Библиотека VERILOG-описаний арифметических операций в поле Галуа

Аркадий Поляков, Мехди Тайлеб, Незхат Тайлеб (Москва)

В статье рассматриваются особенности библиотеки модулей высокоуровневых описаний на языке VERILOG параллельных арифметических операций (сложение, инверсия, умножение) в поле Галуа. Библиотека может быть использована при разработке систем передачи информации. Оцениваются временные и ресурсные параметры аппаратной реализации модулей на ПЛИС типа FPGA фирмы Xilinx.

Введение

Поля Галуа (Galois Fields – GF), названные в честь французского математика Эвариста Галуа, или конечные поля (Finite Fields), широко используются в различных областях современной информационной техники, связанных с передачей, приёмом и обработкой цифровой информации. Это, в частности, помехоустойчивое кодирование (коды Рида-Соломона), цифровая обработка сигналов, криптография, тестирование БИС и т.п. [1, 2]. От эффективности реализации арифметических операций (в первую очередь, операции умножения) в этих полях существенно зависят аппаратные и временные характеристики соответствующих информационных систем.

Таблица 1. Поле Галуа для m = 4 и p = 19

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

Упрощённое представление о полях Галуа может быть дано следующим образом. Рассмотрим некоторое количество (*начальное множество*) различных чисел (*символов, элементов поля*). Все числа, которые могут быть получены из начального множества путём применения стандартных арифметических операций (сложение, вычитание, умножение и деление), образуют *поле*. Некоторые поля, как, например, множество целых чисел, являются *бесконечными*. В отличие от таких полей, поля Галуа являются *конечными*, т.е. обладают тем полезным свойством, что результатом операции (GF-операции) над одним или несколькими элементами конечного множества является другой элемент того же множества. Например, в поле Галуа, используемом для помехоустойчивого кодирования символов информации в устройстве чтения-записи DVD-дисков, всего 256 элементов – числа от 0 до 255. Операция сложения 2+2 в таком поле даёт результат, не равный 4.

Поля Галуа характеризуются двумя параметрами: m и p. Параметр m определяет число двоичных разрядов, необходимых для двоичного представления символа множества, а также определяет число элементов множества как 2^m. Таким образом, в поле GF(2^4), где m = 4, имеется всего 16 элементов, и для двоичного представления каждого из них достаточно четырёх двоичных разрядов.

Параметр p, или *генерирующий полином*, определяет порядок, в котором элементы поля следуют друг за другом. Например, полином $p(x)$ для поля GF(2^4) может быть таким: $p(x) = 1 + x + x^4$. Часто используют сокращённое обозначение полинома как двоичного числа разрядностью $m + 1$, т.е. в нашем случае, если старшие разряды слева, p = 19 в десятичной системе, или 10011 в двоичной, или $1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$. Обозначим корень полинома α, т.е. $\alpha^4 = \alpha + 1$.

Элементы поля GF(2^4) представлены в таблице 1 в трёх формах.

1. Степенная форма: нулевой элемент равен 0, первый равен 1, второй равен α в первой степени и т.д.
2. Полиномиальная форма: $x = k_0 \times 1 + k_1 \times \alpha + k_2 \times \alpha^2 + k_3 \times \alpha^3$, где $k_0, k_1, k_2, k_3 = \{0, 1\}$ (старшие разряды справа).
3. Двоичная форма (старшие разряды в данном примере справа!).

Для разработчиков цифровых систем передачи информации была создана параметризованная (параметры m, p) библиотека VERILOG-описаний операций в поле Галуа. Язык VERILOG, наряду с языком VHDL, является общепризнанным стандартом высокоуровневого описания аппаратуры (HDL – Hardware Description Language), используемым при верификации проектов и их реализации в заданном проектировщиком логическом и конструктивном базисе [3]. Общая алгоритмическая компонента языка VERILOG – это язык Си, а не язык АДА (Паскаль), как у VHDL, а его специализированная компонента примерно такая же, как у VHDL, но выражается несколько другими средствами.

Библиотека модулей в определённой части (операция инверсии) учитывает характеристики программируемых логических интегральных схем (ПЛИС), и в частности, ПЛИС типа FPGA фирмы Xilinx (www.xilinx.com). Одной из особенностей этого типа ПЛИС является реализация логических функций с помощью т.н. таблиц решений (логических таблиц, Look Up Table – LUT) и нали-

чие блочной оперативной памяти (Block RAM).

Современные ПЛИС типа FPGA содержат до нескольких десятков тысяч LUT и сотен блоков памяти ёмкостью от 18 Кбит (VIRTEX-4) до 36 Кбит (VIRTEX-5), конфигурируемых в качестве 1-портовой или 2-портовой синхронной памяти с длиной слова от 1 до 36 разрядов.

Библиотечные модули

Операция сложения

В поле Галуа легче всего реализуются операции сложения и вычитания. Это просто *m*-разрядная логическая операция «исключающее ИЛИ» (XOR, сложение по модулю 2) над её аргументами – двоичными векторами. Например, в таблице 1 двоичное представление второго элемента поля GF(2^4) равно 0100, и результат операции 0100 XOR 0100 равен 0000.

Ниже приведено VERILOG-описание параметризованного модуля *gfadd_m*, выполняющего операцию сложения в поле Галуа. Отметим, что в языке VERILOG символ «^» означает логическую операцию «исключающее ИЛИ» (XOR). Комментарий отделён символами //.

```
module gfadd_m(in1, in2, out1);
//описание интерфейса модуля
//gfadd_m
parameter m=8;
//значение параметра m
//по умолчанию=8
input [m-1:0] in1;
//m-разрядные входы in1, in2
input [m-1:0] in2;
output [m-1:0] out1;
//m -разрядный выход out1
assign out1 = in1^in2;
//оператор вычисления функции
//XOR и присваивания
//в переменную out1
endmodule
```

Тем из читателей, кто знаком с языком VHDL, некоторое представление о языке VERILOG даст пример описания того же модуля *gfadd_m* на языке VHDL:

```
Library IEEE;
Use IEEE.std_logic_1164.all;
entity gfadd_m is
--описание интерфейса модуля
generic (m: positive:=8);
port (in1,in2:in
std_logic_vector(m-1 downto 0);
out1: out std_logic_vector(m-1
downto 0)
);
end;
architecture beh of gfadd_m is
--описание тела модуля
begin
out1 <= in1 XOR in2;
--оператор вычисления функции
XOR и присваивания в out1
end;
```

При использовании системы автоматизированного синтеза XST САПР ISE v8.2i фирмы Xilinx и значении параметра $m = 8$ аппаратная реализация *gfadd_m* на ПЛИС типа FPGA требует всего 8 LUT.

Операция умножения

Известно большое число исследований, посвящённых методам аппаратной реализации операции умножения в этих полях [4, 5], и в частности, на базе ПЛИС типа FPGA.

Алгоритм параллельного умножения, предложенный Мастровито (Mastrovito), позволил получить оценки сложности аппаратной реализации в $m^2 - 1$ одноразрядных вентилей XOR2 плюс m^2 одноразрядных вентилей 2И (AND2). В последующих работах по развитию этого подхода эти оценки были несколько улучшены до порядка $m^{1,6}$ вентилей XOR2.

Ниже приведено VERILOG-описание интерфейса параметризованного модуля *gfmul* (обозначим его как вариант P), реализующего умножение (стандартное значение $m = 8$, $p = 285$) [4]:

```
module gfmul(a,b,c);
//умножение, вариант P по методу
//[4]
 // GF PARAMETERS
 parameter m=8;
//разрядность символа поля m
//по умолчанию=8
 parameter [m:0] p=285;
//p - генерирующий
//полином=2**8+2**5+1
 //Internal parameters - вспомо-
 //гательные внутренние параметры
 parameter [m-1:1] p1= p[m-1:1];
 parameter v=m*2-2;
 //PORTS - описание портов модуля
 input [m-1:0] a,b;
//этот модуль предполагает, что
//старшие разряды слева
 output [m-1:0] c;
```

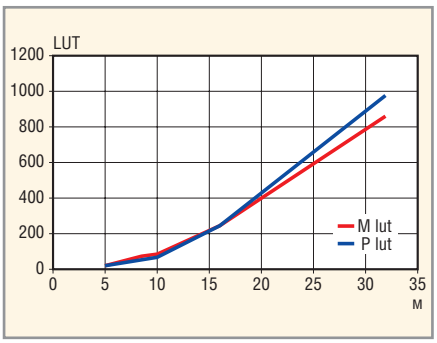

Рис. 1. Графики зависимости объёма аппаратуры умножителей *M* и *P* от параметра *m*

Оценки вариантов схемной реализации модуля *gfmul* на кристалле ПЛИС фирмы Xilinx типа XCV-41x60 для разных *m* и *p* представлены в таблице 2 в столбцах с префиксом P.

Синтезатор XST фирменного САПР Xilinx ISE 8.2 строит схемы, сложность которых, измеряемая в LUT, примерно пропорциональна квадрату *m* (см. табл. 2 и рис. 1).

Для обеспечения возможности динамического изменения генерирующего полинома *p* используется другой модуль – *gfmul_p*(*a,b,c,p*), в котором в список сигналов введён сигнал *p*. Платой за эту возможность является более сложная и медленная схема. При $m = 8$ и $p = 285$ она имеет задержку 7,23 нс и требует 89 LUT, т.е. примерно в полтора раза больше, чем модуль *gfmul*.

Ниже приведён интерфейс другого параметризованного модуля *GF_MUL*, более эффективно реализующего умножение (стандартное значение $m = 5, p = 37$). В этом модуле реализован алгоритм работы [5]. Вместо параметра *p* используется эквивалентный ему параметр *q*, состоящий из нескольких элементов GF. Например, для поля ($m = 5, p = 37$), *q* – это вектор из четырёх значений элементов поля ($\alpha^6, \alpha^7, \alpha^8, \alpha^9$).

Таблица 2. Зависимость объёма аппаратуры и временной задержки от *m* для модулей *GF_MUL* и *gfmul*

m	*p*	M lut	M del (ns)	P lut	P del (ns)
5	37	20	2,702	20	2,07
8	301	70	3,28	53	4,76
10	1033	84	3,274	75	3,37
12	4179	145	3,847	121	4,02
16	75763	245	3,87	244	7,51
32	7115993485	866	4,49	976	23,54

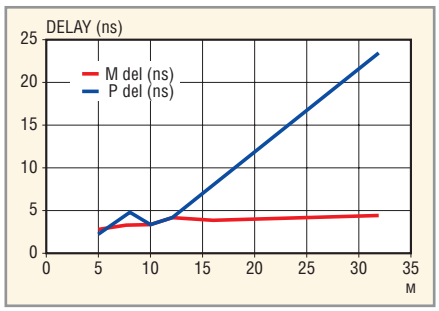

Рис. 2. Графики зависимости задержки (DELAY) умножителей *M* и *P* от параметра *m*

```
module GF_MUL(A,B,C);
 //Parameters
 parameter m=5;
 parameter
q=20'b10010100101101010010;
 //Ports
 input [m-1:0] A, B;
//старшие разряды справа
 output [m-1:0] C;
```

Зависимости сложности и задержки схемы модуля *GF_MUL* для различных *m* и *p* представлены в таблице 2 в столбцах с префиксом M. Видно, что если при малых *m* оба варианта умножителей (P и M) имеют примерно равные показатели, то при больших *m* (*m* > 16) временная задержка варианта M (M del) гораздо меньше (см. рис. 2).

Операция инверсии

Формулы для вычисления инверсии в поле Галуа [6] прямо вытекают из теоремы Ферма. Не вдаваясь в математику, можно сказать, что инверсия вычисляется как цепочка операций умножения и возведения в квадрат, которое, в свою очередь, реализуется как умножение величины самой на себя. Например, для GF(2^4) инверсия (I) элемента x ($I(x)$) вычисляется по формуле:

$$I(x) = x^{-1} = x^2 x^{2^2} x^{2^3} x^{2^4}.$$

Текст описания параметризованного модуля *inverse_comb* для вычисления инверсии с использованием *gfmul* представлен ниже:

```
parameter m= 8;
//параметры поля Галуа
parameter p= 285;
input [m-1:0] x;
        output [m-1:0] y;
        wire [m-1:0] mtmp[1:m-1];
wire [m-1:0] inv[1:m-1];
wire [m-1:0] inv_rez;
genvar i;
gfmul #(m,p) INV_M1(x, x,
mtmp[1]);
//beta^2
assign inv[1]=mtmp[1];
generate
for (i=1; i<m-1; i=i+1)
begin :MM
gfmul #(m,p) INV_MN(mtmp[i],
mtmp[i], mtmp[i+1]);
gfmul #(m,p) INV_MK(inv[i],
mtmp[i+1],inv[i+1]);
end
endgenerate
assign y=inv[m-1];
endmodule
```

Если при $m = 5$ и $p = 59$ комбинационная схема *inverse_comb* имеет вполне приемлемые показатели, то при $m = 8$ и $p = 285$ количество LUT равно 362, а задержка составляет 25 нс.

Очевидно, что для таких значений m ресурсные и временные затраты на реализацию инверсии модулем *inverse_comb* слишком велики. Можно попытаться использовать табличные решения (ПЗУ). В блоке памяти (Block RAM) объёмом 16 Кбит удаётся таблично реализовать инверсию до $m = 9$, а при $m > 9$ можно использовать несколько блоков.

В модуле *ROM2_POL* предложено решение для $m = 8$ на базе 2-портовой памяти, которая позволяет одновременно работать с двумя таблицами.

```
//the first file to
//ADR= from 0 0000 0000 to 0
//1111 1111
//the second file to  ADR= from
//1 0000 0000 to 1 1111 1111
module
ROM2_POL(CLKA,CLKB,WE,EN,OUT_EN,A
DRA,ADRB ,DI,DOA,DOB);
//Parameters
parameter adr_nbits=8;
parameter data_nbits=8;
parameter
file_name1="inverse_table_8_0_285
.rom";
parameter
file_name2="power_table_8_239_0_2
85.rom";
//Input Ports
input CLKA,CLKB,WE,EN,OUT_EN;
input [adr_nbits-1:0] ADRA,ADRB;
input [data_nbits-1:0] DI;
//Output Ports
output reg [data_nbits-1:0]
DOA,DOB;
//DOA-выход табл1-inverse_tabl
//Internal ROM duble size! 9
//bits addr!
reg [data_nbits-1:0] rom
[0:2**(adr_nbits+1)-1];
reg [data_nbits-1:0]
DOA_AUX,DOB_AUX;
initial begin
//заполнение ПЗУ из файлов
$readmemb(file_name1,rom,0,2**(ad
r_nbits)-1);
$readmemb(file_name2,rom,2**(adr_
nbits),2**(adr_nbits+1)-1);
end
//Behavioural Statements
//FIRST OUT PORT
always @(posedge CLKA)
if(EN)begin
if(WE)
//при WE=0 имеем ПЗУ
rom[{1'b0,ADRA} ]<=DI;
else
DOA_AUX<=rom[ {1'b0,ADRA} ];
if(OUT_EN)
DOA<=DOA_AUX;
        end
//SECOND OUT PORT
always @(posedge CLKB)
if(EN)begin
DOB_AUX<=rom[{1'b1,ADRB}];
if(OUT_EN)
DOB<=DOB_AUX;
end
endmodule //ROM2_POL
```

Рассмотренная библиотека VERILOG-модулей параллельных арифметических операций в полях Галуа была использована при разработке декодера кода Рида-Соломона.

Литература

1. *Sylvester J.* Reed Solomon Codes. Electrobit. January 2001.
2. *Moon T.K.* Error correction coding, mathematical methods and algorithms. John Wiley & Sons, 2005.
3. *Поляков А.К.* Языки VHDL и VERILOG в проектировании цифровой аппаратуры. Солон-П, 2003.
4. *Iliev N., Stine J., Juchimiec N.* Digital Finite – Field Multiplier for Reed-Solomon Channel codes in GF(2^8) with programmable basis polynomial. IIT VLSI LAB, 2003.
5. *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.
6. *Choi S., Kim K., Lee W., Kim K.* A Finite Field Inversion Circuit for Higher-Speed communications. KERI. Korea, 2003.

Новости мира News of the World Новости мира

Toshiba перейдёт на 43 нм в течение года?

Намереваясь опередить компанию Samsung Electronics в технологической гонке, Toshiba планирует в конце 2007/начале 2008 г. запустить производство флэш-памяти типа NAND по 43-нм проектным нормам. Переход на более прецизионные нормы позволит Toshiba существенно сократить удельную стоимость микросхем, получаемых с кремниевой пластины.

По оценкам издания Nikkei business daily, при 43-нм производстве количество чипов, получаемых с одной пластины, увеличивается примерно на 40% по сравнению с 56-нм. Таким образом, Toshiba будет иметь потенциальный 40-процентный запас по снижению цен на свою продукцию, что даст ей неоспоримые преимущества перед конкурентами. Как известно, на данный момент технологическим лидером в этой отрасли является компания Samsung, которая ещё в марте начала отгрузки образцов 50-нм NAND-чипов.

Потеснит ли Toshiba своего главного конкурента в технологической гонке? Успеет ли она вовремя и без задержек перейти на инновационное производство? Пока ответить на эти вопросы сложно, ведь сам производитель ещё даже официально не подтвердил свои планы по переходу на 43 нм. Источник утверждает, что к концу текущего года Toshiba построит завод для 43-нм производства в юго-западной префектуре Мие (Mie Prefecture), что в Японии. Этот завод станет четвёртым по производству чипов памяти в Японии.

cdrinfo.com

20 DRAM-чипов в упаковке толщиной 1,4 мм

Молодая компания Akita Elpida Memory (создана летом 2006 г. по инициативе Elpida, известного производителя DRAM-памяти) сообщила о разработке нового метода упаковки чипов. С его помощью ей удалось впервые в мире поместить 20 полупроводниковых кристаллов DRAM в одной MCP-упаковке (multi-chip package) толщиной всего 1,4 мм.

Для достижения успеха инженеры Akita Elpida разработали инновационную технологию для утонения (шлифовки) кристаллов толщиной 30 мкм перед упаковкой, метод соединения слоёв с помощью тончайших проводников, технику впрыскивания канифоли в микроскопические отверстия. Компания намерена тесно сотрудничать с производителями оборудования для дальнейшего продвижения своей разработки и коммерциализации производства.

Хочется отметить важность подобных разработок в свете беспрерывного процесса миниатюризации портативной техники и растущих требований к её производительности. В этой области работает множество полупроводниковых компаний. Из недавних достижений стоит отметить разработки таких производителей, как IBM и Samsung Electronics.

www.3dnews.ru

Samsung на пути к созданию ОЗУ нового поколения

Одним из важнейших технологических достижений в полупроводниковой отрасли за последний месяц стала разработка компанией IBM методики так называемой «трёхмерной» упаковки чипов. Нечто подобное на днях анонсировала и компания Samsung Electronics.

Как сообщается в пресс-релизе, Samsung разработала метод упаковки чипов памяти, использующий технологию TSV (through silicon vias, внутрикремниевые межсоединения). По заявлению компании, это позволит существенно ускорить память, уменьшить энергопотребление и габариты микросхем.

Новая упаковка называется WSP (wafer-level-processed stacked package). Она может вмещать четыре чипа DDR2 DRAM плотностью 512 Мбит (4 × 512 Мбит). Используя такие двухгигабитные структуры, Samsung может создать модули ОЗУ ёмкостью 4 Гб.

Инновационный технологический метод Samsung устраняет необходимость в относительно длинных металлических проводниках, которые соединяют между собой традиционные «двухмерные» чипы и их составные элементы, заменяя эти проводники внутрикремниевыми соединениями. Межсоединения TSV представляют собой вертикальные каналы диаметром порядка единиц микрон, протравленные в кремниевой пластине с помощью лазера и заполненные проводником – медью. Такие внутрикремниевые соединения позволяют располагать кристаллы плотнее и создавать более тонкие упаковки. Межсоединения through-silicon vias покрыты алюминием, который играет роль экрана, в результате чего снижаются перекрестные помехи. Конкретные сроки внедрения новой разработки в массовое производство пока не называются.

www.3dnews.ru

После Intel о 450-мм пластинах заговорила TSMC

Компания TSMC (Taiwan Semiconductor Manufacturing Company) сформировала группу, заданием которой является оценка осуществимости перехода на производственный процесс с использованием кремниевых пластин диаметром 450 мм. Представители TSMC подтверждают заинтересованность в переходе на 450-мм пластины, но отмечают, что о каких-либо сроках внедрения нового производства речь пока идти не может. Напомним, что на Форуме IDF Spring 2007, который недавно завершился в Пекине, компания Intel также выразила сильную заинтересованность в 450-мм производстве.

На данный момент в полупроводниковой индустрии лидерство продолжают удерживать 200-мм фабрики, которые могут похвастаться объёмом производства в 380...390 тыс. пластин в месяц. 300-мм фабрики постепенно набирают обороты, и уже сегодня количество чипов, изготавливаемых на новых производственных линиях за месяц, эквивалентно производству 200 тыс. 200-мм пластин.

Переход на 450-мм пластины понизит удельную стоимость микросхем, но первоначальные вложения в такое производство в три раза превышают инвестиции в 300-мм производство. Поэтому, как считают эксперты, компаниям стоит задуматься о переходе именно на 300-мм пластины – это самое оптимальное решение на сегодняшний день. В 2009 г. 300-мм фабрики полностью вытеснят старые 200-мм.

По оценкам специалистов IEK (Taiwan's Industrial Economics and Knowledgde Center), среди тайваньских компаний в будущем одними из первых 450-мм фабрики построят TSMC, Powerchip Semiconductor Corporation (PSC), Nanya Technology и ProMOS Technologies. Но когда будет построена первая 450-мм фабрика? На этот вопрос пока никто не может дать определённый ответ.

digitimes.com