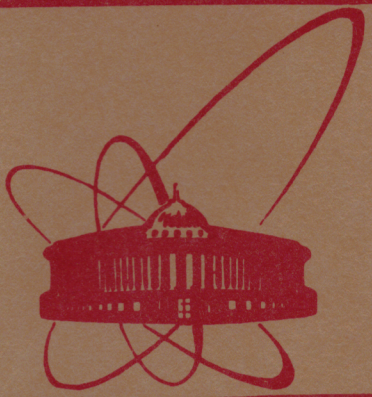

объединенный
институт
ядерных
исследований
дубна

P11-80-484

Н.М.Никитюк

МЕТОД СИНДРОМНОГО КОДИРОВАНИЯ И ЕГО ПРИМЕНЕНИЕ ДЛЯ БЫСТРОГО АППАРАТНОГО ОТБОРА СОБЫТИЙ НА ОСНОВЕ ПРОЦЕССОРОВ, ОПЕРИРУЮЩИХ В ПОЛЕ ГАЛУА $GF(2^m)$

Направлено в "Nuclear Instruments and Methods"

1980

Никитюк Н.М.

P11-80-484

Метод синдромного кодирования и его применение для быстрого аппаратного отбора событий на основе процессоров, оперирующих в поле Галуа $GF(2^m)$

Предложенный ранее метод синдромного кодирования для сжатия данных, считываемых с МПК, обобщается на случай его применения для регистрации координат зарегистрированных событий. Рассматриваются вопросы выполнения арифметических и алгебраических операций над элементами поля Галуа и их аппаратная реализация. Приводится методика расчета специализированного процессора для параллельного вычисления координат трех искр и дается оценка его быстродействия.

Работа выполнена в Лаборатории высоких энергий ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна 1980

P11-80-484

Nikityuk N.M.

1. ВВЕДЕНИЕ

Увеличение объема информации, поступающей от многоканальных детекторов ядерных частиц, привело к необходимости более тщательного изучения вопросов оптимального кодирования, методов съема и обработки информации. Решению этих задач посвящен ряд интересных работ. В последнее время особенно интенсивно развивается техника специализированных процессоров, предназначенных для выработки триггера, определения координат зарегистрированных событий и построения треков [1-3]. Однако при кодировании данных, поступающих от многопроволочных пропорциональных камер /МПК/, на наш взгляд, не всегда учитываются особенности работы МПК, в которых регистрируется ограниченное число частиц, сравнительно небольшое по отношению к общему числу проволочек, содержащихся в МПК. Поэтому на первом этапе обработки данных, поступающих от МПК, целесообразно проводить их фильтрацию и сжатие. Один из методов сжатия данных применительно к МПК предложен нами в работах [4,5,20]. Известна также работа [6], в которой аналогичный метод сжатия данных предлагается использовать для обработки информации, поступающей от датчиков, расположенных на космических объектах. В данной работе этот метод получил название метода синдромного кодирования. Этим термином мы будем пользоваться в дальнейшем.

2. МЕТОД СИНДРОМНОГО КОДИРОВАНИЯ

Кратко суть метода синдромного кодирования заключается в следующем /рис.1/. На передающей стороне имеется n датчиков, причем предполагается, что одновременно может сработать лишь небольшая часть /10-20%/ от общего их количества. Число одновременно сработавших датчиков обозначим через t. Если в заданный момент времени не сработал ни один датчик, то мы получим нулевое кодовое слово, а появление единиц в процессе срабатывания датчиков рассматривается как добавление вектора ошибки к нулевому кодовому слову. Это слово /в случае отсутствия сработавших датчиков - нулевое слово/ поступает на вход устройства, формирующего синдром кодового слова. Устройство располагается на передающей стороне. На выходе формирователя

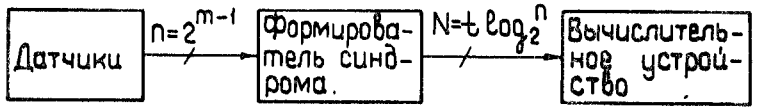

Рис.1. Блок-схема системы передачи данных с использованием метода синдромного кодирования.

синдрома число каналов передачи уменьшается до $N = t \log_2 n$. Так, если положить $n = 63$, $t = 3$, то $N = 18$. Далее по кодовому слову N в вычислительном устройстве можно определить номера сработавших датчиков. Известно много различных типов корректирующих кодов. Эти вопросы рассмотрены подробно в известных книгах по теории кодирования [7,8]. В данной работе используется широко известный класс кодов Боуза-Чаудхури-Хоквингема /БЧХ-коды/. Декодирование таких кодов сводится к задаче решения алгебраического уравнения, корни которого определяют местоположение ошибок в кодовом слове, и в случае синдромного кодирования корни уравнения определяют координаты сработавших датчиков. При этом операции выполняются над элементами поля Галуа $GF(2^m)$, в котором существенно упрощается выполнение арифметических операций над кодовыми словами.

Известно несколько способов декодирования кодов БЧХ [7-12]. В данной работе рассматривается известный метод решения уравнений второй и третьей степени, который относительно легко реализуется при помощи комбинационных схем [10-12]. Кроме того, устройства для решения уравнений второй и третьей степени являются базовыми для решения уравнений более высоких степеней [12].

3. ВЫПОЛНЕНИЕ АЛГЕБРАИЧЕСКИХ ОПЕРАЦИЙ В ПОЛЕ ГАЛУА

В отличие от традиционных методов двоичной арифметики над числами, представленными в позиционной системе счисления, которые широко используются для обработки данных в современной ядерной электронике в методе синдромного кодирования, как мы уже отмечали выше, арифметические и алгебраические операции выполняются в расширенном поле Галуа $GF(p^m)$, где p - простое число и называется характеристикой поля. Для двоичной системы счисления $p = 2$, а m - целое число. Правилам построения конечных полей Галуа посвящен ряд работ [13-16]. Интерес к этому предмету в настоящее время существенно возрос в связи с развитием техники больших интегральных схем [17]. С целью облегчения чтения данной статьи для читателя, незнакомого

с правилами выполнения операций над элементами поля $GF(2^m)$, ниже и в процессе изложения будут приводиться основные и необходимые сведения об этих правилах, которые не претендуют на полноту изложения и общность. Число ненулевых элементов /слов/ конечного поля равно некоторой степени его характеристики, т.е. $n = 2^m - 1$. Число различных элементов поля называется его порядком. Все элементы конечного поля можно получить при помощи неприводимых многочленов, таблицы которых приведены в книге [7] /приложение В/. Так, в работе [5] для построения блока сжатия данных МПК, имеющей $n = 63$ проволочки, нами был выбран неприводимый полином шестой степени $f(X) = X^6 + X + 1$, $(m = 6)$. Это значит, что число ненулевых элементов поля равно $2^m - 1$. Следует подчеркнуть, что знак + нами будет использован для обозначения операции сложения по модулю 2. Среди элементов конечного поля выделяются m линейно независимых /базисных/ элементов. Поле, образованное при помощи полинома $f(X)$, имеет следующие базисные элементы: $1\ (a^0)$, a^1, a^2, a^3, a^4 и a^5. Один из этих элементов, a^1, является корнем многочлена $f(X)$, и поэтому каждый ненулевой элемент этого поля может быть представлен как некоторая степень элемента a^1. Это значит, что мультипликативная группа конечного поля носит циклический характер. Наименьшее положительное число n, для которого $a^n = a^0 = 1$, называется порядком элемента a^1. Если порядок элемента a^1 равен n, то элементы $1, a^1, a^2, \ldots, a^{n-1}$ различны. Так, в нашем примере $n = 2^{m-1} = 63$ и поэтому, например, $a^{126} = (a^{63})^2 = a^0 = 1$; $a^{64} = a^{63} \times a^1 = a^1$; $a^{75} = a^{63} \times a^{12} = a^{12}$ и т.д. Учитывая, что a^1 - корень многочлена $f(X)$, остальные элементы поля $GF(2^m)$ можно получить, исходя из уравнения $a^6 + a^1 + 1 = 0$, т.е. $a^6 = a^1 + 1$; $a^7 = a^2 + a^1$; $a^8 = a^3 + a^2$; $a^9 = a^4 + a^3$; $a^{10} = a^5 + a^4$; $a^{11} = a^5 + a^1 + 1$; $a^{12} = a^1 + a^2 + a^6 = a^1 + a^2 + 1 + a^1 = 1 + a^2$ и т.д.

Элементы поля удобно также представлять в виде многочлена степени $m-1$: $d_0 a^0 + d_1 a^1 + d_2 a^2 + d_3 a^3 + \ldots + d_{m-1} a^{m-1}$, где коэффициенты $d_0, d_1, \ldots, d_{m-1}$ принимают значения 0 или 1. Так, для элемента $a^9 = a^4 + a^3$ $m-1$ $d_0 = d_1 = d_2 = d_5 = 0$ и $d_4 = d_3 = 1$. В приложении 1 приведены элементы поля $GF(2^6)$. Нередко элементы поля рассматриваются как векторы, тогда величины $d_0, d_1, d_2, d_3, \ldots, d_{m-1}$ рассматриваются как координаты вектора. Так же как и в двоичной арифметике при выполнении операций над элементами поля, имеются некоторые отличия в правилах вычисления "вручную" и машинным способом. Это касается таких операций, как умножение, возведение в степень, деление и извлечение квадратного корня. Операции умножения и деления вручную производятся очень просто: степень произведения элементов равна сумме степеней сомножителей, причем суммирование степеней производится по модулю 2^m. Операция деления элемента a на элемент b равносильна

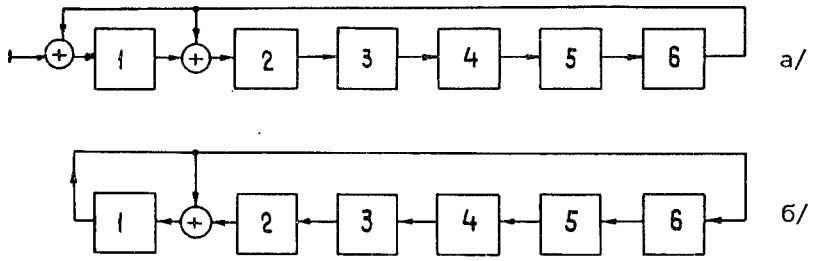

Рис.2. Счетчики в поле Галуа по модулю многочлена X^6+X+1;
а/ устройство для счета в прямом направлении;
б/ реверсивный счетчик. 1,2,3,4,5,6 - ячейки сдвигового регистра.

операции умножения элемента a на инверсный элемент b^{-1}. Инверсный элемент b^{-1} элемента b определяется из условия: $b \times b^{-1} = 1$. Так, для элемента a^9 инверсным элементом будет a^{54}, так как $a^{54} \times a^9 = a^{63} = 1$. При операциях вручную инверсный элемент получается просто: из числа $2^m - 1$ надо вычесть степень данного элемента и тогда величина разности будет равна степени инверсного элемента. Например, инверсным элементом для элемента a^{25} будет a^{38}; так как 63 - 25 = 38.

Извлечение квадратного корня из элемента, имеющего четную степень, не вызывает затруднений. Так, если i - четное число, то $(a^i)^{1/2} = a^{i/2}$. Если же степень i - число нечетное, то степень элемента, соответствующего $(a^i)^{1/2}$, будет равна $\frac{i+n}{2}$. Например, $(a^5)^{1/2} = a^{34}$, так как $\frac{5+63}{2} = 34$. Операция возведения в степень элементов поля выполняется так же, как и возведение в степень обычных чисел, с той лишь разницей, что эта операция выполняется по модулю n. Например, $(a^{60})^{12} = a^{720} = a^{63 \cdot 11} \times a^{27} = a^{27}$. Операции сложения и вычитания в поле $GF(2^m)$ равносильны и выполняются по модулю два.

4. АППАРАТНАЯ РЕАЛИЗАЦИЯ НЕКОТОРЫХ ОПЕРАЦИЙ В ПОЛЕ ГАЛУА

4.1. Счетчики. Для получения последовательностей элементов в поле Галуа как в прямом, так и в обратном направлении применяются сдвиговые регистры с логической обратной связью /7-8/. Структура связей в таких счетчиках зависит от неприводимого полинома, выбранного для построения поля, поэтому среди неприводимых полиномов одинаковой степени следует выбирать тот, который имеет наименьшее число ненулевых коэффициентов. На рис.2 приведены счетчики в поле Галуа для счета в прямом и обратном направлении по модулю многочлена X^6+X+1 соответственно. Если в младший разряд регистра, представленного на рис.2а, поместить единицу, а в остальные разряды - нули, то последовательные сдвиги регистра дадут представление последовательных степеней элемента a^1 в форме, в какой они приведены в приложении. Наличие обратной связи из старшего разряда в младшие позволяет получать значение $a^6 = a^1 + 1$. Сдвиг влево /рис.2б/ соответствует делению на a^1, так что единица переноса, выходящая из ячейки младшего разряда, дает значение $a^{-1} = 1 + a^5$:

4.2. Умножение и возведение в степень. Умножение двух элементов поля при заданном базисе a^0, a^1, a^2, a^3, и a^4 и a^5 можно производить, если представить эти элементы в виде многочленов /14/. Так, если представить один элемент в виде $A = a^0 b_0 + a^1 b_1 + a^2 b_2 + a^3 b^3 + a^4 b^4 + a^5 b_5$, а другой - в виде $B = a^0 c_0 + a^1 c_1 + a^2 c_2 + a^3 c_3 + a^4 c_4 + a^5 c_5$, то прямое умножение этих многочленов по модулю 6 даст произведение двух элементов поля, которое просто реализуется при помощи элементов "И" и "Исключающее ИЛИ". Обозначая соответствующие координаты элемента произведения через g_0, g_1, g_2, g_3, g_4 и g_5, получим следующие выражения для произведения двух элементов:

$$g_0 = b_0c_0 + b_1c_5 + b_2c_4 + b_3c_3 + b_4c_2 + b_5c_1,$$

$$g_1 = b_2c_4 + b_2c_5 + b_3c_3 + b_3c_4 + b_4c_2 + b_5c_2 + b_0c_1 + b_1c_0 + b_1c_5 + b_4c_3 + b_5c_1,$$

$$g_2 = b_0c_2 + b_1c_1 + b_3c_4 + b_3c_5 + b_4c_3 + b_4c_4 + b_5c_2 + b_5c_3 + b_2c_0 + b_2c_5,$$

$$g_3 = b_0c_3 + b_1c_2 + b_3c_0 + b_3c_5 + b_4c_4 + b_4c_5 + b_5c_4 + b_5c_3 + b_2c_1,$$

$$g_4 = b_0c_4 + b_1c_3 + b_2c_2 + b_3c_1 + b_4c_0 + b_4c_5 + b_5c_4 + b_5c_5,$$

$$g_5 = b_0c_5 + b_1c_4 + b_2c_3 + b_3c_2 + b_4c_1 + b_5c_0 + b_5c_5.$$

/1/

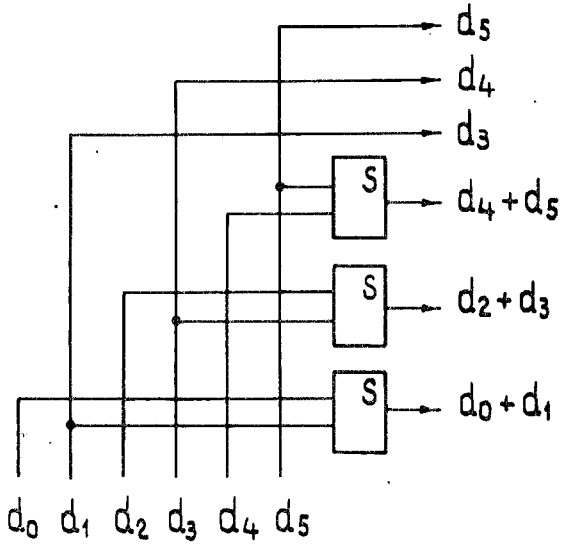

Рис.3. Схема для вычисления квадратного корня из любого элемента по $GF(2^6)$ по модулю многочлена X^6+X+1 .

Если в равенстве /1/ положить $A=B$, то получим выражения для возведения элемента поля в квадрат: $g_0=b_0+b_3$, $g_1=b_3$; $g_2=b_1+b_4$; $g_3=b_4$, $g_4=b_2+b_5$ и $g_5=b_5$. Выражения для возведения элемента поля в более высокие степени можно получить при помощи ЭВМ, используя как исходные равенства /1/.

4.3. Извлечение квадратного корня и решение уравнения второй степени. Извлечение квадратного корня в поле характеристики 2 является операцией линейной и поэтому аппаратно реализуется довольно просто. В таком поле выполняются соотношения $(X+Y)^2=X^2+Y^2$ и $(X+Y)^{1/2}=X^{1/2}+Y^{1/2}$. В работе /18/ дано правило получения выражения для извлечения квадратного корня и решение уравнения второй степени. Из базисных элементов поля a^0, a^1, a^2, a^3, a^4 и a^5 получаем другой базис следующим образом: $(a^0)^{1/2}=a^0$, $(a^1)^{1/2}=a^{32}$; $(a^2)^{1/2}=a^1$, $(a^3)^{1/2}=a^{33}$, $(a^4)^{1/2}=a^2$ и $(a^5)^{1/2}=a^{34}$. Тогда выражение для извлечения квадратного корня из элемента $a^0d_0+a^1d_1+a^2d_2+a^3d_3+a^4d_4+a^5d_5$ сводится к решению матричного уравнения

$$[d_0,d_1,d_2,d_3,d_4,d_5]\cdot\begin{bmatrix}1\\a^{32}\\a^1\\a^{33}\\a^2\\a^{34}\end{bmatrix}=[d_0,d_1,d_2,d_3,d_4,d_5]\begin{bmatrix}100000\\100100\\010000\\010010\\001000\\001001\end{bmatrix}. \quad /2/$$

Например, $(a^{25})^{1/2}=a^{44}$ или

$$[010001]\times\begin{bmatrix}100000\\100100\\010000\\010010\\001000\\001001\end{bmatrix}=101101=a^{44}.$$

На рис.3 приведена схема для вычисления квадратного корня из любого элемента поля $GF(2^6)$.

4.4. Решение квадратного уравнения. Нахождение корней Y_1 и Y_2 квадратного уравнения $Y^2+Y=d$ /3/ сводится к вычислению выражений вида /8,18/ :

$$Y_1=\sum_{i=0}^{m-1}d_i\,y_i \quad \text{и} \quad Y_2=Y_1+1,$$

где

$$y_0=d_0,\ y_1=d_0+d_1+d_5;\quad y_2=d_1+d_2+d_3+d_5;$$

$$y_3=d_0;\ y_4=d_0+d_3+d_5;\quad y_5=d_0+d_1+d_2+d_4+d_5 .$$

Здесь $d_0\div d_5$ - коэффициенты в представлении элемента в виде многочлена $(d=d_0a^0+d_1a^1+d_2a^2+d_3a^3+d_4a^4+d_5a^5)$.

На рис.4 приведена схема для решения уравнения /3/.

Для решения квадратного уравнения в общем виде $X^2+\sigma_1X+\sigma_2$ /4/ необходимо сделать подстановку $X=\sigma_1Y$. Тогда уравнение /4/ приводится к виду /3/, где $d=\sigma_2/\sigma_1^2$. После нахождения корней уравнения /3/ корни уравнения /4/ получаются из выражений: $X_1=\sigma_1Y_1$ и $X_2=\sigma_1Y_2$.

4.5. Вычисление инверсного элемента. Для вычисления инверсного элемента B^{-1} для элемента B необходимо этот элемент возвести в степень 2^m-2, так как $B\times B^{2^m-2}=B^{2^m-1}=1$, или $m-1$ раз повторить итерацию: $\{[(B)^2B]^2B\ldots B\}^{2}$ /21/.

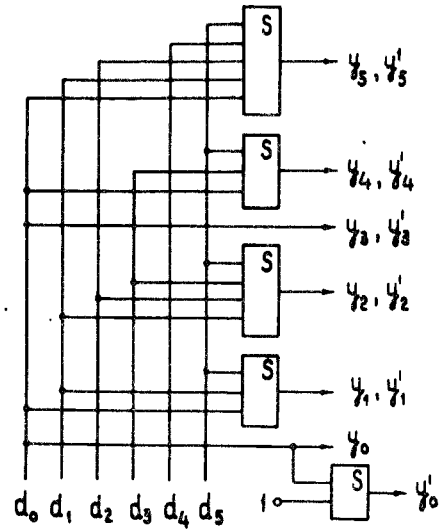

Рис.4. Схема для решения квадратного уравнения $Y^2+Y=d$ в поле $GF(2^6)$ по модулю многочлена X^6+X+1.

5. ПРИМЕР РАСЧЕТА КООРДИНАТНОГО ПРОЦЕССОРА

Рассмотрим конкретный пример расчета координатного процессора для МПК, содержащей $n=63$ проволочки и при условии, что число одновременно сработавших проволочек не превышает трех. Процесс расчета и построения такого процессора состоит из нескольких этапов.

1. Построение блока сжатия данных, поступающих с МПК. В работе[5] нами показано, что для случая, когда $n=63$ и $t=3$, блок сжатия данных занимает одну плату КАМАК. Для построения схемы блока требуется 60 корпусов микросхем типа SN 74180. На выходе блока получается 18-разрядный код, представляющий собой симметрические функции S_1, S_3 и S_5. Для составления принципиальной схемы блока сжатия необходимо построить матрицу проверочных соотношений H^T, которую можно вычислить на ЭВМ. Для краткости мы здесь приводим только первые 6 строк и последнюю 63-ю строку матрицы H^T. Эта матрица состоит из трех колонок. Каждая колонка состоит из шести столбцов. В первой колонке записываются элементы $GF(2^6)$ в порядке возрастания степеней элементов; вторая колонка состоит из соответствующих элементов, возведенных в куб, и третья колонка - из соответствующих элементов, возведенных в пятую степень. Номера строк в матрице H^T соответствуют номерам проволочек, а номера столбцов - разрядам синдрома S_1, S_3 и S_5. Для составления принципиальной схемы блока сжатия достаточно в матрице H^T элементы a^i заменить двоичными эквивалентами. Тогда позиции единиц в такой матрице определяют способ соединения выходов усилителей МПК с входами схем проверки на четность.

$$H^T=\begin{array}{|c|c|c|c||c|c|c|}\hline
* & 1 & 1 & 1 & 100000 & 100000 & 100000 \\ \hline
 & 2 & a^1 & a^3 & a^5 & 010000 & 000100 & 000001 \\ \hline
 & 3 & a^2 & a^6 & a^{10} & 001000 & 110000 & 000011 \\ \hline
* & 4 & a^3 & a^9 & a^{15} & 000100 & 000110 & 000101 \\ \hline
 & 5 & a^4 & a^{12} & a^{20} & 000010 & 101000 & 001111 \\ \hline
* & 6 & a^5 & a^{15} & a^{25} & 000001 & 000101 & 010001 \\ \hline
 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline
 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline
 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline
 & 63 & a^{62} & a^{60} & a^{58} & 100001 & 100111 & 111111 \\ \hline
\end{array}$$

Номера проволочек

S_1 S_3 S_5

Для определенности положим, что одновременно поступили сигналы с 1-й, 4-й и 6-й проволочек. Эти позиции в матрице H^T обозначены символом *. Обозначив эти координаты через X_1, X_2 и X_3, получим:

$$S_1=X_1+X_2+X_3; \quad S_3=X_1^3+X_2^3+X_3^3;$$

$$S_5=X_1^5+X_2^5+X_3^5,$$

где /5/

$$S_1=a^0+a^3+a^5=a^{23}, \quad S_3=a^0+a^9+a^{15}=a^{61} \text{ и}$$

$$S_5=a^0+a^{15}+a^{25}=a^{35}.$$

Для решения системы /5/ воспользуемся известными соотношениями между симметрическими функциями S_j и элементарными симметрическими функциями σ_i, которые для $t=3$ имеют вид /для двоичной системы счисления/:

$$S_1=\sigma_1; \quad S_3+S_2\sigma_1+S_1\sigma_2+\sigma_3=0; \quad S_5+S_4\sigma_1+S_3\sigma_2+S_2\sigma_3=0, \quad /6/$$

где $S_2=S_1^2$ и $S_4=S_2^2=S_1^4$. Если $S_1^3+S_3\neq 0$, то система /6/ имеет решение:

$$\sigma_1=S_1; \quad \sigma_2=\frac{S_1^2S_3+S_5}{S_1^3+S_3}; \quad \sigma_3=\frac{S_1S_5+S_3^2+S_1^3S_3+S_1^6}{S_1^3+S_3}. \qquad /7/$$

Следует отметить, что если $\sigma_3\neq 0$, то сигнал поступил от трех проволочек /или более трех в общем случае/; если $\sigma_3=0$, но $\sigma_2\neq 0$, то сигнал поступил от двух проволочек. Если же

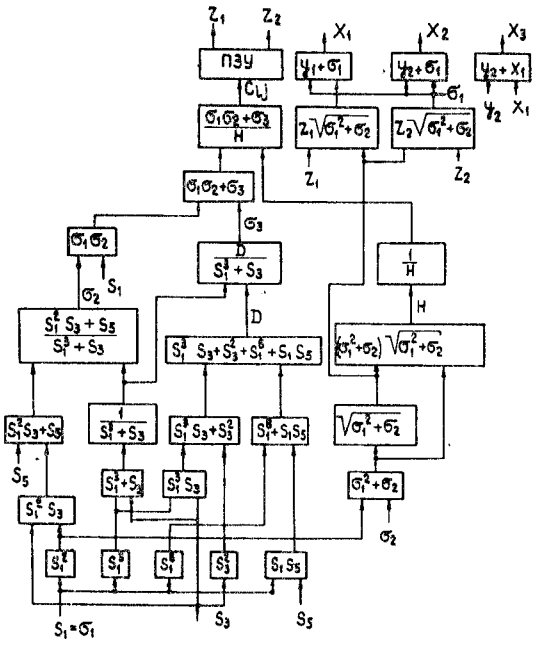

Рис.5. Блок-схема процессора для одновременного вычисления трех координат.

$S_1^3 + S_3 = 0$, то сигнал поступил от одной проволочки и $S_1 = \sigma_1$ есть ее координата. Подставляя значения S_1, S_3 и S_5 в уравнения /7/, получим $\sigma_2 = a^{34}$ и $\sigma_3 = a^8$. Для нахождения координат трех проволочек, от которых поступили сигналы, необходимо решить уравнение

$$X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3 = X^3 + a^{23}X^2 + a^{34}X + a^8 = 0. \quad /8/$$

С целью решения уравнения /8/ табличным методом [11,12] при помощи последовательных подстановок $X = Y + \sigma_1$ и $Y = Z(\sigma_1^2 + \sigma_2)^{1/2}$ оно приводится к виду

$$Z^3 + Z = C, \quad /9/$$

где $C = \frac{\sigma_1\sigma_2 + \sigma_3}{(\sigma_1^2 + \sigma_2)(\sigma_1^2 + \sigma_2)^{1/2}}$.

Как показано в работах [11,12], уравнение /9/ имеет три различных корня только при определенном наборе значений C /см. табл./. Так, при $n = 63$ и $t = 3$ число таких констант равно 10. Причем в памяти достаточно хранить два значения корня для каждого C, а третий корень получается из соотношения $X_3 = X_1 + X_2 + S_1$. Продолжим рассмотрение нашего примера. Вычисляем $C = a^{55}$. Из таблицы получаем $Z_1 = a^{44}$ и $Z_2 = a^{60}$. Далее $Y_1 = a^{62}$, $Y_2 = a^{15}$, и, соответственно, $X_1 = a^3$, $X_2 = a^0$ и $X_3 = X_1 + X_2 + S_1 = a^0 + a^3 + a^{23} = a^5$.

На рис.5 приведена блок-схема процессора для параллельного вычисления трех координат. В качестве ПЗУ для хранения решений можно использовать мультиплексоры, как это показано на рис.6. Используя 6 микросхем типа SN 74152, можно получить, например, для 8 значений C_i соответственно 8 решений или можно разработать и изготовить программируемую логическую матрицу.

Таблица

Решения для $n = 63$ и $t = 3$.

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

6. ОЦЕНКА БЫСТРОДЕЙСТВИЯ

При оценке быстродействия системы будем исходить из того, что число зарегистрированных искр $t = 3$, а для построения схемы сжатия и процессора используются ТТЛ-схемы с диодами Шотки [19]. Отсчет времени будем производить от начала поступления сигналов с усилителей МПК на блок сжатия данных, в котором они задерживаются на $T_c = 30$ нс, что соответствует задержкам сигналов от двух микросхем типа SN74S180. Далее сигналы, соответствующие коду S_1, S_3, S_5, поступают на вход процессора /рис.5/. Для определенности рассмотрим путь прохождения сигналов, соответствующих коду S_1. Будем считать задержку сигналов

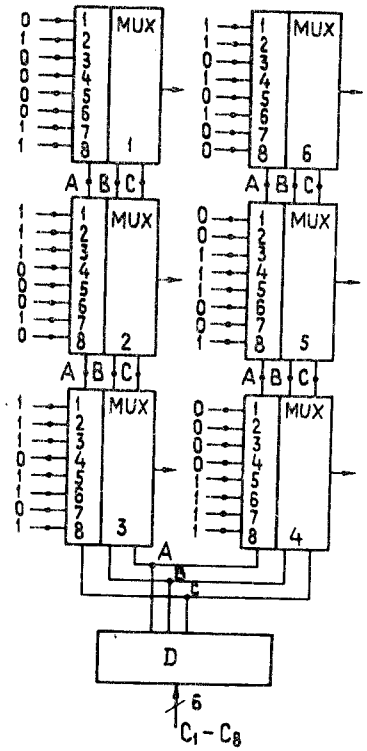

Рис.6. Пример схемы для получения решений уравнения третьей степени.

T_M на схемах умножения двух элементов и задержку T_d на схемах возведения в степень одинаковой. Она складывается из задержки на микросхеме SN74S08 и задержки на элементе SN74S180, что в сумме составляет 21 нс. Время T_1, требуемое для вычисления инверсного элемента, составляет 36 нс, и оно складывается из задержки на микросхеме SN74S08 и задержки на двух микросхемах SN74S180. Если ПЗУ выполнить на основе мультиплексора типа SN74S151, то задержка T_R в ПЗУ составит 12 нс. На сложение по модулю 2 двух элементов достаточно времени $T_A = 7$ нс. Тогда суммарное T_s, необходимое для сжатия данных и вычисления координат трех искр, зарегистрированных в МПК, можно приблизительно оценить из следующего выражения:

$$T_S = T_C + 4T_M + T_I + 3T_A + T_R =$$

$$= 30 + 84 + 36 + 21 + 12 = 185 \text{ нс.}$$

7. ЗАКЛЮЧЕНИЕ

В работе рассмотрен один из методов сжатия и определения координат искр, зарегистрированных в МПК, основанный на применении алгебраической теории кодирования. Показано, что для некоторых частных, но часто встречающихся на практике случаев, можно создавать быстродействующие устройства сжатия данных, схемы отбора по числу искр, зарегистрированных в МПК, и процессоры для вычисления координат искр. Причем все три этапа: сжатие, отбор и вычисление координат выполняются без применения элементов памяти и тактирующих сигналов, и поэтому быстродействие такого устройства определяется задержками логических сигналов в комбинационных схемах. В случае, когда $t > 5$, можно применить последовательные методы декодирования, которые подробно изложены в работах [7,8], а также сочетание параллельных методов с последовательными [12]. Возможен и другой путь определения координат зарегистрированных искр, при котором не требуется нахождения корней алгебраических уравнений высоких степеней [20]. Суть его заключается

в том, что если датчики расположить в виде матрицы и вычислить проверочные соотношения отдельно по строкам и столбцам такой матрицы /например, используя правило получения синдрома по модифицированному коду Хэмминга/, то, конечно, кодовое расстояние будет равно произведению кодовых расстояний исходных кодов. Однако для декодирования кода Хэмминга решения алгебраического уравнения не требуется. Следует также отметить, что в случае, когда t велико /15-20/, можно сжатие данных выполнять аппаратным способом, а вычисление координат производить в режиме офф-лайн.

Следует также отметить, что все элементы процессора, которые реализуются при помощи комбинационных схем, поддаются точному аналитическому расчету как вручную, так и на ЭВМ /для $m > 6$/ [21].

ПРИЛОЖЕНИЕ

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

a^0 = I00000	a^{2I}= IIOIII	a^{42}= OIOIII
a = OIOOOO	a^{22}= OOIOII	a^{43}= IIIOII
a^2 = OOIOOO	a^{23}= IOOIOI	a^{44}= IOIIOI
a^3 = OOOIOO	a^{24}= IOOOIO	a^{45}= IOOIIO
a^4 = OOOOIO	a^{25}= OIOOOI	a^{46}= OIOOII
a^5 = OOOOOI	a^{26}= IIIOOO	a^{47}= IIIOOI
a^6 = IIOOOO	a^{27}= OIIIOO	a^{48}= IOIIOO
a^7 = OIIOOO	a^{28}= OOIIIO	a^{49}= OIOIIO
a^8 = OOIIOO	a^{29}= OOOIII	a^{50}= OOIOII
a^9 = OOOIIO	a^{30}= IIOOII	a^{5I}= IIOIOI
a^{I0}= OOOOII	a^{3I}= IOIOOI	a^{52}= IOIOIO
a^{II}= IIOOOI	a^{32}= IOOIOO	a^{53}= OIOIOI
a^{I2}= IOIOOO	a^{33}= OIOOIO	a^{54}= IIIOIO
a^{I3}= OIOIOO	a^{34}= OOIOOI	a^{55}= OIIIOI
a^{I4}= OOIOIO	a^{35}= IIOIOO	a^{56}= IIIIIO
a^{I5}= OOOIOI	a^{36}= OIIOIO	a^{57}= OIIIII
a^{I6}= IIOOIO	a^{37}= OOIIOI	a^{58}= IIIIII
a^{I7}= OIIOOI	a^{38}= IIOIIO	a^{59}= IOIIII
a^{I8}= IIIIOO	a^{39}= OIIOII	a^{60}= IOOIII
a^{I9}= OIIIIO	a^{40}= IIIIOI	a^{6I}= IOOOII
a^{20}= OOIIII	a^{4I}= IOIIIO	a^{62}= IOOOOI
		a^{63}= IOOOOO

ЛИТЕРАТУРА

1. Verkerk C. Special Purpose Processors. CERN-Data Handling Division, 1974, DD/74/27, p.40.
2. Verkerk C. Special Purpose Processors for High Energy Physics Applications. CERN-Data Handling Division, 1977, DD/77/6, p.14.
3. Barsotti E. et al. A Modular Trigger Processing for High Energy Physics Experiments. Fermi National Accelerators Laboratory, 1978, FN-312, 2530.000.
4. Nikityuk N.M., Radzhabov P.S., Shafranov M.D. A New Method of Information Registration from Multiwire Proportional Chambers "Nucl.Instr. and Meth.", 1978, Vol.155, No 1, p.485-489.
5. Никитюк Н.М., Раджабов Р.С., Шафранов М.Д. "Приборы и техника эксперимента", 1978, № 4, с.95-98;
   Ancheta Teofilo C. Syndrome-Source-Coding and Its Universal Generalization - IEEE Trans. on Inf.Theory", 1976, Vol.IT-22, No 4, p.432-436.
7. Peterson W.W., Weldon E.J. Error Correcting Codes MIT, 1971.
8. Berlekamp E.R. Algebraic Coding Theory. McGrow-Hill, 1968.
9. Блох Э.Л. О методе декодирования для кодов Боуза-Чоудхури, исправляющих тройные ошибки. "Известия Академии Наук СССР"; "Техническая кибернетика", 1964, № 3, с.30-37.
10. Banerji R.B. A Decoding Procedure for Double-Error Correcting Bose-Ray-Chaudhuri Codes - "Proc.IRE", 1961, Vol.49, No 10, p.1585.
11. Polkinghorn F. Decoding of Double and Triple Error Correcting Bose-Chaudhuri Codes - IEEE Trans. on Inf. Theory", 1966, Vol.IT-12, No 4, p.480-481.
12. Chien R.T., Cunmingham B.D., Oldham I.B. Hybrid Methods for Finding Roots of a Polynomial with Application to BCH Decoding - "IEEE Trans. on Inf.Theory", 1969, Vol.IT-15, No 2, p.329-335.
13. Bartee T.C., Schneider P.I. Computation with Finite Fields - "Information and Control", 1963, Vol.6, No 1, p.79-98.
14. Tanaka H. et al. Computation Over Galois Fields Using Shift Registers. - "Information and Control", 1968, Vol.13, No 1, p.75-84.
15. Pradham D.K. A Theory of Galois Switching Functions - "IEEE Trans. on Comput.", 1978, Vol.C-27, No 3, p.239-248.
16. Benjauthrit B., Reed I. Galois Switching Functions and Their Applications - "IEEE Trans. on Comput.", 1976, Vol.C-25, No 1, p.78-86.

17. Laws B.A., Ruchforth C.K. A Cellular-Array Multiplier for CF (2^m). - "IEEE Trans. on Comput.", 1971, Vol.C-20, No 12.
18. Berlekamp E.R., Rumsey H., Solomon G. On the Solution of Algebraic Equations Over Finite Fields. - "Information and Control", 1967, Vol.10, p.553-564.
19. Texas Instruments Incorporated. The TTL Data Book for Design Engineers.
20. Никитюк Н.М., Раджабов Р.С., Шафранов М.Д. Устройство для считывания информации с координатной камеры - "Бюллетень изобретений", 1978, № 14, с.171.
21. Гайдамака Р.И., Никитюк Н.М. Расчет спецпроцессора, оперирующего элементами поля Галуа GF(2^m) с помощью программы, написанной на языке SCOONSCHIP. ОИЯИ, Р10-12702, Дубна, 1979, с.6.

Рукопись поступила в издательский отдел
9 июля 1980 года.

ТЕМАТИЧЕСКИЕ КАТЕГОРИИ ПУБЛИКАЦИЙ ОБЪЕДИНЕННОГО ИНСТИТУТА ЯДЕРНЫХ ИССЛЕДОВАНИЙ

Индекс	Тематика
1.	Экспериментальная физика высоких энергий
2.	Теоретическая физика высоких энергий
3.	Экспериментальная нейтронная физика
4.	Теоретическая физика низких энергий
5.	Математика
6.	Ядерная спектроскопия и радиохимия
7.	Физика тяжелых ионов
8.	Криогеника
9.	Ускорители
10.	Автоматизация обработки экспериментальных данных
11.	Вычислительная математика и техника
12.	Химия
13.	Техника физического эксперимента
14.	Исследования твердых тел и жидкостей ядерными методами
15.	Экспериментальная физика ядерных реакций при низких энергиях
16.	Дозиметрия и физика защиты
17.	Теория конденсированного состояния
18.	Использование результатов и методов фундаментальных физических исследований в смежных областях науки и техники