



объединенный  
институт  
ядерных  
исследований  
дубна

P10-84-841

Р.И.Гайдамака, Н.М.Никитюк, В.П.Шириков

КОМПЛЕКС ПРОГРАММ  
ДЛЯ АВТОМАТИЗАЦИИ  
ЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ  
УСТРОЙСТВ СЖАТИЯ ИНФОРМАЦИИ,  
РАЗРАБАТЫВАЕМЫХ НА БАЗЕ  
АЛГЕБРАИЧЕСКОЙ ТЕОРИИ КОДИРОВАНИЯ

Направлено в журнал "Автоматика  
и вычислительная техника"

1984

В работах /2-11/ рассмотрены вопросы применения теории кодирования для создания устройств сжатия данных, регистрируемых в годоскопических системах многопроводочных пропорциональных камер /МПК/. Было показано, что, используя эту теорию, можно строить эффективные параллельные шифраторы на несколько событий, быстродействующие устройства для комбинаторного отбора событий.

Данная работа посвящена описанию комплекса программ для автоматизации логического проектирования и моделирования подобных устройств. Программы написаны на языках аналитических преобразований Schoonschip и Reduce, а также на автокоде для ЭВМ ЕС-1010 /12,13/.

#### ПРОГРАММА НАХОЖДЕНИЯ ЭЛЕМЕНТОВ ПОЛЯ ГАЛУА

Элементы поля Галуа  $GF(2^m)$  /ЭПГ/ - многочлены переменной  $X$ , принимающей значения 0 или 1 с коэффициентами, равными 0 или 1, для которых операции сложения, вычитания, умножения и деления определены специальным образом /1/.

Программа TABL для заданного неприводимого многочлена степени  $m$  вычисляет  $2^m - 1$  элементов поля Галуа  $GF(2^m)$ . Например при  $m = 3$  для неприводимого многочлена  $X^3 + X + 1$  элементами поля Галуа /2<sup>3</sup>/ являются многочлены  $a^0 = 1$ ;  $a^1 = X$ ;  $a^2 = X^2$ ;  $a^3 = X + 1$ ;  $a^4 = X^2 + X$ ;  $a^5 = X^2 + X + 1$ ;  $a^6 = X^2 + 1$ ;  $a^7 = 0 = 1$ .

Программа написана на языке Schoonschip.

#### ПРОГРАММА СОСТАВЛЕНИЯ МАТРИЦЫ ПРОВЕРОЧНЫХ СООТНОШЕНИЙ

Матрица  $H^T$  имеет вид

$$H^T = \begin{vmatrix} 1 & 1 & & 1 \\ a & a^3 & & a^{(2t-1)} \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ a^{n-1} & a^{3(n-1)} & \dots & a^{(2t-1)(n-1)} \end{vmatrix}$$

Число строк этой матрицы равно числу разрядов входной информации /например, числу проводочек МПК/, число столбцов - числу разрядов выходной сжатой информации /синдрома/

Программа MATR, написанная на языке Reduce, вычисляет коэффициенты полиномов, являющихся элементами матрицы  $H^T$ .

#### ПРОГРАММА МОДЕЛИРОВАНИЯ РАБОТЫ УСТРОЙСТВА СЖАТИЯ ИНФОРМАЦИИ

Приведенная выше матрица проверочных соотношений /матрица связей/  $H^T$  является, по существу, принципиальной схемой устройства сжатия информации /УСИ/. Для моделирования его работы используется программа RACH, написанная на автокоде для ЭВМ ЕС-1010.

В основу программы положен алгоритм У.Питерсона<sup>/1/</sup>. Координаты сработавших проволочек определяются из уравнения

$$X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3 = 0. \quad /1/$$

Прежде всего вычисляются  $\sigma_1, \sigma_2, \sigma_3$  по следующим формулам:

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

$S_1, S_2, S_3$  - формируются в блоке сжатия информации, а в память ЭВМ  $S_1, S_2, S_3$  поступают в виде  $n$ -разрядных слов.

Программа вычисляет элементарные симметрические функции  $\sigma_1, \sigma_2, \sigma_3$  по формулам /2/; затем, подставив их значения в выражение /1/, поступаем следующим образом.

Берем массив элементов поля Галуа  $GF(2^m)$ . Поочередно подставляем каждый элемент массива в уравнение /1/. Те элементы, которые удовлетворяют этому уравнению, и соответствуют номерам сработавших проволочек.

Программа позволяет опознать три возможных случая.

$S_1^3 = S_3$  - это означает, что сработала одна проволочка. Тогда  $S_1$  содержит двоичную информацию определенного элемента поля, что соответствует номеру сработавшей проволочки.

$S_1^3 \neq S_3$  - в этом случае вычисляются элементарные симметрические функции  $\sigma_1, \sigma_2, \sigma_3$  и подстановкой всех ненулевых элементов поля в уравнение /1/ поочередно определяется количество и номера сработавших проволочек.

Для этих же целей написана программа CONST, реализующая усложненный, но более эффективный алгоритм.

#### ПРОГРАММА ВЫЧИСЛЕНИЯ ДЕТЕРМИНАНТА МАТРИЦЫ

Программа DET, написанная на языке Reduce, вычисляет коэффициенты полинома, являющегося детерминантом матрицы<sup>/9/</sup>

$$L_t = \begin{vmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ S_2 & S_1 & 1 & 0 & \dots & 0 \\ S_4 & S_3 & S_2 & S_1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ S_{2t-4} & S_{2t-5} & S_{2t-6} & S_{2t-7} & \dots & S_{2t-3} \\ S_{2t-2} & S_{2t-3} & S_{2t-4} & S_{2t-5} & \dots & S_{2t-1} \end{vmatrix}.$$

Порядок матрицы - от 3 до 10-вычислен на ЭВМ.

#### ПРОГРАММА ВЫЧИСЛЕНИЯ ПЕРЕКЛЮЧАТЕЛЬНОЙ ФУНКЦИИ

Программа КОЕФ, написанная на языке Reduce, вычисляет переключательную функцию, представленную в виде

$$f(x) = G(0) + g_1 x + g_2 x^2 + \dots + g_{2^m-1} x^{2^m-1}. \quad /1/$$

Программа включает в себя подпрограмму вычисления коэффициентов  $g(k)$  по формуле

$$g(k) = \sum_{i=1}^{2^m-1} \alpha_i^{-k} [G(0) + G(j)], \quad /2/$$

$G(0)$  - значение функции при  $x = 0$ ;  $G(j)$  - текущее значение функции на выходе логического устройства;  $\alpha_i$  - элементы поля Галуа.

#### ПРОГРАММЫ ЭЛЕМЕНТАРНЫХ АНАЛИТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Кроме программ, описанных выше, комплекс включает в себя программы вычисления обратного многочлена /программа INV/и умножения многочленов /программа BOOL /.

Программы INV и BOOL написаны на языке Schoonschip.

Для вычисления обратного многочлена используется следующий алгоритм

$$B^{-1} = B^2 \cdot B^4 \dots B^{2(2^{n-1})} = \{ |B|^2 |B|^2^{n-1} \dots \}$$

Программа BOOL выполняет умножение двух элементов поля Галуа, представленных в виде многочленов:

$$A = A_0 \alpha^0 + A_1 \alpha + \dots + A_{2^m-1} \alpha^{2^m-1}; \quad B = B_0 \alpha^0 + B_1 \alpha + \dots + B_{2^m-1} \alpha^{2^m-1}.$$

Эта же программа позволяет возводить многочлен в степень, если положить  $V = A.C$  помощью программы BOOL можно спроектировать устройство для аппаратного умножения и возведения в степень многочленов от элементов поля Галуа  $GF(2^m)$ .

#### ЗАКЛЮЧЕНИЕ

Созданный комплекс программ используется при проектировании устройств сжатия информации, поступающей в ходе ядерно-физического эксперимента с многопроводочных пропорциональных камер.

#### ЛИТЕРАТУРА

1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. "Мир", М., 1976.
2. Блох Э.Л. "Известия Академии Наук СССР", "Техническая кибернетика", 1964, №3, с. 30-37.
3. Никитюк Н.М., Шафранов М.Д., Раджабов Р.С. "Приборы и техника эксперимента", 1978, №4, с. 95-98.
4. Никитюк Н.М. "Приборы и техника эксперимента", 1983, №3, с. 74-80.
5. Никитюк Н.М. ОИЯИ, P11-81-784, Дубна, 1981.
6. Никитюк Н.М. ОИЯИ, P11-80-484, Дубна, 1980.
7. Гайдамака Р.И., Раджабов Р.С. ОИЯИ, 10-1183, Дубна, 1977.
8. Гайдамака Р.И., Никитюк Н.М. ОИЯИ, P10-12-702, Дубна, 1979.
9. Гайдамака Р.И., Калинин В.А., Шириков В.П. ОИЯИ, P13-82-678, Дубна, 1982.
10. Гайдамака Р.И., Никитюк Н.М., Шириков В.П. В кн.: Совещание по системам и методам аналитических вычислений на ЭВМ и их применению в теоретической физике. Дубна, 1982. ОИЯИ, D11-83-511, Дубна, 1983, с. 246-252.
11. Гайдамака Р.И., Никитюк Н.М., Шириков В.П. В кн.: Аналитические вычисления на ЭВМ и их применение в теоретической физике. ОИЯИ, D11-80-13, Дубна, 1980, с. 181-185.
12. Reduce-2 user's MANUAL. UCP-19, Univ. of Utah, Salt Lake City, 1973.
13. Strubbe H. Comp.Phys.Comm., 1974, p. 8.

Рукопись поступила в издательский отдел  
24 декабря 1984 года.

Гайдамака Р.И., Никитюк Н.М., Шириков В.П. P10-84-841  
Комплекс программ для автоматизации логического проектирования устройств сжатия информации, разрабатываемых на базе алгебраической теории кодирования

Описан комплекс программ для аналитических преобразований выражений со специальными полиномами, являющимися элементами полей Галуа  $GF(2^m)$ . Эти программы используются для разработки принципиальных схем устройств сжатия информации, мажоритарных схем совпадений и устройств, реализующих переключательные функции. В комплекс входят также программы декодирования сжатой информации. Созданный комплекс программ используется при проектировании устройств сжатия информации, поступающей в ходе ядерно-физического эксперимента с многопроводочных пропорциональных камер.

Работа выполнена в Лаборатории вычислительной техники и автоматизации, ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна 1984

Перевод Н.С.Панковой

Gajdamaka R.I., Nikitjuk N.M., Shirikov V.P. P1P-84-841  
The Complex of Programs for Automation of Logical Designing of Data Compressed Devices, Developed on the Basis of Algebraic Soding Theory

The complex of programs for analytical transformations of expressions with special polynoms, which are the elements of Galua  $GF(2^m)$  fields is described. This programs are used for the development of principal schemes of data compression devices, majority coincidence schemes and for devices realized the switch function. This complex also contains the programs of compressed data decoding.

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

Preprint of the Joint Institute for Nuclear Research. Dubna 1984