Саак Андрей Эрнестович – Южный федеральный университет; e-mail: saak@tgn.sfedu.ru; 347928, ГСП-17А, г. Таганрог, пер. Некрасовский, 44; тел., факс: 88634393373; кафедра государственного и муниципального управления; зав. кафедрой.

Saak Andrey Ernestovich – Southern Federal University; e-mail: saak@tgn.sfedu.ru; 44, Nekrasovskiy, Taganrog, GSP-17A, 347928, Russia; phone, fax: +78634393373; the department of state and municipal administration; head of department.

УДК 004.272.2

В.М. Амербаев, Р.А. Соловьев, Д.В. Тельпухов, А.Н. Щелоков

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МОДУЛЯРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР ПРИ ПРОЕКТИРОВАНИИ АППАРАТНЫХ ОДНОТАКТНЫХ УМНОЖИТЕЛЕЙ

Были рассмотрены методы построения модулярных вычислительных структур на базе специальных систем оснований. Сравнение эффективности рассматриваемых подходов производилось при проектировании многоразрядного однотактного умножителя, как типичной задачи для области цифровой обработки сигналов, которая является приоритетной областью приложения модулярных вычислительных структур. Были рассмотрены особенности построения модульных и немодульных узлов, а также принципов обнаружения ошибок для модулярных вычислительных структур. Базисом для рассматриваемых модулярных систем служат специальные наборы оснований на базе традиционного трехмодульного набора $\{2^n-1,\ 2^n,\ 2^n+1\}$*, а также перспективного четырехмодульного набора оснований* $\{2^k-1,\ 2^k+1,\ 2^{k+1}-1,\ 2^{k+1}+1\}$*. Был разработан IP генератор функциональных Verilog описаний умножителей для рассматриваемых подходов, включая традиционную двоичную реализацию. С помощью современного САПР Synopsys Design Compiler в базисе библиотеки стандартных ячеек 45нм. были получены оценки аппаратных и временных затрат в диапазоне разрядностей входных данных от 3 до 64 бит.*

Модулярные вычислительные структуры; модулярные умножители; специальные системы оснований; модульные операции; немодульные операции; система остаточных классов.

V.M. Amerbaev, R.A. Solovyev, D.V. Telpukhov, A.N. Schelokov

A SURVEY ON EFFICIENCY OF MODULAR COMPUTING STRUCTURES FOR SINGLE-CYCLE HARDWARE MULTIPLIER DESIGN

Methods for constructing modular computing structures based on special moduli sets are presented in this paper. Efficiency comparison of the proposed computational structures was carried out on single-cycle multipliers design, as a typical task for digital signal processing, that is a prior field for residue number systems application. Implementation features of modular and non-modular units, as well as error detection principles for modular structures were considered. Traditional three moduli set $\{2^n-1,\ 2^n,\ 2^n+1\}$ *and perspective four moduli set* $\{2^k-1,\ 2^k+1,\ 2k+1-1,\ 2k+1+1$ *serve as a basis for considered residue number system structures. IP core generator for functional Verilog descriptions for the multipliers based on these approaches, including traditional binary implementation was designed. With the help of modern CAD Synopsys Design Compiler in the standard cell library basis of 45nm. hardware and time costs estimates were obtained in the range of 3 to 64 input data bits.*

Modular computing structures; modular multipliers; special moduli sets; modular operations; non-modular operations; residue number system.

Введение. На протяжении тридцати лет в отечественной и зарубежной литературе активно ведется обсуждение эффективности модулярных вычислительных структур в современной микроэлектронике, а особенно в области цифровой обработки сигналов [1]. Цифровая обработка сигналов характеризуется большим количеством арифметических операций над массивами данных и предъявляет повышенные требования к энергопотреблению, надежности и производительности. Особенности ЦОС позволяют воспользоваться основными преимуществами модулярных структур: параллельной обработкой в каналах малой разрядности, отсутствием переносов между разрядами, возможностью контроля и самокоррекции в процессе выполнения арифметических операций.

В многочисленных статьях предлагаются различные модулярные схемы, исполненные в разных специальных базисах, показаны их свойства и преимущества перед другими схемами, однако вопросы эффективности в сравнении с двоичными структурами в широком диапазоне изменения параметров зачастую остаются без должного внимания. Таким образом, встает вопрос об объективной оценке эффективности модулярных вычислительных структур в сравнении с двоичными аналогами на современных средствах САПР. В качестве задачи для сравнения была выбрана задача однотактного умножения, как наиболее критичная для задач ЦОС.

Операция умножения чрезвычайно важна в микроэлектронике. Каждый современный микропроцессор имеет эту операцию в составе своего набора команд, но зачастую этого бывает недостаточно. В широком классе различных приложений требуется ускоренное выполнение операции умножения за один такт. Хорошо известно, что в области цифровой обработки сигналов, производительность сигнальных процессоров определяется задержкой на блоках «умножения с накоплением», центральным звеном которых являются рассматриваемые в статье устройства. В этих случаях операцию однотактного умножения и даже блоки «умножения с накоплением» выносят за пределы ядра и реализуют аппаратно, обеспечивая требуемый уровень быстродействия. Использование модулярных принципов, в этом контексте, может способствовать улучшению характеристик этих аппаратных блоков.

Все модулярные вычислительные структуры имеют схожую архитектуру (рис. 1). Различный выбор оснований позволяет строить более эффективные преобразователи, либо упрощает выполнение тех или иных арифметических операций внутри каналов, но, как правило, никак не влияет на архитектуру модулярного устройства.

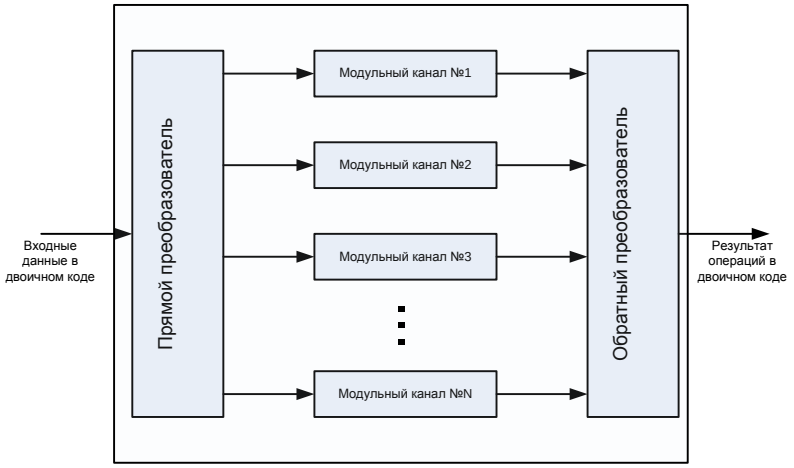


Рис. 1. Структурная схема модулярного блока

Считается, что задержка прямых и обратных преобразователей при масштабировании модулярной системы растет незначительно [2, 3], а задержка модульных каналов определяется наибольшим модулем. Тогда, задержку модулярного устройства можно оценить так:

$$\Delta = \Delta_{\text{fwd}} + \Delta_{\text{rws}} + \Delta_{\text{ch}}, \quad (1)$$

где Δ – общая задержка модулярного устройства, Δ_{fwd} – задержка прямого преобразователя, Δ_{rws} – задержка обратного преобразователя, Δ_{ch} – задержка старшего модульного канала.

Таким образом, если упрощенно считать задержку на преобразователи константой, не зависящей от количества оснований, то можно сделать вывод, что на небольших диапазонах превзойти в быстродействии двоичные схемы не удастся. Преобразователи в модулярных структурах – являются сложными устройствами с точки зрения аппаратной реализации. Действительно, для малобитных умножителей и сумматоров эффективнее использовать традиционные схемы, так как в модулярном исполнении преобразователи нивелируют все преимущества модулярных структур. Однако при увеличении размерности входных данных умножителя, а в общем случае, при усложнении схемы – модулярные структуры будут сокращать отставание за счет того, что задержки на преобразователях растут медленно, а все вычисления производятся по параллельным каналам. Тогда, начиная с какого-то момента, производительность модулярных схем превысит производительность двоичных. От того, когда этот момент произойдет – зависит целесообразность практического использования модулярной арифметики в микроэлектронных узлах. Но определить это можно только на практике, проведя широкую серию экспериментов, последовательно наращивая размерность входных данных.

Для исследования этого вопроса были выбраны модулярные схемы со специальными наборами оснований. Давно известный трехмодульный набор $\{2^t - 1,\ 2^t,$ $2t+1\}$, а также современный набор из четырех не попарно взаимнопростых оснований $\{2^t - 1,\ 2^t + 1,\ 2^{t+1} - 1,\ 2^{t+1} + 1\}$ [4]. В качестве эталонного двоичного умножителя был использован умножитель, автоматически генерируемый из высокоуровневого описания, системой автоматизированного проектирования Design Compiler фирмы Synopsys.

Описание используемых модулярных структур. Трехмодульная модулярная система вида $\{2^k - 1,\ 2^k,\ 2^k + 1\}$ является наиболее изученной с точки зрения аспектов реализации на двоичной элементной базе. Пользуясь близостью к степени двойки, удается эффективно реализовывать модульные арифметические операции, а также прямые и обратные преобразователи. Прямые и обратные преобразователи для таких модулярных структур хорошо изучены и описаны в литературе [5].

Куда больший интерес представляет современная перспективная система из четырех модулей $\{2^k - 1,\ 2^k + 1,\ 2^{k+1} - 1,\ 2^{k+1} + 1\}$. Эта система не является попарно взаимно простой, что несколько сокращает её динамический диапазон, что с другой стороны открывает некоторые возможности, связанные с корректирующими свойствами.

Динамический диапазон этой системы характеризуется следующим параметром:

$$\text{M} = \text{НОК}\left(2^{\text{k}} - 1, 2^{\text{k}} + 1, 2^{\text{k+1}} - 1,\ 2^{\text{k+1}} + 1\right),$$

где НОК – наименьшее общее кратное.

Что бы найти M, требуется определить наибольший общий делитель (НОД) для всех четырех модулей. Так как $2^{\text{k}} - 1$ и $2^{\text{k}} + 1$, а также $2^{\text{k+1}} - 1$ и $2^{\text{k+1}} + 1$ взаимнопросты, то необходимо найти наибольший общий делитель их попарного произведения. Не трудно показать, что:

$$\text{НОД}(2^{2k} - 1, 2^{2k+2} - 1) = 3.$$

Таким образом, количество всех чисел, представимых в этой системе ограничивается параметром:

$$M = \frac{(2^{2k}-1)\cdot(2^{2k+2}-1)}{3}.$$

Прямые преобразователи, равно как и умножители по основаниям $2^k - 1$ и $2^k + 1$, полностью повторяют аналогичные устройства в трехмодульном наборе, описанном ранее. Интерес представляет операция восстановления числа из представления в остатках.

Обратный преобразователь для рассматриваемого набора строится на базе так называемой китайской теоремы об остатках третьей версии (CRT III). При детальном рассмотрении, то что в [6] называется CRT III, по сути является ни чем иным, как обратным преобразователем на основе преобразования в полиадический код, в несколько видоизмененном виде. За основу взята стратегия «разделяй и властвуй», которая подразумевает итеративное сведение сложной задачи к набору тривиальных задач (такая же стратегия используется, например, в БПФ). Базисом CRT III является формула восстановления числа по двум остаткам x_1 и x_2 , по основаниям p_1 и p_2:

$$\mathrm{X} = x_1 + p_1 \cdot \left|\left|p_1\right|_{p_2}^{-1} \cdot \left|x_2 - x_1\right|_{p_2}\right|_{p_2}. \quad (2)$$

Как мы можем видеть, формула описывает восстановление числа на базе перевода в полиадический код. Архитектура такого преобразователя можно изобразить следующим образом:

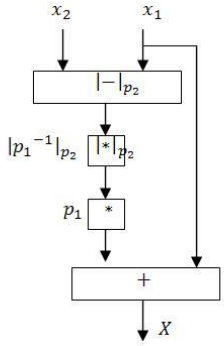


Рис. 2. Базисный элемент обратного преобразователя CRT III

В том случае, если два рассматриваемых основания не взаимнопросты и имеют общий множитель *d*, формула принимает вид:

$$X = x_1 + p_1 \cdot \left|\left|\frac{p_1}{d}\right|_{\frac{p_2}{d}}^{-1} \cdot \frac{x_2 - x_1}{d}\right|_{\frac{p_2}{d}}. \quad (3)$$

В нашем случае, для системы модулей из четырех элементов, обратный преобразователь будет состоять из двух уровней. На первом уровне считаются промежуточные значения X_1 и X_2 по формуле (2), а затем по формуле (3) будет восстановлено искомое число.

Рассмотрим теперь возможности данной системы по обнаружению ошибок. Поскольку область всех возможных комбинаций значений вычетов в рассматриваемой системе больше чем область разрешенных комбинаций, то появляется возможность с некоторой вероятностью отлавливать ошибки, возникающие в процессе вычислений или передачи данных. Если говорить точнее, то область разрешенных значений в три раза меньше области всех возможных комбинаций (за счет общего множителя), и любое искажающее воздействие, которое переводит число из разреженной области в другую, может быть обнаружено. Избыточность данной системы в контексте надежных модулярных схем очень мала, поэтому все, на что мы можем рассчитывать – это обнаружение однократной ошибки с некоторой вероятностью.

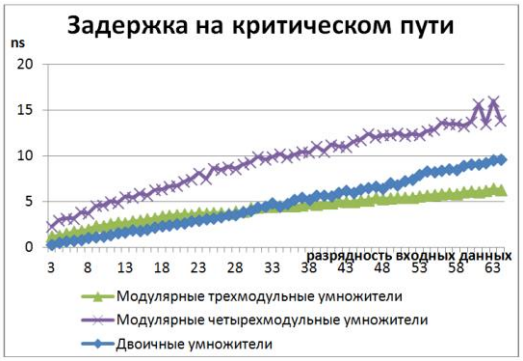
Для определения признака возникновения ошибки обратимся к формуле (3). Можно показать, что $\frac{x_2-x_1}{3}$ является целым числом только для разрешенных значений системы, в то время как запрещенные значения дают дробный результат. Таким образом, признаком возникновения ошибки может служить делимость $x_2 - x_1$ на 3.

Теперь возникает вопрос, с какой вероятностью, и в каких модульных каналах мы можем обнаружить ошибку? Определение вероятностных параметров проводилось эмпирически по методу Монте-Карло. Стоит также отметить, что общий сомножитель, тройку, имеют только два из четырех модулей, причем для четных n – $\text{НОК}(2^n - 1, 2^{n+1} + 1) = 3$, для нечетных $\text{НОК}(2^n + 1, 2^{n+1} - 1) = 3$.

Проведенные программные тесты показывают, что ошибку можно обнаружить только в тех модульных каналах, которые связаны между собой общим сомножителем. Иными словами, в тех модульных каналах, которые являются взаимнопростыми с другими каналами, любое искажение информации переводит корректное число в разрешенную область, и обнаружить наличие ошибки невозможно. Для тех двух каналов, которые имеют тройку в качестве общего сомножителя, вероятность обнаружения ошибки, не зависимо от n составила 66 %.

Стоит отметить, что под одиночной ошибкой в модулярной арифметике традиционно понимается искажение значения вычета в каком-то одном модульном канале, вплоть до инвертирования всех битов. Для микроэлектронных устройств, подверженных радиационным и иным воздействиям, имеет смысл также рассматривать ошибки, которые инвертируют отдельные биты в двоичном представлении вычетов. В этом контексте одиночная ошибка заключается в инвертировании одного бита в каком-либо модульном канале. Программные эксперименты были проведены и для данного типа ошибок. Вероятность обнаружения одиночной «битовой» ошибки в двух связанных модульных каналах оказалась равной 100 %. Это говорит о том, что инвертирование любого бита в одном из этих двух каналов, приведет к тому, что полученное число окажется в запрещенной области, и ошибка будет обнаружена. Сами по себе вопросы, связанные с корректирующими свойствами модулярных кодов по отношению к «битовым» ошибкам, представляется перспективным направлением для дальнейших исследований.

Результаты экспериментов. Синтез проводился в базисе 45 нм в библиотеке NangateOpenCellLibrary.lib с помощью САПР Synopsys Design Compiler. В качестве двоичного варианта умножителя, использовался встроенный умножитель Synopsys. Все схемы были реализованы на языке описания аппаратуры Verilog HDL. Для создания такого большого числа схем были созданы автоматизированные генераторы функциональных описаний. Онлайн версии генераторов представлены на сайте разработчиков *www.vscripts.ru* [7–9]. Результаты синтеза представлены на рис. 3.



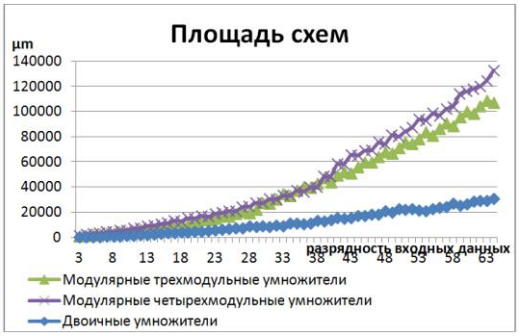


Рис. 3. Результаты синтеза однотактовых умножителей

Заключение. Как и предполагалось, модулярные схемы на малых разрядностях проигрывают двоичным аналогам. Однако, по мере роста входных разрядностей разрыв сокращается, и уже на 32 битных входах задержка модулярной схемы умножителя на наборе $(2^k - 1,\ 2^k,\ 2^k + 1)$ оказывается равной задержке двоичного умножителя. После 32 бит в случаях, когда требуется повышенное быстродействие – целесообразно использовать именно модулярный вариант умножителя. Площадь модулярных схем также оказалась предсказуемо высокой. Модулярный набор из четырех оснований проявил себя значительно хуже. Более детальный анализ результатов синтеза показал, что это обстоятельство связанно с трудностью реализации деления на 3 в составе обратного преобразователя. Эта операция отнимает до 50 % от общей производительности схемы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Soderstrand M.A. et al.* Residue Number System Arithmetic: Modern Applications in Digital Signal Processing // IEEE Press. – 1986.
2. *Тельпухов Д.В.* Построение обратных преобразователей модулярной логарифметики для устройств цифровой обработки сигналов // Информационные технологии. – 2011. – № 4. – С. 60-64.
3. *Амербаев В.М. Тельпухов Д.В.* Обратный преобразователь модулярной арифметики с использованием неточного ранга для задач ЦОС // Известия высших учебных заведений. Электроника. – 2013. – № 1. – С. 41-46.
4. *Sousa L.* Efficient Method for Magnitude Comparison in RNS Based on Two Pairs of Conjugate Moduli // Computer Arithmetic, 2007. ARITH '07. 18th IEEE Symposium. – P. 240-250.
5. *Omondi A., Premkumar A.B.* Residue Number Systems: Theory and Impemetation. – London. Imperial College Press, 2007. – 310 p.
6. *Yuke Wang.* Residue-to-Binary Converters Based On New Chinese Remainder Theorems // IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing. – March 2000. – Vol. 47, No. 3. – P. 197-205.
7. *Соловьев Р.А., Тельпухов Д.В.* Генератор Verilog для многобитных умножителей на базе модулярной арифметики [Электронный ресурс]: vscripts. 2013. URL: http://vscripts.ru/2013/high-bit-int-multiplication.php.
8. *Соловьев Р.А., Тельпухов Д.В.* Генератор Verilog для многобитных умножителей на базе модулярной арифметики [Электронный ресурс]: vscripts. 2013. URL: Генератор Verilog для бинарных умножителей на базе модулярного базиса 2^n-1, 2^n+1, 2^n+1-1, 2^{n+1}+1.
9. *Соловьев Р.А., Тельпухов Д.В.* Генератор Verilog для бинарных умножителей на базе иерархического метода [Электронный ресурс]: vscripts. 2013. URL: http://vscripts.ru/2013/high-bit-int-multiplication-hierarchical.php.

REFERENCES

1. *Soderstrand M.A. et al.* Residue Number System Arithmetic: Modern Applications in Digital Signal Processing, *IEEE Press*. 1986.
2. *Teljpukhov D.V.* Postroenie obratnykh preobrazovateley modulyarnoy logarifmetiki dlya ustroystv tsifrovoy obrabotki signalov [Building reverse converters modular logaritmiche for devices of digital processing of signals], *Informacionnye tekhnologii* [Information technology], 2011, No. 4, pp. 60-64.
3. *Amerbaev V.M. Telpukhov D.V.* Obratnyy preobrazovatel modulyarnoy arifmetiki s ispolzovaniem netochnogo ranga dlya zadach COS [Inverter modular arithmetic using inaccurate rank for tasks CSO], *Izvestiya vysshikh uchebnykh zavedeniy. Elektronika* [Izvestia of Higher Schools. Electronics], 2013, No. 1, pp. 41-46.
4. *Sousa L.* Efficient Method for Magnitude Comparison in RNS Based on Two Pairs of Conjugate Moduli, *Computer Arithmetic, 2007. ARITH '07. 18th IEEE Symposium*, pp. 240-250.
5. *Omondi A., Premkumar A.B.* Residue Number Systems: Theory and Impemetation. London. Imperial College Press, 2007, 310 p.
6. *Yuke Wang.* Residue-to-Binary Converters Based On New Chinese Remainder Theorems, *IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing*, March 2000, Vol. 47, No. 3, pp. 197-205.
7. *Solovev R.A., Telpukhov D.V.* Generator Verilog dlya mnogobitnihkh umnozhiteley na baze modulyarnoy arifmetiki [Generator Verilog for multi-bit multipliers based on modular arithmetic]: vscripts. 2013. Available at: http://vscripts.ru/2013/high-bit-int-multiplication.php.
8. *Solovev R.A., Teljpukhov D.V.* Generator Verilog dlya mnogobitnykh umnozhiteley na baze modulyarnoy arifmetiki [Generator Verilog for multi-bit multipliers based on modular arithmetic]: vscripts. 2013. Available at: Generator Verilog dlya binarnykh umnozhiteley na baze modulyarnogo bazisa 2n-1, 2n+1, 2n+1-1, 2n+1+1.
9. *Solovev R.A., Teljpukhov D.V.* Generator Verilog dlya binarnykh umnozhiteley na baze ierarkhicheskogo metoda [Generator Verilog for binary multipliers on the basis of hierarchical method]: vscripts. 2013. Available at: http://vscripts.ru/2013/high-bit-int-multiplication-hierarchical.php.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.Ф. Адамов.

Амербаев Вильжан Мавлютинович – Федеральное государственное бюджетное учреждение науки Институт проблем проектирования в микроэлектронике Российской академии наук (ИППМ РАН); e-mail: ippm@ippm.ru; 124365, Москва, Зеленоград, ул. Советская, 3; тел.: +74997299890; отдел методологии вычислительных процедур; д.т.н; г.н.с.

Соловьев Роман Александрович – e-mail: turbo@ippm.ru; отдел методологии вычислительных процедур; руководитель отдела; к.т.н.

Тельпухов Дмитрий Владимирович – e-mail: nofrost@inbox.ru; отдел методологии вычислительных процедур; н.с.; к.т.н.

Щелоков Альберт Николаевич – e-mail: schan@ippm.ru; зам. директора; к.ф.-м.н.

Amerbaev Viljan Mavlutinovich – The Institute for Design Problems in Microelectronics of the Russian Academy of Science (IPPM RAS); e-mail: ippm@ippm.ru; 3, Sovetskaya street, Zelenograd, Moscow, 124365, Russia; phone: +74997299890; the department of computing procedure methodology; chief researcher; dr. of eng. sc.

Solovyev Roman Alexandrovich – e-mail: turbo@ippm.ru; department of computing procedure methodology; head of department; cand. of eng. sc.

Telpukhov Dmitry Vladimirovich – e-mail: nofrost@inbox.ru; department of computing procedure methodology; researcher; cand. of eng. sc.

Schelokov Albert Nikolaevich – e-mail: schan@ippm.ru; deputy director; cand. of ph.-m. sc.