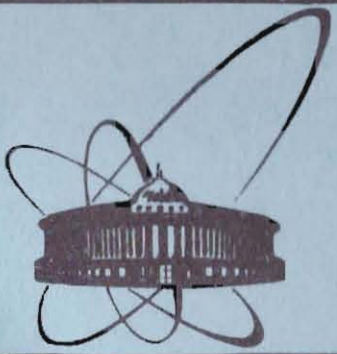

объединенный
институт
ядерных
исследований
дубна

Р10-84-865

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

РАСЧЕТ ПЕРЕКЛЮЧАТЕЛЬНЫХ ФУНКЦИЙ, ПРЕДСТАВЛЕННЫХ ЭЛЕМЕНТАМИ ПОЛЯ ГАЛУА $GF(2^m)$

Направлено в журнал
"Автоматика и вычислительная техника"

1984

Александров И.Н. и др.
Р10-84-865

Расчет переключательных функций,
представленных элементами поля Галуа $GF(2^m)$

Рассматриваются вопросы расчета переключательных функций с помощью ЭВМ. Входные и выходные переменные являются элементами поля Галуа $GF(2^m)$, что позволяет любую переключательную функцию m аргументов представить в виде полинома 2^m-1 степени. Приводятся примеры расчета конкретных схем. Перспективность такого направления синтеза переключательных функций заключается в том, что для их расчета можно использовать современные мощные ЭВМ и системы программирования. В результате открываются возможности для комплексной автоматизации проектирования больших интегральных схем, начиная от задания таблиц соответствия входов и выходов, минимизации, получения булевых выражений, описывающих структуру таких схем, вывод на терминал принципиальных схем, кончая разводкой печатных плат или созданием топологии интегральных схем.

Работа выполнена в Лаборатории вычислительной техники и автоматизации ОИЯИ.

Препринт Объединенного института ядерных исследований. Дубна 1984

Перевод Н.С.Панковой

Alexandrov I.N. et al.
P10-84-865

The Calculation of Switched Functions,
Produced by Elements of Galua Field of $GF(2^m)$

The question of calculation of switched functions with the help of computer is considered. Input and output variables is the elements of Galua field $GF(2^m)$, that allows to present any switched function arguments as m polynom of 2^m-1 power. The examples of calculation of concrete schemes are presented. The perspectiveness of such trends of synthesis of switched functions is in the fact, that for their computation the modern computers and programming systems may be used. As the result the possibilities for complex automation of large integral schemes designation, beginning from the set of tables of input and output correspondence, minimization, receiving of the bool expressions, described the schemes structure, printing-out to terminal principal schemes, ending with the spreading of printed board or the creation of integral schemes topology.

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

Preprint of the Joint Institute for Nuclear Research. Dubna 1984

В настоящее время переключательные функции, представленные элементами поля Галуа, находят все более широкое применение для синтеза логических схем при построении устройств сжатия и преобразования данных в ядерно-физических экспериментах.

Теория поля Галуа $GF(2^m)$ является естественным продолжением известной теории Булева поля. Представление переключательных функций в виде элементов поля Галуа $GF(2^m)$ /галуа-переключательные функции - ГПФ/ имеет ряд преимуществ:

- над переключательными функциями можно выполнять алгебраические операции, что упрощает проблему минимизации и ее формального представления;
- поскольку состояние входов и выходов комбинационной схемы или последовательностного автомата кодируется элементами поля Галуа, то следующее состояние можно представить как полиномиальную функцию текущего состояния и текущего выхода;
- представление переключательной функции в виде полинома, в котором как коэффициенты, так и переменные являются элементами поля Галуа $GF(2^m)$, при большом числе переменных ($m>3$) позволяет использовать стандартные системы программирования и современные мощные ЭВМ для расчета устройств дискретной логики;
- представление переключательной функции в виде полинома имеет еще и то преимущество, что описание многозначных и многоуровневых схем имеет весьма компактный вид.

Фундаментальные свойства ГПФ подробно изложены в [1]. В данной работе для расчета ГПФ в основном использован язык PL/1 и ЭВМ ЕС-1033. Любую переключательную функцию $f(x)=f(x_1,x_2,x_3\ldots x_m)$ m аргументов в поле Галуа $GF(2^m)$ можно представить в виде полинома [2,3]:

$$f(x_0,x_1,\ldots,x_{m-1}) = B(0)+A(1)x+A(2)x^2+A(3)x^3+\ldots+A(2^m-1)x^{2^m-1}. \quad /1/$$

Здесь и далее знак + будет обозначать сумму по модулю 2, а коэффициенты A(k) вычисляются из выражения:

$$A(k) = \sum_{i=1}^{2^m-1} a_i^{-k}\,[B(0)+B(a_j)], \quad k=1,2,3,\ldots 2^m-1, \qquad /2/$$

где $B(j)=B(a_j)$ - элементы подстановки, которые берутся из таблицы соответствия входов и выходов, B(0)- значение функции на нуле. Таким образом, для получения алгебраического выражения, с помощью которого реализуется необходимая логическая схема, заданная таблицей, достаточно выполнить следующие процедуры:

- по выбранному неприводимому полиному определяются все ненулевые элементы поля Галуа $GF(2^m)$;
- вычисляются коэффициенты $A(k)$;
- производится разложение коэффициентов $A(k)$ и степеней x по базисным элементам выбранного поля;
- приводятся подобные члены.

Известно, что любой ненулевой элемент в поле $GF(2^m)$ может быть представлен в виде $x_0 a^0 + x_1 a + x_2 a^2 + x_3 a^3 + \ldots + x\, a^m$; где $x_i \subset GF(2^m)$.

Рассмотрим несколько простых примеров.

Пример 1. $m = 3$. Заметим, что при $m \leq 3$ коэффициенты $A(k)$ могут быть без труда вычислены вручную. Составим таблицу соответствия. Слева в таблице показана последовательность ненулевых элементов поля Галуа $GF(2^m) - a_j$ и даны их двоичные эквиваленты, подаваемые на вход. Справа в таблице соответствия располагаются значения последовательности элементов, которые необходимо получить на выходе.

Таблица 1

$x=\{x_0x_1x_2\}$ / входы		$B(a_j)$ /		выходы
0	= 000	0	= 000	00
a^0	= 100	a^0	= 100	10
a	= 010	a^0	= 100	10
a^2	= 001	a^0	= 100	10
a^3	= 110	a^1	= 010	01
a^4	= 011	a^1	= 010	01
a^5	= 111	a^3	= 110	11
a^6	= 101	a^1	= 110	11
a^7	= 101	a	= 010	01
a^8	= 100			

В табл.1 элементы поля Галуа $GF(2^3)$, a^0, a^1, a^2, a^3, a^4, a^5, a^6 получены с помощью неприводимого полинома следующим образом.

Выбран неприводимый полином

$$X^3 + X + 1. \qquad /3/$$

Считаем, что элемент a^1 является корнем полинома /3/; a^0, a^2 - базисные элементы поля. В соответствии с правилами выполнения

операций в поле Галуа [4-7] получим остальные ненулевые элементы поля: подставив a^1 в выражение /3/, имеем: $a^3 + a + 1$; отсюда

$a^3 = a + 1$; $a^4 = a^3 \cdot a = a^2 + a$;

$a^5 = a^4 \cdot a = a^3 + a^2 = a^2 + a + 1$;

$a^6 = a^5 \cdot a = a^3 + a^2 + a = a^2 + 1$.

Нетрудно заметить, что с помощью табл.1 описывается работа обычного комбинационного сумматора на три входа и два выхода, как показано в табл.2.

Таблица 2

входы $x_0x_1x_2$	выходы СП
0 0 0	0 0
1 0 0	1 0
0 1 0	1 0
0 0 1	1 0
1 1 0	0 1
0 1 1	0 1
1 1 1	1 1
1 0 1	0 1

Здесь x_0, x_1, x_2 - значения первого, второго слагаемых и входа переноса, С, П - значения суммы и переноса на выходе сумматора. Для нашего примера, как это видно из табл.1, элементы подстановки B(1), B(2), B(3), B(4), B(5), B(6), B(7) представляют собой элементы поля $GF(2^3)$ a^0, a^0, a^0, a^1, a^3, a^1 соответственно. Тогда численное значение коэффициента A(1) получается из выражения

$$A(1) = \frac{a^0}{a^0} + \frac{a^0}{a^1} + \frac{a^0}{a^2} + \frac{a}{a^3} + \frac{a}{a^4} + \frac{a^3}{a^5} + \frac{a}{a^6} =$$

$$= a^0 + a^0 a^6 + a^0 a^5 + a^1 a^4 + a^1 a^3 + a^3 a^2 + a \cdot a =$$

$$= a^0 + a^6 + a^5 + a^5 + a^4 + a^5 + a^2 = a^0 + a^6 + a^4 + a^5 + a^2 = a^0 = 100.$$

Здесь операция деления двух элементов поля A и B заменена операцией умножения элемента A на инверсный элемент B^{-1} в соответствии с правилами, принятыми в поле Галуа $GF(2^m)$. Далее имеем:

$$A(2) = \frac{a^0}{(a^0)^2} + \frac{a^0}{(a)^2} + \frac{a^0}{(a^2)^2} + \frac{a}{(a^3)^2} + \frac{a}{(a^4)^2} + \frac{a^3}{(a^5)^2} + \frac{a}{(a^6)^2} =$$

$$= a = 010.$$

Аналогичные вычисления дают:

$A(3)=a^0=100$; $A(4)=A(7)=0$; $A(5)=a^4=011$; $A(6)=a^6=101$.

С учетом проведенных вычислений выражение /1/ имеет вид:

$$f(x)=x+ax^2+x^3+a^4x^5+a^6x^6. \qquad /4/$$

В принципе с помощью выражения /4/ можно построить схему одноразрядного сумматора. Однако такая схема была бы слишком громоздкой, т.к. для ее реализации потребовались бы схемы возведения в степень и схемы умножения двух элементов в поле Галуа $GF(2^3)$. Поэтому выражение /4/ целесообразно упростить, для чего достаточно коэффициенты a^4, a^6 и переменные x, x^2, x^3, x^5, x^6 представить в виде полиномов от базисных элементов. Например: $a^4=a^1+a^2$, $a^6=1+a^2$, $x^2=x_0+x_2a+(x_1+x_2)a^2$ и т.д. /см. Приложение/. Исходя из этого, имеем:

$$f(x)=(x_0+x_1a+x_2a^2)+a[x_0+x_2a+(x_1+x_2)a^2]+$$

$$+(x_0+x_1+x_2+x_1x_2)+[(x_1+x_0x_1+x_0x_2)a+(x_2+x_0x_1)a^2]+$$

$$+(a+a^2)[(x_0+x_1+x_2+x_1x_2)+(x_1+x_2+x_0x_2)a+(x_1+x_0x_1+x_0x_2)a^2]+$$

$$+(1+a^2)[(x_0+x_1+x_2+x_1x_2)+(x_2+x_0x_1)a+(x_1+x_2+x_0x_2)a^2].$$

После умножения и приведения подобных получим следующие булевы выражения, с помощью которых описывается работа одноразрядного полного сумматора: $C=x_0+x_1+x_2$; $\Pi=x_0x_1+x_0x_2+x_1x_2$. Оба равенства реализуются при помощи двух полусумматоров ПС1 и ПС2 /рис.1/. Такая схема получается, если для построения полусумматора использовать известную схему, состоящую из элементов И, ИЛИ и НЕ. Однако следует отметить, что в связи с развитием техники интегральных микросхем при создании схем дискретной логики все более широкое применение находит базис "Исключающее ИЛИ" и элемент И. Как показывают расчеты, при $m \geq 4$ трудоемкость вычислений резко возрастает, и в таких случаях возникает необходимость в использовании ЭВМ.

Пример 2. $m=4$. Рассчитаем схемы последовательностного автомата, на вход которого в заданные моменты времени последовательно подаются в порядке возрастания степеней элементы поля Галуа $GF(2^4)$, образованные над неприводимым полиномом X^4+X+1, а на выходе получаются элементы этого же поля, но в заданной последовательности. Зададим таблицу соответствия /см.табл.3/.

Слева в табл.3 представлена последовательность 15 ненулевых элементов поля $GF(2^4)$ и их двоичные эквиваленты. Справа даны значения элементов, которые необходимо получить на выходе схемы.

Таблица 3

входы $x=\{x_0x_1x_2x_3\}$	выходы $f(x)$
0=0000	0
a^0 = 1000	a =0100
a = 0100	0 =0000
a^2 = 0010	a^7 =1101
a^3 = 0001	a^5 =0110
a^4 = 1100	a^5 =0110
a^5 = 0110	a^{11}=0111
a^6 = 0011	a^{13}=1011
a^7 = 1101	a^0 =1000
a^8 = 1010	a^3 =0001
a^9 = 0101	a^{14}=1001
a^{10}= 1110	a^{14}=1001
a^{11}= 0111	0 =0000
a^{12}= 1111	a^2 =0010
a^{13}= 1011	a^4 =1100
a^{14}= 1001	a^0 =1000

Последовательность элементов поля $GF(2^4)$ в порядке возрастания их степеней получается довольно просто с помощью счетчика в поле Галуа $GF(2^4)$, который представляет собой сдвиговый регистр с логическими обратными связями /см. табл.3/ [7]. Если в младший разряд поместить единицу, а в остальные разряды - нули, то последовательные сдвиги регистра дают представление последовательных степеней элемента A, корня многочлена x^4+x+1, в такой же в точности форме, в какой они приведены в табл.3 слева, причем произвольный элемент A в поле $GF(2^4)$ имеет вид $A_0a^0+A_1a+A_2a^2+A_3a^3$. Для построения схемы, которая выполняла бы по существу функцию преобразования 4-разрядных кодов в соответствии с табл.3, необходимо прежде всего вычислить значения 16 коэффициентов в полиномиальном представлении функции 4 переменных:

$$f(x_0,x_1,x_2,x_3)=A(0)+A(1)x+A(2)x^2+A(3)x^3+A(4)x^4+A(5)x^5+A(6)x^6+$$

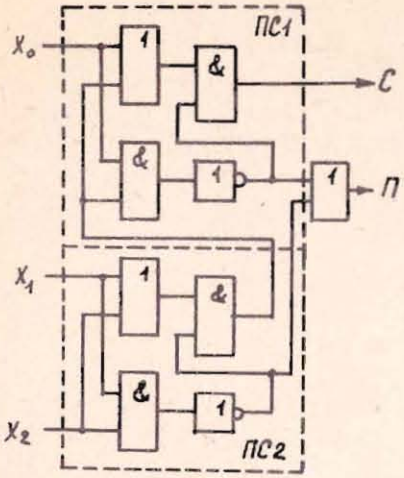

Рис.1. Принципиальная схема одноразрядного комбинационного сумматора. ПС1, ПС2 - полусумматоры.

$$+ A(4)x^4 + A(5)x^5 + A(6)x^6 +$$

$$+ A(7)x^7 + A(8)x^8 + A(9)x^9 +$$

$$+ A(10)x^{10} + A(11)x^{11} + A(12)x^{12} +$$

$$+ A(13)x^{13} + A(14)x^{14} + A(15)x^{15} ,$$

степени x в базисном виде и привести подобные. В результате получатся следующие выражения, разложенные по базисным элементам a^0, a , a^2 , a^3 :

$$x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_0x_1x_3 + x_1x_2x_3 + x_0x_1x_2x_3 \qquad <a^0>$$

$$x_0 + x_2 + x_3 + x_1x_3 + x_0x_1x_3 + x_1x_2x_3 \qquad <a>$$

$$x_3 + x_0x_1 + x_0x_3 + x_1x_2 + x_1x_3 + x_1x_2x_3 + x_0x_1x_2x_3 \qquad <a^2>$$

$$x_2 + x_1x_3 + x_0x_1x_3 + x_0x_2x_3 . \qquad <a^3>$$

Все необходимые вычисления для примера 2 выполнены на ЭВМ ЕС-1033. С этой целью была составлена программа на языке PL/1, которая выполняет вычисления в поле Галуа $GF(2^4)$,где $m \leq 12$, занимает 130К оперативной памяти. Заданные величины - число переменных m, неприводимый полином, значения $B(a_i)$ для всех a_i.

На данном этапе возможности программы таковы, что в процессе вычисления коэффициентов при каждом базисном элементе суммарное количество символов в сомножителях должно быть одинаковой длины / x_i считаем за один символ/ и не должно превышать 250. Вычисления выполняются итеративно:

$$F_k - F_{k+1}x + A_k ; \quad F_{2^m-1} = A_{2^m-1} ; \quad k = 2^m - 2 - 1 ; \quad A_0 = B(0) .$$

При $m = 4$ и $m = 5$ время, затрачиваемое центральным процессором, составляет 1 и 5 мин соответственно.

На рис.1 приведена принципиальная схема, в которой используются обычные ТТЛ-микросхемы, выпускаемые промышленностью. Нетрудно проверить, что данная схема выполняет функцию последовательностного автомата в соответствии с табл.2. Такие схемы

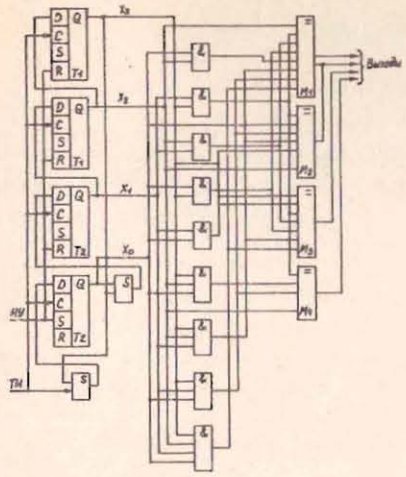

Рис.2. Принципиальная схема, реализующая уравнения /4/. Т1÷Т2 - D -триггеры, S - сумматор по модулю 2; М1-М4 - микросхемы 155ИП2, ТИ - тактовые импульсы, НУ - начальная установка.

могут быть использованы для получения заданной последовательности двоичных слов, например, в устройствах с микропрограммным управлением и пр. Для одновременного сложения по модулю 2 нескольких слагаемых можно применить микросхему типа 155ИП2 /рис.2/, которая имеет 8 входов, или микросхему К500НЕ160 на 12 входов /схемы проверки на четность/ [8].

При двухкаскадном включении схем проверки на четность можно просуммировать одновременно до 64 и 144 слагаемых соответственно и т.д. [9].

Пример 3. Расчет схемы для суммирования двух трехразрядных чисел с переносом. Очевидно, что такая схема имеет шесть входов для слагаемых /предполагаем, что вход для переноса от младшего разряда/, два выхода для суммы и один выход для переноса. В нашем примере это значит,что вычисления должны быть произведены над переключательной функцией шести переменных в поле Галуа $GF(2^6)$,состоящем из 63 ненулевых элементов, которые интерпретируются как 6-разрядные двоичные слова или как аргументы функции шести переменных x_0 , x_1 , x_2 , x_3 , x_4 , x_5 . Выбираем неприводимый полином шестой степени $x^6 + x + 1$. Таблица неприводимых полиномов до 34-й степени включительно приведена в [7]. В результате вычислений на ЭВМ получим следующие выражения:

$$x_0x_3 + x_0x_1x_4 + x_1x_3x_4 + x_0x_1x_2x_5 + x_0x_2x_4x_5 + x_1x_2x_3x_5 + x_2x_3x_4x_5 \qquad <a^0>$$

$$x_0 + x_3 + x_0x_4 + x_1x_2x_5 + x_2x_4x_5 \qquad <a>$$

$$x_1 + x_4 + x_2x_5 \qquad <a^2>$$

$$x_2 + x_5 . \qquad <a^3>$$

Заметим, что задание таблицы работы устройства, аналогичного рассмотренному в данном примере, можно автоматизировать, т.к.,

в отличие от последовательностного автомата, закон его функционирования заведомо известен.

ЗАКЛЮЧЕНИЕ

Приведенные в данной работе расчеты переключательных функций являются в основном экспериментальными. Полученные данные подтверждают возможность использования современных ЭВМ для автоматизированного синтеза переключательных функций относительно большого числа переменных / m порядка $2 \le m \le 12$/, а при совершенствовании программы может быть и больше. Основные совершенствования должны быть направлены на уменьшение времени счета на центральном процессоре и требуемой емкости ОЗУ. На этом пути имеются большие резервы. Наиболее трудоемкими являются вычисления, связанные с нахождением выражений для возведения в степень элементов и разложения их по базисным элементам с целью упрощения выражений. Но поскольку алгебра в поле Галуа $GF(2^m)$ является модулярной, то есть возможность по выбранным неприводимым полиномам выполнить эти операции заведомо, и результат хранить во внешней памяти.

Как видно из приведенных выше примеров, при таком методе синтеза переключательных функций, в качестве базовых элементов используются элементы И, сумматоры по модулю два и многовходовые схемы проверки на четность, которые по существу состоят из однотипных сумматоров по модулю 2 на два входа.

В связи с развитием техники интегральных микросхем, вопросам синтеза схем, в которых используются элементы И и сумматоры по модулю два, уделяется большое внимание /10,11/. В частности, это объясняется следующими факторами:

- нет необходимости вводить инверсию переменных, поскольку элемент инверсии содержится внутри сумматора;
- каноническое представление переключательной функции Рида-Маллера также реализуется более просто в базисе И, "исключающее ИЛИ" /12-14/;
- логические схемы, которые реализуют переключательные функции в базисе И и сумматор по модулю 2, как показывает опыт /10/, получаются более простыми по сравнению с базисом И, НЕ, хотя теоретически этот вопрос остается открытым. Этот фактор важен также с точки зрения построения многофункциональных БИС, состоящих из однотипных ячеек-сумматоров по модулю два;
- аналогичный базис широко используется при создании универсальных генераторов функций и динамически программируемых модулей, в интегральном исполнении /15/.

Расчет ГПФ с помощью ЭВМ открывает новые возможности для комплексной автоматизации проектирования устройств дискретной логики, начиная от задания таблиц, описывающих работу схемы, и кончая разводкой печатной платы или топологии интегральной схемы /ИС/.

ПРИЛОЖЕНИЕ

Описание поля Галуа $GF(2^m)$

Поле Галуа $GF(2^m)$ содержит 2^m-1 различных элементов, которые образуют циклический код. Среди них m элементов являются линейно-независимыми. Остальные элементы поля получаются путем линейной комбинации этих элементов. Более просто их можно получить с помощью неприводимых полиномов. Для определенности положим, что $m=3$. Неприводимый полином в данном случае является x^3+x+1. Линейно-независимыми элементами поля при $m=3$ будут $a^0 = 100$; $a^1 = 010$; $a^2 = 001$. С помощью линейно-независимых элементов поля Галуа любой другой элемент поля может быть представлен в виде многочлена. Представим, например, один из элементов в виде $A = A_0a^0 + A_1a^1 + A_2a^2$, тогда любой другой элемент поля будет отличаться от данного значениями коэффициентов A_0, A_1 и A_2, т.е. он будет, например, иметь вид $B = B_0a^0 + B_1a^1 + B_2a^2$, причем коэффициенты A_0, A_1, A_2 и B_0, B_1, B_2 в двоичной системе счисления принимают лишь значения 0 или 1. Предположив, что элемент a^1 является корнем полинома x^3+x+1, получим выражение a^3+a+1. В поле Галуа операции сложения и вычитания равнозначны и выполняются по модулю 2.

Таким образом, исходя из описанного выше, получим остальные элементы поля в рассматриваемом примере, когда $m=3$.

$$a^3 = a^1 + a^0 = 110; \quad a^4 = a^3a^1 = a^2 + a^1 = 011;$$

$$a^5 = a^4a^1 = a^2 + a^3 = a^2 + a^0 + a^1 = 111;$$

$$a^6 = a^5a^1 = a^3 + a^1 + a^2 = a^0 + a^1 + a^1 + a^2 = a^0 + a^2 = 101;$$

$$a^7 = a^6a^1 = a^1 + a^3 = a^1 + a^0 + a^1 = a^0.$$

Получается семь различных элементов поля $GF(2^3)$. Затем, в силу цикличности, как видим, все повторяется, т.е. $a^7 = a^0$; $a^8 = a^1$ и т.д. Здесь малой буквой a обозначен конкретный элемент поля. Учитывая, что $a^0 = 100$ - единичный элемент, получим $a^0 \cdot a^0 = a^0$.

Умножение двух элементов поля выполняется путем прямого умножения элементов, представленных в виде многочлена, т.е.

$$A * B = (A_0a^0 + A_1a^1 + A_2a^2) * (B_0a^0 + B_1a^1 + B_2a^2) =$$

$$= A_0a^0B_0a^0 + A_0a^0B_1a^1 + A_0a^0B_2a^2 + A_1a^1B_0a^0 + A_1a^2B_1 +$$

$$+ A_1a^3B_2 + A_2a^2B_0a^0 + A_2B_1a^3 + A_2B_2a^4.$$

Далее приведем подобные и вынесем общий множитель за скобки:

$$A * B = a^0(A_0B_0 + A_1B_2 + A_2B_1) + a^1(A_0B_1 + A_1B_0 + A_1B_2 + A_2B_1 + A_2B_2) +$$

$$+ a^2(A_0B_2 + A_1B_1 + A_2B_0 + A_2B_2).$$

Обозначив коэффициенты при a^0, a^1, a^2 через C_0, C_1, C_2 соответственно, получим:

$$C_0 = A_0B_0 + A_1B_2 + A_2B_1$$

$$C_1 = A_0B_1 + A_1B_0 + A_1B_2 + A_2B_1 + A_2B_2 \qquad /1/$$

$$C_2 = A_0B_2 + A_1B_2 + A_2B_0 + A_2B_2.$$

Устройства для параллельного умножения двух элементов в поле Галуа $GF(2^m)$ известны и описаны в литературе [3,5]. Если в выражении /1/ положим $A = B$, то получим выражения для возведения элемента поля $GF(2^3)$ в квадрат:

$$C_{02} = A_0A_0 + A_1A_2 + A_2A_1 = A_0 ;$$

$$C_{12} = A_0A_1 + A_1A_0 + A_1A_2 + A_2A_1 + A_2A_2 = A_2 ;$$

$$C_{22} = A_0A_2 + A_1A_1 + A_2A_0 + A_2A_2 = A_1 + A_2 .$$

Причем, как упоминалось выше, следует учесть, что $A_0A_0 = A_0$ и $A_1A_2 + A_2A_1 = 0$, т.е. если суммируется четное число одинаковых членов, то сумма равна нулю, а если суммируется нечетное число одинаковых членов, то результат равен одному члену, например, $A_1B_1 + A_1B_1 + A_1B_1 = A_1B_1$.

Путем итерации можно получить выражения для возведения элемента поля Галуа $GF(2^3)$ в куб, в четвертую, пятую и шестую степени.

$A^3 = A\,A^2$;

$C_{03} = A_0 + A_1 + A_2 + A_1A_2$; $C_{13} = A_0A_1 + A_0A_2 + A_1$; $C_{23} = A_0A_1 + A_2$;

$A^4 = A\,A^3$;

$C_{04} = A_0$; $C_{14} = A_1 + A_2$; $C_{24} = A_1$;

$A^5 = A\,A^4$;

$C_{05} = A_0 + A_1 + A_1A_2 + A_2$; $C_{15} = A_0A_2 + A_1A_2$; $C_{25} = A_0A_1 + A_1 + A_0A_2$;

$A^6 = A\,A^5$;

$C_{06} = A_0 + A_1 + A_2 + A_1A_2$; $C_{16} = A_2 + A_0A_1$; $C_{26} = A_1 + A_2 + A_0A_2$.

По полученным выражениям нетрудно построить схемы для возведения элемента поля $GF(2^3)$ в необходимую степень, используя элементы И и сумматоры по модулю 2.

Заметим, что при $m > 3$ умножение двух элементов поля и возведение их в степени чрезмерно громоздки, и получение выражений вручную весьма затруднительно. Есть программа, написанная на языке Schoonschip, реализующая данные операции.

ЛИТЕРАТУРА

1. Benjauthrit B., Reed I. Switching Functions on Computers, 1978, vol.C-27, w.8, p.757.
2. Menger K.C. IEEE Transaction on Computers, 1969, vol.C-18, No.3, p.241-250.
3. English W.R. IEEE Transaction on Computers, 1981, vol-C-30, No.3, p.225-229.
4. Bartec T.C., Schneider P.I. Information and Control, 1963, vol.6, No.1, p.79-98.
5. Tanaka H. et al. Information and Control, 1968, vol.13, No.1, p.75-84.
6. Никитюк Н.М. ОИЯИ, 11-80-484, Дубна, 1980.
7. Питерсон У. Коды, исправляющие ошибки. "Мир", М., 1964.
8. Аналоговые и цифровые интегральные микросхемы. /Под ред. Якубовского/. "Сов. радио", М., 1978.
9. Гайдамака Р.И. и др. ОИЯИ, Р13-82-628, Дубна, 1982.
10. Mukhopadhyay A.Schmitz. IEEE Transaction on Computers, 1970, vol.C-19, No.2, p.132.
11. Kodandapani K.L. Electronic Letter, 1973, vol.9, No.13, p.286.
12. Swamy S. IEEE Transaction on Computers, 1972, vol.C-21, No.9, p.1008.
13. Kodandapani K.L., Setlur R.V. IEEE Transaction on Computers, 1975, vol.C-24, No.6, p.628.
14. Pradhan D.K., Patel A.M. IEEE Transaction on Computers, 1975, vol.C-24, No.2, p.206.
15. Suarez R.E., Chang O., Aclam V. IEEE Transaction on Computers, 1981, vol.C-30, No.1, p.79.

Рукопись поступила в издательский отдел
29 декабря 1984 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
19.	Биофизика