УДК 681.140

В.И. Барсов

Украинская инженерно-педагогическая академия, Харьков

МЕТОДЫ СЖАТИЯ ТАБЛИЧНЫХ ЦИФРОВЫХ ДАННЫХ В МОДУЛЯРНОЙ АРИФМЕТИКЕ

Рассмотрены методы реализации информационного сжатия цифровых данных результатов выполнения одновременно арифметических операций сложения, вычитания и умножения в модулярной арифметике.

Ключевые слова: *цифровые данные, модулярная арифметика.*

Введение

Одним из перспективных направлений повышения пользовательской производительности, достоверности и надежности функционирования вычислительных комплексов в реальном времени, при решении сложных научно-технических задач, является внедрение нетрадиционных методов представления и обработки информации в числовых системах с параллельной структурой, и в частности, в так называемых модулярных системах счисления, обладающих максимальным уровнем внутреннего параллелизма в организации процесса переработки информации. К таким системам счисления относится и непозиционная система счисления в модулярной арифметике (МА).

Известная непозиционная система счисления в остаточных классах, как отмечается в [1, 2], обладает важным свойством независимости остатков числа друг от друга по принятой системе оснований. Этот аспект открывает перспективные направления в создании не только новой машинной модулярной арифметики, но и принципиально новой схемной реализации архитектуры вычислительных комплексов (ВК).

Основными преимуществами МА являются возможность разработки и внедрения высокоэффективных алгоритмических и аппаратных архитектур вычислительных структур параллельно-конвейерного типа. При этом обеспечивается, во-первых, высокая степень интеграции и унификации арифметических блоков и вычислительных узлов и, во-вторых, использования уникальных корректирующих свойств непозиционных кодовых структур при обнаружении и исправлении, а также при контроле ошибок в динамике вычислительного процесса, т.е. в реальном времени без останова вычислений. И, наконец, использования свойств машинной арифметики в МА позволяет организовать высокопроизводительную реализацию вычислительных процессов, требующих больших объемов вычисле-

ний. В свете изложенного необходимо дать характеристику основным свойствам МА.

1. Независимость остатков. Это свойство дает возможность строить архитектуру ВК в виде набора независимых вычислительных трактов (отдельных вычислителей, функционирующих по своему определенному модулю m_i в МА). При этом время реализации арифметических операций определяется временем реализации в вычислительном тракте ВК по наибольшему основанию m_n МА. Следовательно, ошибки, возникающие за счет отказов (сбоев) схем двоичных разрядов в произвольном вычислительном тракте ВК, не «размножаются» в соседние тракты (остаются в пределах одного остатка), что дает возможность повысить достоверность вычислений в МА.

2**.** Равноправность остатков**.** Любой остаток a_i числа $A = (a_1, a_2, \ldots, a_n)$ несет информацию обо всем исходном числе. Использование этого свойства совместно с первым свойством и идеей структурного резервирования, может позволить синтезировать надежностную модель ВК в МА, соответствующую модели динамического резервирования в позиционных системах счисления (ПСС).

3. Малоразрядность остатков**.** Это свойство позволяет существенно повысить быстродействие выполнения арифметических операций как за счет малоразрядности построения вычислительных трактов ВК, так и за счет возможности применения (в отличии от ПСС) табличной арифметики, где арифметические операции сложения, вычитания и умножения выполняются практически в один такт[4, 5].

Основные свойства МА обуславливают высокое быстродействие выполнения арифметических операций за счет возможности представления и реализации алгоритмов машинной арифметики в конвейерно-табличной (матричной) форме. Поскольку все основные достоинства МА более полно проявляются при использовании табличного принципа реализации арифметических операций, т.е. при использовании табличных (матричных) коммутаторов, реализующих модульные операции, логично предположить, что по мере совершенствования и развития технологии производства запоминающих устройств на БИС и СБИС в виде логических программируемых матриц (ПЛМ) или программируемых логических интегральных схем (ПЛИС), составляющих основу для реализации табличных методов вычислений в МА, интенсивность исследований в направлении создании табличных алгоритмов реализации модульных операций будет возрастать.

Целью статьи является разработка и дальнейшее совершенствование методов табличной арифметики в МА и, в частности, разработка универсальных табличных методов информационного сжатия цифровых данных результатов выполнения одновременно арифметических операций сложения, вычитания и умножения в модулярной арифметики на основе использования кода табличного умножения (КТУ).

Анализ последних исследований. Операционное устройство (ОУ) ВК в МА принципиально может быть выполнено следующим образом: в сумматорном варианте (на базе малоразрядных двоичных сумматоров) [1]; при использовании кольцевых регистров сдвига (КРС) [5]; используя прямой логический метод [4] и в табличном (матричном) варианте [5].

При построении ОУ на основе использования первых двух вариантов каждый остаток числа в МА, представленный двоичным кодом, обрабатывается независимо от других, и время выполнения всей операции определяется временем, необходимым для получения результата по наибольшему основанию.

Отметим основные недостатки этих двух вариантов выполнения арифметических операций:

– некоторая сложность синтеза двоичных сумматоров и КРС;

– значительное время преобразования информации, определяемое величиной максимального основания МА, что существенно для ВК с большой разрядной сеткой;

– сложность технической реализации операции умножения;

– не эффективное использование двоичных элементов разрядной сетки ВК, вследствие возможной избыточности представления максимальных чисел.

Эффективным методом повышения надежности и производительности ВК является использование при реализации арифметических операций матричных схем на основе использования постоянных запоминающих устройств (ПЗУ), ПЛМ, а также ПЛИС. Малая потребляемая мощность, повышенные надежностные характеристики и компактность матричных схем открывают широкие перспективы использования их в качестве основных составляющих структуры ОУ ВК.

Из проведенных исследований [1, 2, 5] очевидно, что вопросы, связанные с выполнением арифметических операций табличными методами (посредством ПЗУ), целесообразно рассматривать лишь в применении к ВК в МА.

Отметим достоинства матричного (табличного) варианта построения ВК в МА:

– матричные схемы имеют высокую конструктивную надежность, так как реализуются в виде компактных ПЗУ; в этом случае ВК строится по блочному принципу, что улучшает ремонтопригодность ВК (в частности, уменьшается среднее время восстановления);

– простота построения матричных схем и дешифраторов, имеющих количество выходов равное величине основания МА;

– высокое быстродействие: результат операции может быть получен в момент поступления входных операндов, т.е. в один такт; таким образом, время выполнения арифметических операций в МА сравнимо с тактовой частотой вычислителя, что принципиально невозможно для позиционного ВК.

Поиск путей повышения производительности и надежности ВК, за счет упрощения его структуры, привел к необходимости разработки табличных методов и алгоритмов реализации модульных операций, позволяющих повысить эффективность применения табличной арифметики.

В [1] показано, что при применении методов специального кодирования информации в МА (целью которых является сокращение элементов таблиц ПЗУ, реализующих результаты выполнения арифметических операций) позволяет добиться того, что количество оборудования ОУ при табличном построении может быть не больше количества оборудования необходимого при сумматорном принципе построения ОУ ВК в МА.

Под табличной реализацией арифметических операций $c_i = f(a_i, \beta_i)$ понимается организация такой таблицы, в которой каждой комбинации входных величин a_i и β_i соответствует одно и только одно значение выходной величины c_i.

Изложение основного материала

Вначале рассмотрим известный табличный метод реализации операции модульного умножения. с использованием КТУ. Составим таблицу $a_i\beta_i \pmod{m_i}$ модульного умножения для произвольного основания m_i МА. Эта таблица симметрична относительно левой (главной) и правой диагоналей, а также вертикали и горизонтали. Симметричность относительно левой диагонали определяется коммутативностью операции $a_i\beta_i$ умножения, а симметричность относительно правой диагонали определяется тем, что

$$(m_i - a_i)(m_i - \beta_i) \equiv a_i\beta_i (\mathrm{mod}\ m_i).$$

Симметричность относительно вертикали и горизонтали определяется из условия кратности значения модуля сумме симметричных чисел таблицы умножения:

$$a_i\beta_i + a_i(mi - \beta_i) \equiv 0 (\mathrm{mod}\ m_i);$$
$$a_i\beta_i + \beta_i (m_i - a_i) \equiv 0 (\mathrm{mod}\ m_i).$$

Исходя из вышеизложенного очевидно, что для табличной реализации операции модульного умножения $a_i\beta_i \pmod{m_i}$ достаточно иметь числовую информацию только о ее восьмой части. Отсюда возникает возможность упростить таблицу (количество схем совпадения И матричного ПЗУ) модульного умножения (отметим, что уменьшение таблицы в восемь раз приводит к необходимости производить предварительный анализ величин входных операндов a_i и β_i.) Использование этого варианта увеличивает время и техническую сложность реализации данной арифметической операции.

Для наиболее эффективной реализации операции $a_i\beta_i \pmod{m_i}$ применяются методы специального кодирования, позволяющие в четыре раза уменьшить таблицу модульного умножения. Решение поставленной задачи возможно в результате применения специальных кодов. Рассмотрим один из вариантов выполнения операции модульного умножения посредством использования КТУ (табл. 1 и 2 для $m_i = 5$).

Пусть даны входные операнды a_i и β_i. Значения $a_i(\beta_i)$, лежащие в диапазоне $[0, (m_i - 1)/2)$, могут быть закодированы произвольным способом, а значения $a_i(\beta_i)$, лежащие в диапазоне $[(m_i + 1)/2, m_i - 1)$, кодируется как m_i - a $(m_i - \beta_i)$. Для отличия диапазонов вводится следующий индекс (признак) КТУ:

$$\gamma_a(\gamma_\beta) = \begin{cases} 0, \text{ если } 0 \le a_i(\beta_i) \le (m_i - 1)/2; \\ 1, \text{ если } (m_i + 1)/2 \le a_i(\beta_i) \le m_i - 1. \end{cases}$$

Алгоритм определения результата операции модульного умножения посредством КТУ следующий:

если заданы два операнда в КТУ $a_i = (\gamma_a, a_i'), \beta_i = (\gamma_\beta, \beta_i')$, то для того, чтобы получить произведение этих чисел по модулю m_i, достаточно найти произведение $a_i'\beta_i' (\mathrm{mod}\ m_i)$ и инвертировать его обобщенный индекс γ_i в случае, если γ_a отлично от γ_β, т.е.

$$a_i\beta_i (\mathrm{mod}\ m_i) = (\gamma_i, a_i'\beta_i' (\mathrm{mod}\ m_i)),$$

где

$$\gamma = \begin{cases} \overline{\gamma}_i, \text{ если } \gamma_a \ne \gamma_\beta; \\ \gamma_i, \text{ если } \gamma_a = \gamma_\beta; \end{cases} \quad a_i' = \begin{cases} a_i, \text{ если } \gamma_a = 0; \\ m_i - a_i, \text{ если } \gamma_a = 1. \end{cases}$$

При использовании данного алгоритма ПЗУ, реализующее операцию модульного умножения, конструктивно уменьшаются в четыре раза. При выполнении операции табличными методами в некоторых случаях возможно дополнительное уменьшение оборудования за счет того, что строится не единая таблица для модульных операций, а k боле мелких таблиц, позволяющих дать ответы по каждому из k разрядов результата, где k – разрядность регистра, необходимая для хранения цифр остатка по рассматриваемому основанию m_i МА.

До настоящего времени вопросы эффективной реализации арифметических операций сложения и вычитания с использованием КТУ в литературе либо не рассматривались, либо такая реализация считалась исследователями невозможной. Основная

трудность заключается в том, что довольно сложно синтезировать табличные алгоритмы выполнения этих модульных операций, так как таблицы реализации модульных операций сложения и вычитания различны по своей цифровой структуре, вследствие чего они не обладают теми свойствами симметрии, которыми обладают таблицы модульного умножения. Однако совершенно иные результаты можно получить, исследуя возможности реализации одной модульной операции с помощью таблиц, реализующих обратную ей операцию, и наоборот.

При исследовании цифровых свойств таблиц модульных операций сложения и вычитания доказано следующее аналитическое соотношение

$$\left[\ (\gamma_a, a'_i)+(\gamma_\beta, \beta'_i)\ \right]+ \\ +\left\{\ \left[m_i-(\gamma_a, a'_i)\ \right]-(\gamma_\beta, \beta'_i)\ \right\}=0(\bmod m_i), \quad (1)$$

где $a_i=(\gamma_a, a'_i)$, $\beta_i=(\gamma_\beta, \beta'_i)$ – входные операнды, представленные в КТУ. Запишем выражение (1) в виде

$$(\gamma_a, a'_i)+(\gamma_\beta, \beta'_i)=m_i-\left\{\left[m_i-(\gamma_a, a'_i)\right]-(\gamma_\beta, \beta'_i)\right\}. \quad (2)$$

Из выражения (2) следует, что для получения результата операции модульного сложения в КТУ достаточно знать результат операции модульного вычитания, т.е. возникает возможность эффективно (с точки зрения уменьшения количества оборудования ПЗУ) использовать КТУ одновременно для трех модульных операций: умножения, сложения и вычитания.

На основе выражения (2) может быть разработан метод, позволяющий осуществлять выполнение любой из трех арифметических операций в МА: умножение, сложение и вычитание. В соответствии с выражением (2) составим поэтапный алгоритм реализации операции модульного сложения.

Первый этап. Уменьшаемое $a_i=(\gamma_a, a'_i)$ инвертируется по модулю m_i, т.е. получим следующее выражение: $\overline{a}_i=((\gamma_a+1)\bmod 2, a'_i)$. Вычитаемое (γ_β, β'_i) оставляем без изменений.

Второй этап**.** Посредством ПЗУ, реализующего операцию модульного вычитания, по входным операндам a'_i и β'_i определяется результат операции $(a'_i-\beta'_i)\bmod m_i$. Как и для алгоритма модульного умножения индекс γ_i результата операции модульного вычитания формируется в соответствии со значениями индексов соответствующих операндов, т.е. в соответствии со значениями $(\gamma_a + 1) \bmod 2$ и γ_β, где

$$\gamma_i=\begin{cases}\overline{\gamma}, \text{ если } (\gamma_a+1)\bmod 2\neq\gamma_\beta;\\ \gamma, \text{ если } (\gamma_a+1)\bmod 2=\gamma_\beta.\end{cases}$$

Следовательно, результат операции модульного вычитания будет иметь следующий вид:

$$(\gamma_i, (a'_i-\beta'_i)\bmod m_i).$$

Третий этап. Полученный результат модульного вычитания инвертируем по модулю m_i:

$$((\gamma_i+1)\bmod 2, (a'_i-\beta'_i)\bmod m_i),$$

где индекс КТУ результата операции равен значению

Это и будет искомый результат модульного сложения.

Последовательность выполнения полученного алгоритма схематично можно представить в упрощенном виде следующим образом:

$$(a_i-\beta_i)\to\left[(m_i-a_i)-\beta_i\right]\to \\ \to\left\{m_i-\left[(m_i-a_i)-\beta_i\right]\right\}\to(a_i+\beta_i).$$

Таким образом, несмотря на различие цифровой структуры таблиц модульных операций сложения, вычитания и умножения, нами получен новый оригинальный табличный алгоритм для реализации арифметических операций в МА. С помощью этого алгоритма можно построить конструктивно простое и высоконадежное ОУ ВК в МА, основу которого составляют три отдельных ПЗУ, каждое из которых реализует только 0,25 части соответствующей полной таблицы модульных операций умножения (табл. 2) и вычитания (табл. 4) (первое ПЗУ – II-квадрант таблицы умножения (табл. 5); второе и третье ПЗУ – соответственно I (табл. 7) и II (табл. 6) квадранты табл. 4 вычитания). В этом плане код табличного умножения приобрел новое качество и стал универсальным табличным кодом для выполнения трех арифметических операций в МА.

Рассмотрим еще один возможный вариант построения алгоритма выполнения арифметических операций в МА.

Из выражения (1) следует, что

$$(\gamma_a, a'_i)-(\gamma_\beta, \beta'_i)=\left\{(\gamma_a, a'_i)+\left[m_i-(\gamma_\beta, \beta'_i)\right]\right\}. \quad (3)$$

Из выражения (3) следует, что результат операции модульного вычитания можно получить посредством ПЗУ, реализующего операцию модульного сложения. В этом случае алгоритм будет иметь следующий вид.

Первый этап**.** В соответствии с выражением (3) второе слагаемое β'_i инвертируем по модулю m_i:

$$\overline{\beta}_i=((\gamma_\beta+1)\bmod 2, \beta'_i).$$

Второй этап. С помощью ПЗУ для модульного сложения по входным операндам a'_i и β'_i определим значение модульной суммы в виде $(a'_i+\beta'_i)\bmod m_i$.

Окончательный результат выполнения операции модульного вычитания будет иметь следующий вид:

Таблица 1

a_i	КТУ		a_i	КТУ	
	γ_a	a_i'		γ_a	a_i'
1	0	1	3	1	2
2	0	2	4	1	1

Таблица 2

β_i \ a_i	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Таблица 3

β_i \ a_i	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таблица 4

β_i \ a_i	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

Таблица 5

β_i \ a_i		1	2
		4	3
1	4	1	2
2	3	2	4

Таблица 6

β_i \ a_i		1	2
		4	3
1	4	0	1
2	3	4	0

Таблица 7

β_i \ a_i		2	1
		3	4
1	4	2	3
2	3	1	2

Таблица 8

β_i \ a_i		1	2
		4	3
1	4	2	3
2	3	3	4

Таблица 9

β_i \ a_i		2	1
		3	4
1	4	4	0
2	3	0	1

$$\left(\left(\gamma_\beta + 1\right) \bmod 2, \left(a_i' + \beta_i'\right) \bmod m_i\right),$$

где индекс КТУ результата операции равен значению

Схематично этот алгоритм может быть представлен в виде

$$\left(a_i + \beta_i\right) \rightarrow \left[a_i + \left(m_i - \beta_i\right)\right] \rightarrow \left(a_i - \beta_i\right).$$

При реализации модульных операций посредством второго алгоритма основу ОУ составляют также три табличных ПЗУ, каждое из которых реализует 0,25 части соответствующей полной таблицы модульных операций умножения (табл. 2) и сложения (табл. 3)(первое ПЗУ – II-квадрант таблицы умножения (табл. 5); второе и третье ПЗУ – соответственно I (табл. 9) и II (табл. 8) квадранты табл. 3 сложения).

При реализации арифметических операций умножения, сложения и вычитания второй предложен-

ный алгоритм позволяет за меньшее время и с меньшими аппаратными затратами (по сравнению с первым алгоритмом) выполнять в МА данные арифметические операции.

Выводы

В статье рассмотрены методы реализации информационного сжатия цифровых данных результатов выполнения одновременно трёх арифметических операций в модулярной арифметике, в основе которых лежат предложенные табличные алгоритмы. Данные алгоритмы (основанные на использовании КТУ) несмотря на различие свойств цифровых данных структур таблиц, реализующих модульные операции $(a_i \otimes \beta_i) \bmod m_i$, позволяют реализовать всего 0,25 части каждой из полных таблиц, что ранее предполагалось невозможным. При реализации модульных операций сложения и вычитания КТУ приобрел новые качества и стал общим для выполнения всех трех вышеперечисленных арифметических операций в МА.

Таким образом, при выполнении посредством предложенного метода всех трех арифметических операций можно добиться сокращения до 75% оборудования ПЗУ (например, для первого алгоритма используются табл. 5, 6 и 7; для второго алгоритма – табл. 5, 8 и 9), посредством которых реализуются данные операции, что в свою очередь, в зависимости от длины машинного слова (величины разрядной сетки), позволит сократить до ≈ (50 – 60)% оборудования табличного операционного устройства ВК в МА. Можно также предположить, что с увеличением длины разрядной сетки ВК (что характерно для современной тенденции развития вычислительных средств информационно-управляющих и информационно-расчетных систем), эффективность применения предложенного метода существенно возрастает.

Результаты проведенных исследований могут быть использованы в системах и устройствах обработки в реальном времени больших массивов цифровой информации: при решении задач цифровой фильтрации, криптографических преобразованиях в полях Галуа, при разработке криптографических систем на основе использования преобразований Хартли, а также при необходимости реализации модульных преобразований в устройствах с повышенными требованиями по быстродействию выполнения сложных расчетных задач в целочисленной модульной арифметики, например, при решении задачи по обеспечению необходимого уровня стойкости криптографических средств за счет выполнения арифметических операций над целыми числами.

Список литературы

1. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.

2. Барсов В.І. Створення відмовостійких упровляючих обчислювальних комплексів автоматизованих систем контролю і управління електроспоживанням на основі модулярної арифметики / В.І. Барсов // Вісник ХНТУСГ ім. П. Василенка. – Х., 2007. – Т. 2, вип.. 57. – С. 77-82.

3. Метод повышения производительности и отказоустойчивости нейрокомпьютеров обработки криптографической информации автоматизированных систем управления специального назначения на основе модулярной арифметики / В.И. Барсов, В.А. Краснобаев, А.А. Замула, О.В. Зефірова // Прикладная радиоэлектроника: научно-технический журнал. – Х.: ХНУРЭ, 2007. – Т. 6, вып. 2. – С. 282- 287.

4. Методы многоверсионной обработки информации в модулярной арифметике: монография / В.И. Барсов, В.А. Краснобаев, А.А. Сиора, И.В. Авдеее. – Х.: МОН, УИПА, 2008. – 459 с.

5. Жихарев В.Я. Методы и алгоритмы реализации арифметических операций в классе вычетов / В.Я. Жихарев, Юнес Эль Хандасси, В.А. Краснобаев // Открытые информационные и компьютерные интегрированные технологии. – Х.: НАКУ «ХАИ», 2003. – Вып. 20. – С. 84-101.

6. Патент на корисну модель. Пристрій складання і віднімання чисел за модулем системи залишкових класів / Краснобаєв В.А., Барсов В.І. – № 35147 від 10.09.2008.

Поступила в редколлегию 10.11.2008

Рецензент: д-р техн. наук, проф. А.Ю. Соколов, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

МЕТОДИ СТИСНЕННЯ ТАБЛИЧНИХ ЦИФРОВИХ ДАНИХ В МОДУЛЯРНІЙ АРИФМЕТИЦІ

В.І. Барсов

Розглянуто методи реалізації інформаційного стиснення цифрових даних результатів виконання одночасно арифметичних операцій складання, віднімання і множення в модулярній арифметиці.

Ключові слова: *цифрові дані, модулярна арифметика.*

METHODS OF COMPRESSION OF TABULAR DIGITAL DATA IN MODULAR TO ARITHMETIC

V.I. Barsov

The methods of realization of informative compression of these digital results of implementation simultaneously of arithmetic operations of addition, deduction and increase in modular arithmetic are considered.

Keywords: *digital data, modular arithmetic.*