ОСОБЕННОСТИ РЕАЛИЗАЦИИ ОПЕРАЦИЙ УМНОЖЕНИЯ ЭЛЕМЕНТОВ ПОЛЯ ГАЛУА НА FPGA

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Листопад Е.В.

Петровский А.А. – д.т.н.,профессор

При построении современных систем обработки информации зачастую возникает необходимость эффективной реализации арифметических операций над элементами поля Галуа. Особый интерес представляет операция умножения в поле, как наиболее требовательная к аппаратным ресурсам и ограниченная с точки зрения быстродействия. При этом от эффективности реализации данной операции существенно зависят аппаратные и временные характеристики соответствующей системы обработки информации.

Поля Галуа (Galois Field – GF) или конечные поля (Finite Fields) широко применяются во многих областях современной вычислительной техники, связанных с обработкой, приемом и передачей цифровой информации. Это, в частности, цифровая обработка сигналов [1,2], криптография, помехоустойчивое кодирование, верификация БИС и т.п.

Поля Галуа описываются двумя основными параметрами: m и p. Параметр m указывает число двоичных разрядов, использующихся для двоичного представления символа множества, а также определяет количество элементов множества как 2^m. Таким образом, в поле $GF(2^4)$, где $m=4$, содержится всего 16 элементов, и для двоичного представления каждого из них необходимо четыре двоичных разряда. Параметр *p* (генерирующий полином) указывает порядок, в котором элементы поля Галуа следуют друг за другом. Например, генерирующий полином $p(x)$ для поля $GF(2^4)$ может быть следующим: $p(x)=1+x^3+x^4$. Часто используется представление полинома в виде двоичного числа с разрядностью $m+1$. В данном случае, если старшие разряды располагаются слева, то $p=25$ в десятичной системе, или 11001 в двоичной, или $1\cdot 2^4+1\cdot 2^3+0\cdot 2^2+0\cdot 2^1+1\cdot 2^0$. Обозначим корень полинома a, тогда $a^4=a^3+1$.

Элементы поля $GF(2^4)$ приведем в таблице 1 в трех представлениях [3].

Таблица 1 – Поле Галуа для *m=4* и *p=25*

Степенное представление	Полиномиальное представление	Бинарное представление
0	0	0000
1	1	1000
a	a	0100
a^2	a^2	0010
a^3	a^3	0001
a^4	$1+a^3$	1001
a^5	$1+a+a^3$	1101
a^6	$1+a+a^2+a^3$	1111
a^7	$1+a+a^2$	1110
a^8	$a+a^2+a^3$	0111
a^9	$1+a^2$	1010
a^{10}	$a+a^3$	0101
a^{11}	$1+a^2+a^3$	1011
a^{12}	$1+a$	1100
a^{13}	$a+a^2$	0110
a^{14}	a^2+a^3	0011

Степенное представление: нулевой элемент равен 0, первый равен 1, второй равен a и т.д.

Полиномиальное представление: $x=k_0\cdot 1+k_1\cdot a+k_2\cdot a^2+k_3\cdot a^3$, где $k_0,k_1,k_2,k_3=\{0,1\}$ (старшие разряды справа).

Бинарное представление или двоичная форма (старшие разряды справа).

Одним из достоинств операций в поле Галуа является возможность их параллельной реализации. Это в свою очередь позволяет рассматривать их как адекватные архитектуре ПЛИС типа FPGA.

Операция умножения элементов поля Галуа выполняется как умножение двух определенных многочленов по модулю третьего многочлена (по которому построены элементы поля).

Рассмотрим поле с параметрами $m=16$ и $p=126977$, в котором опишем особенности аппаратной реализации операций умножения. Как видно из параметров поля, операнды для произведения являются 16-битными. Учитывая необходимость приведения результата операции по модулю генерирующего полинома (так как вычисления выполняются в поле) определено два варианта аппаратной реализации.

Первый вариант предусматривает умножение за 16 шагов. При этом на каждом шаге выполняется умножение на 1 бит операнда и

осуществляется приведение по модулю полинома. Были разработаны 3 экспериментальные реализации для данного варианта умножения. Реализация 1 выполняет умножение за 16 тактов (за 1 такт 1 шаг умножения с приведением). Реализация 2 выполняет умножение за 8 тактов (за 1 такт выполняется 2 шага умножения с приведением, при этом анализируется 2 бита операнда). Реализация 3 выполняет умножение за 4 такта (за 1 такт выполняется 4 шага умножения с приведением, при этом анализируется 4 бита операнда). Для получения корректных значений рабочей тактовой частоты для каждой реализации применялась схема тестирования (Рисунок 1), предусматривающая установку регистров на входах и выходах оцениваемых итеративных процессоров умножения.

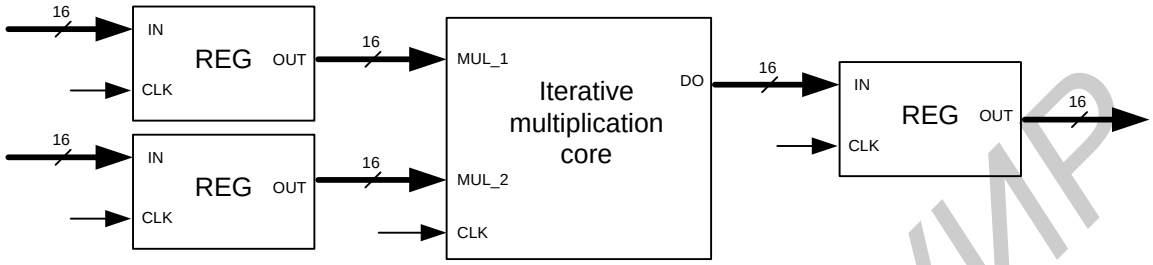

Рис. 1 – Структура тестового блока

Следует отметить, что все 3 реализации способны работать на достаточно высоких частотах. В таблице 2 приведены характеристики экспериментальных вариантов итеративных процессоров, выполняющих операцию умножения за 16 шагов.

	Количество тактов	Ресурсы FPGA, Slices	Частота, МГц	Производительность, Мбит/с
Реализация 1	16	17	390	371,9
Реализация 2	8	24	291	555,0
Реализация 3	4	55	204	778,2

Таблица 2 – Характеристики реализаций, предусматривающих умножение за 16 шагов

Второй вариант предусматривает умножение в 2 шага: непосредственно умножение 16-битных операндов с получением 32-битного промежуточного результата и приведение его по модулю полинома к 16-битному результату. В случае реализации за один такт всей операции умножения с приведением (Реализация 4) удалось получить вариант, способный работать на частоте, сопоставимой с реализацией 3. Выполнено усовершенствование реализации, учитывающее природу строения кристалла ПЛИС (6-входовые элементы LUT кристалла Xilinx Spartan 6). Была применена двухступенчатая схема умножения (Реализация 5). На первой ступени логические операции были описаны в виде 6-входовых логических элементов, которым при синтезе были поставлены в соответствие 6-входовые элементы LUT на кристалле. На второй ступени описаны логические операции над результатами первой ступени вычислений, и реализовано приведение по модулю полинома. В результате описанного подхода удалось достаточно эффективно реализовать умножение за 2 такта с достижением высокой тактовой частоты. В таблице 3 приведены характеристики экспериментальных вариантов итеративных процессоров, выполняющих операцию умножения за 2 шага. Характеристики получены с использованием схемы тестирования, изображенной на рисунке 1.

	Количество тактов	Ресурсы FPGA, Slices	Частота, МГц	Производительность, Мбит/с
Реализация 4	1	50	197	3006,0
Реализация 5	2	46	284	2166,7

Таблица 3 – Характеристики реализаций, предусматривающих умножение за 2 шага

Следует отметить, что лучшие показатели производительности были достигнуты на реализациях, предусматривающих умножение в 2 шага. При этом для устройств с генератором тактовых импульсов (ГТИ), работающим на частоте до 200 МГц рекомендуется к применению реализация 4, а для устройств с ГТИ, работающим на частоте свыше 200 МГц – реализация 5.

Списокиспользованныхисточников:

1. Reyhani Massolem A., Hasan M.A. Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over GF(2^m). IEEE Transaction on Computers. 2004. V. 63. № 8.
2. José Luis Imaña, Low Latency GF(2^m) Polynomial Basis Multiplier. IEEE Transaction on Circuits and Systems. 2011. V. 58. № 5.
3. АркадийПоляков, МехдиТайлеб, НезхатТайлеб. Библиотека VERILOG описаний арифметических операций в поле Галуа. Современная электроника. 2007. № 5.