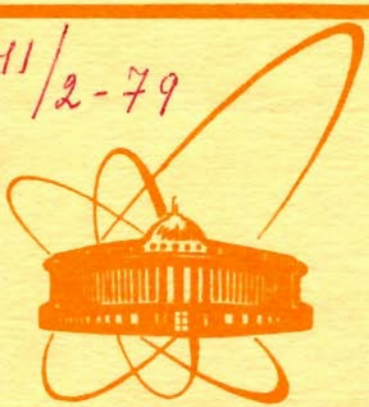

объединенный
институт
ядерных
исследований
дубна

Р10 - 12702

Р.И.Гайдамака, Н.М.Никитюк

РАСЧЕТ СПЕЦПРОЦЕССОРА, ОПЕРИРУЮЩЕГО ЭЛЕМЕНТАМИ ПОЛЯ ГАЛУА $GF(2^m)$, С ПОМОЩЬЮ ПРОГРАММЫ, НАПИСАННОЙ НА ЯЗЫКЕ SCHOONSCHIP

1979

P10 - 12702

Р.И.Гайдамака, Н.М.Никитюк

РАСЧЕТ СПЕЦПРОЦЕССОРА, ОПЕРИРУЮЩЕГО ЭЛЕМЕНТАМИ ПОЛЯ ГАЛУА $GF(2^m)$, С ПОМОЩЬЮ ПРОГРАММЫ, НАПИСАННОЙ НА ЯЗЫКЕ SCHOONSCHIP

Направлено на рабочее совещание по системам и методам аналитических вычислений на ЭВМ и их применению в теоретической физике, Дубна, 1979 г.

Гайдамака Р.И., Никитюк Н.М.

P10 - 12702

Расчет спецпроцессора, оперирующего элементами поля Галуа $GF(2^m)$, с помощью программы, написанной на языке SCHOONSCHIP

Выполнен расчет спецпроцессора, оперирующего элементами поля Галуа $GF(2^m)$. Расчет производился с помощью программы определения координат зарегистрированных в многоканальных детекторах частиц с многопроволочных пропорциональных камер/МПК/, написанной на языке SCHOONSCHIP. При этом производилось построение элементов поля Галуа по заданным неприводимым многочленам степени m; была построена матрица проволочных соотношений H^T, на основе которой получен блок сжатия информации; определялся синдром $S_j = \sum_{i=1}^{t} x_i^j$, $j = 1,2,3,\ldots 2t-1$, вычислялись элементарные симметрические функции σ_t; по алгоритму У.Питерсона определялись разряды, несущие информацию о сработавших проволочках МПК.

Работа выполнена в Лаборатории вычислительной техники и автоматизации ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна 1979

Gaidamaka R.I., Nikityuk N.M.

P10 - 12702

The Calculation of a Special Processor Operating By Elements of Galua $GF(2^m)$ Field by means of the SCHOONSCHIP Program

The calculation of special processor operating by elements of Galua $GF(2^m)$ field is performed. The computation was produced by means of the SCHOONSCHIP program of determination of coordinates of registered particles in multichannel detectors from multiwire proportional chambers. At the same time the construction of Galua field according to given irreducible polynomials of m was made. The matrix of wire correlations H^T was constructed, by means of which the block of information compression was received; the syndrome $s_j = \sum_{i=1}^{t} x_i^j$, $j=1,2,3,\ldots 2t-1$ was determined; elementary symmetric functions have been calculated; by means of Y.Piterson algorithm the classes with information about runned wires MIIK were defined.

The investigation has been performed at the Laboratory Computing Techniques and Automation, JINR.

Preprint of the Joint Institute for Nuclear Research. Dubna 1979

Известно, что теория многих кодов, служащих для исправления ошибок, базируется на теоремах линейной алгебры. В последнее время появился ряд работ, в которых предлагается использовать теорию алгебраического кодирования при разработке аппаратуры для сжатия данных и определения координат зарегистрированных в многоканальных детекторах частиц с многопроволочных пропорциональных камер /МПК/ [1-3].

Если рассматривать появляющуюся информацию с МПК как кодовое слово, состоящее из одних нулей, появление единиц в разрядах данного слова как ошибки, то с помощью синдрома корректирующего кода можно обнаружить и "исправить" появившиеся "ошибки", которые определяют координаты сработавших проволочек МПК.

Разрядность синдрома корректирующего кода значительно меньше разрядности кодового слова, поэтому запись в память ЭВМ синдрома, содержащего всю информацию о номерах сработавших проволочек, ощутимо сокращает массив информации с МПК и время считывания ее в память ЭВМ. Для построения блока сжатия данных [2] и декодирования синдрома корректирующего кода необходимо построение матрицы проверочных соотношений, которая состоит из элементов расширенного поля Галуа $GF(2^m)$ и последующих операций над этими элементами [4-6]. Здесь: 2 - характеристика поля, m - степень неприводимого многочлена, с помощью которого образуются элементы поля.

В качестве примера рассмотрим многочлен пятой степени $GF(2^m)$:

$$f(x) = x^5 + x^2 + 1 . \qquad /1/$$

Положим, что $\alpha^0 = 1000$, $\alpha = 01000$, $\alpha^2 = 00100$, $\alpha^3 = 00010$, $\alpha^4 = 00001$ - элементы поля Галуа $GF(2^5)$. α - корень многочлена /1/. Тогда остальные 26 элементов поля можно вычислить из уравнения $\alpha^5 = \alpha^2 + 1$, т.е.

$$\alpha^5 = 00100 + 1000 = 10100,$$
$$\alpha^6 = \alpha^5 \cdot \alpha = \alpha^3 + \alpha = 00010 + 01000 = 01010,$$
$$\alpha^7 = \alpha^6 \cdot \alpha = \alpha^4 + \alpha^2 = 00001 + 00100 = 00101$$

и т.д., причем в силу цикличности группы

$$\alpha^{31} = \alpha^0 = 10000 = 1 . \qquad /2/$$

Поэтому если мы возьмем, например, произведение $\alpha^{25}\cdot\alpha^{26}=\alpha^{51}$, то, учитывая /2/, получим $\alpha^{51}=\alpha^{31}\cdot\alpha^{20}=\alpha^{0}\cdot\alpha^{20}=\alpha^{20}$.

Используя неприводимые многочлены более высоких степеней, можно получить необходимое число различных элементов в группе: 64, 128, 256, 512 и т.д. Таблица неприводимых многочленов приведена в работе /7/.

В поле Галуа $GF(2^m)$ такие операции арифметических действий, как сложение, вычитание, равносильны и вычисляются по модулю 2. Поэтому аппаратное сложение двух и более элементов не представляет затруднений и реализуется при помощи стандартных микросхем.

Аппаратное умножение и деление параллельным способом реализуется при помощи схем И и ИЛИ, и для получения необходимых булевых выражений производятся операции над многочленами, представляющими элементы поля.

Представим элементы в виде многочленов. Перемножив их почленно, приведя подобные по модулю 2, получим булево выражение для умножения двух элементов поля Галуа.

Например, выразим множимое через

$$A=a_0\alpha^0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4, \qquad /3/$$

множитель через

$$B=b_0\alpha^0+b_1\alpha+b_2\alpha^2+b_3\alpha^3+b_4\alpha^4, \qquad /4/$$

их произведение через

$$C=c_0\alpha^0+c_1\alpha+c_2\alpha^2+c_3\alpha^3+c_4\alpha^4, \qquad /5/$$

где

$$c_0=a_0b_0+a_1b_4+a_2b_3+a_3b_2+a_4b_1+a_4b_4,$$

$$c_1=a_0b_1+a_1b_0+a_2b_4+a_3b_3+a_4b_2,$$

$$c_2=a_0b_2+a_1b_1+a_1b_4+a_2b_0+a_2b_3+a_3b_2+a_3b_4+a_4b_1+a_4b_3+a_4b_4,$$

$$c_3=a_0b_3+a_1b_2+a_2b_1+a_2b_4+a_3b_0+a_3b_3+a_4b_2,$$

$$c_4=a_0b_4+a_1b_3+a_2b_2+a_3b_1+a_3b_1+a_3b_4+a_4b_0+a_4b_3+a_4b_4.$$

Коэффициенты a_i, b_i, c_i в уравнениях /3/, /4/, /5/ принимают значения 0 или 1 в зависимости от элемента поля. Заметим, что при большом значении m получение булевых выражений вручную является весьма затруднительным процессом. В связи с этим умножение многочленов типа /3,4/, приведение подобных, возведение в квадрат, получение других, более

высоких степеней, а также булевых выражений для аппаратной реализации инверсного элемента производится на ЭВМ.

Известно, что операция деления элементов A и B поля Галуа выполняется по правилу $\frac{A}{B} = A \cdot B^{-1}$, где B^{-1} есть инверсный элемент от элемента B. ($B \neq 0$).

Существует несколько алгоритмов для вычисления инверсного элемента. С целью единообразия нами был выбран следующий алгоритм:

$$B^{-1} = B^2 B^4 B^8 \ldots B^{2m-1} = \{[\,|B|^2 B]^2 \ldots B\}^2, \qquad /6/$$

т.е. каждый шаг требует умножения текущего значения на B и возведения результата в квадрат m - 1 раз.

Расчет спецпроцессора по выбранному алгоритму заключается в следующем:

1. Построение элементов по заданным неприводимым многочленам степени m.

2. Построение матрицы проверочных соотношений H^T, на основе которой получен блок сжатия информации.

Общий вид матрицы H^T:

$$H^T = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha & \alpha^3 & \ldots & \alpha^{2t-1} \\ \vdots & \vdots & & \vdots \\ \alpha^{n-1} & \alpha^{3(n-1)} & \ldots & \alpha^{(2t-1)(n-1)} \end{vmatrix},$$

3. Определение синдрома /7,8,9/:

$$S_j = \sum_{i=1}^{t} X i^j \quad , \quad j = 1,2,3 \ldots 2t-1,$$

t - количество ошибочных разрядов в кодовом слове.

4. Вычисление элементарных симметрических функций σ_t по формулам

$$\sigma_1 = S_1 :$$

$$\sigma_2 = (S_1^2 \cdot S_3 + S_5)/(S_1^3 + S_3);$$

$$\sigma_3 = (S_1 \cdot S_5 + S_3^2 + S_1^3 \cdot S_3 + S_1^6)/(S_1^3 + S_3).$$

5. Определение разрядов, в которых произошла ошибка /координаты сработавших проволочек из МПК/, по алгоритму У.Питерсона /7/.

При расчете отдельных устройств спецпроцессора, связанного с громоздкими аналитическими вычислениями, была написана программа в системе SCHOONSCHIP.

Программа состоит из описания типа используемых переменных, Z - выражений, которые необходимо преобразовать, подстановок и команд, применяемых при вычислении данных Z - выражений, команд, образующих циклы, команд для запоминания результатов вычислений в памяти, команд исполнения.

Одна из секций программы реализует схему умножения. Двенадцать других секций преобразуют поэтапно выражение /6/. Последняя секция вычисляет инверсный элемент B^{-1} от B. Предпочтение программе на языке SCHOONSCHIP отдано из тех соображений, что она превосходит программы, написанные на других языках /используемые для аналитических вычислений/, как по простоте написания, так и по быстродействию.

Программа насчитывает около 500 перфокарт. Время счета по ней составляет около 5 минут.

ЛИТЕРАТУРА

1. Nikitjuk N.M., Rodzhabov R.S., Shafranov M.D. A New Method of Information Registration from Multiwire Proportional Chambers. Nuclear Instr. and Meth., 1978, v. 155, n. 3, p. 485-489.
2. Никитюк Н.М., Раджабов Р.С., Шафранов М.Д. Блок параллельного кодирования информации с многопроволочных пропорциональных камер. ПТЭ, 1978, № 4, с. 95-97.
3. Ancheta T.C. Syndrome-Source-Couding and its Universal Generalization. IEEE Trans. on Information Theory. 1976, v. IT-22, n. 4, p. 432-436.
4. Bartee T.C., Schneider P.I. Computation with finite Fields. Information and Control, 9163, v. 6, p. 73-98.
5. Davida G.I. Inverse of Elements of a Galois Field.Electronic Letters, 1972, v. 8, n. 21, p. 578-520.
6. Pradhan D.K. A Theory of Galois Switching Functions.IEEE Trans. on Computers, 1978, v.C.27, p. 239-248.
7. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. "Мир", М., 1976.
8. Van der Waerden B.L. Modern Algebra, F.Ungar Publishing Co., New York, v. 1,2.
9. Riordan J. An Introduction to Combinatorial Analysis, John Wiley and Sons, Inc., New York, 1958.

Рукопись поступила в издательский отдел
27 июля 1979 года.