И. Н. Александров, В. М. Котов, Н. М. Никитюк, Применение переключательных функций в полях Галуа GF(2^m) для синтеза универсальных динамически программируемых модулей, *Автомат. и телемех.*, 1995, выпуск 9, 137–148

УДК 519.714

© 1995 г. **И.Н. АЛЕКСАНДРОВ,**
В.М. КОТОВ, канд. техн. наук,
Н.М. НИКИТЮК, д-р техн. наук
(Объединенный институт ядерных исследований, Дубна)

ПРИМЕНЕНИЕ ПЕРЕКЛЮЧАТЕЛЬНЫХ ФУНКЦИЙ В ПОЛЯХ ГАЛУА GF(2^m) ДЛЯ СИНТЕЗА УНИВЕРСАЛЬНЫХ ДИНАМИЧЕСКИ ПРОГРАММИРУЕМЫХ МОДУЛЕЙ

Рассмотрена возможность применения полиномиальных форм построения переключательных функций в полях Галуа GF(2^m), показана перспективность их использования при синтезе универсальных динамически программируемых логических модулей. Рассмотрены варианты синтеза схем как для полностью, так и не полностью определенных функций. Приведен пример универсального динамически программируемого модуля четырех переменных.

1. Введение

В задачах анализа и синтеза комбинационных схем, задаваемых таблицей истинности, в последнее время находят все большее применение полиномиальные формы представления булевых функций в виде полинома Жегалкина [1, 2]. Эти формы имеют однородную алгебраическую структуру и хорошо реализуются в современной микроэлектронике. Однако трудоемкость вычисления коэффициентов в полиномах Жегалкина достаточно высока и существенно растет с увеличением числа переменных. В [3, 4] показано, что систему булевых функций можно представить в виде обобщенного арифметического полинома, что позволяет более удобно выполнять параллельные вычисления систем булевых функций. Известен также метод построения полиномов в поле Галуа GF(2^m), который основан на интерпретации входов и выходов переключательной схемы как элементов поля. Это направление исследовано в работах [5–7]. В [5] приведено выражение для непосредственного вычисления коэффициентов полиномиального разложения. Результаты этой работы были использованы для расчета переключательных схем с целью синтеза комбинационного сумматора и последовательностного автомата [8].

Цель данной работы – показать эффективность полиномиального разложения в полях Галуа для синтеза универсального динамически программируемого логического модуля (УДПЛМ), т.е. модуля, реализующего любую логическую функцию с заданным количеством входов и выходов с возможностью динамической (в темпе поступления входных данных) настройки модуля на конкретную функцию.

2. Основные понятия и определения. Базовая теорема разложения

Поля Галуа являются естественным расширением булевого поля. Они хорошо изучены и имеют широкий спектр применений [9–11]. Любая переключательная функция с m входами и m выходами имеет не более 2^m значений. Таким образом, она задана над конечным полем, часто называемым полем Галуа GF(p^m). Число p называется основанием поля и должно быть простым. Будем рассматривать случай $p = 2$, однако все результаты справедливы и для других простых p, поэтому актуальность данного направления еще больше возрастет с появлением эффективных устройств многозначной логики.

Введем поле коэффициентов GF(2) с элементами 0 и 1, операцией сложения по модулю 2 в качестве операции сложения и конъюнкцией в качестве операции умножения. В этом поле операции сложения и вычитания полностью идентичны. Зададим над GF(2) поле $GF(2^m)$ как поле полиномов степени меньше m с коэффициентами из GF(2). Роль переменной в этих полиномах будет играть вместе со своими степенями примитивный корень неприводимого многочлена степени m. В этом случае говорят, что неприводимый многочлен порождает поле. Корень называется примитивным, если среди его 2^m-1 различных степеней нет совпадающих. Таким образом, степени примитивного полинома покрывают все конечное поле $GF(2^m)$. Операцией сложения в этом поле служит обычная операция сложения полиномов, где сложение коэффициентов осуществляется в поле GF(2). Умножением является умножение полиномов по модулю порождающего многочлена. В этом поле выполняются все обычные аксиомы полей. Приведем дополнительно некоторые свойства конечных полей, полезные для понимания материала (подробнее см. в [5]).

Свойство 1. Для любого $X \in GF(2^m)$: $X + X = 0$.

Свойство 2. Для любого ненулевого $X \in GF(2^m)$: $X^{m-1} = 1$.

Свойство 3. Для любых $X, Y \in GF(2^m)$: $(X+Y)^2 = X^2 + Y^2$.

Свойство 4. Для любого неединичного $X \in GF(2^m)$: $\sum_{k=1}^{2^m-1} X^k = 1$.

Первые m степеней примитивного корня α^0, α, α^2, $\alpha^3, \ldots, \alpha^{m-1}$ являются линейно независимыми и могут служить базисом поля Галуа. Это значит, что любой элемент X поля представим в виде:

$$X = a_0 * \alpha^0 + a_1 * \alpha + \cdots + a_{m-1} * \alpha^{m-1}, \tag{1}$$

где $a_i \in 0, 1$. Рассматривая любое двоичное число $(a_0, a_1, \ldots, a_{m-1})$ длины m в качестве набора коэффициентов a_i из (1), можно интерпретировать его как элемент поля Галуа.

Теорема 1 (разложения). Любую переключательную функцию $f(X)$ можно представить, причем единственным образом, в виде:

$$f(X) = f(0) + \sum_{i=1}^{2^m-1} G_i X^i, \tag{2}$$

$$G_i = \sum_{j=1}^{2^m-1} \alpha_j^{-i}(f(0) - f_j), \tag{3}$$

где $f_j = f(\alpha_j)$, и $\alpha_j = \alpha^j$ – j-я степень α.

Доказательство теоремы 1 приведено в [5]. В [6] приведены теоремы, подобные данной, для случая многозначных функций. Теорема 1 является базовой для построения УДПЛМ.

3. Построение полинома для динамически настраиваемой переключательной схемы

Исходя из (1), можно подсчитать в общем виде:

$$\begin{aligned}
&X = a_0\alpha^0 + \cdots + a_{m-1}\alpha^{m-1},\\
&X^2 = (a_0\alpha^0 + \cdots + a_{m-1}\alpha^{m-1})(a_0\alpha^0 + \cdots + a_{m-1}\alpha^{m-1}),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&X^{2^m-1} = (a_0\alpha^0 + \cdots + a_{m-1}\alpha^{m-1})^{2^m-1}.
\end{aligned}$$

Производя возведение в степень путем умножения (1) самого на себя нужное число раз, получим все X^i из (2) в полиномиальном виде. Подсчитав для конкретной переключательной функции коэффициенты G_i по формуле (3) и подставив эти значения вместе со степенями X в полиномиальном виде в (2), после приведения подобных можно получить систему полиномов Жегалкина. Каждый полином будет представлять собой коэффициент при базисном элементе α^i. Этот способ получения полиномов подробно изложен в [8, 12]. Однако в этом случае значения G_i будут как бы зашиты в схеме, за счет чего общий вид полиномов несколько упростится, но при этом теряется возможность настройки схемы на разные функции. Для УДПЛМ необходимо, чтобы наряду с переменной X коэффициенты G_i также являлись входными для модуля.

Представим G_i в общем полиномиальном виде через базис так же, как мы представили X в (1): $G_i = b_{i_0}\alpha^0 + \cdots + b_{i_{m-1}}\alpha^{m-1}$. Данное выражение вместе со всеми выражениями для X^i подставим в (2). В результате получим искомый полином для УДПЛМ, в котором X и все G_i являются переменными, заданными через разложение по базису. На его основе можно синтезировать УДПЛМ, причем X и все G_i являются входами для схемы. Для настройки УДПЛМ на конкретную функцию достаточно подсчитать значения всех G_i для этой функции по формуле (3) и занести их в регистры хранения. При работе УДПЛМ значения G_i подаются на входы схемы вместе со значениями X. В приложении представлен полиномиальный вид соответственно X^k и GX^k для $m = 4$ и неприводимого полинома $X^4 = X+1$ (таблица неприводимых полиномов для $m \leqslant 34$ приведена в [9]). Получаемые для X^k выражения достаточно громоздки, поэтому все вычисления целесообразно производить на ЭВМ.

Используя тот факт, что $X^k = XX^{k-1}$, можно несколько упростить схему УДПЛМ за счет увеличения числа каскадов в ней, т.е. за счет увеличения времени задержки. Например, можно реализовать схемно только четные степени X (их выражения в среднем проще), а нечетные получить на следующем каскаде, реализовав операцию умножения $X^{2l+1} = YX$, где Y – выходы схемы для X^{2l} и l=1,2,...,$(2^{m-1}-1)/2$. Различные способы реализации операции умножения, сложения и деления приведены в [13–19].

Используя тот факт, что выражения для X^{2^l}, $l = 0, 1, \ldots, m-2$ существенно проще (это сразу вытекает из свойства 3), можно также упростить схему, увеличивая число ее каскадов.

Пример 1. Для поля Галуа GF(2^4) и неприводимого полинома $X^4 = X + 1$ (2) приобретает вид:

$$F(X) = F(0)+G_1X+G_2X^2+\cdots+G_{15}X^{15} = F(0)+[G_1X+G_2X^2+G_3X^3]+$$
$$+ X^4[G_4+G_5X+G_6X^2+G_7X^3]+X^8[G_8+G_9X+G_{10}X^2+G_{11}X^3]+$$
$$+ X^{12}[G_{12}+G_{13}X+G_{14}X^2+G_{15}X^3].$$

Подставляя выражения для G_i и X^k согласно приложению, получим двухкаскадную схему вычисления любой четырехвходовой переключательной функции. Первый каскад представляет собой вычисление выражений в квадратных скобках, второй – реализация оставшихся операций умножения и сложения. Однако выражения для X^3, X^{12} все еще велики. Используя только выражения для X, X^2, X^4, X^8, получим следующее выражение для $F(X)$:

$$F(X) = F(0) + G_1X + G_2X^2 + G_3X^2X + G_4X^4 + G_5X^4X + G_6X^4X^2 +$$
$$+ G_7X^4X^2X + G_8X^8 + G_9X^8X + G_{10}X^8X^2 + G_{11}X^8X^2X + G_{12}X^8X^4 +$$
$$+ G_{13}X^8X^4X + G_{14}X^8X^4X^2 + G_{15}X^8X^4X^2X =$$
$$= F(0) + [X^8(G_8 + G_{12}X^4)] + [G_1 + X^8(G_9 + G_{13}X^4)]X + [G_2 + G_3X +$$
$$+ X^8(G_{10} + G_{11}X + G_{14}X^4)]X^2 + [G_4 + G_5X + (G_6 + G_7X)X^2]X^4 +$$
$$+ G_{15}[(X^8X^4)(X^2X)].$$

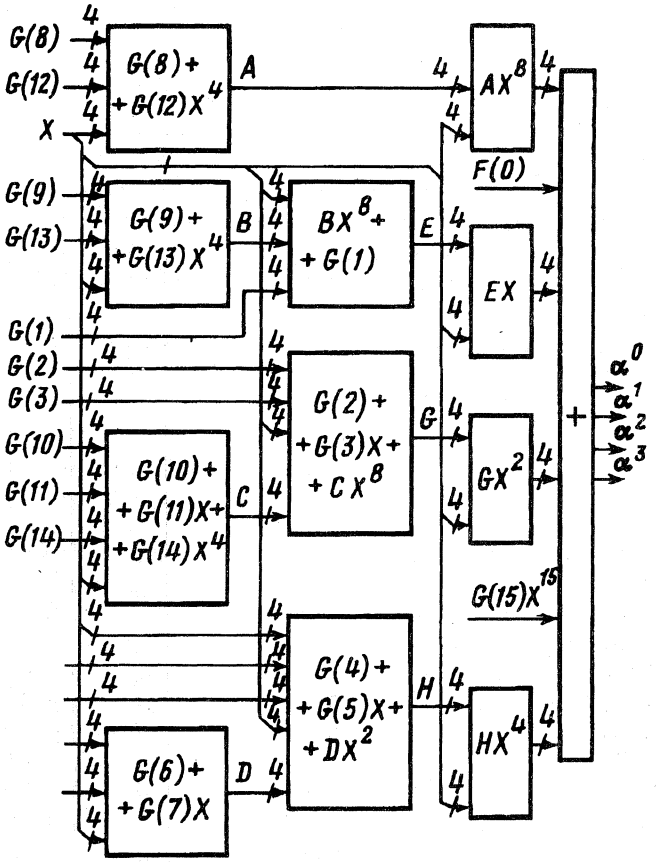

Рис. 1. Структурная схема для реализации УДПЛМ на 4 входа и 4 выхода

На рис. 1 приведена структурная схема реализации последнего выражения для УДПЛМ на 4 входа и 4 выхода.

Рассмотрим более подробно возможности быстрого вычисления выражений (3). Для вычисления G_i можно использовать саму схему УДПЛМ. Достаточно в регистры хранения G_i занести F_i для всех $i = 1, \ldots, 2^m - 1$ и, последовательно подавая на вход схемы значения $X = \alpha^{-k}$, где $k = 1, \ldots, 2^m - 1$, на выходе будем получать искомые значения G_k (для $k = 2^m - 1$ дополнительно прибавляется еще значение $F(0)$) с минимальным временем задержки (2 наны на одно G_k для однокаскадной УДПЛМ). Если при перенастройке УДПЛМ с одной функции на другую меняется лишь небольшое количество значений выходов, объемы вычислений для (3) можно резко сократить. Так, при изменении одного значения выхода в точке α_k со старого F_{k_c} на новое $F_{k_н}$ (3) сводится к следующему: $G_{i_н} = G_{i_c} + (F_{k_н} - F_{k_c})\alpha_k^{-i}$ для всех $i = 1, \ldots, 2^m - 1$. Возможно также использование систолических систем для вычисления G_i. В этом случае накопление значений G_i производится последовательно за $2^m - 1$ шагов. Схема работы одного шага, занимающего $2^m - 1$ такта времени работы систолической системы, приведена на рис. 2. Очевидно, что вычисление выражения (2) еще проще, чем (3), осуществляется в систолической системе, например по схеме Горнера. Несмотря на то, что скорость вычислений в систолических системах достигает 5 млрд. операций в секунду, в силу того, что процесс вычисления значения $F(X)$ итеративный, для определенного класса задач временные задержки выходного сигнала могут оказаться недопустимо большими. В этом случае в зависимости

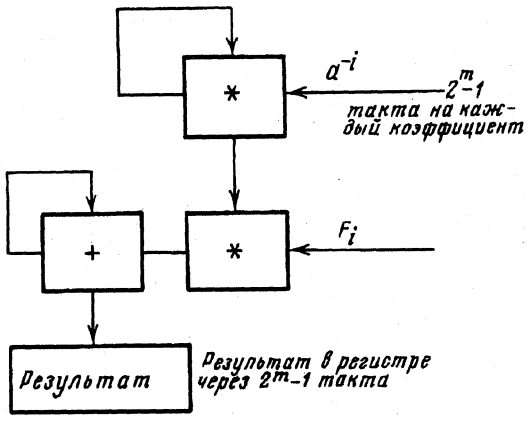

Рис. 2. Структурная схема получения значений коэффициентов G_i в систолической системе. $*$ – операция умножения в поле Галуа, $+$ – сумма по модулю 2, F_i – значение функции в точке α^i

от требований по быстродействию систолические вычисления можно распараллеливать. Например, для $m = 6$, $2^m - 1 = 63$ можно реализовать вычисление $F(X)$ как сумму $F(X) = F1 + F2 + F3 + F4$. Здесь $F1, F2, F3$ и $F4$ – частичные суммы из (2) при i: от 0 до 15 для $F1$, от 16 до 31 для $F2$, от 32 до 47 для $F3$ и от 48 до 63 для $F4$. Вычисления $F1, F2, F3$ и $F4$ производятся параллельно, начальные значения X^{16}, X^{32} и X^{48} для $F2, F3$ и $F4$ вычисляются напрямую по схемам, подобным указанным в приложении. Таким образом, для вычисления $F(X)$ вместо 63 тактов работы систолической системы понадобится 16 тактов работы при четырехкратном увеличении аппаратуры в систолической системе.

4. Построение m входового УДПЛМ с помощью УДПЛМ меньшего числа входов

С ростом m сложность выражения для УДПЛМ возрастает, поэтому было бы целесообразно получать значения любой переключательной функции m входов m выходов через УДПЛМ, рассчитанные на меньшее число входов-выходов, т.е. работающие в полях Галуа меньших порядков. Рассмотрим любую функцию F на m входов m выходов. Область ее определения X – это множество всех двоичных чисел длины m. Пусть Y – область значений F (двоичные числа длины не более m). Будем считать, что входы(выходы) функции расположены слева направо. Назовем для удобства m_1 левых входов(выходов) функции младшими, остальные $m_2 = m - m_1$ входов(выходов) – старшими (у нас $m > m_1 \geqslant m_2$). Разобьем X на 2^{m_2} класса K_i: элемент x из X принадлежит K_i, если его старшие разряды представляют собой число i в двоичном виде. Каждый класс содержит 2^{m_1} элемента, они отличаются только младшими разрядами. На каждом K_i определим по паре функций F_{i_1} и F_{i_2} следующим образом. Любое x, принадлежащее K_i, представимо в виде $(x_1, x_2, \ldots, x_{m1}, x_{m1+1}, \ldots, x_m)$, причем $(x_{m+1}, \ldots, x_m)$ постоянно для любого x из K_i. Если $y = F(x)$, то y также представим в виде $(y_1, y_2, \ldots, y_{m_1}, y_{m_1+1}, \ldots, y_m)$ и по определению для $x \in K_i$ считаем $F_{i_1}(x) = (y_1, \ldots, y_{m_1})$ и $F_{i_2} = (y_{m_1+1}, \ldots, y_m)$. Так как для каждого K_i старшие разряды входных значений – это константа, можно брать для любой F_{i_l}, где $l = 1, 2$, в качестве входов только младшие разряды, а потому и реализовать ее в m_1 входов-выходов УДПЛМ. Для каждой F_{i_l} подсчитаем по (3) коэффициенты $G_{i_l j}$ для $i_l = 0, \ldots, 2^{m_2} - 1$, $j = 1, \ldots, 2^{m_1} - 1$. Обозначим через

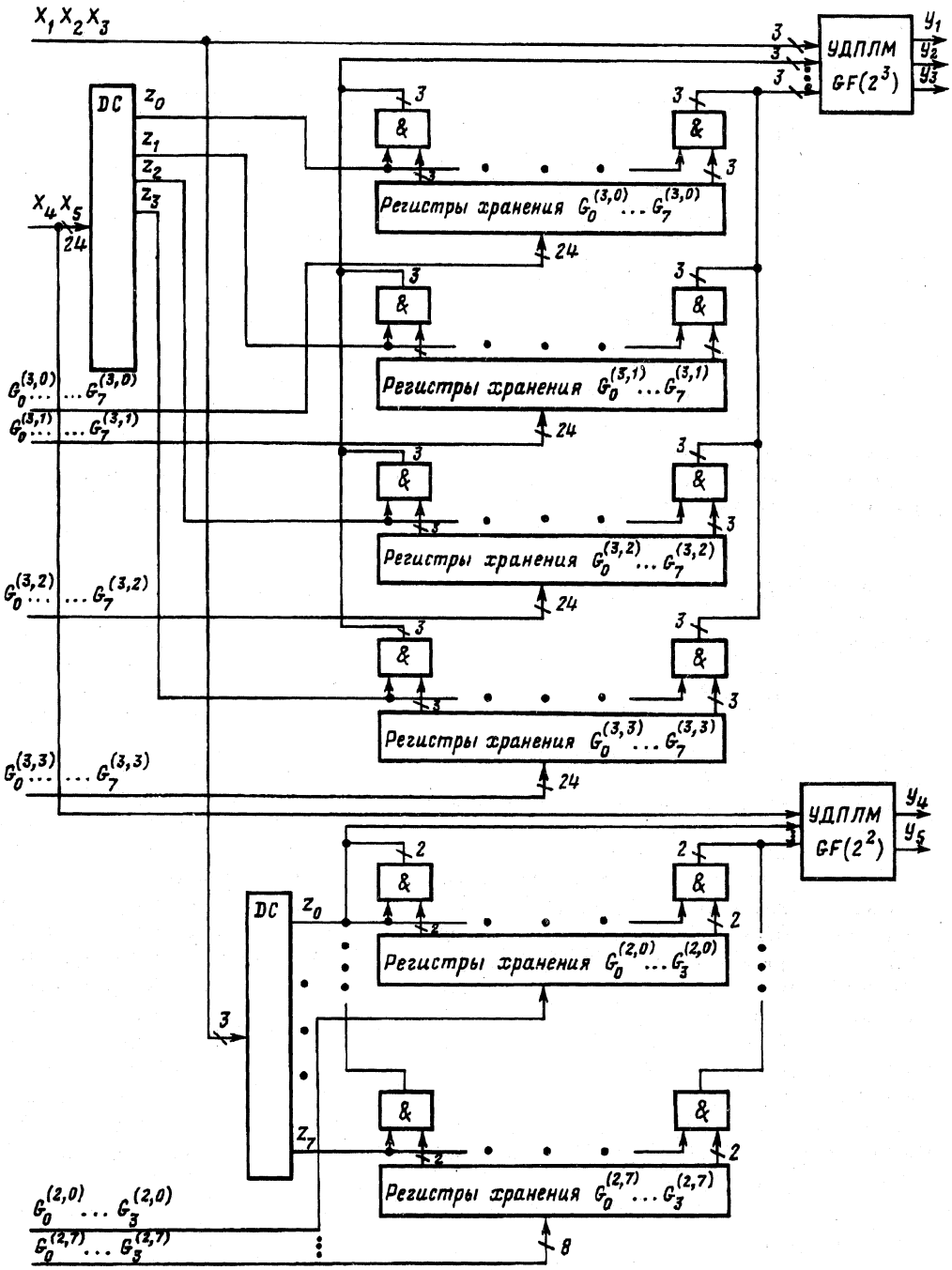

Рис. 3. Структурная схема УДПЛМ для $m = 5$, $m_1 = 3$ и $m_2 = 2$. $G_i^{(j,k)}$ – i-й коэффициент для поля $\mathrm{GF}(2^j)$ для $k = (x_5, x_4)$ при $j = m_1$ и $k = (x_3, x_2, x_1)$ при $j = m_2$, & – поразрядная конъюнкция векторного со скалярным входом

Значения функций $f1$ и $f2$

$x3\,x2\,x1$	$f2\,f1$
$0 = (000)$	$0 = (00)$
$\alpha = (010)$	$\alpha^0 = (01)$
$\alpha^2 = (100)$	$0 = (00)$
$\alpha^4 = (110)$	$\alpha^0 = (01)$
$\alpha^0 = (001)$	$\alpha^0 = (01)$
$\alpha^3 = (011)$	$\alpha^3 = (11)$
$\alpha^6 = (101)$	$\alpha = (10)$
$\alpha^5 = (111)$	$\alpha^3 = (11)$

x'_i входной элемент из K_i, у которого младшие разряды равны нулю. Тогда можно получить значения функции F через операции в поле $\mathrm{GF}(2^{m_1})$ (отдельно младшие и старшие разряды) по формуле, аналогичной (2):

$$F_{i_1}(x) = \sum_{i=0}^{2^{m_2}-1} F(x'_i)p(i,x) + \sum_{j=1}^{2^{m_1-1}} G'_{i_1 j} X^j,$$

$$G'_{i_1 j} = \sum_{i_1=0}^{2^{m_2}-1} G_{i_1 j p(i,x)},$$

где $X = (x_1, \ldots, x_{m_1})$, $p(i,x)$ равно 1, когда старшие разряды x совпадают с i в двоичном представлении, и равно нулю в противном случае. Иными словами, $p(i,x)$ – это терм из всех $(x_{m_1+1}, \ldots, x_{m_2})$, причем x_k берется с отрицанием, если на k-й позиции числа i в двоичном представлении стоит 0. Для получения всех разрядов выходов требуется два УДПЛМ на m_1 вход-выход. Возможен вариант с УДПЛМ на m_1 вход-выход плюс УДПЛМ на m_2 вход – выход. Тогда опять все $G_{i_1 j}$ подаются на первую УДПЛМ, а $G_{i_2 j}$ подаются на вторую УДПЛМ (но имеющую уже m_2 входов – выходов), причем для второй УДПЛМ роль старших разрядов играют младшие и наоборот. В этом случае объем памяти для хранения настроечных коэффициентов в точности равен требуемой памяти для УДПЛМ на m входов-выходов, но сами схемы для УДПЛМ проще ввиду меньшего числа входов. Укрупненная структурная схема для $m = 5$, $m_1 = 3$ и $m_2 = 2$ представлена на рис. 3. Очевидно, задача упрощается для класса функций, у которых число выходов меньше числа входов. В этом случае можно взять m_1 равным числу выходов и УДПЛМ для получения значений F_{i_2} не нужны. Так, если бы в структурной схеме рис. 3 на $m = 5$ входов приходилось бы 3 выхода, 8 массивов для $\mathrm{GF}(2^2)$ отсутствовали бы.

Пример 2. Построить полином для кортежа булевых функций $f2 * f1$ (см. таблицу), заданных их таблицей истинности.

Для поля $\mathrm{GF}(2^3)$ по (2), (3) с учетом того, что $X^3 = X + 1$, получим:

$$F(X) = \alpha^6 X + \alpha^5 X^2 + \alpha^3 X^3 + \alpha^3 X^4 + \alpha^3 X^5 + \alpha^3 X^6 + \alpha^3 X^7.$$

Если же провести разбивку по x_1, то в $\mathrm{GF}(2^2)$ с учетом $X^2 = X + 1$ для $x_1 = 0$ получим полином $F(X) = \alpha^2 X + \alpha X^2$, а для $x_1 = 1$ получим $F(X) = \alpha^0 + \alpha^2 X + \alpha X^2 + \alpha^2 X^3$. Схема реализации данного примера в УДПЛМ для поля $\mathrm{GF}(2^3)$ и на основе поля $\mathrm{GF}(2^2)$ представлена на рис. 4. Так как по условию заданы только 2 выхода, то в схеме на рис. 4, *б* часть, реализующая операции в поле $\mathrm{GF}(2)$, отсутствует.

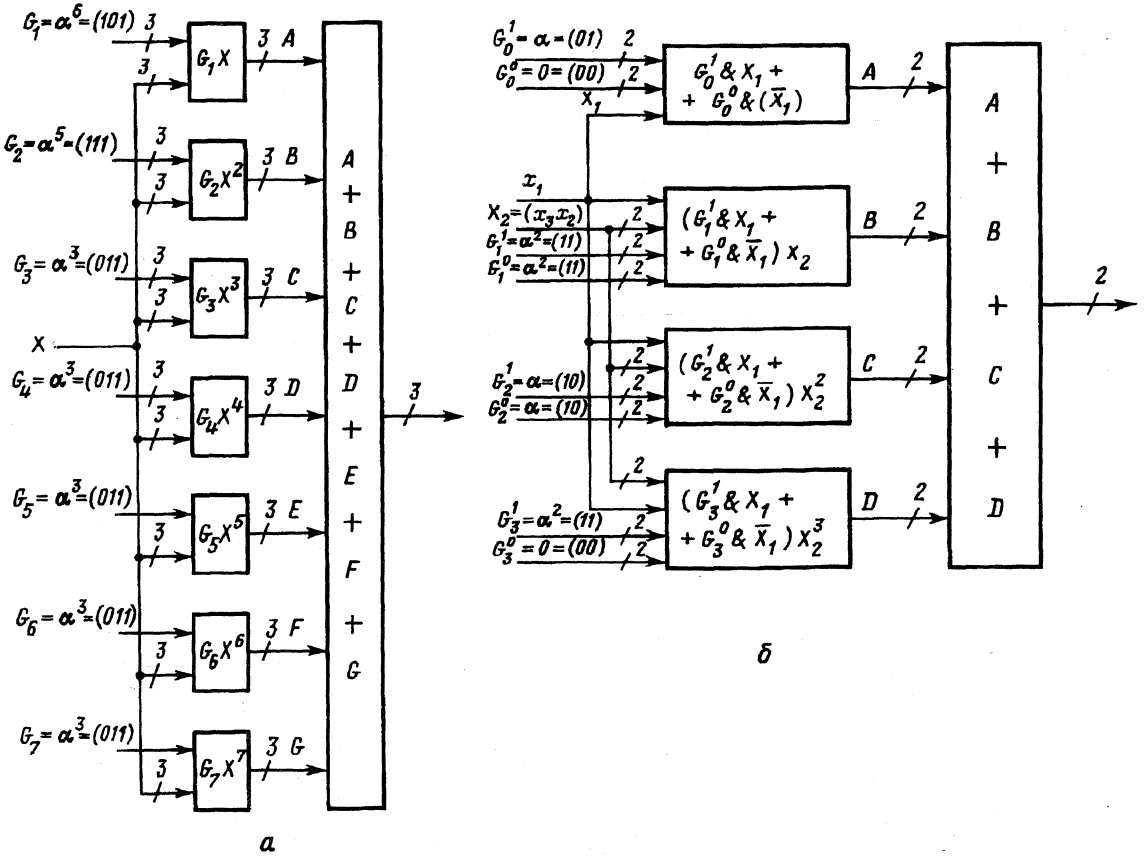

Рис. 4. Структурная схема реализации заданной в таблице функции на 3 входа и 2 выхода в УДПЛМ полей $GF(2^3)$ и $GF(2^2)$. *а* – реализация в поле $GF(2^3)$, X – входная переменная, G_i – коэффициенты, *б* – реализация в поле $GF(2^2)$, $X = (x_3, x_2, x_1)$ – входная переменная, $X_2 = (x_3, x_2)$ и $X_1 = (x_1, x_1)$. G_i^j – i-й коэффициент в поле $GF(2^2)$ для $x_1 = j$, $\overline{X}_1 = (\overline{x}_1, \overline{x}_1)$

Заметим, что в поле $\mathrm{GF}(2^3)$ при реализации G_i в самой схеме $F(X) = (a_0 \oplus a_1 \oplus \oplus a_0a_1 \oplus a_0a_2 \oplus a_0a_1a_2)\alpha^0 + (a_0a_1 \oplus a_0a_2 \oplus a_0a_1a_2)\alpha$, где a_0, a_1, a_2 – булевы переменные и $X = a_0\alpha^0 + a_1\alpha + a_2\alpha^2$. Это случай, когда мы доводим схему до уровня полинома Жегалкина, однако теряется возможность перенастройки. Условия задачи составлены на основе примера 1 в [20], где требовалось получить обобщенный арифметический полином. Для этого кортежа функций он равен $D(X) = x_1 + x_2 + x_1x_2 + x_1x_3 - x_1x_2x_3$. В $D(X)$ все операции являются операциями десятичной арифметики.

5. Построение УДПЛМ для не полностью определенных переключательных функций

При синтезе переключательных функций приходится иметь дело с большим, практически важным классом не полностью определенных функций [21]. В работах [22, 23] получены интересные результаты в задаче построения минимальных полиномиальных форм для не полностью определенных функций. Однако в [22] подсчет коэффициентов форм связан с решением систем линейных уравнений. В [23] дан класс полиномиальных форм с быстрым подсчетом коэффициентов, но накладываются ограничения по входам на класс функций, для которых такие формы могут быть построены. Ниже будет показано, что для функций с относительно большим числом заданных значений целесообразно использовать полиномиальные формы в полях Галуа. Возможны два подхода. Первый – доопределить функцию нулями и применить методы, изложенные в предыдущих разделах. Этот вариант вполне приемлем для большого класса задач. Однако он менее предпочтителен, если число входов велико (m=13 и больше), а число определенных значений функции много меньше $2^m - 1$. Второй подход связан с получением массивов промежуточных коэффициентов. Его целесообразно использовать, если в УДПЛМ класс входов фиксирован (причем нет ограничений на то, какие именно входы фиксируются), а меняются только значения выходов переключательных функций. Пусть задано L значений функции ($L \ll 2^m - 1$). Будем представлять функцию $F(X)$ в виде

$$F(X) = F(0) + \sum_{k=1}^{L} A_k X^k, \tag{4}$$

$$A_k = \sum_{j=1}^{L} K_{jk}\big(F(j) + F(0)\big), \tag{5}$$

где коэффициенты K_{jk} зависят только от массива входов X. Матрица коэффициентов K_{jk} получается путем решения матричного уравнения $KY = E$. Все матрицы имеют размеры $L \times L$. E – единичная матрица, K – матрица искомых коэффициентов K_{jk} и Y:

$$Y = \begin{pmatrix} X_1 & X_2 & X_3 & \dots & X_L \\ X_1^2 & X_2^2 & X_3^2 & \dots & X_L^2 \\ X_1^3 & X_2^3 & X_3^3 & \dots & X_L^3 \\ \dots & \dots & \dots & \dots & \dots \\ X_1^L & X_2^L & X_3^L & \dots & X_L^L \end{pmatrix},$$

где $X_1, \dots, X_L$ – входы переключательной функции, на которых она определена. Уравнение легко решается обычными алгебраическими методами, например методом Гаусса, но с операциями умножения, деления и сложения в поле Галуа.

Так как для $X{=}0$ справедливость (4), (5) очевидна, возьмем любое ненулевое X_i. Для доказательства верности (4), (5) достаточно выражение из (5) подставить в (4) с $X = X_i$:

$$F(X_i) = F(0) + \sum_{k=1}^{2^L} X_i^k \left(\sum_{j=1}^{2^L} K_{jk}\big(F(j) + F(0)\big) \right) =$$

$$= F(0) + \sum_{k=1}^{2^L} \sum_{j=1}^{2^L} \left(X_i^k \left(K_{jk}\big(F_j + F(0)\big) \right) \right) =$$

$$= F(0) + \sum_{j=1}^{2^L} \big(F_j + F(0)\big) \sum_{k=1}^{2^L} X_i^k K_{jk}.$$

Осталось заметить, что из $KY = E$ следует, что внутренняя сумма равна нулю для всех $j \neq i$ и равна единице для $j{=}i$. Здесь X_j – вход функции, на котором ее значение равно F_j. Отсюда сразу следует, что $F(X_i) = F(0) + F_i + F(0) = F_i$, что и требовалось доказать. Имея матрицу K из (5), легко, в том числе и в систолических системах, получить значения настроечных коэффициентов A_k, используемых в (4). Сам полином (4) реализуется идентично вычислениям полинома (2). Матрицу K можно хранить в более дешевой внешней памяти, получая и подкачивая по мере надобности коэффициенты настройки A_k. В данном варианте мы, по сути, обнулили все коэффициенты при степенях X, больших L, поэтому выражения для этих степеней X не нужны. Так как по условию $L \ll 2^m - 1$, получаемые в данном варианте схемы для указанного класса задач более экономичны. Отметим, что можно решать впрямую уравнение $AY = F$ (здесь A – вектор настроечных коэффициентов для (4)). Однако в этом случае получение настроечных коэффициентов для каждой новой функции будет связано с решением системы линейных уравнений. Это ведет к увеличению времени получения настроечных коэффициентов, что не всегда приемлемо для рассматриваемого класса задач.

6. Заключение

Показано, что представление переключательных функций в виде полинома в поле Галуа является перспективным для расчета и синтеза УДПЛМ. Поскольку такие модули являются функционально полными, они могут применяться вместо ППЗУ. В отличие от ППЗУ, УДПЛМ являются чисто комбинационными, не содержащими дешифраторы, поэтому задержки сигналов в них сведены к минимуму, хотя и могут увеличиваться с увеличением числа каскадов. Для получения максимального быстродействия необходимо использовать один каскад и реализовать его в виде интегральной схемы. Для занесения коэффициентов настройки можно дополнительно встроить программно управляемый интерфейс, для увеличения скорости перенастройки УДПЛМ, используя как систолические системы, так и саму УДПЛМ.

ПРИЛОЖЕНИЕ

Пример получения полиномиального вида выражений X^k и GX^k для поля Галуа $GF(2^4)$ с неприводимым полиномом $X^4 = X + 1$

Пусть $X = a_0\alpha^0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ и $G = b_0\alpha^0 + b_1\alpha^1 + b_2\alpha^2 + b_3\alpha^3$, где α – корень неприводимого полинома $X^4 = X + 1$, а $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in GF(2)$ и являются переменными коэффициентами, задающими X и G. Тогда $X^2 = (a_0\alpha^0 + a_1\alpha + a_2\alpha^2 +$

$+a_3\alpha^3)(a_0\alpha^0+a_1\alpha+a_2\alpha^2+a_3\alpha^3)=a_0\alpha^0+a_0a_1\alpha+a_0a_2\alpha^2+a_0a_3\alpha^3+a_0a_1\alpha+a_1\alpha^2+$
$+a_1a_2\alpha^3+a_1a_3\alpha^4+a_0a_2\alpha^2+a_1a_2\alpha^3+a_2\alpha^4+a_2a_3\alpha^5+a_0a_3\alpha^3+a_1a_3\alpha^4+a_2a_3\alpha^5+a_3\alpha^6=$
$=a_0\alpha^0+a_1\alpha^2+a_2\alpha^4+a_3\alpha^6=a_0\alpha^0+a_1\alpha^2+a_2(\alpha+\alpha^0)+a_3(\alpha^3+\alpha^2)=(a_0\oplus a_2)\alpha^0+a_2\alpha+$
$+(a_1\oplus a_3)\alpha^2+a_3\alpha^3)$. Получено полиномиальное представление для X^2. Аналогично для $k=3,\ldots,15$, беря полиномиальные выражения для X^{k-1} и X и перемножая их, получаем все степени X. Расчет выражений GX^k, $k=1,\ldots,15$ осуществляется по той же схеме, где в качестве сомножителей берутся полиномиальные выражения для G и соответствующей степени X. В частности, $GX=(a_0b_0\oplus a_3b_1\oplus a_2b_2\oplus a_1b_3)\alpha^0+$
$+(a_1b_0\oplus a_0b_1\oplus a_3b_1\oplus a_2b_2\oplus a_3b_2\oplus a_1b_3\oplus a_2b_3)\alpha+(a_2b_0\oplus a_1b_1\oplus a_0b_2\oplus a_3b_2\oplus a_2b_3\oplus$
$\oplus a_3b_b3)\alpha^2+(a_3b_0\oplus a_2b_1\oplus a_1b_2\oplus a_0b_3\oplus a_3b_3)\alpha^3$.

СПИСОК ЛИТЕРАТУРЫ

1. *Поспелов Д.А.* Логические методы анализа и синтеза схем. М.: Энергия, 1974.
2. *Авсаркисян Г.С., Брайловский Г.С.* Представление логических функций в виде полиномов Жегалкина // Автоматика и вычисл. техника. 1975. № 6. С. 6–8.
3. *Малюгин В.Д.* Реализация булевых функций арифметическими полиномами // АиТ. 1982, № 4. С. 84–93.
4. *Малюгин В.Д.* Реализация кортежей булевых функций посредством линейных арифметических полиномов // АиТ. 1984. № 2. С. 114–122.
5. *Menger K.S.* A Transform for Logic Networks // IEEE Trans. on computers. 1969. V. C-18. № 3. P. 241–250.
6. *Benjauthrit B., Reed S.* Galois Switching Functions and their Applications // IEEE Trans. on computers. 1976. V. C-25. № 1. P. 78–86.
7. *English W.R.* Synthesis of Finite State Algorithms in a Galois GF(p^n) // IEEE Trans. on computers. 1981. V. C-30. № 3. P. 225–229.
8. *Александров И.Н., Гайдамака Р.И., Никитюк Н.М., Шириков В.П.* Расчет переключательных функций, представленных элементами поля Галуа GF(2^m). Препринт ОИЯИ Р10-84-865. Дубна, 1984.
9. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976.
10. *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.
11. *Никитюк Н.М.* Вопросы оптимального кодирования в годоскопических системах // Приборы и техника эксперимента. 1983. № 3. С. 74–81.
12. *Александров И.Н., Гайдамака Р.И., Никитюк Н.М.* Применение аналитических вычислений для расчета логических схем и спецпроцессоров // Аналитические вычисления на ЭВМ и их применение в теоретической физике. Тр. международного совещания. Дубна: ОИЯИ, 1985. С. 295–300.
13. *Yeh C.S., Reed I.S., Truong T.K.* Systolic Multipliers for Finite Fields GF(2^m) // IEEE Trans. on computers. 1984. V. C-33. № 4. P. 357–360.
14. *Wang C.C., Truong T.K., Shao H.M. a.o.* VLSI Architectures for Computing Multiplications and Inverses in GF(2^m) // IEEE Trans. on computers. 1985. V. C-34. № 8. P. 709–717.
15. *Никитюк Н.М.* Совмещенные операции в поле Галуа GF(2^m) и их применение. Препринт ОИЯИ Р11-87-54. Дубна, 1987.
16. *Hsu I.S., Truong T.K., Deutsch L.J., Reed I.S.* A Comparison of VLSI Architecture of Finite Field Multipliers Using a Dual, Normal, or Standard Bases // IEEE Trans. on computers. 1988. V. 37. № 6. P. 735–739.
17. *Wang C.C.* An Algorithm to Design Finite Field Multipliers Using a Self-Dual Normal Basis // IEEE Trans. on computers. 1989. V. 38. № 10. P. 1457–1460.
18. *Pincin A.* A New Algorithm for Multiplication on Finite Fields // IEEE Trans. on computers. 1989. V. 38. № 7. P. 1045–1049.

19. *Никитюк Н.М* Быстрый алгоритм для выполнения операций умножения в поле Галуа GF(2^m) // Управляющие системы и машины. 1990. № 6. С. 21–28.
20. *Малюгин В.Д., Кухарев Г.А., Шмерко В.П.* Преобразования полиномиальных форм булевых функций. Препринт Института проблем управления, Москва, 1986.
21. *Брейтон Р.К., Хэчтел Г.Д., Санджованни-Винчителли А.Л.* Синтез многоуровневых комбинационных логических схем // Тр. Института инженеров по электронике и радиоэлектронике. 1990. Т. 78. № 2. С. 38–83.
22. *Авсаркисян Г.С.* Полиномиальные формы частичных булевых функций и некоторые их приложения // Изв. АН СССР. Техн. кибернетика. 1983. № 5. С. 50–58.
23. *Авсаркисян Г.С.* Рекуррентные полиномиальные формы частичных булевых функций // Изв. АН СССР. Техн. кибернетика. 1987. № 4. С. 131–135.

Поступила в редакцию 31.03.94