УДК 638.322

**В.П. ТАРАСЕНКО, А.К. ТЕСЛЕНКО, А.И. РОГОВЕНКО**

***Национальный технический университет Украины "КПИ", Украина***

# СОЗДАНИЕ ПАРАМЕТРИЧЕСКИХ ЯДЕР (SOFTCORES) ДЛЯ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ В КОНЕЧНЫХ ПОЛЯХ

В статье на основе анализа предложенных ранее методов аппаратной реализации операций в конечных полях на одномерном каскаде конструктивных модулей рассматривается реализация на ПЛИС с использованием языка VHDL оптимизированных по аппаратным затратам параметрических ядер в зависимости от вариантов кодирования внутренних состояний. Параметром настройки на конкретную реализацию является порядок поля.

**конечные поля, одномерный каскад однотипных конструктивных модулей, VHDL, ПЛИС, сумматор по переменному модулю**

При решении многих задач обеспечения гарантоспособности и информационной стойкости компьютерных систем используются операции в конечных полях. Примером может служить защита от негативных антропогенных влияний (ассиметричные криптографические преобразования) или от техногенных влияний (коды для обнаружения и исправления ошибок) [1,2]. С развитием техноглогии ПЛИС существенно расширилась практическая возможность выполнения специализированных вычислений путем аппаратной реализации, которая ранее не всегда была экономически оправдана. Одним из направлений аппаратной реализации операций в конечных полях является использование одномерных каскадов конструктивных модулей (ОККМ). В работах [3,4] теоретически обоснована возможность и опре-делены характеристики реализации на ОККМ базовых операций в основном конечном поле любого заданного порядка. С другой стороны, в практике применения ПЛИС широкое распространение получило применение оптимизированных решений (softcores), представленных, например, на языке VHDL. При этом указанные решения имеют параметрический характер, когда пользователь путем задания соответствующих параметров (например, разрядности данных) определяет конкретную реализацию.

Для выявления оптимальной реализации параметрического ядра данным методом было произведено исследование влияния кода класса эквивалентности на аппаратные затраты.

В данном случае под аппаратными затратами подразумевается количество слайсов (slices) в ПЛИС типа FPGA или макроячеек (macrocells) в CPLD которые занимает ядро. Определение оптимальности реализации заключается в поиске такого варианта кодирования классов эквивалентности, которое приводит к минимальному количеству требуемых ресурсов ПЛИС.

Работа проводилась в САПР Active HDL 7.1 с использованием библиотек Xilinx. Параметрическое ядро было реализовано с помощью языка VHDL. Основой ядра является структура конструктивного модуля, описанная в [1], представленная на рис.1.

Каждая из комбинационных схем реализации конструктивного модуля представляет собой отдельный асинхронный процесс. Конструктивные модули объединяются в линейную структуру требуемой разрядности с помощью конструкции generic.

Проверка работоспособности физической реализации параметрического ядра производилась на ПЛИС семейства Spartan 3E в составе устройства

"Spartan 3E Starter Kit", путем сравнения с результатом выполнения операции полученным от ядра реализованного по классической схеме.

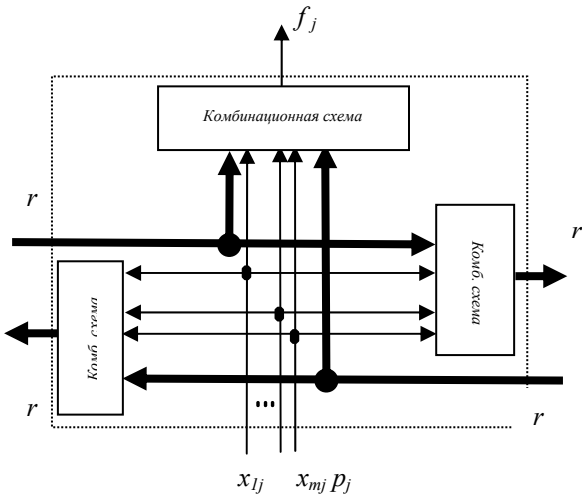


Рис. 1. Структура конструктивного модуля

Исследования проводились для нескольких семейств ПЛИС в каждом из типов. Одна и та же реализация параметрического ядра, в данном случае четырехразрядная, проходила синтез и имплементацию для каждого из семейств, после чего анализировалось количество занимаемых ресурсов ПЛИС. Средства имплементации были настроены на оптимизацию по скорости.

Критические значения объема требуемых ресурсов ПЛИС приведены в табл. 1.

Таблица 1

Критические значения количества слайсов, занимаемых четырехразрядным параметрическим ядром в FPGA

| № | Код | | Семейства ПЛИС типа FPGA | | | |
|---|---|---|---|---|---|---|
| | | | Virtex II | Virtex IV | Spartan 2 | Spartan 3 |
| 1 | 1234 | 2314 | 34 | 34 | 34 | 34 |
| 2 | 1243 | 2134 | 27 | 27 | 28 | 27 |
| 3 | 1243 | 2314 | 34 | 34 | 34 | 34 |
| 4 | 1342 | 3421 | 28 | 28 | 28 | 28 |
| 5 | 4312 | 1423 | 36 | 36 | 36 | 36 |
| 6 | 4312 | 2314 | 37 | 37 | 37 | 37 |
| 7 | 2341 | 1423 | 46 | 46 | 47 | 46 |
| 8 | 2341 | 1432 | 47 | 47 | 47 | 47 |
| 9 | 2341 | 2314 | 43 | 43 | 43 | 43 |
| 10 | 2341 | 2341 | 41 | 41 | 41 | 41 |
| 11 | 2341 | 3214 | 44 | 44 | 44 | 44 |

Исходя из результатов представленных в табл. 1, видно, что в зависимости от комбинаций кодирования классов эквивалентности количество занимаемых в FPGA слайсов может отличаться, вплоть до 74%. В ПЛИС типа CPLD (табл. 2) различие размеров реализации не столь значительно и может изменяться на 36%. Таким образом, при выборе определённой кодировки можно добиться существенной экономии ресурсов ПЛИС.

Таблица 2

Критические значения количества и макроячеек, занимаемых четырехразрядным параметрическим ядром в CPLD

| № | Код | | Семейства ПЛИС типа CPLD | |
|---|---|---|---|---|
| | | | Coolrunner | Coolrunner 2 |
| 1 | 1234 | 2314 | 31 | 31 |
| 2 | 1243 | 2134 | 25 | 25 |
| 3 | 1243 | 2314 | 29 | 29 |
| 4 | 1342 | 3421 | 26 | 26 |
| 5 | 4312 | 1423 | 29 | 29 |
| 6 | 4312 | 2314 | 32 | 32 |
| 7 | 2341 | 1423 | 32 | 32 |
| 8 | 2341 | 1432 | 33 | 33 |
| 9 | 2341 | 2314 | 38 | 38 |
| 10 | 2341 | 2341 | 31 | 31 |
| 11 | 2341 | 3214 | 34 | 34 |

Для проверки верности данного подхода к реализации параметрических ядер с различной функциональностью была дополнительно реализована операция вычитания в остатках по переменному модулю и проведены исследования влияния комбинаций кодирования на количество требуемых ресурсов. Критические значения требуемых ресурсов ПЛИС приведены в табл. 3 и табл. 4.

Для всех вариантов кодирования изменение максимальной рабочей частоты не превышало 3%. Но дабы исключить все неточности программной модели следует ещё провести дополнительные исследования изменения максимальной тактовой частоты при различных кодировках на физическом уровне. Из таблиц 1 - 4 видно, что размер реализации практически не зависит от семейства ПЛИС, что дает возможность создавать уни-версальные параметрические модули ориентированные только на тип ПЛИС.

Таблица 3

Критические значения количества слайсов, занимаемых четырехразрядным параметрическим ядром FPGA

| № | Код | | Семейства ПЛИС типа FPGA | | | |
|---|---|---|---|---|---|---|
| | | | Virtex II | Virtex IV | Spartan 2 | Spartan 3 |
| 1 | 1243 | 231 | 22 | 22 | 23 | 22 |
| 2 | 1243 | 213 | 28 | 28 | 29 | 28 |
| 4 | 1342 | 312 | 23 | 23 | 23 | 23 |
| 5 | 4312 | 132 | 31 | 31 | 31 | 31 |
| 6 | 4312 | 231 | 32 | 32 | 32 | 32 |
| 7 | 2341 | 213 | 41 | 41 | 41 | 41 |
| 8 | 1234 | 321 | 41 | 41 | 41 | 41 |
| 9 | 2341 | 312 | 38 | 38 | 38 | 38 |

Таблица 4

Критические значения количества макроячеек, занимаемых четырехразрядным параметрическим модулем в CPLD

| № | Код | | Семейства ПЛИС типа CPLD | |
|---|---|---|---|---|
| | | | Coolrunner | Coolrunner 2 |
| 1 | 2341 | 132 | 22 | 22 |
| 2 | 1243 | 231 | 19 | 19 |
| 4 | 1342 | 312 | 20 | 20 |
| 5 | 1243 | 123 | 27 | 27 |
| 6 | 4312 | 132 | 22 | 22 |
| 7 | 4312 | 231 | 27 | 27 |
| 8 | 1234 | 321 | 28 | 28 |
| 9 | 2341 | 312 | 32 | 32 |

Применительно к операции умножения в остатках по переменному модулю данный подход дает следующие результаты. Параметрическое ядро имеет несколько отличную структуру от структуры представленной на рис. 1. У него присутствует два выхода первичной функции, на одном формируется остаток сдвига влево на один разряд, на втором формируется остаток частичного произведения [3]. Для количественной оценки требуемых ресурсов для реализации n-разрядного умножителя возьмем его реализацию со средней ресурсоемкостью для $n$=4 и произведем его исследования при различных значениях $n$. Результаты исследований представлены в табл. 5. Из результатов приведенных в табл. 5 можно сделать выводы, что умножители на основе ОККМ имеют преимущество при реализации в ПЛИС не имеющих аппаратных модулей умножения, а так же в случае, необходимости реализации операции умножения, разрядность которой существенно превышает разрядность аппаратно реализованных умножителей.

Таблица 5

Количественная оценка требуемых ресурсов для параметрического ядра умножения в остатках по переменному модулю

| № | Разрядность | | Семейства ПЛИС | | | |
|---|---|---|---|---|---|---|
| | | | ОККМ | | Функция САПР | |
| | | | CPLD (2C256) | FPGA (3S400) | CPLD (2C256) | FPGA (3S400) |
| 1 | 8 | 8 | 29% | 1% | 41% | 1% |
| 2 | 16 | 16 | 82% | 3% | - | 3% |
| 3 | 32 | 32 | - | 9% | - | 15% |
| 4 | 128 | 128 | - | 33% | - | - |
| 5 | 256 | 256 | - | 86% | - | - |

## Литература

1. Харченко В.С. Гарантоздатність комп'ютерних систем: проблеми і результати // Авіаційно-космічна техніка і технологія. – 2005. № 7 (23). – С. 352-376.

2. Тарасенко В.П., Михайлюк А.Ю., Тесленко О.К., Осипов О.С. Методологічні та термінологічні аспекти інформаційної стійкості освітніх комп'ютерних технологій та мереж // Радіоелектронні та комп'ютерні системи). – 2006. – №7. – С. 123-134.

3. Тарасенко В.П., Тесленко А.К. Реализация основных арифметических операций над остатками на одномерных каскадах конструктивных модулей // Управляющие системы и машины. – 2003. – № 3 (185) – С. 29-42.

4. Тарасенко В.П., Тесленко О.К. Реалізація операцій в скінчених полях на одновимірному каскаді конструктивних модулів // Системні дослідження та інформаційні технології. – 2006. – № 2. – С. 12.

*Поступила в редакцию 28.01.2008*

**Рецензент:** д-р техн. наук, проф. В.В, Лукин, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.