УДК 681. 03

КОНЦЕПЦИЯ СОЗДАНИЯ БЫСТРОДЕЙСТВУЮЩИХ И НАДЕЖНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СРЕДСТВ ОБРАБОТКИ ЦИФРОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ КОДОВ МОДУЛЯРНОЙ АРИФМЕТИКИ

А.А. СИОРА, В.А. КРАСНОБАЕВ, А.А. ЗАМУЛА, В.И. БАРСОВ, Ж.В. ДЕЙНЕКО, О.Е. БАРЫЛЬНИК

Предложен принцип создания надежных и сверхбыстродействующих систем обработки цифровой информации на основе использования кодов модулярной арифметики.

The paper suggests a principle of creating reliable and super high-speed systems of digital information processing on the basis of using modular arithmetic codes.

ВВЕДЕНИЕ

Существующие системы обработки цифровой информации (СОИ) отличаются всё более сложными задачами, которые требуют своего решения. Однако сложность решаемых СОИ задач опережает темпы нарастания мощности существующих ЭВМ. В этом аспекте, основными направлениями совершенствования вычислительных устройств обработки информации в реальном времени является повышения пользовательской производительности и безотказности функционирования, за счет обеспечения необходимого (заданного) уровня отказоустойчивости. Все множество вычислительных систем в позиционных системах счисления (ПСС), как правило, в двоичной, можно разделить на четыре основные группы: так, применение SISD-архитектуры (одиночный поток команд и одиночный поток данных) обеспечивает доминирующее положение в классической Фон-Неймановской архитектуры. В таких машинах обработка цифровой информации происходит последовательно, команды выполняются друг за другом, при этом каждая команда инициирует, как правило, одну скалярную операцию. Использование параллельной работы интерфейса ввода-вывода информации и процессора, совмещение операций, выполняемых отдельными блоками и узлами арифметико-логического устройства, не позволяют эффективно реализовать параллельные вычислительные системы реального времени. Следовательно, возможности по повышению быстродействию современных позиционных СОИ, базирующихся на классической архитектуре последовательного выполнения операторов, практически достигли своего предельного значения; вычислительные системы второй группы - MISD–архитектуры (множественный поток команд и одиночный поток данных) большой практической реализации не получили. Задачи, в которых несколько процессоров могли бы эффективно обрабатывать один поток данных, в науке и технике пока неизвестны; основу третьей группы вычислительных систем составляют устройства, разработанные на основе SIMD-архитектуре (одиночный поток команд и множественный поток данных). Применение SIMD-архитектуры позволяет реализовать высокоскоростные системы реального времени. С их помощью эффективно решаются задачи матричных исчислений, задачи решения систем алгебраических и дифференциальных управлений, задачи теории поля и пр. Среди множества задач, решаемых вычислительными системами с такой архитектурой, особое место занимают задачи цифровой обработки сигналов, которые являются наиболее оптимальными для SIMD – структуры. Данная архитектура вычислительной системы ориентирована на параллельно-конвейерное выполнение наиболее трудоемких вычислительных операций. Обеспечение предельной для данного уровня технологии производительности вычислительной системы возможно только за счет применения нетрадиционной арифметики, в которой процесс распараллеливания осуществляется на уровне арифметических операций; альтернативным решением проблемы решения задач повышенной вычислительной сложности в реальном масштабе времени является применение MIMD-архитектуры (множественный поток команд и множественный поток данных). Этот класс предполагает, что в вычислительной системе есть несколько устройств обработки команд, объединенных в единый комплекс и работающих каждый со своим потоком данных и команд. Однако, несмотря на все преимущества, отмеченные выше, такие как наличие собственной памяти у каждого процессорного элемента (ПЭ) и независимость вычислительного процесса ПЭ, системы с массовым параллелизмом породили целый ряд проблем, связанных с описанием и программированием коммутаций процессов и управления ими. В то же самое время отсутствие математической базы, позволяющей решить данные проблемы, является основным сдерживающим фактором широкого применения MIMD-систем с массовым параллелизмом. Очевидно, что дальнейшее поступательное развитие вычислительной техники напрямую связано с переходом к параллельным вычислениям. Данный переход открывает новые возможности в области совершенствования и развития вычислительных устройств. Цель статьи – показать эффективность использования кодов модулярной арифметики для повышения производительности обработки информации и отказоустойчивости функционирования средств обработки дискретной информации.

ОСНОВНАЯ ЧАСТЬ

Возможными действенными резервами повышения надежности, отказоустойчивости и живучести функционирования, а также пользовательской производительности вычислений являются использования вычислительных структур, специализированных вычислителей и спецпроцессоров, созданных на использовании принципа распараллеливания решаемой задачи (алгоритма) на всех уровнях и этапах обработки информации. Концепция параллелизма давно привлекала внимание специалистов своими потенциальными возможностями повышения производительности и надежности вычислительных систем. Проводимые теоретические, экспериментальные и промышленные разработки в этом направлении позволили обосновать основные принципы построения параллельных вычислительных систем. Именно с подобными системами связывается в настоящее время перспектива дальнейшего наращивания вычислительной мощности.

В 2005 году исполнилось 50 лет после опубликовании статьи чешского инженера М. Валаха, в которой впервые была выдвинута идея использовать для операций над компьютерными числами вместо операций кольца вычетов по модулю $M=2^n$ операции кольца вычетов по модулю $M = m_1 m_2 ... m_n$, где $m_1, m_2, ..., m_n$ – попарно взаимно-простые числа. В вычислительной практике это была выдающаяся идея, так как все кольцевые операции по модулю $M = m_1 m_2 ... m_n$ сводились к гомоморфной параллельной реализации тех же операций по малым модулям $m_1, m_2, ..., m_n$. Известная китайская теорема об остатках, которая до этого трактовалась как структурная теорема абстрактной алгебры, гарантировала указанный параллелизм в вычислениях над целыми числами, при условии, что результат кольцевых операций принадлежит диапазону целых чисел, определяемому произведением модулей $M = m_1 m_2 ... m_n$. Эта идея привлекла внимание большой группы ученых. Возникло новое научное направление – модулярная арифметика [1]. На основе использования трех основных свойств (независимость, равноправность и малоразрядность остатков, определяющих кодовую структуру) модулярная арифметика по сравнению с ПСС обладает следующими существенными преимуществами:

– возможность распараллеливания вычислений на уровне декомпозиции операндов, что существенно повышает их быстродействие;

– пространственное разнесение элементов данных с возможностью их асинхронной независимой обработки;

– возможность табличного выполнения арифметических операций базового набора и полиномиальных функций с однотактной выборкой результата модульной операции;

– возможность создания цифровых устройств с обнаружением сбоев и отказов, а также самокорректирующихся и высоконадежных цифровых устройств;

– возможность коррекции ошибок в динамике вычислительного процесса путем добавления малых (а, следовательно, и более надежных, чем в позиционных процессорах) резервных блоков, аппаратурные затраты которых пропорциональны объему соответствующих табличных вычислителей;

– обеспечение отказоустойчивости вычислительных структур на основе реконфигурации структуры вычислителя;

– обеспечение точных вычислений в целочисленной области, ограничение диапазона промежуточных результатов вычислений;

– меньшая сложность вычислительных алгоритмов для отдельных классов задач;

– обеспечение особого свойства структуры модулярного вычислителя, обеспечивающего отсутствие эффекта размножения ошибок вычислений.

Перечислим основные принципы, положенные в основу построения параллельных вычислительных систем:

– модульность создания архитектуры вычислительных систем;

– способность системы к адаптации решаемых задач (алгоритмов, операций), к самонастройке и самоорганизации;

– обеспечение необходимого уровня надежности, отказоустойчивости и живучести.

Перечислим недостатки модулярной арифметики.

Трудности выполнения известных алгоритмов немодульных операций на современной элементной базе.

Ограничение сферы эффективности МА целочисленной арифметикой.

Относительная сложность сопряжения с существующей двоичной индустрией.

Недостаточная широта классов вычислительных проблем эффективных модулярных вычислений.

Некоторая временная и аппаратурная сложность преобразования чисел из позиционной системы в МА и обратно.

Совокупность положительных и отрицательных свойств модулярной арифметики определяет следующие классы задач, в которых она существенно эффективнее позиционной арифметики: криптографические и модульные преобразования, обработка сигналов, обработка (сжатие) изображений, обработка данных большой (сотни бит) разрядности в реальном времени, матричная обработка больших массивов информации, нейрокомпьютерная обработка информации. При решении задач следующего типа применение модулярной арифметики в общем случае не целесообразно: обработка данных в формате с плавающей запятой и обработка данных с высокой долей логических и немодульных операций. Распараллеливания вычислений может осуществляться по-разному. В принципе распараллеливание может быть

осуществлено на нескольких уровнях: на уровне построения физических моделей объектов или процессов, создания математических моделей, позволяющих организовать параллельную обработку информации, на уровне метода решения, на уровне алгоритмов известных методов, на уровне программ, на уровне арифметических операций, на уровне обменов информации в вычислительных системах, ввода и вывода данных.

Одним из наиболее перспективных направлений в разработке высокоскоростных вычислительных систем является переход к распараллеливанию на уровне арифметических операций. В современных и перспективных алгоритмах, использующих аппарат линейной алгебры, основными вычислительными процедурами являются операции типа перемножения векторов и матриц, обращение матриц, поиска собственных векторов и собственных значений матриц, решение систем линейных алгебраических уравнений.

Одним из наиболее перспективных направлений решения данных проблем является переход к вычислениям в нетрадиционной арифметике с нетрадиционным представлением операндов. Из множества нетрадиционных арифметик, развитых теоретически, наибольшее применение в вычислительных системах нашли следующие: модулярная арифметика в системе остаточных классов (в классе вычетов); коды Фибоначчи; арифметика в знакологарифмической системе счисления; модулярная комплексная арифметика Гаусса (триплексные числа, кватернионы, бикватернионы и пр.); арифметика в кольце полиномов.

Существующая в последние годы в вычислительной технике тенденция к распараллеливанию вычислений связана с непрерывном ростом требований к производительности вычислительных средств. В то же самое время процессоры, составляющие значительную часть аппаратной реализации вычислительной техники, относятся к числу наименее надежных устройств, доля отказов и сбоев которых составляет более 50 процентов от общего числа отказов и сбоев аппаратуры. При этом среднее время ликвидации последствий последних, как правило, на 6-8 порядков превышает среднюю продолжительность выполнения одной задачи.

Наиболее перспективным путем разрешения данного противоречия является придание процессорам свойства устойчивости к отказам в процессе функционирования. Согласно вычислительная система является отказоустойчивой (Fault-tolerant system), если при возникновении отказа сохраняет свои функциональные возможности в полном (fail-safe) или уменьшенном (fail-soft) объеме. При этом отказоустойчивость обеспечивается сочетанием избыточности системы и наличии процедур обнаружения и устранения ошибок. Во втором издании английского толкового словаря по вычислительным системам, выпущенным издательством Oxford University Press, fail-safe устойчивость к отказам (с амортизацией отказов) характеризует способность вычислительной системы обеспечивать обслуживание, несмотря на возникновение отказа, хотя и с понижением качества, то есть находясь в состоянии постепенного снижения эффективности. Именно в таком контексте будет рассматриваться далее понятие отказоустойчивость и устойчивость к отказам.

Данное свойство обеспечивает вычислительному устройству возможность выполнения заданных действий, и после возникновения отказов за счет снижения в допустимых пределах каких-либо показателей качества функционирования. Таким образом, учет вышесказанного обуславливает актуальность исследований в сфере разработки методов повышения отказоустойчивости в процессе функционирования высокоскоростных процессоров.

Основным методом, который широко применяется при построении отказоустойчивых вычислительных устройств и систем, является резервирование. Существует большое количество различных способов резервирования, но для любого из них характерна очень высокая избыточность. Даже при коррекции одиночных ошибок чаще всего приходится увеличивать объем оборудования как минимум в три раза. Столь высокая избыточность объясняется тем, что при применении резервирования практически полностью игнорируются все специфические свойства вычислительного устройства, защищаемого от ошибок или отказов.

Качественным скачком в направлении обеспечения отказоустойчивости вычислительных устройств является широкое применение кодов, способных обнаруживать и корректировать возникающие ошибки. Характерной чертой таких кодов является наличие двух взаимозависимых частей: информационной и контрольной.

Анализ причин, по которым модулярная арифметика, имеющая явные преимущества при решении ряда важнейших вычислительных задач, не получила должного практического применения, показал следующее:

– силовое прекращение работ по созданию модулярных ЭВМ в СССР стало мощным психологическим фактором на пути развития модулярной арифметики; разработки модулярных ЭВМ были закрыты в институтах, связанных с промышленностью, в результате многие из ведущих специалистов прекратили свои работы в этой области, многие перешли в академические и учебные институты, т.е. в сферу чисто теоретических исследований;

– модулярная арифметика нетрадиционная, достаточно сложная математическая дисциплина и трудна для восприятия большинству специалистов в вычислительной технике и в микроэлектронике; в ВУЗах программа для этих специальностей соответствующая математическая подготовка, как правило, не предусмотрена; о серийно производимых и реально существующих и работающих

модулярных ЭВМ (на строго засекреченных тогда объектах) научной общественности ничего известно не было, а слух о «провале» такого проекта получил широкую огласку, в результате, во многих учебных изданиях модулярная арифметика (как и о троичной системе счисления, кодах Фибоначчи и т.п.) представляется как реально теоретически возможное экзотическое, но малоперспективное направление, отвергнутых реальной практической жизнью; в этом аспекте уже априорно программируется негативное отношение молодых специалистов к идеи разработки и практическому применению модулярной арифметике;

– с появлением микропроцессоров, БИС и СБИС высокой сложности, наряду с положительным их влиянием на вычислительную технику, превратившим ее из продукции штучного и мелкосерийного производства в продукцию массовую, имеется и негативная сторона этого явления, так, с появлением микропроцессоров многие разработчики ЭВМ были лишены возможности реализации своих новых идей и технических решений, они попали под диктат производителей микропроцессоров, были вынуждены применять фактически навязанные им стандартные микропроцессоры; в результате во всем мире количество коллективов, разрабатывающих новые ЭВМ, значительно сократилось, развитие вычислительной техники как науки резко затормозилось; за последние 30-35 лет практически ничего принципиально нового в серийно выпускаемых ЭВМ не появилось, в основном эксплуатируются идеи, рожденные в шестидесятых – семидесятых годах прошлого столетия; остатки вычислительной техники, как науки, с генерацией новых идей и решений, переместились в академические и учебные институты, в область теоретических исследований, это еще более усугубило проблемы развития модулярной арифметики, которая по иным причинам и на несколько лет раньше оказалась в подобном же положении; ситуация изменяется в настоящее время с развитием систем автоматизации проектирования на основе стандартных технологий и библиотек сложных элементов и дезинтеграции процессов создания интегральных схем с введением режимов Fables (разработка в автономных дизайн-центрах) и Foundry (производства по проектам других фирм), однако, для МА и здесь имеются определенные сложности: требуется создание специальных библиотек, хотя эта задача в научном плане не сложная, но требующая существенных организационных и финансовых затрат;

– существенным тормозом в развитии модулярной арифметики является организационная и информационная разобщенность ученых и инженеров, работающих в этом направлении; действительно, при огромном количестве публикаций по МА, они, как правило, труднодоступны, научные контакты между разрозненными группами специалистов недостаточно развиты, и доступная информация о проводимых исследованиях и результатах отсутствует, никакой координации исследований нет; все это существенно снижает эффективность проводимых работ, не позволяет в полной мере использовать имеющийся научный потенциал для достойного развития модулярной арифметики.

В настоящее время интерес к модулярной арифметике вновь существенно возрос, и это обусловлено двумя основными причинами:

– резко возросшими требованиями к вычислительным ресурсам прикладных систем в связи с бурным развитием криптографии, новых методов обработки и передачи сигналов и изображений, и т.п.;

– развитием современных программируемых логических интегральных схем, а также достижениями систем проектирования в микроэлектронике, предоставившими инженеру-системотехнику возможность реализовать свои технические решения в виде заказной интегральной схемы в режиме Fables и т.п.

За прошедшие 50 лет в развитии модулярной арифметики достигнуты значительные результаты. На первом этапе наибольшие успехи в становлении и применении МА были достигнуты в СССР под руководством И.Я. Акушского и Д.И. Юдицкого. Возглавляемым ими коллективом ученых и инженеров были разработаны и построены ряд модулярных ЭВМ, по производительности, надежности и экономичности превосходивших всех своих отечественных и зарубежных современников. ЭВМ К-340А выпускались в серийном производстве, они до сих пор (около 40 лет) работают на объектах военного назначения, демонстрируя свою высокую надежность. Однако по причинам, не имеющим ничего общего с научными, техническими или экономическими соображениями, в первой половине семидесятых годов работы по созданию модулярных ЭВМ с СССР в административном порядке были прекращены. Сам факт прекращения работ, при полном отсутствии информации об его истинных причинах, сыграл очень негативную роль в развитии модулярной арифметики в стране. Центры дальнейших работ по модулярной арифметике переместились из промышленных институтов, имеющих свои производства и работающих по заказам для обеспечения вычислительной техникой мощных радиоэлектронных систем, переместились в академические и учебные институты, в сферу чисто теоретических исследований. Дальнейшие попытки создания реальных вычислительных устройств на основе МА подавлялись чиновниками, имевшими некоторую информацию о прекращении работ над модулярными ЭВМ и, не зная истинных причин, делавшими из этого искаженные выводы о бесперспективности модулярной арифметики. Однако усилиями множества ученых-энтузиастов модулярная арифметика продолжала развиваться. Были решены основные теоретические вопросы модулярной арифметики, разработан ее математический аппарат. Получен ряд интересных результатов не только в теорети-

ческом плане, но и в практическом использовании модулярной арифметики. Наблюдается рост интереса к применению МА в смежных областях науки и техники, требующих наряду с быстрой обработкой информации увеличения ее достоверности [1-3].

Теоретические исследования в ряде стран перешли в разряд проблемно-ориентированных: надежные и сверхпроизводительные арифметические расширители, нейрокомпьютеры в МА, бортовые системы обработки информации, оптические устройства памяти и обработки, оптоэлектронные матричные процессоры, арифметические ускорители для ПЭВМ, процессоры быстрой обработки криптографической информации, разрядно-аналоговые моделирующие ЭВМ, СОИ, спецпроцессоры реализации задач БПФ и ДПФ и пр.

ВЫВОДЫ

Существует целый ряд классов (типов) задач, важнейших для современного уровня развития науки, промышленности, экономики и систем безопасности, которые на основе использования модулярной арифметики могут быть решены значительно эффективнее, чем на традиционных позиционно-двоичных СОИ. Вместе с тем необходимо отметить также, что модулярная арифметика развивается, разрабатываются новые методы и алгоритмы выполнения операций, что неуклонно расширяет сферу ее эффективности.

Литература.

[1] Труды Юбилейной Международной научно-технической конференции «50 лет модулярной арифметике», Россия, Москва, Зеленоград, 23-25 ноября 2005, издательство МИЭТ. – 520 с.

[2] *Барсов В.И., Краснобаев В.А., Зефирова О.В., Замула А.А.* Метод повышения производительности и отказоустойчивости нейрокомпьютеров обработки криптографической информации автоматизированных систем управления специального назначения на основе модулярной арифметики // Прикладная радиоэлектроника. Научно-технический журнал. – Том 6. 2007. № 2. – С. 282-287.

[3] *В.А. Краснобаев, В.И. Барсов, Е.В. Яськова.* Отказоустойчивые вычислительные системы на основе модулярной арифметики: концепции, методы и средства // Радіоелектронні і комп'ютерні системи. – 2007. – № 8 (27). – С. 82-90.

Поступила в редколлегию 16.09.2008

Сиора Александр Андреевич – председатель правления ЗАО «Научно-производственное предприятие» «РАДИЙ», кандидат технических наук. Область научных интересов: создание систем обработки информации и управления объектами критического применения.

Краснобаев Виктор Анатолиевич, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенко, доктор технических наук, профессор, Заслуженный изобретатель Украины, Почётный радист СССР. Область научных интересов: теоретическое обоснование и практическое создание сверхбыстродействующих и высокоотказоустойчивых вычислительных структур в модулярной арифметике.

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, кандидат технических наук, доцент. Область научных интересов: технологии защиты информации в информационно-телекоммуникационных системах.

Дейнеко Жанна Валентиновна, старший преподаватель факультета последипломного образования ХНУРЭ, соискатель кафедры информатики ХНУРЭ. Область научных интересов: математическое моделирование, изучение систем нелинейной динамики, построение фазовых портретов нелинейных систем, проектирование многозначной логики.

Барыльник Ольга Евгеньевна, специалист кафедры БИТ ХНУРЭ. Область научных интересов: защита информации в информационно-телекоммуникационных системах