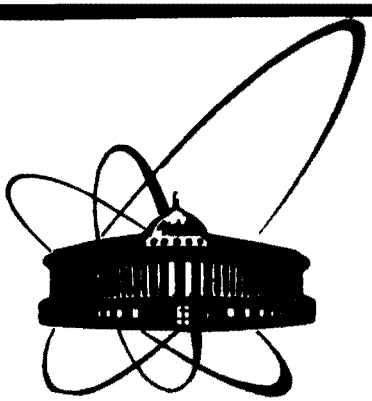

объединенный
институт
ядерных
исследований
дубна

Р11-87-54

Н.М.Никитюк

СОВМЕЩЕННЫЕ ОПЕРАЦИИ В ПОЛЕ ГАЛУА $GF(2^m)$ И ИХ ПРИМЕНЕНИЕ

Направлено в журнал "Управляющие системы и машины"

1987

I. Введение

В последнее десятилетие интенсивно развивается такое важное направление в информатике, как цифровая обработка сигналов, которая в теоретическом аспекте базируется на методах абстрактной алгебры, таких как группы, поля, кольца, быстрые алгоритмы и проч. /I,2/. В статье /I/, вышедшей в 1985 г., отмечается, что основная задача в этом направлении состоит в том, чтобы вскрыть тесную связь между цифровой обработкой сигналов и кодами с обнаружением ошибок. Однако следует отметить, что в работах советских авторов постановка и решение задачи объединения теории и практики цифровой обработки сигналов и теории корректирующих кодов начались еще 20 лет назад. Так, в 1966 г. И.В. Витенко и А.П. Стаховым был обнаружен "фибоначчиев" алгоритм измерения, который нашел применение при создании таких массовых приборов, как АЦП и ЦАП, имеющих ряд полезных свойств: возможность самоконтроля, отсутствие состязаний в процессе уравновешивания кодов, высокую точность и проч. Все это является следствием введения позиционного избыточного кода. Была развита также теория позиционных избыточных систем счисления и их применение в ЦВМ /3/.

Другим примером может служить применение алгебраической теории кодирования для создания различного рода устройств сжатия данных, поступающих от большого количества позиционно-чувствительных датчиков /4-6/. В таких устройствах используется свойство синдрома кодового слова нести информацию о координатах ошибок, возникающих в процессе передачи данных. Эффект сжатия проявляется в том, что исходное слово рассматривается как нулевое кодовое слово, а появлению событий в некотором числе датчиков ставятся в соответствие векторы ошибок. В конечном итоге передаче подлежит синдром кодового слова, в котором число единиц при условии, что одновременно срабатывает ограниченное число датчиков /порядка 10-20%/, меньше, чем число каналов передачи. Результатом такого подхода явилась разработка нового типа устройств - параллельных шифраторов на t событий ($t>1$), которые являются аналогами параллельных декодеров, применяемых в теории и практике кодирования, и специализированных процессоров для быстрого отбора событий в ядерно-физических экспериментах / 7/.

Как известно, вычислительные операции в теории кодирования выполняются с использованием алгебры Галуа. Теоретическая и практическая значимость такой алгебры существенно возрастает в связи с развитием таких направлений, как космическая связь, в которой широко ис-

пользуются коды Рида-Соломона /8/, галуа-переключательные функции, где переменные и коэффициенты представляются в виде элементов поля Галуа /9-II/, создание универсальных динамически программируемых модулей /I2/ и сигнатурный анализ /I3-I4/.

Исторически сложилось так, что развитие и применение нашли в основном последовательные методы выполнения операций в поле Галуа. Параллельные алгоритмы для выполнения операций умножения и деления в поле Галуа описаны в работе /I5/. В работе /I6/ приводится метод параллельного вычисления инверсного элемента. В связи с развитием микроэлектроники реализация параллельных алгоритмов в поле Галуа становится все более привлекательной и экономически обоснованной. Цель данной работы состоит в том, чтобы, используя специфику теории поля Галуа, обосновать возможность одновременного параллельного выполнения операций над выражениями, содержащими несколько элементов, в том числе и таких, которые находятся под степенью. Подобные операции автором условно названы совмещенными операциями. Возможно, что с теоретической точки зрения выполнение таких операций является очевидным. Однако, как отмечают теоретики, широкое внедрение в практику алгебраической теории тормозится из-за сложности восприятия инженерами математического аппарата современной абстрактной алгебры. Исходя из этих соображений, а также из того факта, что алгебра Галуа носит модулярный характер, реализация совмещенных операций в данной работе рассматривается на конкретных примерах .

2. Основные понятия теории поля Галуа

Мы будем рассматривать только конечное поле, содержащее p элементов, или поле Галуа, которое обозначается как $GF(p)$. Более того, с целью упрощения изложения и, исходя из того, что в настоящее время наиболее широкое применение находят логические схемы с двумя устойчивыми состояниями, мы ограничимся рассмотрением поля $GF(2)$, которое содержит два элемента I и 0, и расширенного поля, которое обозначается как $GF(2^m)$.

В поле $GF(2)$ имеют место следующие таблицы сложения и умножения:

+	0	I
0	0	I
I	I	0

·	0	I
0	0	0
I	0	I

Сложение и умножение ассоциативны и коммутативны, а умножение, как обычно, дистрибутивно относительно сложения: $A(B + C)=AB+AC$. Каждый элемент A имеет единственный противоположный элемент A, такой, что $A+(-A)=0$. Заметим, что в арифметике по модулю два операции сложения и вычитания равносильны. Далее, каждый ненулевой элемент A имеет

единственный обратный элемент $1/A$, такой, что $A\cdot 1/A = 1$. Для каждого элемента A выполняются равенства $0+A=A=1\cdot A$ /I,2/. Поле $GF(2)$ называется основным полем. В дальнейшем мы будем рассматривать расширенное поле степени m над основным полем. Такое поле имеет обозначение $GF(2^m)$. Расширенное поле создается путем добавления элемента a к полю $GF(2)$. Элемент a, называемый примитивным элементом, является корнем неприводимого полинома степени m . Таблицы неприводимых полиномов над полем $GF(2)$ вплоть до 34-й степени приведены в приложении В /I7/. Расширенное поле состоит из всех полиномов степени m-I или меньше, и все операции выполняются по модулю неприводимого многочлена степени m .

Роль и значение примитивного элемента в образовании поля описывается следующей теоремой /I8/: в конечном поле порядка n существует такой элемент a, что каждый ненулевой элемент этого поля может быть представлен как некоторая степень элемента a. Другими словами, если поле содержит элемент a, то оно должно содержать и все степени $a, a^2, a^3, \ldots a^{2^m-1}$. Далее, так как поле содержит мультипликативный обратный каждого ненулевого элемента, то ему принадлежат также $a^{-1}, a^{-2}, \ldots a^{-(2^m-1)}$. Наименьшее из положительных чисел n , для которых $a^n=1$ (1- вектор), т.е. $a^n=a^0$, называется порядком элемента a или, что то же самое: порядок элемента a равен числу различных степеней этого элемента.

Ниже в качестве примера мы будем рассматривать поле Галуа $GF(2^4)$, образованное над неприводимым полиномом X^4+X+1 (I). В этом поле имеется четыре линейно независимых элемента: $a^0 = 1000$, $a = 0100$, $a^2 = 0010$ и $a^3 = 0001$, причем элемент a является корнем полинома (I), так что имеем равенство: $a^4 = a + 1 = a + a^0 = 1100$. Из этого равенства нетрудно получить остальные элементы поля: $a^5 = a^4\cdot a = a^2 + a = 0110$, $a^6 = a^3 + a^2 = 0011$, $a^7 = a^4 + a^3 = a^0 + a^1 + a^3 = 1101$ и т. д. , $a^{15} = a^{14}\cdot a = (a^0 + a^3)a = a^0 + a + a = 1 = a^0 = 1000$.

В табл.I даны представления элементов поля $GF(2^4)$. Видно, что элементы поля Галуа можно представить четырьмя способами: в виде степеней примитивного элемента a, в виде полинома m-I степени, в виде двоичного эквивалента и в виде минтермов $X = (X_0, X_1, X_2, X_3)$, где X - элемент поля, а X_0, X_1, X_2, X_3- двоичные переменные. В виде полинома m- I степени два произвольных элемента в поле Галуа $GF(2^4)$ представляются следующим образом: $A = A_0a^0 + A_1a + A_2a^2 + A_3a^3$ и $B = B_0a^0 + B_1a + B_2a^2 + B_3a^3$, где A_0- A_3 и B_0- B_3 могут принимать значение 0 или I. Следует отметить, что в поле Галуа, в отличие от бесконечного поля с позиционной системой счисления, нет таких понятий, как одно число больше другого. Однако этот факт не умаляет прикладного

значения теории конечных полей в современной вычислительной технике.

Таблица I

I	2	3	4
0	0	0000	$\bar{X}_0\bar{X}_1\bar{X}_2\bar{X}_3$
a^0	I	I000	$X_0\bar{X}_1\bar{X}_2\bar{X}_3$
a^1	a	0I00	$\bar{X}_0X_1\bar{X}_2\bar{X}_3$
a^2	a^2	00I0	$\bar{X}_0\bar{X}_1X_2\bar{X}_3$
a^3	a^3	000I	$\bar{X}_0\bar{X}_1\bar{X}_2X_3$
a^4	I $+a$	II00	$X_0X_1\bar{X}_2\bar{X}_3$
a^5	$a+a^2$	0II0	$\bar{X}_0X_1X_2\bar{X}_3$
a^6	a^2+a^3	00II	$\bar{X}_0\bar{X}_1X_2X_3$
a^7	I $+a+a^3$	II0I	$X_0X_1\bar{X}_2X_3$
a^8	I $+a^2$	I0I0	$X_0\bar{X}_1X_2\bar{X}_3$
a^9	$a+a^3$	0I0I	$\bar{X}_0X_1\bar{X}_2X_3$
a^{10}	I $+a+a^2$	III0	$X_0X_1X_2\bar{X}_3$
a^{11}	$a+a^2+a^3$	0III	$\bar{X}_0X_1X_2X_3$
a^{12}	I $+a+a^2+a^3$	IIII	$X_0X_1X_2X_3$
a^{13}	I $+a^2+a^3$	I0II	$X_0\bar{X}_1X_2X_3$
a^{14}	I $+a^3$	I00I	$X_0\bar{X}_1\bar{X}_2X_3$
$a^{15}=$ I			

3. Операции умножения и возведения в степень

Выполнение операции умножения вручную выглядит весьма просто: степень элемента произведения равна сумме степеней сомножителей. При этом учитывается цикличность поля. В табл. 2 приведена таблица умножения двух элементов A и B в поле $GF(2^4)$. Например, если $A = a^{12}$ и $B = a^9$, то произведение $A*B = a^{21} = a^{15}\cdot a^6 = a^6$. Такие таблицы можно использовать для составления другого рода таблиц, с помощью которых программируются ПЗУ (табл.3). Выпускаемые промышленностью микросхемы К500РЕI49 и К556РТ4 емкостью 256x4 бит можно использовать для построения схемы умножения двух элементов в поле $GF(2^4)$. Если же применить двухкаскадное включение таких схем, то можно построить схему для одновременного умножения четырех элементов, как это показано на рис.I.

Операцию возведения в степень можно рассматривать как частный

Таблица 2
Умножение двух элементов в поле Галуа $GF(2^4)$

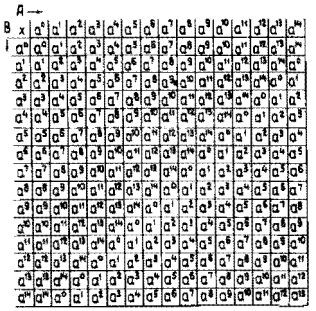

Таблица 3
Часть таблицы для программирования ПЗУ типа К500РЕI49

N	A	B	A	B	A×B
0	0000	0000	0	0	0 0
1	0000	0001	0	1	0 0
2	0000	0010	0	2	0 0
3	0000	0011	0	3	0 0
.	. .	. .	.	.	. .
15	0000	1111	0	F	0 0
16	0001	0000	1	0	0 0
17	0001	0001	1	1	21
18	0001	0010	1	2	42
19	0001	0011	1	3	41
20	0001	0100	1	4	84
21	0001	0101	1	5	84 21
22	0001	0110	1	6	8 2
23	0001	0110	1	7	8 1
24	0001	1000	1	8	1
25	0001	1001	1	9	2
26	0001	1010	1	A	42 1
27	0001	1011	1	B	4

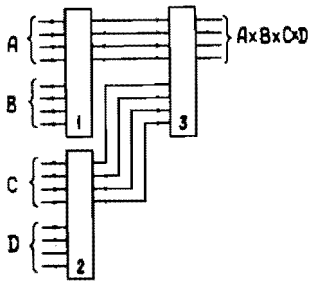

Рис.I. Схема для умножения 4 элементов в поле Галуа $GF(2^4)$.
I-3 - ПЗУ типа К500РЕI49.

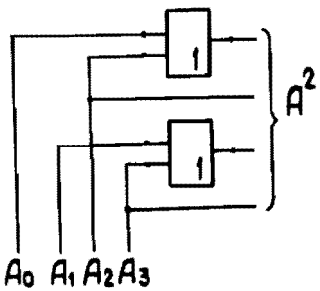

Рис.3. Схема для возведения элемента A в квадрат в поле Галуа $GF(2^4)$. Микросхема - К500ЛП107.

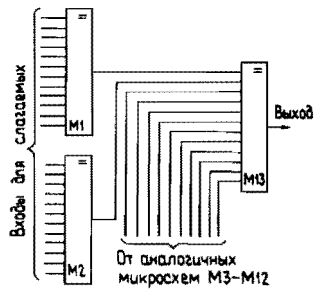

Рис.2. Схема сумматора по модулю два на I44 входа.
I-I3 - микросхемы К500ИЕI60.

случай умножения K раз одного и того же элемента. Например, если элемент $A = a^4$ и $K = 8$, то $(A)^K = (a^4)^8 = a^{32} = (a^{15})^2 a^2 = a^2$. Следует отметить, что для реализации возведения в степень требуется меньше логических элементов, чем для схемы умножения, хотя бы потому, что число входов ППЗУ в первом случае должно быть в два раза меньше. Если требуется высокое быстродействие, то операцию умножения можно реализовать с помощью микросхем малой степени интеграции. Имеем

$$P = A \times B = (A_0 a^0 + A_1 a + A_2 a^2 + A_3 a^3)(B_0 a^0 + B_1 a + B_2 a^2 + B_3 a^3) = \quad (1)$$
$$= P_0 a^0 + P_1 a + P_2 a^2 + P_3 a^3, \text{ где коэффициенты } P_0, P_1, P_2 \text{ и}$$

P_3 представляют собой булевы функции, определяемые из выражений / 2/:

$$P_0 = A_0 B_0 + A_1 B_3 + A_2 B_2 + A_3 B_1 \qquad \langle a^0 \rangle$$
$$P_1 = A_0 B_1 + A_1 B_0 + A_1 B_3 + A_2 B_2 + A_2 B_3 + A_3 B_2 + A_3 B_1 \qquad \langle a \rangle \quad (2)$$
$$P_2 = A_0 B_2 + A_1 B_1 + A_2 B_0 + A_2 B_3 + A_3 B_2 + A_3 B_3 \qquad \langle a^2 \rangle$$
$$P_3 = A_0 B_3 + A_1 B_2 + A_2 B_1 + A_3 B_0 + A_3 B_3 \qquad \langle a^3 \rangle$$

В приложении дан подробный вывод равенств (2).

Пример. Пусть элементы A и B соответственно равны $a^6 = 0011$ и $B = a^{12} = 1111$. Тогда $A \times B = a^{18} = a^3$. Проверка: $A_0 = A_1 = 0$ и $A_2 = A_3 = B_0 = B_1 = B_2 = B_3 = 1$. Из выражений (2) имеем $P_0 = P_1 = P_2 = 0$ и $P_3 = 1$. Окончательно имеем $A \times B = P_3 a^3 = a^3$.

Как видно из выражений (2), для построения схемы умножения двух элементов необходимы логические элементы И и многовходовые сумматоры по модулю два, которые по существу представляют схемы проверки на четность. На рис.2 в качестве примера приведена схема такого сумматора на 144 входа, которая построена на однотипных микросхемах К500 ИЕ160. Для этих же целей можно использовать микросхемы КП55ИП2 и К531ИП5. Используя выражения (2), можно получить соотношения для одновременного умножения трех, четырех и т.д. элементов.

Если в выражениях (2) положить A=B, то получим равенства, с помощью которых можно построить схему для возведения элемента A в квадрат:

$$P_0^2 = A_0 A_0 + A_1 A_3 + A_2 A_2 + A_3 A_1 = A_0 + A_2 \qquad \langle a^0 \rangle$$
$$P_1^2 = \cancel{A_0 A_1} + \cancel{A_1 A_0} + \cancel{A_1 A_3} + A_2 A_2 + \cancel{A_2 A_3} + \cancel{A_3 A_2} + \cancel{A_3 A_1} = A_2 \qquad \langle a \rangle \quad (3)$$
$$P_2^2 = \cancel{A_0 A_2} + A_1 A_1 + \cancel{A_2 A_0} + \cancel{A_2 A_3} + \cancel{A_3 A_2} + A_3 A_3 = A_1 + A_3 \qquad \langle a^2 \rangle$$
$$P_3^2 = \cancel{A_0 A_3} + \cancel{A_1 A_2} + \cancel{A_2 A_1} + \cancel{A_3 A_0} + A_3 A_3 = A_3$$

На рис.3 приведена принципиальная схема для возведения элемента A в квадрат. Если выполнить умножение

$$A \times A^2 = (A_0 a^0 + A_1 a + A_2 a^2 + A_3 a^3)\left[(A_0 + A_2) a^0 + A_2 a + (A_1 + A_3) a^2 + A_3 a^3)\right],$$

то получим выражения для возведения элемента A в куб:

$$P_0^3 = A_0 + A_0 A_2 + A_1 A_2 + A_1 A_3 \qquad \langle a^0 \rangle$$
$$P_1^3 = A_0 A_1 + A_0 A_2 + A_2 A_3 + A_3 \qquad \langle a \rangle \quad (4)$$
$$P_2^3 = A_0 A_2 + A_2 + A_1 A_2 + A_0 A_1 + A_1 A_3 + A_0 A_3 + A_2 A_3 \qquad \langle a^2 \rangle$$
$$P_3^3 = A_2 A_3 + A_1 + A_2 + A_1 A_3 + A_3 \qquad \langle a^3 \rangle$$

По аналогии можно получить выражения для возведения элемента A и в другие степени. Пример. Пусть элемент $A = 1001$, т.е. $A_0 = A_3 = 1$ и $A_1 = A_2 = 0$. Тогда $A^3 = a^{42} = a^{12}$. Из выражений (4) имеем $P_0 \div P_3 = 1$.

Как уже отмечалось выше, операция деления элемента A на элемент B равносильна умножению элемента A на элемент B, инверсный к элементу B. При вычислениях вручную степень инверсного элемента равна $2^m - 1$ минус степень исходного элемента. Так, если $B = a^5$, то $B^{-1} = a^{10}$, поскольку 15 - 10 = 5. Проверка дает $a^5 \cdot a^{10} = a^{15} = a^0 = 1$. Вычисление инверсного элемента, представленного в полиномиальном виде, рассмотрено в работе /16/.

4. Выполнение совмещенных операций

Под совмещенными операциями в поле Галуа будем подразумевать одновременное выполнение таких операций, как умножение нескольких элементов (больше двух), вычисление сложных выражений, содержащих множители (делители) под степенью, а также таких, которые содержат сумму сложных выражений, многочленов и проч. В силу конечности поля в результате вычислений сколь угодно сложных выражений в конечном итоге получается значение одного из элементов данного поля.

Возможно, что с теоретической точки зрения такой вывод является очевидным. Однако автору неизвестны работы, в которых совмещенные операции использовались в инженерной практике. Причина такого явления, видимо, кроется в недооценке практического значения модулярной алгебры. Следует отметить, что вычисления вручную, особенно при величинах $m > 4$, становятся громоздкими. Поэтому в Объединенном институте ядерных исследований для этих целей используются системы аналитических преобразований и вычислений на больших ЭВМ /19/. Выполнение совмещенных операций и их применение мы рассмотрим на конкретных примерах.

Допустим, что мы хотим получить коэффициенты при a^0, a^1, a^2 и a^3 для совмещенной операции $BA^2 = (B_0 a^0 + B_1 a + B_2 a^2 + B_3 a^3)\left[(A_0 + A_2) a^0 + A_2 a + (A_1 + A_3) a^2 + A_3 a^3\right]$. Более детально процесс вычисления соответствующих коэффициентов K_0, K_1, K_2, и K_3 приведен в приложении. Эти значения равны:

$$K_0 = B_0A_0 + B_0A_2 + B_2A_1 + B_3A_2 + B_1A_3 + B_2A_3 \qquad \langle a^0 \rangle$$
$$K_1 = B_0A_2 + B_1A_2 + B_2A_1 + B_1A_3 + B_3A_2 + B_3A_1 + B_3A_3 + B_1A_0 \qquad \langle a \rangle$$
$$K_2 = B_0A_1 + B_0A_3 + B_1A_2 + B_2A_0 + B_2A_2 + B_3A_1 \qquad \langle a^2 \rangle \quad (5)$$
$$K_3 = B_0A_3 + B_1A_1 + B_1A_3 + B_2A_2 + B_3A_0 + B_3A_2 + B_3A_3 \qquad \langle a^3 \rangle$$

Пример. Пусть $B = a^3$ и $A = a^{12}$, тогда $BA^2 = a^3 (a^{12})^2 = a^{27} = a^{12}$. Поскольку $B_3 = A_0 = A_1 = A_2 = A_3 = I$ и $B_0 = B_1 = B_2 = 0$, то $K_0 = K_2 = K_1 = K_3 = I$. Или, другими словами, $BA^2 = a^3 (a^{12})^2 = a^{12}$.

В работах /20,21/ автором предложены варианты логических ячеек для аппаратной реализации умножения (деления типа BA^K (B/A^K), где $K = I \div 2^{m-2}$, которые могут быть выполнены в виде интегральных микросхем (рис.4). При $m = 4$ ячейка состоит из матрицы логических элементов И, I4 групп сумматоров по модулю два и четырех мультиплексоров MI-M4, каждый из которых имеет по I4 информационных и 4 адресных входа для выбора номера информационного канала. Выходы матрицы элементов И соединены со входами соответствующих групп сумматоров по модулю два таким образом, чтобы при поступлении заданного кодового слова на адресные входы мультиплексоров на выходах ячейки формировался бы результат одного из произведений (частного) типа BA^K (B/A^K). Практически это значит, что с помощью одной ячейки, содержащей I6 контактов, можно вычислять I4 различных произведений (частных), начиная от произведения (частного) BA (B/A) и кончая произведением (частным) BA^{14} (B/A^{14}). Аналогично можно построить логические ячейки для реализации более сложных выражений.

Из-за отсутствия таких стандартных ячеек для реализации совмещенных операций можно использовать модули ППЗУ, выпускаемые промышленностью. В табл.4 приведена таблица умножения элемента B на элемент A^3. С помощью такой таблицы нетрудно построить таблицу для программирования модуля ППЗУ. Следует отметить, что сложность реализации того или иного выражения в поле Галуа следует оценивать не по виду алгебраического выражения, а по числу входов ППЗУ.

Количество различных выражений, в которых можно использовать совмещенные операции, неисчислимо. Поэтому имеет смысл рассмотреть наиболее типичные и интересные с практической точки зрения примеры.

5. Применение совмещенных операций

I. Синтез переключательных функций (ПФ). Теория поля Галуа $GF(2^m)$ является естественным продолжением теории булева поля m переменных. Однако представление ПФ в поле Галуа имеет ряд преимуществ.

- Над ПФ можно выполнять алгебраические операции, что упрощает проблему минимизации и ее формального представления.

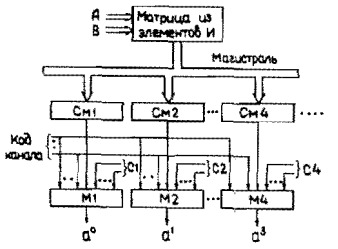

Рис.4. Логическая ячейка для реализации умножения типа BA^K:

См1-См4 - сумматоры по модулю два,

M1-M4 - мультиплексоры,

C1-C4 - выходы других групп сумматоров по модулю два.

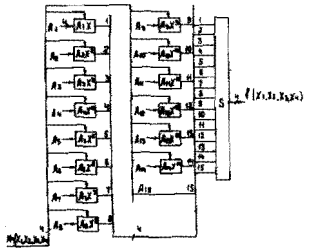

Рис.5. Блок-схема универсального динамически программируемого модуля.

A →

B ↓ / BA^3	a^0	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}
a^0	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}
a^1	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}
a^2	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}
a^3	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0
a^4	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1
a^5	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2
a^6	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3
a^7	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4
a^8	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5
a^9	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6
a^{10}	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7
a^{11}	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8
a^{12}	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9	a^{12}	a^0	a^3	a^6	a^9
a^{13}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}	a^{13}	a^1	a^4	a^7	a^{10}
a^{14}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}	a^{14}	a^2	a^5	a^8	a^{11}

Таблица 4
Умножение элемента B на элемент A^3

- Поскольку состояния входов и выходов комбинационной схемы или последовательностного автомата кодируются элементами поля Галуа, то следующее состояние можно представить как полиномиальную функцию текущего состояния и текущего выхода.
- Представление ПФ в виде полинома, в котором как коэффициенты, так и переменные являются элементами поля Галуа при большом числе переменных ($m > 3$), позволяет использовать стандартные аналитические системы программирования и современные мощные ЭВМ для расчета сложных устройств дискретной логики.
- Описание многозначных и многоуровневых (в недвоичном случае) схем приобретает весьма компактный вид.

Известно, что любую ПФ $f(X) = (X_0, X_1, \ldots X_{m-1})$ m аргументов можно представить в виде полинома /9-II/:

$$f(X_0, X_1, \ldots X_{m-1}) = B(0) + A(1)X + A(2)X^2 + A(3)X^3 + \ldots A(2^m-1)x^{2^m-1},$$

где $X = X_0a^0 + X_1a + X_2a^2 + \ldots X_{m-1}a^{m-1}$ - элемент (6)

поля $GF(2^m)$ (обобщенная входная переменная), а коэффициенты

$$A(K) = \sum_{i=1}^{2^m-1} a_i^{-K}\,[B(0) + B(A_j)],\ K = 1,2,3,\ldots 2^m - 1. \quad (7)$$

В последнем равенстве значения $B(a_j)$ - элементы подстановки, которые берутся из таблицы соответствия входов и выходов, $B(0)$ - значение функции на нуле. Так, при $m = 4$ равенство (7) имеет вид (при $B(0) = 0$)

$$f(X_0, X_1, X_2, X_3) = A(1)X + A(2)X^2 + A(3)X^3 + \ldots + A(14)X^{14} + A(15)X^0.$$

С помощью данного соотношения можно реализовать все 65536 ПФ 4 переменных, для чего необходимо знать коэффициенты $A(K)$. Как это следует из равенства (7), вычисление таких коэффициентов сводится к вычислению выражений типа B/A^K с последующим суммированием по модулю два. Для реализации динамически программированного логического устройства необходимо иметь логические модули для выполнения совмещенной операции типа AX^K. На рис.5 приведена блок-схема универсального динамического модуля 4 переменных /II,I2,22/. Модуль содержит 4 информационных входа и 4 выхода. Для подачи коэффициентов настройки требуется 15x4 входов. Если для выполнения операции типа BA^K использовать ППЗУ К500РЕ149, то такие схемы получаются однотипными.

Декодирование кодов, исправляющих ошибки. Наиболее популярными кодами, имеющими алгебраическую структуру, являются БЧХ-коды и коды Рида-Соломона. В частности, для БЧХ-кода, исправляющего три ошибки, имеет место следующее равенство: $X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3 = 0$, (8)

где $X = X_1, X_2, X_3$ - координаты ошибочных позиций. В свою очередь S_1, S_3 и

S_5 - симметрические функции, получаемые из матрицы проверочных соотношений БЧХ-кода /I7/. Из соотношения (8) видно, что совмещенные операции могут быть успешно использованы для построения быстродействующих декодеров.

Свойство синдрома БЧХ-кода нести в себе информацию не только о количестве ошибок при передаче кодового слова, но и в сжатом виде содержать данные об их позициях было использовано для создания нового типа параллельных шифраторов и логических процессоров для быстрого отбора событий в ядерно-физических экспериментах /4-7,23, 24/.

Метод сжатия информации на основе синдромного кодирования может быть использован и в других многодатчиковых системах, где число одновременно сработавших датчиков мало по сравнению с их общим количеством.

В связи с бурным развитием космической связи в зарубежной литературе большое внимание уделяется совершенствованию кодирующих и декодирующих устройств для кодов Рида-Соломона /25-27/. С помощью таких кодов можно эффективно исправлять как независимые ошибки, так и пакеты ошибок. По определению кодовое слово в коде Рида-Соломона содержит $2^m - I$ символов, причем каждый символ имеет m бит. Среди этих символов имеется $2^m - I - 2E$ информационных символов и $2E$ проверочных, где E - гарантируемое число символов, исправляемых кодом. Если рассматривать $2^m - I - 2E$ информационных символов в качестве коэффициентов полинома

$$f(X) = X^{2E}\left(C_{2^m-1-2E} + C_{2^m-2}X + \ldots + C_1 X^{2^m-1-2E}\right),$$

где C представляют собой передаваемый символ, то $2E$ проверочных символов могут быть получены как коэффициенты полинома $f(X)/g(X)$, здесь $g(X)$ - генераторный полином кода, который определяется как

$$g(X) = \prod_{i=1}^{2E} (X - \alpha^i),$$

где a^i - примитивный элемент поля Галуа $GF(2^m)$. Таким образом, модули, реализующие совмещенные операции, могут быть использованы для построения быстродействующих устройств кодирования и декодирования кодов Рида-Соломона.

Заключение

Интенсивное развитие методов цифровой обработки сигналов приводит к необходимости разработки быстрых алгоритмов /28/, необходимых для построения различного рода специализированных процессоров. В данной работе показано, что, используя хорошо разработанный математический

аппарат теории кодов, исправляющих ошибки, который базируется на теории конечных полей Галуа, можно эффективно решить ряд задач в области цифровой обработки сигналов. Это касается особенно таких, как синтез переключательных функций, создание универсальных динамически программируемых модулей, кодирующих и декодирующих устройств, создание приборов для сигнатурного анализа и проч. При решении этих задач можно эффективно использовать параллельные методы выполнения операций в поле Галуа, рассмотренные в данной работе.

Приложение

Вычисление булевых выражений для реализации операции умножения двух элементов в поле Галуа $GF(2^4)$.

Имеем

$$A = A_0a^0 + A_1a + A_2a^2 + A_3a^3 \text{ и } B = B_0a^0 + B_1a + B_2a^2 + B_3a^3.$$

Тогда прямое произведение A B дает

$$A\times B = (A_0a^0 + A_1a + A_2a^2 + A_3a^3)(B_0a^0 + B_1a + B_2a^2 + B_3a^3) = A_0a^0B_0a^0 +$$
$$+ A_0a^0B_1a + A_0a^0B_2a^2 + A_0a^0B_3a^3 + A_1aB_0a^0 + A_1B_1a^2 + A_1B_2a^3 + A_1B_3a^4 +$$
$$+ A_2a^2B_0a^0 + A_2a^3B_1 + A_2B_2a^4 + A_2B_3a^5 + A_3B_0a^3a^0 + A_3B_1a^4 + A_3B_2a^5 +$$
$$+ A_3B_3a^6. \qquad (9)$$

Полученное выражение упрощаем с учетом того, что $a^0 = I$, а элементы a^4, a^5 и a^6 разлагаем по базисным: $a^4 = I + a^3$, $a^5 = a + a^2$ и $a^6 = a^2 + a^3$. После подстановки значений этих элементов в выражение (9) получим

$$A\times B = A_0B_0 + A_0B_1a + A_0B_2a^2 + A_0B_3a^3 + A_1B_0a^1 + A_1B_1a^2 + A_1B_2 + A_1B_3 +$$
$$+ A_1B_3a + A_2B_0a^2 + A_2B_1a^3 + A_2B_2 + A_2B_2a + A_2B_3a + A_2B_3a^2 + A_3B_0a^3 +$$
$$+ A_3B_1 + A_3B_1a + A_3B_2a + A_3B_2a^2 + A_3B_3a^2 + A_3B_3a^3.$$

Приведение подобных членов выполняется по правилу: сумма четного числа членов равна нулю, а сумма нечетного числа членов равна одному из них. Сгруппировав отдельно члены при a^0, a, a^2 и a^3, получим

$P_0 = A_0B_0 + A_1B_3 + A_2B_2 + A_3B_1$ $\quad <a^0>$

$P_1 = A_0B_1 + A_1B_0 + A_1B_3 + A_2B_2 + A_3B_1 + A_2B_3 + B_2A_3$ $\quad <a>$

$P_2 = A_0B_2 + A_1B_1 + A_2B_0 + A_3B_3$ $\quad <a^2>$

$P_3 = A_0B_3 + A_1B_2 + A_2B_1 + A_3B_0 + A_3B_3$ $\quad <a^3>$

С учетом изложенного нетрудно получить выражения для реализации произведения типа B A^2:

$$B\times A^2 = (B_0a^0 + B_1a + B_2a^2 + B_3a^3)((A_0 + A_2)a^0 + A_2a + (A_1 + A_3)a^2 + A_3a^3)).$$

После аналогичных действий и упрощения получим

$K_0 = B_0A_0 + B_0A_2 + B_2A_1 + B_2A_3 + B_3A_2 + B_1A_3$ $\quad <a^0>$

$K_1 = B_0A_2 + B_1A_0 + B_1A_2 + B_2A_1 + B_2A_3 + B_3A_2 + B_3A_1 + B_3A_3 +$ a

$K_2 = B_0A_1 + B_0A_3 + B_1A_2 + B_2A_0 + B_2A_2 + B_3A_1 + B_2A_3$ $\quad <a^2>$

$K_3 = B_0A_3 + B_1A_1 + B_1A_3 + B_2A_2 + B_3A_0 + B_3A_2 + B_3A_3$ $\quad <a^3>$

Литература

1. Блейхат Р.Э. Алгебраические поля, обработка сигналов, контроль ошибок. ТИИЭР, 1985, том.73, № 5, с.30.
2. Лабунец В.Г. Алгебраическая теория сигналов и систем. Издательство Красноярского университета, Красноярск, 1984.
3. Стахов А.П. Коды золотой пропорции.М.,"Радио и связь", 1984.
4. Никитюк Н.М., Раджабов Р.С., Шафранов М.Д. Параллельный шифратор для многопроволочных пропорциональных камер. ПТЭ, 1978, № 4, с.95.
5. Никитюк Н.М. Метод синдромного кодирования и его применение для быстрого аппаратного отбора событий на основе процессоров, оперирующих в поле Галуа $GF(2^m)$. Препринт ОИЯИ, Р11-80-484, Дубна, 1980.
6. Никитюк Н.М. Вопросы оптимального кодирования в годоскопических системах. ПТЭ, 1983, № 3, с.74.
7. Никитюк Н.М. Процессор для определения координат частиц в координатной пропорциональной камере. Бюллетень ОИ, 1981, № 39, Авт. свид. № 875408, с.259.
8. **In-Shek Hsu, Reed I.S., Truong T.K. et al. The VLSI Implementation of a Reed-Solomon encoder Using Berlekamp's bit-serial multiplier algorithm. IEEE Transactions on computers, 1984, vol.c-33, No.10, p. 906.**
9. **Munger K.S. A Transform for logic networks . IEEE Transaction on Computers, 1969, vol.C-18, No.3, p.241.**
10. **Benjauthrit B., Reed I.S. On the fundamental structure of Galois switching functions. IEEE Transactions on computers, 1978, vol.c-27, No.8, p.757.**
11. Александров И.Н., Гайдамака Р.И., Никитюк Н.М., Шириков В.П. Расчет переключательных функций, представленных элементами поля Галуа $GF(2^m)$. Препринт ОИЯИ, 1984, Р10-84-865, Дубна.
12. Никитюк Н.М. Новый способ построения универсального логического модуля. Препринт ОИЯИ, Р11-85-365, Дубна, 1985.

I3. Смирнов Н.И., Стручков А.А., Судовцев В.А. Диагностика неисправностей в цифровой радиоаппаратуре на БИС. Зарубежная радиоэлектроника , I979, № I, с.53.
I4. Новик Г.Х. О достоверности сигнатурного анализа. Автоматика и телемеханика , I985, № 5, с.I57.
I5. **Bartee T.C., Sneider P.I. Computation with finite fields.Information and Control, 1963, vol.6, No.1, p.79.**
I6. **Davida G.I. Inverse of elements of a Galois field. Electronic letters., 1972, vol.8, N 21, p.518.**
I7. Питерсон У., Уалдон Э. Коды, исправляющие ошибки. Мир , М.,I976.
I8. Колесник В.Д., Мирончиков Е.Т. Декодирование циклических кодов. "Связь", М., I968, с.23I.
I9. Гайдамака Р.И., Никитюк Н.М., Шириков В.П. Комплекс программ для автоматизации логического проектирования устройств сжатия информации, разрабатываемых на базе алгебраической теории кодирования. Препринт ОИЯИ, PIO-84-84I, Дубна, I984.
20. Никитюк Н.М. Устройство для умножения и возведения в степень двух элементов в поле Галуа $GF(2^m)$. Авт.свидетельство № I236457, бюллетень ОИ, № 2I, I986, с.I99.
2I. Никитюк Н.М. Устройство для выполнения операций возведения в степень, деления и умножения двух элементов в поле Галуа $GF(2^m)$. Авт.свид. № I236458 , бюллетень ОИ, № 2I, I986, с.I99.
22. Никитюк Н.М. Устройство для реализации переключательных функций в поле Галуа $GF(2^m)$. Авт.свид. № I23486I, бюллетень ОИ, I986, № 20, с.229.
23. Калинников В.А, Никитюк Н.М. Устройство для отбора t ядерных частиц из N частиц.Бюллетень ОИ, Авт.свид. № I075829,I984,№ 47,с.2II.
24. Гайдамака Р.И., Калинников В.А., Никитюк Н.М. Новый способ построения мажоритарных схем совпадений. Препринт ОИЯИ, PI3-82-628, Дубна, I982.
25. **Berlekamp E.R. Bit-serial Reed-Solomon Encoders. IEEE Trans. on Inf. Theory, 1982, vol.IT-28, No.6, p.869**
26. **Liv K.Y.Architecture for VLSI Design of Reed-Solomon Encoders. IEEE Transaction on Computers, 1982, vol.C-31, No.2, p.170**
27. **Shao H.M., Truong T.K. ,Deutsch L.J.,et al. A VLSI Design of a Pipeline Reed-Solomon Dekoder. IEEE Transaction on Computers, 1985, vol.c-37, No.5, p.383**
28. Вариченко Л.В., Лабунец В.Г., Раков М.А. Абстрактные алгебраические системы и цифровая обработка сигналов. "Наукова Думка", Киев, I986.

Рукопись поступила в издательский отдел
4 февраля I987 года.

Никитюк Н.М. P11-87-54
Совмещенные операции в поле Галуа $GF(2^m)$ и их применение

Описан метод одновременного и параллельного выполнения операций в поле Галуа $GF(2^m)$ над выражениями, содержащими несколько элементов, в том числе и таких выражений, которые находятся под степенью. Приводятся примеры использования предложенных алгоритмов для синтеза переключательных функций многих переменных, для построения декодирующих устройств таких важных кодов, исправляющих ошибки, как БЧХ-коды и коды Рида-Соломона. Рассматриваются также вопросы применения совмещенных операций для создания универсальных динамически программированных модулей и специализированных процессоров.

Работа выполнена в Лаборатории высоких энергий ОИЯИ.
Препринт Объединенного института ядерных исследований. Дубна 1987

Перевод О.С.Виноградовой

Nikityuk N.M. P11-87-54
Combined Operations in Galois Field $GF(2^m)$ and Their Application

A method for simultanous and parallel execution of operations in Galois field $GF(2^m)$ for expressions containing several elements including those under degree are described. Examples of suggested algorithms for a synthesis of many variable digital functions, for creation of coders and decoders of such important correcting codes as BCH-codes and Reed-Solomon codes are given. Problems of using combined operations for designing universal dynamic programing modules and special purpose processors are considered.

The investigation has been performed at the Laboratory of High Energies, JINR.
Preprint of the Joint Institute for Nuclear Research. Dubna 1987