Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.315

Неверович
Дмитрий Владимирович

Разработка математических и аппаратных алгоритмов преобразования из позиционной системы счисления в модулярную и обратно

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-40 80 03 Вычислительные машины и системы

Научный руководитель
Шабинская Елена Владимировна
ведущий научный сотрудник НИИПФП им. А.Н. Севченко БГУ, к.т.н.

Минск 2017

ВВЕДЕНИЕ

Обработка больших объемов информации тесно связана с задачей вычислений над числами большой разрядности (>100 двоичных разрядов). Вычисления над числами больших разрядностей встречаются, например, в криптографии, в устройствах обработки информации в реальном времени (распознавании речи и образов), при анализе синоптических и геофизических данных, в задачах стратегического назначения.

Модулярная арифметика является параллельной формой обработки информации в которой вычисления производятся над остатками от деления на заранее выбранные модули {p1,p2,p3…,pN}. За счет арифметических вычислений над мало разрядными основаниями от деления достигается высокая скорость вычислений. Обработка данных с использованием модулярной арифметики включает 3 этапа: преобразование информации из позиционного представления в модулярное, арифметические вычисления и обратное преобразование модулярного представления в позиционное. Основным преимуществом модулярной арифметики является реализация арифметических операций, вычисление которых происходит на втором этапе. Однако, математически и аппаратные вычисления сложны в реализации преобразования одной системы счисления в другую. в том числе в области криптографии.

Целью данной работы является изучение и реализация алгоритмов модулярной арифметики на ПЛИС и практическое исследование полученных результатов.

Объект исследования: алгоритмы вычислений модулярной арифметики.

Предмет исследования: теоретический и практические аспекты реализации устройств модулярной арифметики.

Задачи:

Изучение алгоритмов модулярной арифметики, основанные на китайской теореме об остатках и полиадическом коде.

Разработка моделей алгоритмов преобразования.

Проведение экспериментальных исследований разработанных моделей на FPGA.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

В настоящий момент в различных сферах деятельности человека существуют задачи, решение которых предусматривает использование вычислений с числами большой разрядности.

Такие задачи возможны в криптографии, астрономии, математике, в сфере информационных технологий. При проведении арифметических операций с числами большой разрядности зачастую применение стандартного механизма обработки больших чисел дает малую скорость работы. Возникновение ошибок при вычислении не является редким явлением что приводит к большим временным затратам на решение исходной задачи. Данную проблему можно разрешить воспользовавшись переводом чисел из позиционной системы счисления в систему остаточных классов - это даст возможность распараллелить обработку арифметических операций.

В работе рассматриваются особенности применения модулярной арифметики для чисел большой разрядности. Описывается аппаратная реализация устройств на основе модулярной арифметики. Анализируются реализации сумматоров на основе традиционного подхода и модулярной арифметики на FPGA.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Изначально модулярная арифметика рассматривалась как интересный, сугубо теоретический вопрос из–за сложности производства вычислительных структур для её реализации. Современное развитие технологии интегральных схем сделало возможным использование модулярной арифметики для многих областей цифровой обработки сигналов, распознавания образов и других задач, требующих интенсивных вычислений.

Основным достоинством системы остаточных классов является то, что арифметические операции производятся в ней независимо по каждому из модулей, следовательно, они могут выполняться параллельно по нескольким вычислительным каналам.

Малоразрядность обрабатываемых остатков позволяет для повышения быстродействия арифметических операций в вычислительных каналах применять методы с использованием памяти.

Обобщенная структура устройств цифровой обработки сигналов в модулярной арифметике представлена на рисунке 1. Число x на входе преобразовывается из позиционной системы счисления (ПСС) в модулярное представление в системе остаточных классов в базисе модулей, после чего выполняются независимые вычисления для каждого модуля im. На выходе происходит обратное преобразование из системы остаточных классов в позиционную.

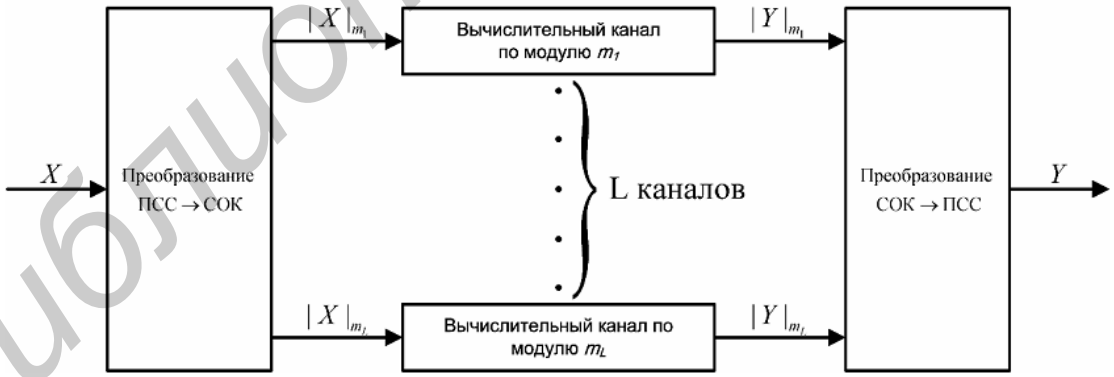

Рисунок 1 – Общая структура устройств цифровой обработки сигналов в СОК

Структура, изображённая на рисунке 1.1, имеет ряд неоспоримых преимуществ при её реализации на интегральных схемах:

1. Независимость каждого канала по отдельному модулю обеспечивает значительную гибкость при планировке и топологическом проектировании кристалла.

2. Реализация таких устройств на основе ПЛИС, обладающих меньшими вентильными ресурсами, может быть легко перепланирована и размещена в несколько кристаллов.

3. При необходимости введение дополнительных избыточных каналов обеспечивает возможность построения отказоустойчивых систем.

4. Малоразрядность остатков. Ввиду малого количества возможных кодовых комбинаций появляется возможность построения табличной арифметики. При этом большинство операций превращаются в однотактовые, осуществляемые простой выборкой из таблиц. По мере совершенствования технологии производства запоминающих устройств с высокой плотностью записи информации, составляющих техническую систему табличного метода вычислений, интерес к СОК неуклонно возрастает.

5. Арифметические операции сложения, умножения и вычитания являются модульными и могут выполнятся за один такт работы системы.

6. Реализация принципа конвейерной обработки информации. Это означает, что при выполнении вычислений модульные и следующие за ним операции удаётся совместить по времени только тогда, когда очередные операции зависят от результатов, текущих, ещё не закончившихся операций. Таким образом, алгоритмы модулярной арифметики обладают конвейерной структурой.

7. Высокая точность, надёжность, способность к самокоррекции. Причём в СОК можно построить непозиционные коды, обнаруживающие и исправляющие ошибки, которые являются полностью арифметическими, то есть в этих кодах информативная и контрольная части равноправны относительно любой операции. Эта особенность предоставляет возможность варьировать корректирующей способностью кода за счёт изменения точности вычислений.

Для реализации устройства преобразования в диссертации были выбраны следующие алгоритмы: алгоритмы на основе китайской теореме об остатках и на основе полиадического кода.

Как сказано ранее основной сложностью реализации устройств модулярной арифметики является реализация обратного и прямого преобразователя. Для упрощения реализации преобразователя обычно выбираются следующие группы модулей $2^n \pm 1, 1^n \pm 3, 2^n \pm 5$.

Таким образом поэтапный алгоритм преобразования из позиционного кода в код системы остаточных классов на основе модулярного сложения выполняется следующим образом, входное число разбивается на группы по n разрядов, где n – двоичный логарифм от выбранного основания. Дальнейшие действия зависят от вида основания:

1. Если основание вида $2^n - 1$, в этом случае группы складываются. Полученный результат является остатком от числа.

2. Если основание вида 2^n, в этом случае результатом будет n последних разрядов входного числа.

3. Если основание вида $2^n + 1$, в этом случае группы складываются, при том, что каждая четная группа складывается с обратным знаком.

4. Если основание вида $2^n + 3$, в этом случае группы складываются и умножатся на константы вида 3^m, при том, что каждая четная группа складывается с обратным знаком.

5. Если основание вида $2^n - 3$, в этом случае группы складываются и умножатся на константы вида 3^m. Полученный результат является остатком от числа.

Для реализации сложения был выбран метод на основе позиционного сложения с прямым преобразованием. Из-за небольшой разрядности выходных данных блоки сумматора и преобразователя получаются компактными по занимаемым ресурсам.

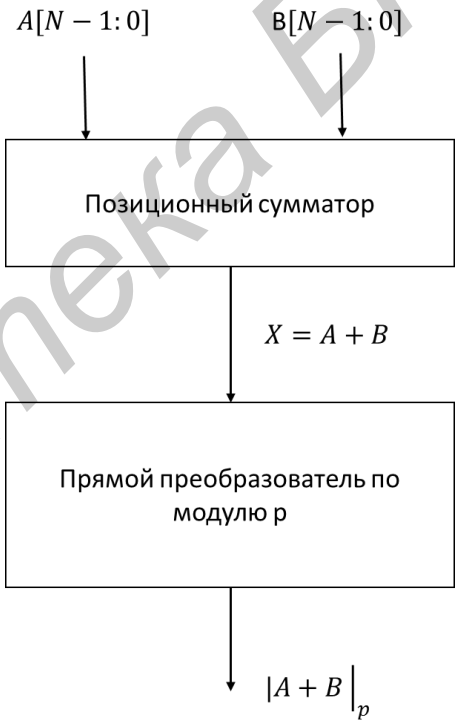

Рисунок 2 – Структурная схема модулярного сумматора на основе позиционного сумматора с прямым преобразователем

Модулярный сумматор на основе позиционного сумматора состоит из двух модулей: модуль позиционного сумматора, модуль прямого преобразователя по модулю.

Первый блок позиционного сумматора представляет собой сумматор со входами одинаковой разрядности на выходе получаем сумму с учетом переноса.

Второй блок прямого преобразователя представляет собой блок прямого преобразователя по основанию p. Прямой преобразователь этого блока получается компактным поскольку требуется взять модуль от небольшого числа с переполнением.

Обратное преобразование на базе полиадического кода, базируется на идее, что число X может быть представлено в системе взаимно простых чисел $p_1, \dots, p_n$:

$$X = a_1 + a_2 p_1 + a_3 p_1 p_2 + \cdots + \\ + a_{n-1} p_1 p_2 \dots p_{n-2} + a_n p_1 p_2 \dots p_{n-1}, \quad (1)$$

где $0 < a_i < p_i$ю.

А коэффициенты a_i:

$$a_1 = x_1, \quad (2)$$
$$a_2 = ||p_1^{-1}|_{p_2} * (x_2 - a_1)|_{p_2},$$
$$a_3 = ||p_2^{-1}|_{p_3} (|p_1^{-1}|_{p_3} * (x_2 - a_1) - a_2)|_{p_3},$$
$$a_4 = ||p_3^{-1}|_{p_4} (|p_2^{-1}|_{p_4} (|p_1^{-1}|_{p_4} * (x_2 - a_1) - a_2) - a_3)|_{p_4},$$
$$\dots$$
$$a_n = ||p_{n-1}^{-1}|_{p_n} (|p_{n-2}^{-1}|_{p_n} (\dots |p_2^{-1}|_{p_n} * (|p_1^{-1}|_{p_n} (x_n - a_1) - a_2) - \cdots) \\ - a_{n-1})|_{p_n}$$

Для использования этого метода требуются константы вида $\left|p_i^{-1}\right|_{p_k}$. Следует заметить, что начинать вычисление a_3 можно как только появилась значение a_1. На основе этой методики построен конвейерный обратный преобразователь.

По представленным выше алгоритмам был реализован генератор VHDL описания устройства модулярного преобразователя на языке Java с произвольно задаваемыми модулями вида $2^n, 2^n \pm 1, 2^n \pm 3, 2^n \pm 5$. Были сгенерированы устройства реализующие полный цикл сложения, включающие в себя: прямой преобразователь, устройство сложения по модулю и обратный преобразователь.

Сравнительный анализ показал, что сумматор с переносом на основе стандартного подхода превосходит по производительности сумматор на модулярной арифметике на малых разрядностях.

Это объясняется тем что сумматор в устройстве на основе модулярной арифметики значительную часть времени преобразования тратит на преобразования из позиционной системы счисления в модулярную и обратно.

Схожий результат наблюдается в случае увеличения разрядности с использованием двух операндов.

Но при увеличении разрядности и при увеличении количества операндов скорости сумматоров на модулярной арифметике и сумматоров на основе традиционного подхода сравниваются. При увеличении разрядности и количества операндов у преобразователя на модулярной арифметике задержка на выходе становится меньше чем у традиционного сумматора. Это объясняется тем что преобразователь на основе традиционного подхода зависит от цепей переноса. А преобразователь на основе модулярной арифметике не требует цепей переноса, и скорость прямого, обратного преобразования и модулярного сложения становится сопоставимыми со скоростью сложения обычного сумматора. С увеличением разрядности сумматор на основе модулярной арифметики будет превосходить обычный сумматор в скорости работы. Что показывает применимость данного типа преобразователей для сложения чисел большой разрядности.

ЗАКЛЮЧЕНИЕ

Магистерская диссертация посвящена разработке устройств модулярной арифметики.

В работе были рассмотрены следующие вопросы: структура модулярного преобразователя, основные алгоритмы преобразования из позиционной системы в модулярную систему (алгоритм, основанный на китайской теореме об остатках и на позиционной системе счисления) и обратно, алгоритмы модулярного сложения и умножения.

Были проведены исследования для разрядностей 50, 100, 150, 200, 250, 300 входных операндов, для разрядности модулей вида $2^n \pm 1, 2^n \pm 3, 2^n \pm 5$.

Создано программное обеспечение, генерирующее VHDL модели устройств модулярной арифметики с использованием алгоритмов на полиадическом коде и основанных на китайской теореме об остатках.

Поскольку FPGA имеет ограниченное количество входов и выходов, максимальная разрядность входных операндов была ограничена 300 разрядами.

В результате проведенного исследования было выяснено, что использование устройств модулярной арифметики на больших разрядностей, начиная с 100 разрядности и 8 операндов, дает преимущество в скорости работы от 5 до 10 процентов, по сравнению с устройствами на основе алгоритма сложения с переносом. Но на разрядностях ниже 100 и при использовании менее 8 операндов применение алгоритма сложения с переносом предпочтительно.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А.] Неверович Д.В. Аппаратное преобразование модулярного кода в позиционный / О.М. Демиденко, Р.В. Борович, С.П. Жогаль // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: Материалы XIX Республиканской научной конференции студентов и аспирантов – Гомель, 2016 – С.54 253 с.