R_5 = S_5 + S_1^2 S_3, \qquad (4)$$

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

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

$$R_{11} = S_{11} + S_1^2 S_9 + S_3^2 S_5 + S_1^6 S_5 + S_1 S_5^2 + S_1^5 S_3^2.$$

Наиболее трудоемким является процесс вычисления элементарных симметрических функций σ_t. Однако метод трансформации переменных[1,4] позволяет по найденному значению σ_2, которое вычисляется относительно просто, затем по формулам (3) определить значения σ_3 и σ_4.

С практической точки зрения такой подход позволяет рационально построить координатный процессор при $t \leq 4$.

2. ТАБЛИЧНЫЙ МЕТОД РЕШЕНИЯ КООРДИНАТНОГО УРАВНЕНИЯ ЧЕТВЕРТОЙ СТЕПЕНИ

Значение σ_2 при $t \leq 4$ равно[1,3]

$$\sigma_2 = \frac{S_1^8 + S_1^7 + S_1^5 S_3 + S_3 S_5}{S_1^6 + S_1 S_5 + S_1^3 S_3 + S_3^2},$$

или в сокращенной записи

$$\sigma_2 = \frac{S_1^8 + T + S_1^5 S_3 + S_3 S_5}{R + G + H + L}, \qquad (5)$$

где значения R, G, H и L вычисляются заранее при определении множественности[1]. Так, $R = S_1^6$, $G = S_1 S_5$ $H = S_1^3 S_3$, $T = S_1 S_7$ и $L = S_3^2$.

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 Галуа $GF(2^6)$, образованными над неприводимым полиномом $X^6 + X + 1$. Таблица 63 ненулевых элементов $GF(2^6)$ дана в приложении /1/. Матрица проверочных соотношений $H^T_{63,30}$ в сокращенной записи, достаточной для решения примеров, имеет вид

$$H^T_{63,30} = \begin{bmatrix} *100000 & 100000 & 100000 & 100000 & 100000 \\ *010000 & 000100 & 000001 & 011000 & 000110 \\ *001000 & 110000 & 000011 & 001010 & 111100 \\ *000100 & 000110 & 000101 & 110111 & 011100 \\ 000010 & 101000 & 001111 & 001110 & 011010 \\ *000001 & 000101 & 010001 & 110100 & 100110 \\ \vdots & & & & \\ 100001 & 100111 & 111111 & 111110 & 111010 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ S_1 & S_3 & S_5 & S_7 & S_9 \end{bmatrix} \begin{matrix} a^0 \\ a^1 \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ \\ a^{62} \\ \\ \end{matrix}$$

Символом * обозначены сработавшие датчики, причем при $t = 4$ достаточно использовать значения S_1, S_3, S_5 и S_7. Допустим, что сработали датчики с координатами $X_1 = a^0$, $X_2 = a^2$, $X_3 = a^0$ и $X_4 = a^5$. Полностью все 63 элемента поля $GF(2^6)$ даны в приложении /1/. Тогда имеем

$$S_1 = \sigma_1 = X_1 + X_2 + X_3 + X_4,$$

или

$$\begin{array}{l} 100000 \\ +\ 001000 \\ +\ 000100 \\ +\ 000001 \\ \hline 101101 \end{array} \quad \text{mod } 2$$

Из приложения /1/ получим $101101 = a^{44}$.

Аналогичные вычисления для $S_3 = X_1^3 + X_2^3 + X_3^3 + X_4^3$, $S_5 = X_1^5 + X_2^5 + X_3^5 + X_4^5$ и $S_7 = X_1^7 + X_2^7 + X_3^7 + X_4^7$ дают $S_3 = a^{46}$; $S_5 = a^{21}$; и $S_7 = a^{31}$ (см. $H^T_{63,30}$).

Далее из (5) имеем $\sigma_2 = a^7$. Подставляя значение σ_2 в равенство (3), получим

$\sigma_3 = a^{49}$, $\sigma_4 = a^{10}$

с учетом значений

$R_1 = S_1 = \sigma_1 = a^{44}$, $R_3 = a^{61}$, $R_5 = a^{43}$; $R_7 = a^{29}$.

В результате уравнение (1) при $t = 4$ имеет вид

$$X^4 + a^{44} X^3 + a^7 X^2 + a^{49} X + a^{10} = 0. \qquad (6)$$

Можно проверить, что корнями уравнения (6) являются координаты X_1, X_2, X_3 и X_4.

4. АЛГОРИТМ ВЫЧИСЛЕНИЯ КООРДИНАТ ПРИ $t = 4$

При $t = 4$ уравнение имеет вид

$$\sigma(X) = X^4 + \sigma_1 X^3 + \sigma_2 X^2 + \sigma_3 X + \sigma_4 . \qquad (7)$$

Автором было исследовано два подхода к решению уравнения (7) табличным методом [2,3]. Расчеты показали, что при использовании алгоритма, описанного в работе [3], возникают неопределенности при выборе координат квадратных уравнений, получаемых в процессе решения.

Путем подстановки $X = (1/y + (\sigma_3 / \sigma_1))^{1/2}$ получим

$$f(y) = \sigma_0' y^4 + \sigma_2' y^2 + \sigma_3' y + \sigma_4' , \qquad (8)$$

где

$$\sigma_0' = \sigma_3^2/\sigma_1^2 + \frac{\sigma_2\sigma_3}{\sigma_1} + \sigma_4 = A/\sigma_1^2, \qquad (9)$$

$$\sigma_1' = 0$$

$$\sigma_2' = \sigma_2 + (\sigma_1\sigma_3)^{1/2} = \sigma_2 + \sqrt{\sigma_1 B + \sigma_1^2\sigma_2} , \qquad (10)$$

$$\sigma_3' = \sigma_1 ,$$

$$\sigma_4' = 1 .$$

Если ввести еще одну подстановку $y = (\sigma_2' / \sigma_0)^{1/2} z$, то получим

$$g(X) = Z^4 + Z^2 + Cz + D , \qquad (11)$$

где

$$C = (\sigma_3' \sigma_0^{1/2}) / \sigma_2'^{3/2} = A/\sqrt{\sigma_2^3}, \tag{12}$$

$$D = \sigma_0' / \sigma_2'^2 = A / \sigma_1^2 C_2^2. \tag{13}$$

Поскольку $t = 4$, то уравнение (7) должно иметь четыре различных корня, поэтому имеем

$$g(X) = (Z^2 + \alpha Z + \beta_1)(Z^2 + \alpha Z + \beta_2), \tag{14}$$

где

$$\begin{aligned} &\alpha^2 + \beta_1 + \beta_2 = 1, \\ &\alpha(\beta_1 + \beta_2) = C, \\ &\beta_1 \beta_2 = D. \end{aligned} \tag{15}$$

Из первых двух уравнений получим $\alpha^3 + \alpha + C = 0$, которое решается табличным методом, при известных значениях α и β находятся из равенств

$$\beta_1^2 + C/\alpha \cdot \beta_1 + D = 0; \quad \beta_1^2 + (1 + \alpha^2)\beta_1 + D = 0. \tag{16}$$

Эти квадратные уравнения решаются табличным методом. Поэтому в конечном итоге решения уравнения (7) сводятся также к табличным методам. Продолжим рассмотрение численного примера.

Из формул (9), (12), (13) имеем

$$\sigma_0' = (a^{49})^2 / a^{88} = a^{12}$$

$$\sigma_2' = a^{55}$$

$$C = a^{62}$$

$$D = a^{28}$$

В результате таких промежуточных вычислений получаем уравнение третьей степени

$$\alpha^3 + \alpha + a^{62} = 0.$$

Из таблицы[1] находим $\alpha_1 = a^{37}$ и $\alpha_2 = a^{39}$. Тогда уравнение (16) можно записать в виде

$$\beta_1^2 + a^{25}\beta_1 + a^{28} = 0. \qquad (17)$$

Решения квадратного уравнения (17) дают

$$\beta_1 = a^{13} \quad \text{и} \quad \beta_2 = a^{15}.$$

В результате получаем два квадратичных уравнения для вычисления $Z_1 \div Z_4$

$$Z^2 + a^{37}Z + a^{13} = 0,$$

$$Z^2 + a^{37}Z + a^{15} = 0,$$

и далее

$$y_1 = a^{32}; \quad y_2 = a^{26}; \quad y_3 = a^{61} \text{ и } y_4 = a^{53},$$

$$X_1 = a^0; \quad X_2 = a^3; \quad X_3 = a^5 \text{ и } X_4 = a^2.$$

Полученные значения X_i соответствуют координатам сработавших позиционно-чувствительных датчиков.

На рис. 1 приведена блок-схема координатного процессора для $t = 4$. Схема составлена таким образом, чтобы для вычисления соответствующих промежуточных значений можно было применить ППЗУ, имеющие $2m$ входов для переменных. Кроме того, здесь также эффективно используется метод выполнения совмещенных операций в поле Галуа $GF(2^m)$. Например, такие выражения, как $(C_3/C_1)^{1/2}$ и $(C_2/C_0)^{1/4}$, вычисляются соответственно с помощью одного ППЗУ. Максимальное время решения уравнения четвертой степени можно вычислить из формулы

$$T_4 = 9T_{ППЗУ} + T_2 + T_3 + 2T_c,$$

где $T_{ППЗУ}$ — задержка в ППЗУ, T_2 и T_3 — время решения квадратного и кубического уравнений соответственно, T_c — время суммирования по модулю два.

Если применить микросхемы 500 серии, то время решения T_4 составит ≈ 320 нс.

ТАБЛИЧНЫЙ МЕТОД РЕШЕНИЯ КООРДИНАТНОГО УРАВНЕНИЯ ПЯТОЙ СТЕПЕНИ

Координатное уравнение пятой степени имеет вид

$$\sigma(X) = X^5 + \sigma_1 X^4 + \sigma_2 X^3 + \sigma_3 X^2 + \sigma_4 X + \sigma_5, \qquad (18)$$

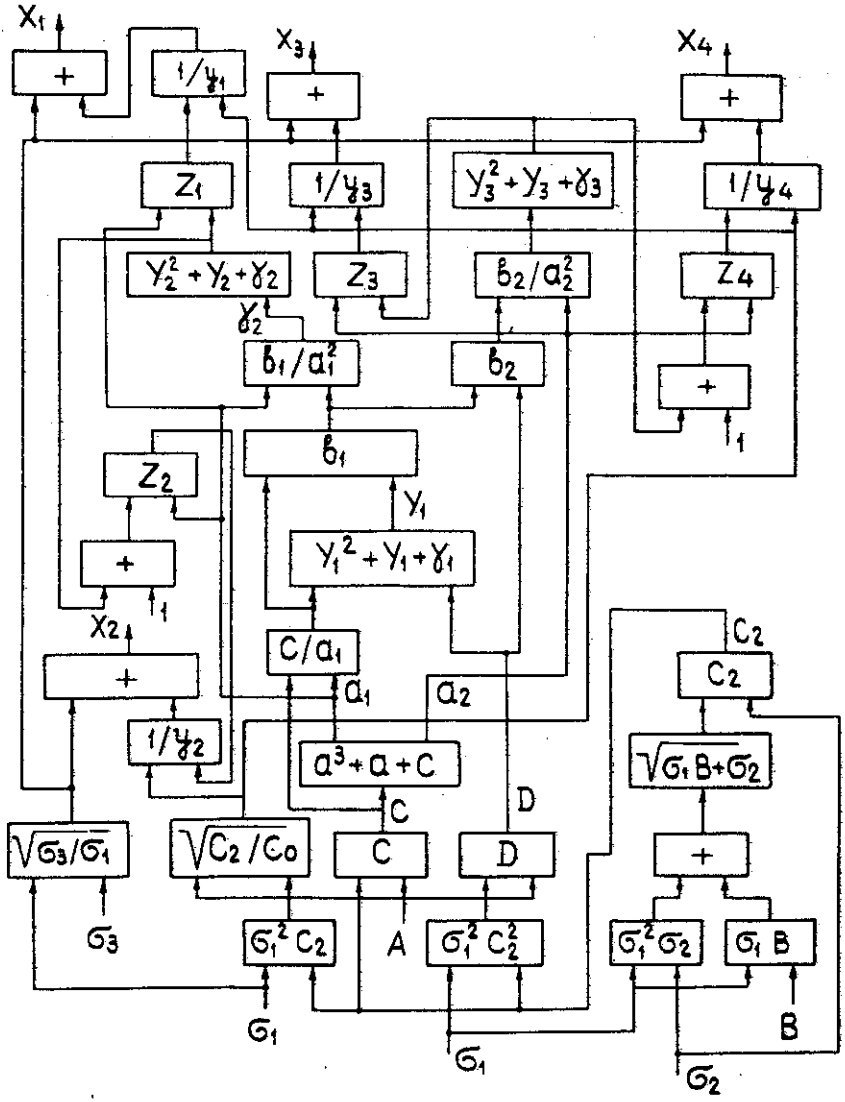


Рис. 1. Блок-схема решения координатного уравнения четвертой степени в поле Галуа GF (2^m) .

где значение σ_2 при $t = 5$, вычисленное из (2), равно

$$\sigma_2 = \frac{S_5S_7 + S_1^2S_5^2 + S_1S_3^2S_5 + S_1^7S_5 + S_1^4S_3S_5 + S_1^3S_9 + S_1^5S_7 + S_3S_9 + S_1^{16} + S_1^6S_3^2}{S_3S_7 + S_1^2S_3S_5 + S_1S_3^3 + S_1^7S_3 + S_7S_1^3 + S_1^5S_5 + S_1^{10} + S_5^2}.$$

Методом трансформации переменных[1] получены следующие соотношения для σ_3, σ_4 и σ_5 при известном σ_2 ($\sigma_1 = S_1$):

$$\sigma_3 = R_3 + R_1\sigma_2; \quad \sigma_4 = \frac{R_7 + R_5\sigma_2}{R_3}; \quad \sigma_5 = R_5 + R_3\sigma_2 + R_1\sigma_4.$$

Путем подстановки $X = y + v$ уравнение (18) приводится к виду

$$f(y) = y^5 + \sigma y^3 + Hy^2 + Iy + r,$$

$$G = \sigma_2; \; H = \sigma_1\sigma_2 + \sigma_3; \; I = \sigma_1\sigma_2 + \sigma_4; \; r = \sigma_1^5 + \sigma_1^2\sigma_3 + \sigma_1\sigma_4 + \sigma_5. \qquad (19)$$

Если равенство имеет пять различных корней, то его можно представить в виде

$$f(y) = (y^3 + vy^2 + by + c)(y^2 + vy + d),$$

где

$$G = v^2 + b + d; \; H = vd + vb + c; \; I = bd + vc;$$

$$J = cd.$$

Более детально аппаратный метод решения уравнения пятой степени см. в[2].

ГИБРИДНЫЙ МЕТОД РЕШЕНИЯ КООРДИНАТНОГО УРАВНЕНИЯ ПРИ $t > 5$

Табличные методы решения координатного уравнения (1) при $t > 5$ автору неизвестны. Для решения полиномов, степень которых превосходит шесть, в работе[2] описан гибридный метод, который предлагается использовать для нахождения координат позиционно-чувствительных детекторов. Рассматриваемый метод базируется на следующей теореме "Об орбите", доказательство которой приводится в[2].

Теорема. Пусть имеются полиномы $\sigma(X)$ и $\sigma'(X)$ над полем $GF(2^m)$:

$$\sigma(X) = X^t + \sigma_1 X^{t-1} + \sigma_2 X^{t-1} + \ldots \sigma_t, \qquad (20)$$

$$\sigma'(X) = X^t + \sigma_1^2 X^{t-1} + \sigma_2^2 X + \ldots \sigma_t^2. \qquad (21)$$

Если β — элемент расширения поля $GF(2^m)$, то β есть корень полинома $\sigma(X)$ тогда и только тогда, когда β^2 есть корень $\sigma'(X)$. Суть теоремы и ее практическое применение рассмотрим на конкретном примере.

Причем с целью упрощения изложения рассматриваем полином пятой степени

$$\sigma(X) = X^5 + a^{40}X^4 + a^{56}X^3 + a^{36}X^2 + a^2X + a^{11}. \qquad (22)$$

Тогда

$$\sigma(X) = X^5 + a^{17}X^4 + a^{49}X^3 + a^9X^2 + a^4X + a^{22}. \qquad (23)$$

в соответствии с теоремой "Об орбите", поскольку $\sigma(X)$ и $\sigma'(X)$ имеют по крайней мере один общий корень. Поэтому у них должен быть наиболее общий делитель (НОД), степень которого отлична от нуля. В соответствии с алгоритмом Евклида НОД полиномов (22) и (23) равен

$$f(X) = a^{20}X^2 + a^{32}X + a^{22}. \qquad (24)$$

Полином $f(X)$ получен путем деления полинома (22) на полином (23), в поле Галуа $GF(2^m)$.

Как нетрудно проверить, корнями полинома (24) являются элементы поля $GF(2^6)$ a° и a^2. Так, при $X_1 = a^\circ$ имеем

$$a^{20} + a^{32} + a^{22} = 0.$$

Далее, разделив полином (22) на полином (24), получим

$$P(X) = X^3a^{43} + X^2a^{33} + a^{36}X + a^{52} =$$

$$= X^3 + a^{53}X^2 + a^{56}X + a^9. \qquad (24')$$

Корни уравнения (24), как известно, решаются методами табличной арифметики. Таким образом, для решения координатных уравнений степени более чем пять гибридным способом необходимо создание быстродействующего специализированного процессора для вычисления НОД и деления в поле Галуа $GF(2^6)$.

ПОСЛЕДОВАТЕЛЬНЫЙ МЕТОД РЕШЕНИЯ КООРДИНАТНОГО УРАВНЕНИЯ В ОБЩЕМ ВИДЕ

Для нахождения координат сработавших позиционно-чувствительных детекторов по методу Питерсона наряду с вычислением значений требуется t схем умножения в возведения в степени переменных с последующим анализом равенства (1) на "о".

В работе [7] с целью упрощения декодирования БЧХ-кодов предложен более экономичный алгоритм для решения координатного уравнения (1), в котором эффективно используется циклический характер по-

ля Галуа. Чаще всего значения σ_t выражаются через значения S_j. Однако известны и другие представления σ_t через корни β_j уравнения (1)

$$\sigma_1 = \sum_{j=1}^{t} X_j,$$

$$\sigma_2 = \sum_{\substack{j,k=1 \\ j<k}}^{t} X_j \cdot \beta_k, \quad \sigma_3 = \sum_{i,j,k=1}^{t} \beta_i \beta_j \beta_k. \tag{25}$$

Так, при $t = 3$, имеем

$$\sigma_1 = X_1 + X_2 + X_3, \quad \sigma_2 = X_1X_2 + X_1X_3 + X_2X_3; \quad \sigma_3 = X_1X_2X_3. \tag{26}$$

Основным свойством равенств (26) является то, что их значение не зависит от того, какую координату X_1, X_2 и X_3 следует считать первой, второй или третьей, так как существенным является не порядок индексов X_j, а их значение. Например, если $X_1 = a^\circ$, $X_2 = a^1$ и $X_3 = a^2$ в поле $GF(2^4)$, то значение $\sigma_1 \div \sigma_3$ не изменяется при перестановке индексов 1, 2 и 3 в значениях $X_1 \div X_3$. Такое свойство σ_t положено за основу описываемого алгоритма.

Путем трансформации $X_j = aX_j$ получаем следующее уравнение

$$\sigma(X) = X^t + \tilde{\sigma}_1 X^{t-1} + \tilde{\sigma}_2 X^{t-2} + \ldots \tilde{\sigma}_t, \tag{27}$$

где

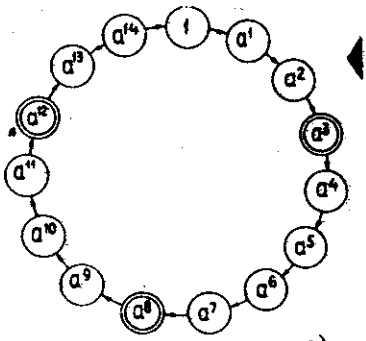
$$\tilde{\sigma}_k = a^k \sigma_k, \quad k = 1,2,\ldots t. \tag{28}$$

В общем виде после τ трансформаций (τ — число циклических сдвигов) получим

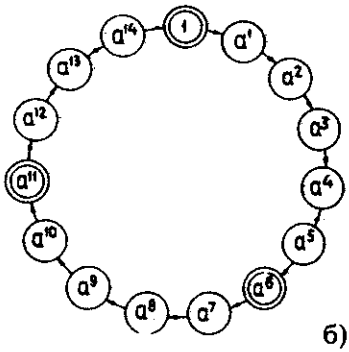
$$\begin{aligned} \tilde{X}_j &= a^\tau X_j, \qquad j = 1,2,\ldots t, \\ \tilde{\sigma}_k &= a^{\tau k} \sigma_k, \qquad k = 1,2,\ldots t. \end{aligned} \tag{29}$$

Следует отметить, что в поле Галуа $GF(2^m)$ $a^n = 2^m - 1$, и поэтому после циклических $2^m - 1$ сдвигов получается степень исходного элемента. Например, элемент a^{19} в поле $GF(2^4)$ $(n = 15)$ равен $a^{15} \cdot a^4 = a^4$.

На рис. 2 приведены значения корней уравнений $X^3 + aX^2 + a^{14}X + a^8$, которые показаны в концентрических окружностях до сдвигов и после двух сдвигов соответственно. Для наглядности рассмотрим конкретный пример. Пусть $n = 2^4 - 1 = 15$, т.е. $m = 4$, и сработали датчики с координатами $X_1 = a^3$, $X_2 = a^8$ и $X_3 = a^{12}$, как это показано на рис. 3, где $\sigma_1 = S_1 = X_1 = a^3$, $\sigma_2 = a^{14}$ и $\sigma_3 = a^{8}$ /8/. Алгоритм на-



а)



б)

Рис. 3. Матрица проверочных соотношений для БЧХ-кода, исправляющего $t = 3$ *ошибки для* $t = 4$ *и* $t = 15$. *Знаком * отмечены сработавшие датчики.*

Рис. 2. Корни уравнения $X^3 + a^1 X^2 + a^{14} X + a^8$ *в поле Галуа* $GF(2^m)$ *до трансформации (слева, в концентрических окружностях) и после трех циклических сдвигов (справа).*

$H^T =$

				Датчики		
α^0	α^0	α^0	1	1000	1000	1000
α^1	α^3	α^5	2	0100	0001	0110
α^2	α^6	α^{10}	3	0010	0011	1110
α^3	α^9	α^{15}	*4	0001	0101	1000
α^4	α^{12}	α^5	5	1100	1111	0110
α^5	α^0	α^{10}	6	0110	1000	1110
α^6	α^3	α^0	7	0011	0001	1000
α^7	α^6	α^5	8	1101	0011	0110
α^8	α^9	α^{10}	*9	1010	0101	1110
α^9	α^{12}	α^0	10	0101	1111	1000
α^{10}	α^0	α^5	11	1110	1000	0110
α^{11}	α^3	α^{10}	12	0111	0001	1110
α^{12}	α^6	α^0	*13	1111	0011	1000
α^{13}	α^9	α^5	14	1011	0101	0110
α^{14}	α^{12}	α^{10}	15	1001	1111	1110
				+ 0001	0101	1000
				+ 1010	0101	1110
				1111	0011	1000
			$S_1 =$	0100	$S_3 =$ 0011	$S_5 =$ 1110

хождения корней уравнения (1) заключается в следующем. Допустим, что один из корней этого уравнения равен $a^\circ = 1$. Тогда имеем

$$\sigma(1) = 1 + \sigma_1 + \sigma_2 + \ldots + \sigma_t = 0,$$

и далее

$$\sum_{k=1}^{t} \sigma_k = \sigma_1 + \sigma_2 + \ldots \sigma_t = 1.$$

Например, при $t = 3$ $\sigma_1 + \sigma_2 + \sigma_3 = 1$, $(a^\circ = 1 = X_1)$.

(30)

Если же корень X_j не равен единице, например, $X_1 = a^{12}$, то путем последовательных умножений на a', получаем $a^{12}\,a^1\,a^1\,a^1 = a^\circ = 1$.

Это значит, что степень корня X_1 равна $15 - 3 = 12$, а значение корня X_1 равно a^{12}. При каждом $t = 3$ в каждом такте необходимо умножать σ_1 на a^1, σ_2 на a^2, σ_3 на a^3 и проверять выполнение соотношения (30). Если это равенство равно 1, то степень корня равна 15 минус число тактов трансформации. Рассмотрим таблицу.

	σ_1	σ_2	σ_3
Начальное состояние	a^1	a^{14}	a^8
После первого шага	a^2	$a^{16} = a^1$	a^{11}
После второго шага	a^3	a^3	a^{14}
После третьего шага	a^4	a^5	$a^{17} = a^2$

Проверяем равенство (30):

$$a^4 + a^5 + a^2 = \begin{array}{r} 1100 \\ 0110 \\ \hline 0010 \\ 1000 \end{array} \mod 2 .$$

В результате получаем, что степень одного из корней равна $15 - 3 = 12$ и т.д.

Таким образом, наряду с простотой устройства, определяющего степени корней координатного уравнения, одновременно получаются логарифмы значений корней X_j, или, попросту, получаются двоичные коды степеней, что позволяет использовать эти данные в специализированных процессорах для дальнейших вычислений.

ЗАКЛЮЧЕНИЕ

Как показала практика [9], метод синдромного кодирования является мощным и эффективным инструментом для создания различного рода устройств, предназначенных для сжатия и обработки данных в спектрометрах физики высоких энергий. При этих относительно небольших значениях множественности $1 \le t \le 5$ имеется возможность для вычисления значения t и координат сработавших датчиков X_j использовать быстродействующие ППЗУ. При $t \ge 5$ можно использовать гибридный метод решения уравнений в поле Галуа $GF(2^m)$.

Поскольку неизвестны быстрые процессоры для нахождения НОД двух полиномов, для понижения степени полинома более предпочтительным можно считать метод[2], основанный на свойствах поля Галуа $GF(2^m)$.

ЛИТЕРАТУРА

1. Никитюк Н.М. — ОИЯИ, Р10-88-853, Дубна, 1988.
2. Chien R.T., Cunningham B.D. — IEEE Trans. on Inf. Theory, 1969, v.IT-15, No.2, p.329.
3. Okano H., Imai H. — IEEE Trans. on Comput., 1987, v.C-36, No.10, p.1165.
4. Berlekamp E.R. — IEEE Trans. on Inform. Theory., 1965, v.IT-11, No.4, p.577.
5. Питерсон У., Уэлдон Э. — Коды, исправляющие ошибки. М.:Мир, 1976, с.332.
6. Nikitjuk N.M., Radzabov R.S., Schafranov M.D. — NIM, 1978, v.155, p.485.
7. Chien R.T. — IEEE Trans. on Inf. Theory, 1964, v.IT-10, No.4, p.357.
8. Никитюк Н.М. — ОИЯИ, Р10-87-254, Дубна, 1987.
9. Gustafsson L., Hagberg E. — NIM, 1988, v.A265, p.521.

Рукопись поступила в издательский отдел
12 января 1989 года.