УДК 004.272.2

Методы построения прямых преобразователей модулярной логарифметики ориентированных на ЦОС

В.М. Амербаев, Д.В. Тельпухов, Е.С. Балака, А.В. Константинов

Учреждение Российской академии наук Институт проблем проектирования в микроэлектронике РАН, Nofrost@inbox.ru

***Аннотация* — Дается определение нового аппарата модулярной логарифметики. Изучается актуальная проблема реализации одной из основных немодульных операций – перевода чисел из традиционной системы счисления в LG-код модулярной логарифметики. Описан высокоэффективный метод поточного преобразования из двоичного представления в LG – код, ориентированный на задачи цифровой обработки сигналов (ЦОС).**

***Ключевые слова* — модулярная логарифметика, LG – код, прямой преобразователь, цифровая обработка сигналов, систолическая структура.**

I. Введение

Задачи относящиеся к цифровой обработке сигналов требуют высоких скоростей передачи данных и тактовых частот, быстрых арифметических модулей и параллельной обработки. Постоянно повышающиеся требования к быстродействию и надежности вычислительных средств побуждают к исследованию и разработке параллельных вычислительных структур. Обладая максимальным уровнем внутреннего параллелизма, особое место среди таких структур занимает модулярная арифметика [1]. Аппарат модулярной логарифметики, в данном контексте, имеет неоспоримые преимущества перед традиционной двоичной арифметикой, однако накладные расходы на немодульные операции могут существенно понизить её эффективность.

Под модулярными логарифметическими устройствами в кольце вычетов по составному модулю N подразумевается устройства, реализующие все арифметические операции над элементами кольца вычетов, посредством дискретного логарифмирования.

Реализация устройств модулярной логарифметики основана на математических свойствах полей Галуа. Одним из наиболее важных свойств таких полей является то, что любой ненулевой элемент поля может быть выражен через некоторое число, называемое первообразным или примитивным корнем.

Индексное представление модулярного числа основывается на понятии первообразного корня по простому модулю m. Первообразным корнем g называется целое число, возведение которого в степени, принадлежащие набору степеней $\{i_n\} = \{0,1,2,\dots,m-2\}$, дает неповторяющиеся вычеты по модулю m. Преобразование строится по следующей формуле:

$q_n = \left|g^{i_n}\right|_m$ где g – первообразный корень числа m.

Исходя из понятия первообразного корня, отображение операции умножения двух модулярных чисел q_k и q_j по простому модулю m на операцию сложения по модулю (m-1) осуществляется по формуле:

$$\left|q_k * q_j\right| \Leftrightarrow g^{\left|i_k+i_j\right|_{m-1}}$$

Отображение по этой формуле называется изоморфизмом между мультипликативной группой $\{q_n\} = \{1,2,3,\dots,m-1\}$ с умножением по модулю m, и аддитивной группой $\{i_n\} = \{0,1,2,\dots,m-2\}$ со сложением по модулю (m-1).

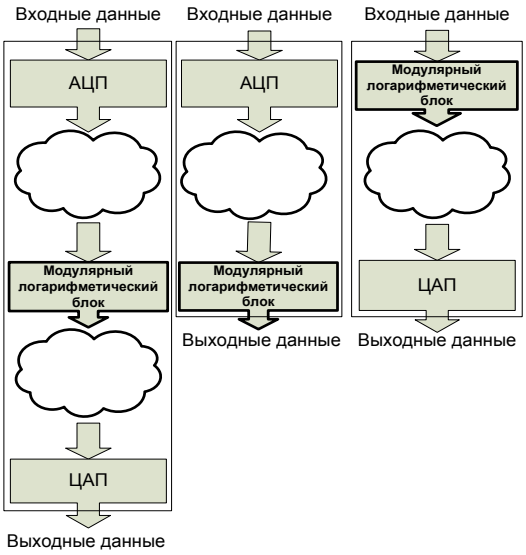
Сложение двух чисел в логарифметике выполняется по правилу:

$$|x+y|_p = \left|w^{log_w|x|_p}\left(1+w^{\left|log_w|y|_p - log_w|x|_p\right|_{p-1}}\right)\right|_p = \left|w^{log_w|x|_p + J_w\left(\left|log_w|y|_p - log_w|x|_p\right|_{p-1}\right)}\right|_p,$$

где $J_w(|u|_{p-1}) = log_w\left|1+w^{|u|_{p-1}}\right|_p$ - так называемый логарифм Якоби [2].

II. Способы построения прямых двоично-модулярных преобразователей

Приложения модулярной логарифметики ограничены кругом вычислительно сложных задач, с преобладающим числом модульных операций сложения, и в особенности умножения, и небольшим числом операций округления и сравнения по величине. В свете этого, наилучшей областью применения аппарата модулярной логарифметики представляется цифровая обработка сигналов. Планируется использовать модулярные логарифмические блоки для ускоренной реализации отдельных задач в составе устройств ЦОС. Исходя из вышесказанного, можно обозначить три возможных месторасположения разрабатываемого модулярного блока относительно аналого-цифровых и цифро-аналоговых преобразователей:



а) б) в)

Рис. 1. Возможные месторасположения разрабатываемого модулярного блока

В первом случае(а), когда модулярный логарифметический блок находится внутри тракта обработки информации, в качестве интерфейса он должен использовать преобразователи из двоичного представления в LG-код и обратно. Однако, если данный блок находится в начале тракта обработки(в), на который подается аналоговый сигнал, или же выполняет заключительную операцию перед выводом сигнала в аналоговой форме(б), то появляется возможность использовать преобразователи аналог – LG код, и LG код – аналог, соответственно. В настоящее время в ИППМ РАН ведутся разработки таких преобразователей. Они позволяют сократить накладные расходы на последовательную реализацию двух преобразователей: «аналого – двоичного» и «двоично - модулярного» путем их интеграции. В данной статье мы более подробно коснемся случаев (а) и (б), а именно – рассмотрим возможные структуры построения прямых преобразователей модулярной логарифметики и предложим несколько высокоэффективных методов, ориентированных на задачи ЦОС.

Преобразователи из двоичного представления в LG – код структурно состоят из двоично – модулярного преобразователя и преобразователя модулярного кода в LG – код. Некоторые архитектуры позволяют объединить эти стадии, тем самым обеспечивая некоторый выигрыш в производительности и аппаратных затратах. Далее рассмотрим варианты построения прямых преобразователей из двоичного представления в модулярное.

Идея построения двоично-модулярных преобразователей заключается в том, что нахождение остатка числа по определенному модулю, по существу, сводится к вычислению модулярных сумм некоторых степеней двойки. Пусть нам дано n-битное число X, и нам необходимо вычислить его остаток по модулю m:

$$X = \sum_{j=0}^{k-1} x_j 2^j$$

$$|X|_m = \left| \sum_{j=0}^{k-1} x_j 2^j \right|_m = \left| \sum_{j=0}^{k-1} \left| x_j 2^j \right|_m \right|_m \quad (1)$$

Частичные суммы $\left|x_j 2^j\right|_m$ могут вычисляться различными способами, что, в частности и предопределяет многообразие возможных архитектур прямого двоично-модулярного преобразователя. В этом аспекте выделяют: последовательные, параллельные и последовательно/параллельные преобразователи.

Самым простым и прямолинейным способом реализации формулы (1) является последовательный преобразователь, состоящий из счетчика, таблицы (реализованной памятью или логикой), сдвигового регистра и накапливающего сумматора [3]. Недостатком столь компактной в аппаратном отношении схемы, является слишком низкое быстродействие: получение остатка для каждого n-битного слова будет длиться n тактов. Несколько улучшить данную схему можно путем параллельной обработки двух и более битов входной последовательности с последующим суммированием в мультиоперандном сумматоре. Идея последующего распараллеливания процесса приводит к структуре, показанной на рис. 3.

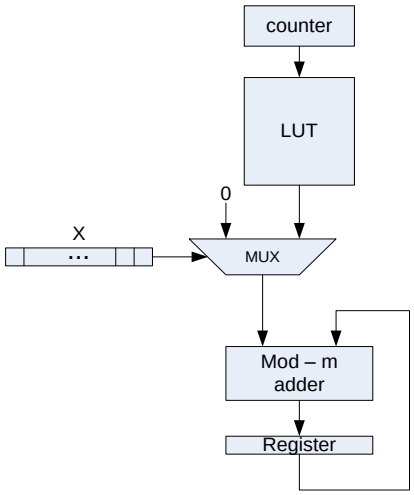


Рис. 2. Последовательный двоично-модулярный преобразователь

Разделив входную последовательность на k блоков, битностью p каждый, перепишем формулу (1), обозначая B_j – значение j-ого блока в двоичной записи.

$$|X|_m = \left| \sum_{j=0}^{k-1} \left| 2^{jp} \cdot B_j \right|_m \right|_m \quad (2)$$

Параллельная структура, в которой все возможные значения $\left|2^{jp} \cdot B_j\right|_m$ хранятся в k таблицах представ-

лена на рисунке 3. Для того, чтобы получить остаток по заданному модулю m, k значений одновременно выдаются из k таблиц, и затем поступают на входы мультиоперандного сумматора. В сравнении с предыдущей, последовательной схемой, данный подход отличается высоким быстродействием, однако очевидным его недостатком являются значительные аппаратные затраты.

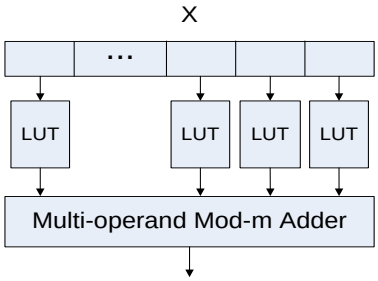


Рис. 3. Параллельный двоично-модулярный преобразователь

Выбор длинны блока B, в общем случае – произвольный. Критерии выбора длинны блока B можно условно разделить на “физические” и “логические”. Под “физическими” критериями понимаются критерии, обусловленные различными аспектами используемых технологий проектирования, в то время как “логические” – опираются на свойство периодичности конкретного модуля. Период нечетного модуля m_i - это минимальное расстояние между двумя возникновениями значения единицы в последовательности степеней двойки, взятых по модулю m_i. Формально, это определение можно записать следующим образом:

$$p(m_i) = min\,\{j | j > 0\; u\; |2^j|_{m_i} = 1\}$$

Таким образом, для того чтобы произвести прямое преобразование, необходимо разбить число на блоки, длинной равной периоду повторения, сложить их, а затем реализовать табличное преобразование. Из рисунков ясно видно, что использование “логического” разбиения, позволяет значительно сократить аппаратные затраты, однако временные характеристики останутся неизменными, так как критический путь для обоих случаев будет состоять из $log_2 n$ – сумматоров и одной таблицы.

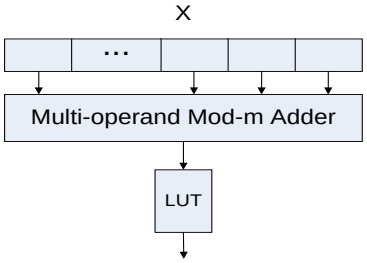


Рис. 4. Модифицированный параллельный двоично-модулярный преобразователь

III. Прямой преобразователь систолической структуры

Удачным решением, сочетающим в себе компактность, присущую последовательным схемам, и быстродействие, сравнимое с быстродействием параллельных структур – является прямой преобразователь систолической структуры [5]. Ячейка систолической структуры изображена на рисунке.

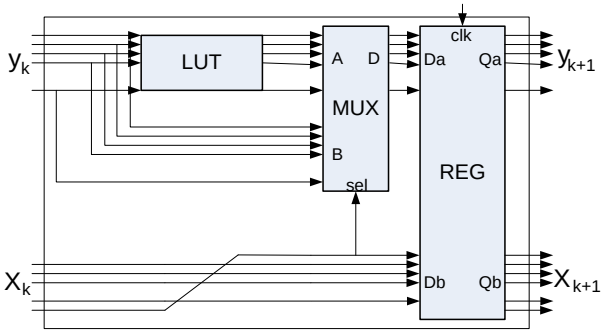


Рис. 4. Ячейка систолического двоично-модулярного преобразователя

Отдельная ячейка состоит из таблицы, мультиплексора и двух регистров, для обеспечения конвейеризации. Взаимосвязь входных и выходных операндов происходит по следующим соотношениям:

$$Y_{k+1} = \left|Y_k + a \cdot X_k^{[0]}\right|_m$$

$$X_{k+1} = ror(X_k)$$

Обозначим разрядность модуля m, по которому ведутся вычисления как $t = \lfloor log_2(m) \rfloor + 1$. Тогда данные с предыдущей стадии, поступающие на вход ячейки по шине Y, имеют битность t. В таблице, в соответствие этим данным ставится значение $|Y_k + 2^k|_m$, где k – порядковый номер систолической ячейки. После этого, по управляющему сигналу $X_k^{[0]}$ мультиплексор выбирает либо значение $|Y_k + 2^k|_m$, вышедшее из таблицы, либо поступившее изначально $|Y_k|_m$. Далее выход мультиплексора, а также циклически сдвинутое значение X_k, поступают на вход регистра, чтобы на следующем такте отправиться на следующую стадию конвейера. Таким образом, для реализации 24-х битного прямого преобразователя потребуется 24 стадии конвейера.

Однако, существует возможность сократить число ячеек систолической структуры, и тем самым добиться выигрыша в производительности и аппаратных затратах. Это становится возможным после модификации первой систолической ячейки. На вход Y модифицированной ячейки подается t бит входного числа, а на вход X – оставшиеся биты. Из нее исключены мультиплексор и сдвиг X, а функция таблицы перепрограммирована на $Y_{k+1} = |Y_k|_m$. Таким образом, первые t стадий модулярного логарифметического преобразователя заменяются на одну упрощенную стадию, а количество регистров, хранящих значение X также уменьшится на t для каждой стадии. Итого мы

имеем $n \cdot (n - t + 1)$ против $n \cdot (n + t)$ регистров для n-битных входных слов. Также с помощью незначительных модификаций, не приводящих к ухудшению производительности, последняя стадия конвейера реализует перевод числа из модулярного представления в LG – код.

IV. Оценки быстродействия и аппаратных затрат

На языке Perl был создан автоматизированный генератор функциональных представлений для создания высокоуровневого VHDL описания систолического прямого преобразователя из двоичного представления в LG код при заданных параметрах модуля и входной разрядности. При задании модуля и разрядности входных слов программа автоматически генерирует 7 файлов компонент в формате VHDL для дальнейшей загрузки в систему автоматизированного проектирования. Были проведены оценки быстродействия и аппаратных затрат для некоторых технологичных[4] модулей 3-8 бит для входных данных разрядности 16 и 24 бита. Все оценки были получены в САПР Synopsys Synplify Pro для ПЛИС фирмы Altera семейства Stratix II, при одинаковых настройках синтезатора.

Результаты проведенного экспериментального исследования показывают, что быстродействие схемы не существенно зависит от длинны конвейера или, что эквивалентно, от разрядности входных данных. Максимальная тактовая частота скачкообразно падает при переходе к модулям большей разрядности, так как увеличивается критический путь за счет усложнения таблиц, в то время как аппаратные затраты изменяются нелинейно. Данное экспериментальное исследование было направлено лишь на обоснование эффективности предложенного метода, однако для решения вопросов связанных с выбором модулей, наиболее подходящих для модулярного логарифметического устройства, требуется провести более полные исследования с большей выборкой.

Таблица 1

Временные и аппаратные оценки

модуль	16 битный вход		24 битный вход		
	частота (MHz)	ALUT/REG			
5	770.1	49/218	5	744.8	112/185
13	978.8	59/204	13	658.6	121/232
29	663.1	73/190	29	658.6	145/250
67	473.9	150/161	67	485.9	275/338
107	434.6	194/163	107	458.9	321/338
139	274.9	164/139	139	282.9	307/365
191	290.4	138/139	191	274.4	243/365
223	260.7	164/136	223	272.6	293/365
251	263.9	75/117	251	245.2	139/391

V. Заключение

В статье были рассмотрены различные способы построения прямых модулярных логарифметических преобразователей, а также предложена высокоэффективная конвейерная структура ориентированная на задачи ЦОС. Был создан автоматизированный генератор функциональных представлений для создания высокоуровневого VHDL описания систолического прямого преобразователя из двоичного представления в LG код. Проведенные исследования полученных моделей показали высокую эффективность предложенного метода. Дальнейшие исследования будут направлены на обобщение данной структуры на обратные преобразователи и другие немодульные операции.

VI. Литература

[1] Виноградов И.М. Основы теории чисел. – Изд. 6-е. – М.: Наука, 1972. – 167 с.

[2] Амербаев В.М., Малашевич Д.Б. Анализ эффективности реализации модульных операций индексной модулярной арифметики // Электроника. Известия вузов. - 2009. (в печати)

[3] Amos Omondi, Premkumar Benjamin. Residue Number Systems: Theory and Impemetation // Imperial Colledge Press, 2007.

[4] В.М. Амербаев, Д.В. Тельпухов, А.В. Константинов Бивалентный дефект модулярных кодов. Выбор технологических модулей, понижающих бивалентный дефект // Проблемы разработки перспективных микро- и наноэлектронных систем – 2008. Сб. научных трудов / под общ. ред. А.Л. Стемпковского. – М.: ИППМ РАН, 2008. – С. 462–465.

[5] Birreck, D., Drolshagen A., Anheier W., Laur R. Implementation of a Binary-to-RNS-Converter // Proc.o.t.Eurochip Workshop o. VLSI Design Training. – 1994. - P. 284 – 289.

[6] M. G. Arnold, Method and Apparatus for Fast Logarithmic Addition and Subtraction, U. S. Patent 5337266, Aug. 9, 1994.

[7] A.P. Preethy, D. Radhakrishnan, RNS-based logarithmic adder // IEE Proc. Computer and Digital Techniques. 2000. V. 147. no. 4. P. 283-287.