

# Принцип факторизации в проблеме проектирования модулярных процессоров

А.Л. Стемпковский, В.М. Амербаев

Институт проблем проектирования в микроэлектронике РАН (ИППМ РАН), ssapra@hotmail.ru

**Аннотация** — Рассматривается принцип факторизации аппаратных средств модулярного процессора, и на его основе изучаются новые структурные решения организации модулярного процессора, исключающие автономное присутствие в структуре арифметического устройства (АУ) процессора аппаратно громоздкого немодульного АУ.

**Ключевые слова** — модулярная арифметика, модулярный процессор.

## I. ВВЕДЕНИЕ

При проектировании вычислительных средств как универсального, так и специализированного назначения, важную роль играет принцип факторизации. Суть его состоит в разбиении объекта проектирования на классы, которые формируются из отдельных автономных блоков, объединяемых в «классы эквивалентностей» согласно тем или иным установкам генеральной идеи проекта. Эти установки могут касаться таких вопросов как:

- учет технических и технологических особенностей используемой элементной базы;
- выбор системы представления данных и методов их обработки;
- формирование спецификаций структурных решений проектируемых блоков и изделия в целом;
- ориентация на ту или иную архитектурную компоновку.

В основе установок генеральной идеи лежат, как правило, такие требования, как:

- повышение производительности;
- минимизация энергозатрат;
- однотипность, а также однородность аппаратных решений и кодовых конструкций обрабатываемых данных и команд управления.

Как известно [1], организация современных компьютеров – многоуровневая. Это высшая фаза действия принципа факторизации в проектировании и разработке организации процессора.

Различают следующие уровни:

- 1) цифровой логический уровень;
- 2) уровень микроархитектуры;
- 3) уровень архитектуры набора команд;
- 4) уровень операционной системы;
- 5) уровень ассемблера;
- 6) уровень языка прикладного программирования.

Первый уровень поддерживается базированием на той или иной системе представления данных в процессоре и, соответственно, на алгоритмах реализации арифметических и логических операций над данными, представленными кодовыми словами принятой системы кодирования. Второй уровень это аппаратное обеспечение реализации всех операций и отношений первого уровня. Третий уровень представляет собой интерпретации (микропрограммы) или непосредственное выполнение всех процедур второго уровня. Четвертый уровень складывается из частичных интерпретаций (операционная система). Пятый уровень – трансляция (ассемблер), шестой – трансляция (компилятор).

Эта факторизация подробно рассмотрена в монографии [1], при этом структура последующего уровня определяется особенностями предшествующего уровня.

В данной статье рассматривается принцип факторизации в задаче проектирования первого уровня организации модулярного процессора.

В настоящее время в разработках вычислительных средств доминирует двоичная система счисления. Это объясняется не только ее технологическими достоинствами, но и тем, что для двоично-кодowego представления чисел специфичны две существенные характеристики: во-первых, простота реализации сдвиговых операций, лежащих в основе режимов вычислений с фиксированной и плавающей точкой; во-вторых, требование однотипности и однородности аппаратных решений арифметических узлов, которые получают положительное решение уже на начальных стадиях проектирования. Действительно, аддитивная операция в кольце целых чисел реализуется однотипно и однородно по каждому разряду позиционного представления операндов с учетом аддитивного

переполнения (т.е. переносов переполнений из младших разрядов в старшие), а операция умножения реализуется посредством сдвиговых процедур, примененных к множителю и, далее, суммированием с множимым сдвинутых копий множителя. Таким образом, в рассматриваемом случае принцип факторизации применительно к арифметическим узлам генетически заложен в систему кодирования чисел. А факторизация в проблемах проектирования организации процессора поднимается на верхние уровни принятия структурных и архитектурных решений.

Что же касается проблемы проектирования модулярных процессоров, то здесь внимание разработчиков изначально концентрировалось на функциональных характеристиках цифрового логического уровня. Традиционно этот уровень разбивался на два класса:

- арифметическое устройство, реализующее все модульные операции модулярной арифметики, и поэтому называемое модульным АУ;
- арифметическое устройство, реализующее все немодульные операции, например, такие как: формирование знака операнда по его модулярному коду; формирование признака аддитивного переполнения; сравнение двух операндов по величине; операция округления; процедуры кодирования и декодирования, используемые в процессах помехоустойчивого модулярного вычисления.

Все это приводило к тому, что традиционно структура модулярного процессора «факторизовалась» по схеме: модульное АУ, немодульное АУ, запоминающее устройство и УУ – устройство управления ими.

При этом параллелизм модулярных кодов учитывался лишь в схемотехнической конструкции модульного и немодульного АУ, как автономных вычислительных блоков. Все это связано с тем, что модулярные вычисления ориентированы на повышение эффективности решения тех задач, где преобладают линейные процедуры, к примеру, процедуры матричной и векторной алгебр большой размерности, задачи спектральной обработки многомерных сигналов, включая обработку данных в различных гиперкомплексных числовых системах и т.п. Недостатком традиционного подхода к проектированию модулярных процессоров было то, что оно постулировало конструктивную необходимость включения в состав цифрового логического уровня громоздкого (с точки зрения аппаратных затрат) устройства – немодульного АУ. Громоздкость немодульного АУ в сравнении с модульным АУ оценивается в единицах аппаратных затрат на модульное АУ величиной большей, чем  $\frac{n(n-1)}{2}$  единиц затрат на одно модульное АУ [2, 3].

Заметим также, что все немодульные операции

являются существенно последовательно-параллельными, и их ускорение средствами распараллеливания к настоящему времени носит мало изученный проблемный характер. Этот факт остро ставит проблему такой разработки цифрового логического уровня модулярного процессора, где реализация немодульного АУ требовала бы материальных затрат, не превышающих затрат на модульное АУ. Решение этой задачи требует пересмотра ранее принятого в проектировании модулярных процессоров принципа факторизации. Этот пересмотр естественно базировать на богатом опыте построения параллельных вычислительных систем различной архитектуры, поскольку модулярный процессор относится к разряду параллельных процессоров.

## II. ВЫЧИСЛИТЕЛЬНЫЙ МОДУЛЬ ПО ОСНОВАНИЮ P

Учет достижений современной микроэлектроники диктует новый подход в реализации принципа факторизации модулярного процессора. Он основан на формировании минимальной автономной вычислительной единицы по каждому основанию вычислительного диапазона компьютера и конструировании модулярного процессора на их основе. Этот подход генетически присутствует в системе модулярного кодирования чисел. Действительно, на элементарном уровне доминируют кольцевые операции по всем базисным основаниям модулярной арифметики  $p_1, p_2, \dots, p_n$ , а операции кольца вычетов  $Z_{p_i} (1 \leq i \leq n)$  однотипны по своей арифметической природе.

Таким образом, принцип факторизации в части проектирования модулярного процессора складывается из двух составляющих:

а) разбиение аппаратных средств цифрового логического уровня на классы эквивалентностей, состоящие из однотипных минимальных структурных единиц, назовем их вычислительными модулями по основаниям  $p_i (1 \leq i \leq n)$  вычислительного диапазона компьютера и будем обозначать их символами  $BM(p_i)$ ;

б) синтез устройств цифрового логического уровня на базе системы вычислительных модулей  $\{BM(p_i)\} (i = 1, 2, \dots, n)$ .

Кодовая, а следовательно и аппаратная спецификация вычислительных модулей зависит от способа кодирования вычетов по каждому основанию  $p_i (1 \leq i \leq n)$  модулярной арифметики.

К настоящему времени известны следующие форматы представления вычетов кольца  $Z_p = Z_{p_1} \times Z_{p_2} \times \dots \times Z_{p_n}$ :

- традиционный (вычетный) [2];
- традиционно-индексный [2, 3, 4];

- логарифмический [5];
- бимодульный [6, 7];
- рекурсивный [8, 9].

По содержанию традиционно-индексная и логарифмическая арифметики кольца  $Z_p$  близки и поэтому будем говорить о логарифметике кольца  $Z_p$ . Эти форматы будем называть кодовыми интерпретациями элементов вычислительных модулей по основаниям  $p_i$  ( $1 \leq i \leq n$ ), а модулярную арифметику, синтезированную на базе вычислительных модулей по основаниям  $p_i$  при фиксированной кодовой интерпретации, называть, соответственно:

- традиционной модулярной арифметикой;
- модулярной логарифметикой;
- бимодульной модулярной арифметикой;
- рекурсивной модулярной арифметикой.

Если отвлечься от кодовой интерпретации элементов вычислительного модуля по основанию  $p$ , то можно говорить об абстрактном вычислительном модуле по основанию  $p$ . Таким образом, вычислительным модулем по основанию  $p$  ( $BM(p)$ )

будем называть вычислительную структуру, которая реализует за номинальную единицу времени все операции кольца вычетов  $Z_p$ .  $BM(p)$  структурно состоит из: входа и выхода; регистров ввода и вывода; сумматоров и умножителей по  $\text{mod } p$ ; ПЗУ-констант, используемых в реализации операций немодульного АУ; ОЗУ, ориентированного на участие вычислительного модуля в реализации планируемых арифметических операций вычислительного процесса, а также внутреннего УУ, организующего реализацию всех команд, поступающих на входы  $BM(p)$  из Центра Управления модулярного процессора.

Таким образом,  $BM(p)$  является полноценной вычислительной единицей кольца вычетов  $Z_p$  для произвольного основания  $p$  из системы оснований  $\{p_i\}$  модулярного процессора, а принцип факторизации в проблеме проектирования модулярных процессоров сводится к разработке наборов вычислительных модулей по базисным основаниям модулярного процессора и синтеза на их основе устройств цифрового логического уровня компьютера.

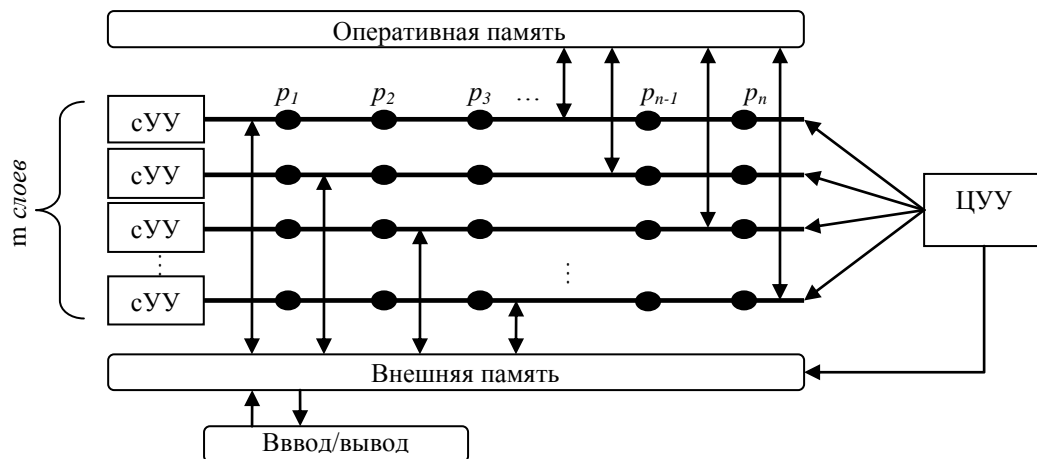


Рис. 1. Структура цифрового логического уровня организации модулярного процессора

### III. СТРУКТУРА ЦИФРОВОГО ЛОГИЧЕСКОГО УРОВНЯ МОДУЛЯРНОГО ПРОЦЕССОРА

Понятие абстрактного модуля по основанию  $p$  позволяет распространить на проблему проектирования цифрового логического уровня модулярного процессора огромный опыт наработок вычислительных систем различной сложности и различного назначения [10, 11]. Так, например, за основу построения цифрового логического уровня модулярного процессора по базисным основаниям  $p_1, p_2, \dots, p_n$  можно принять топологию решетки сети процессоров.

Возникает следующая структура цифрового логического уровня организации модулярного процессора (рис. 1).

На каждом слое сети располагаются:

- сУУ – управляющее устройство слоем; реализует на управляемом слое все немодульные операции по команде с ЦУУ;
- ЦУУ – центральное управляющее устройство сети, которое управляет:
  - параллельными модульными вычислениями каждого слоя сети;
  - осуществляет выборку из оперативной памяти по адресу слоя и обратно, реализует посылку

модулярного кода с каждого слоя в оперативную память;

- управляет работой блоков перевода чисел из позиционного кода в модулярный и засылает их во внешнюю память и обратно, управляет переводом модулярного кода из внешней памяти в позиционный код с передачей его на выход.

Программное управление модулярными вычислениями на сети осуществляется ЦУУ посредством управляющих команд через СУУ каждого слоя сети. ЦУУ имеет в своем составе оперативную память, объем которой определяется проектными условиями, и внешнюю память. ЦУУ осуществляет перевод масштабированных чисел, заданных позиционным кодом в модулярный и, наоборот, заданных модулярным кодом в позиционный. Семантика вычислений, управляемых ЦУУ, сводится к следующему – вычисления с фиксированной точкой; процедуры арифметической самокоррекции [2, 3], т.е. вычисления с обнаружением и исправлением ошибок в кодовом слове без прерывания вычислений, а также с контролем и диагностикой сбоев и отказов в вычислительных модулях при реализации на сети модульных и немодульных операций. Следует отметить, что топология многослойной решетчатой сети цифрового логического уровня организации модулярного процессора позволяет: устранить избыточные аппаратные затраты на реализацию немодульных операций; осуществлять их на любом слое параллельно модульным операциям на других слоях; использовать на каждом слое конструкции помехо-, отказо-, сбоеустойчивых вычислений не только при выполнении модульных, но и немодульных операций. Алгоритмическая часть описанных процедур прозрачна и опирается на опыт отечественных разработок в области машинной арифметики модулярных процессоров.

#### IV. ЗАКЛЮЧЕНИЕ

Проектирование модулярных процессоров на базе принципа факторизации позволяет получить новые более экономичные структурные решения организации модулярных процессоров, устраняющие аппаратную избыточность немодульного АУ.

Решетчатая структура модулярного процессора, базирующаяся на вычислительных модулях по базисным основаниям модулярного процесса, открывает новые возможности для использования системных методов повышения производительности.

#### ЛИТЕРАТУРА

- [1] Таненбаум Э., Архитектура компьютера. 5-ое изд. (+CD). СПб.: Питер, 2009. 844 с.
- [2] Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Соврадио, 1968. 440 с.
- [3] Амербаев В.М. Теоретические основы машинной арифметики. Алма-Ата: Наука КазССР, 1976. 324 с.
- [4] Патент №123995 (РФ). Вычислительный элемент модулярной арифметики; заявитель и патентообладатель ИППМ РАН. - № 2012127097; заявл. 28.06.12; опубл. 10.01.13., Бюл. № 1.
- [5] Стемпковский А.Л., Амербаев В.М., Корнилов А.И. Модулярная логарифметика – новые возможности для проектирования модулярных вычислителей и преобразователей // IV Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем – 2010». Сб. тр. / под общ. ред. академика РАН А.Л. Стемпковского. М.: ИППМ РАН, 2010. С. 368-373.
- [6] Амербаев В.М., Балака Е.С. Бимодульные вычисления над полем Галуа  $GF(p)$  // Вестник Московской государственной академии делового администрирования. Серия: Экономика. 2013. № 1 (20). С. 36-42.
- [7] Амербаев В.М., Балака Е.С. Арифметическое устройство бимодульной арифметики конечного поля  $GF(p)$  // Research Journal of International Studies XX(17). 2013. Ч. 2. P. 5-9.
- [8] Стемпковский А.Л., Амербаев В.М., Соловьев Р.А. Принципы рекурсивных модулярных вычислений // Информационные технологии. 2013. № 2. С. 22-27.
- [9] Патент №103010 (РФ). МПК G06F7/72. Устройство для вычисления по модулю; заявитель и патентообладатель ИППМ РАН. - № 2010148522; заявл. 29.11.2010; опубл. 20.03.2011., Бюл. № 8.
- [10] Тербор К.Дж. Архитектура высоко- производительных вычислительных систем / Пер. с англ. М.: Наука, главная редакция физмат. лит., 1985. 272 с.
- [11] Смирнов А.Д. Архитектура вычислительных систем. Учебное пособие для вузов. М.: Наука, главная редакция физмат. лит. 1990. 320 с.