УДК 681.325.5

МАСШТАБИРОВАНИЕ ЧИСЕЛ В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Д.С. Лопатин, к.т.н. Л.А. Овчаренко
(представил д.т.н. В.П. Ирхин)

Рассмотрен алгоритм масштабирования результата арифметических операций в модулярной системе счисления. Приведены оценки быстродействия и точности указанного алгоритма.

Несмотря на достигнутые успехи в области разработки высокопроизводительных аппаратных средств цифровой обработки сигналов (ЦОС), задача снижения времени выполнения арифметических операций по прежнему является актуальной. Один из перспективных подходов к повышению быстродействия специализированных процессоров (СП) заключается в применении модулярной системы счисления (МСС), которая за счет присущего ей внутреннего параллелизма позволяет реализовать весьма эффективные вычислительные структуры на базе табличных методов выполнения арифметических операций [1, 2].

Значительная часть алгоритмов ЦОС сводится к вычислению сумм парных произведений, в которых один из сомножителей является целым числом, а другой – рациональным. Однако операция умножения целых и рациональных чисел в модулярной арифметике относится к разряду немодульных операций, вследствие чего процедуры ее реализации значительно медленнее, чем арифметические операции базового набора с целыми числами [1, 2].

Известные алгоритмы вычисления в МСС произведения целого числа A и рационального числа b заключаются в представлении рационального числа в виде дроби $b = \frac{B}{M}$, и выполнении операции масштабирования произведения целых чисел [1,2]: $A \cdot b = \frac{A \cdot B}{M}$, где B – целое число, $0 \le B < M$; M – диапазон представления чисел в МСС.

В [3] рассмотрен алгоритм масштабирования, реализующий операцию умножения произвольного целого числа на фиксированное рациональное число.

Цель статьи – предложить быстродействующий алгоритм масштабирования результата в МСС, в котором реализуется операция умножения произвольного целого числа на произвольное рациональное число.

Пусть масштабный коэффициент M равен произведению модулей МСС: $M = \prod_{i=1}^{N} m_i$. Тогда на основании теоремы о делении на произведение взаимно простых целых чисел [2], произведение произвольного целого числа A на произвольное рациональное число $b = \frac{B}{M}$ может быть представлено в виде суммы

$$\frac{A \cdot B}{M} = \sum_{j=1}^{N} \frac{A \cdot B}{m_j} \cdot d_j , \tag{1}$$

в которой целые числа d_j определяются как решение уравнения

$$\frac{1}{M} = \frac{1}{\prod_{j=1}^{N} m_j} = \frac{d_1}{m_1} + \frac{d_2}{m_2} + \ldots + \frac{d_N}{m_N} .$$

В МСС все переменные, а также результаты арифметических операций, должны быть целочисленными [2]. Поэтому результат масштабирования (1) необходимо привести к целому числу путем округления частного. С этой целью представим сумму в (1) в следующей эквивалентной форме:

$$\sum_{j=1}^{N} \frac{A \cdot B}{m_j} \cdot d_j = \sum_{j=1}^{N} \left(d_j \cdot \frac{\left(A - A \bmod m_j\right)}{m_j} \cdot B + d_j \cdot \frac{\left(B - B \bmod m_j\right)}{m_j} \cdot A \bmod m_j \right) + \sum_{j=1}^{N} \frac{A \bmod m_j \cdot B \bmod m_j \cdot d_j}{m_j}. \tag{2}$$

Отметим, что выражения под знаком первой суммы в правой части формулы (2) всегда приводят к целым числам. Тогда округленное значение частного (1) может быть вычислено с помощью приближенного соотношения:

$$\left\langle \frac{A \cdot B}{M} \right\rangle \approx \sum_{j=1}^{N} \left(d_j \cdot \frac{\left(A - A \bmod m_j\right)}{m_j} \cdot B + d_j \cdot \frac{\left(B - B \bmod m_j\right)}{m_j} \cdot A \bmod m_j \right) + \sum_{j=1}^{N} \left\langle \frac{A \bmod m_j \cdot B \bmod m_j \cdot d_j}{m_j} \right\rangle, \tag{3}$$

где $\langle \bullet \rangle$ – символ округления до ближайшего целого числа.

Из (3) видно, что для нахождения модулярного кода частного $\left\langle \frac{A \cdot B}{M} \right\rangle$ необходимо вычислить остатки слагаемых по основаниям $m_i \left(i = \overline{1, N}\right)$:

$$\left(\left\langle\frac{A\cdot B}{M}\right\rangle\right)\bmod\ m_i \approx$$

$$\approx\left(\sum_{j=1}^{N}\left(d_j\cdot\gamma_{i,j}\cdot\beta_i\right)\bmod\ m_i+\left(d_j\cdot\delta_{i,j}\cdot\alpha_j\right)\bmod\ m_i\right)\bmod m_i+\left(q_{i,j}\right)\bmod\ m_i, \tag{4}$$

где $\alpha_i = A\bmod\ m_i$; $\beta_i = B\bmod m_i$; $q_{i,j}=\left(\left\langle\frac{\alpha_j\cdot\beta_j\cdot d_j}{m_j}\right\rangle\right)\bmod m_i$;

$$\begin{cases}\gamma_{i,j}=\left(R_{ij}\cdot\left(\alpha_i-\alpha_j\right)\right)\bmod\ m_i\ ;\\ \delta_{i,j}=\left(R_{ij}\cdot\left(\beta_i-\beta_j\right)\right)\bmod m_i\ ,i\neq j;i,j=\overline{1,N}\ ,\end{cases} \tag{5}$$

R_{ij} определяется из решения сравнения $\left(R_{ij}\cdot m_j\right)\bmod m_i\equiv 1$. Для нахождения остатков $\gamma_{i,i}$ и $\delta_{i,i}$ может быть применен подход, изложенный в [4]. Согласно этому подходу учтем, что для $0\le A<M$ и $0\le B<M$ всегда справедливы неравенства:

$$\begin{cases}0\le\left(A-A\bmod m_i\right)/m_i<M/m_i\ ;\\ 0\le\left(B-B\bmod m_i\right)/m_i<M/m_i\ .\end{cases} \tag{6}$$

Так как нумерация оснований в МСС может быть произвольной [2], то для определения остатков частных $\gamma_{i,i}=\left(\frac{A-A\bmod m_i}{m_i}\right)\bmod m_i$ и $\delta_{i,i}=\left(\frac{B-B\bmod m_i}{m_i}\right)\bmod m_i$ основания $m_k\ \left(k=\overline{1,N}\right)$ перенумеровываются таким образом, чтобы основанию m_i соответствовал номер N в новой системе: $m_k^*=\left\{m_1,\ldots,m_{i-1},m_{i+1},\ldots,m_N,m_i\right\}$. Тогда в полиадическом коде частных $\frac{\left(A-A\bmod m_i\right)}{m_i}$ и $\frac{\left(B-B\bmod m_i\right)}{m_i}$ старший разряд будет равен нулю, а остатки $\gamma_{i,i}$ и $\delta_{i,i}$ могут быть вычислены по формулам [4]:

$$\begin{cases}\gamma_{i,i}=\left(a_1+\sum\limits_{r=1}^{N-1}a_r\cdot\prod\limits_{z=1}^{r-1}m_z^*\right)\bmod m_i;\\ \delta_{i,i}=\left(b_1+\sum\limits_{r=1}^{N-1}b_r\cdot\prod\limits_{z=1}^{r-1}m_z^*\right)\bmod m_i,\end{cases} \tag{7}$$

где a_r и b_r – r-й разряд полиадического кода частных $\frac{(A - A \bmod m_i)}{m_i}$ и $\frac{(B - B \bmod m_i)}{m_i}$, определяемый в соответствии с [5] как $\left(z = \overline{2, N-1}\right)$:

$$\begin{cases} a_z = \left(\left(\gamma^*_{z,i} \cdot \prod_{j=1}^{z-1} R^*_{z\,j} \right) \bmod m^*_z + \sum_{i=1}^{z-1} \left(t_z \cdot a_i \cdot \prod_{j=i}^{z-1} R^*_{z\,j} \right) \bmod m^*_z \right) \bmod m^*_z; \\ b_z = \left(\left(\delta^*_{z,i} \cdot \prod_{j=1}^{z-1} R^*_{z\,j} \right) \bmod m^*_z + \sum_{i=1}^{z-1} \left(t_z \cdot b_i \cdot \prod_{j=i}^{z-1} R^*_{z\,j} \right) \bmod m^*_z \right) \bmod m^*_z. \end{cases} \quad (8)$$

Здесь $R^*_{z\,j}$ находится из решения сравнения $\left(R^*_{z\,j} \cdot m^*_j\right) \bmod m^*_z \equiv 1$;

$a_1 = \gamma^*_{1,i}$; $b_1 = \delta^*_{1,i}$; $t_z = m^*_z - 1$; $\gamma^*_{z,i} = \left(\left(\alpha^*_z - \alpha_i \right) / m_i \right) \bmod m^*_z$;

$\delta^*_{z,i} = \left(\left(\beta^*_z - \beta_i \right) / m_i \right) \bmod m^*_z$; $\alpha^*_z = A \bmod m^*_z$; $\beta^*_z = B \bmod m^*_z$.

Структурная схема блока вычисления $БВ_{i,i}$ остатков частных $\frac{(A - A \bmod m_i)}{m_i}$ и $\frac{(B - B \bmod m_i)}{m_i}$ по основанию m_i, приведена в [4].

Один из вариантов аппаратной реализации алгоритма вычисления остатка числа $\left\langle \frac{A \cdot B}{M} \right\rangle$ по основанию m_i (4) представлен на рис. 1.

Здесь сумматор по модулю m_i выполнен в виде когерентного модулярного сумматора [6], структура блоков $БВ_{i,i}$ вычисления остатков $\gamma_{i,j}$ и $\delta_{i,i}$ представлена в [4], в табличном вычислителе $ТВ1_i$ определяется остаток $q_{i,i} = \left(\left\langle \frac{\alpha_i \cdot \beta_i \cdot d_i}{m_i} \right\rangle \right) \bmod m_i$, табличные вычислители $ТВ2_i$ рассчитывают значения остатков $h_{i,i} = \left(d_i \cdot \beta_i \cdot \gamma_{i,i}\right) \bmod m_i$, $\left(s_{i,i} = \left(d_i \cdot \alpha_i \cdot \delta_{i,i}\right) \bmod m_i\right)$, а структурная схема блока вычисления $БВ_{i,k,}$ остатков $h_{i,j,}$ $q_{i,j}$ и $s_{i,j}$ $\left(j \neq i;\, j, i = \overline{1, N}\right)$ изображена на рис. 2.

В схеме на рис. 2 в табличном вычислителе $ТВ1_j$ определяется остаток $q_{i,j} = \left(\left\langle \frac{\alpha_j \cdot \beta_j \cdot d_j}{m_j} \right\rangle \right) \bmod m_i$, в табличных вычислителях $ТВ3_{i,j}$ –

остатки $\gamma_{i,j} = \left(R_{ij} \cdot \left(\alpha_i - \alpha_j\right)\right) \bmod m_i$ и $\delta_{i,j} = \left(R_{ij} \cdot \left(\beta_i - \beta_j\right)\right) \bmod m_i$, в табличном вычислителе $TB4_{i,l}$ – остаток $h_{i,j} = \left(\gamma_{i,j} \cdot \beta_i \cdot d_j\right) \bmod m_i$, а в табличном вычислителе $TB5_{i,l}$ – остаток $s_{i,j} = \left(\delta_{i,j} \cdot \alpha_j \cdot d_j\right) \bmod m_i$.

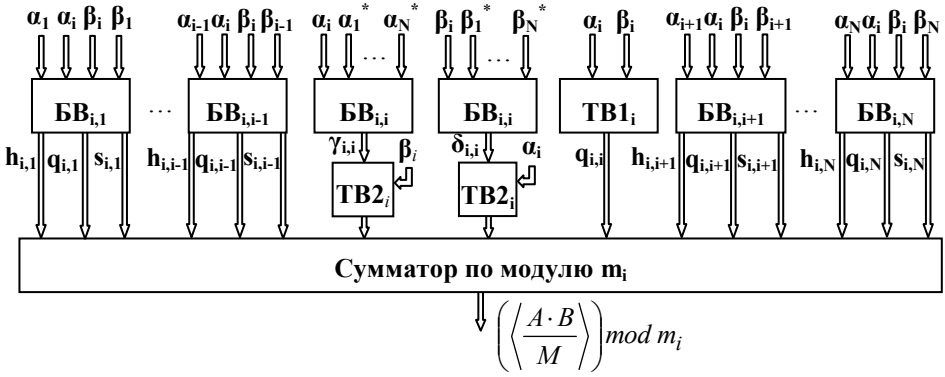

Рис. 1. Устройство для вычисления остатка $\left\langle \frac{A \cdot B}{M} \right\rangle$ по основанию m_i

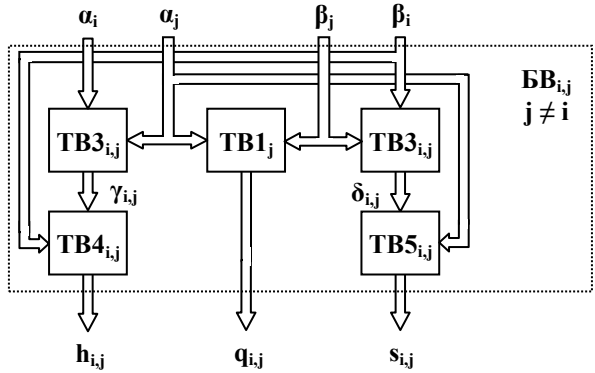

Рис. 2. Схема вычислительного блока $БВ_{i,j}$

Время $t_{AУ}$ в устройстве на рис. 1 вычисления остатка результата округления частного $\left\langle \frac{A \cdot B}{M} \right\rangle$ по основанию m_i $\left(i = \overline{1,N}\right)$ складывается из времени определения остатков $\gamma_{i,i}$ ($\delta_{i,i}$) по основаниям $m_j^* \left(j = \overline{1,N-1}\right)$ в вычислительном блоке $БВ_{i,i}$ – $\tau_{БВ} \approx 2$ нс [4] , времени расчета остатков

$h_{i,i}\left(s_{i,i}\right)$ в табличных вычислителях $TB2_j$ – $\tau_{TB2} \approx 1$ нс [4] и времени сложения $3 \cdot N$ чисел в когерентном модулярном сумматоре – $\tau_{\Sigma} \approx 1$ нс [6]: $t_{AV} = \tau_{БВ} + \tau_{TB2} + \tau_{\Sigma} \approx 4$ нс.

Для иллюстрации работоспособности предложенного алгоритма рассмотрим следующий пример.

Пусть заданы основания МСС: $m_1=3,\ m_2=5,\ m_3=7,\ m_4=11\ (N=4)$, с диапазоном представления чисел $M = \prod_{i=1}^{N} m_i = 1155$. Необходимо найти результат округления частного $\left\langle \frac{A \cdot B}{M} \right\rangle$, где $A=100=(1,0,2,1)$ и $B=100=(1,0,2,1)$.

Находим коэффициенты: $d_1 = 1; d_2 = -4; d_3 = 2; d_4 = 2$.

Для указанных исходных данных получаем значения переменных $h_{i,j}, q_{i,j}, s_{i,j}, \gamma_{i,j}, \delta_{i,j}$, которые сведены в табл. 1–5.

Таблица 1

Значения переменной $h_{i,j}$

i	j			
	1	2	3	4
1	0	1	1	0
2	0	0	0	0
3	3	1	0	1
4	0	8	6	7

Таблица 2

Значения переменной $q_{i,j}$

i	j			
	1	2	3	4
1	0	0	1	0
2	0	0	1	0
3	0	0	1	0
4	0	0	1	0

Таблица 3

Значения переменной $s_{i,j}$

i	j			
	1	2	3	4
1	0	0	2	0
2	3	0	1	3
3	5	0	0	4
4	0	0	1	7

Таблица 4

Значения переменной $\gamma_{i,j}$

i	j			
	1	2	3	4
1	0	2	2	0
2	3	0	4	4
3	5	6	0	2
4	0	9	3	9

Таблица 5

Значения переменной $\delta_{i,j}$

i	j			
	1	2	3	4
1	0	2	2	0
2	3	0	4	4
3	5	6	0	2
4	0	9	3	9

Вычисленный по формуле (4) в соответствии с данными, представленными в табл.1–5, код результата масштабирования $\left\langle \frac{A \cdot B}{M} \right\rangle$ в МСС равен $(2,3,1,8)$, что соответствует числу 8.

Проверка: $\left\langle \frac{A \cdot B}{M} \right\rangle = \langle 8{,}658 \rangle = 9$, т.е. вычисленная с применением данного алгоритма оценка округления отличается от истинного значения на 1.

Сравнение результатов расчета $\left\langle \frac{A \cdot B}{M} \right\rangle$ на основании предложенного алгоритма с истинными значениями округления частного $A \cdot B / M$ при $0 \le A < M$ и $0 \le B < M$ для приведенного в примере набора оснований $m_i \left(i = \overline{1, N}\right)$, показывает, что примерно в 67 % случаев данные совпадают, в 33 % – отличаются на ± 1, и в менее 0.02 % – на ± 2.

Таким образом, разработанный алгоритм масштабирования чисел в МСС обеспечивает погрешность вычисления произведения целого и рационального чисел не хуже и при более высоком быстродействии, чем в аналогичных аппаратных средствах ЦОС, функционирующих в позиционной системе счисления.

ЛИТЕРАТУРА

1. *Чернявский А.С., Данилевич В.В., Коляда А.А., Селянинов М.Ю. Высокоскоростные методы и системы цифровой обработки информации. – Мн.: Белгосуниверситет, 1996. – 376 с.*
2. *Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 440 с.*
3. *Овчаренко Л.А., Дидрих В.Е. Повышение быстродействия цифрового фильтра в модулярной системе счисления // Радиотехника (Россия). – 2002. – № 4 (приложение к журналу).*
4. *Овчаренко Л.А., Лопатин Д.С. Деление числа в модулярном коде на основание системы счисления // Телекоммуникации. – 2002. – № 6.*
5. *Овчаренко Л.А. Когерентный преобразователь модулярного кода // Телекоммуникации. – 2001. – № 6.*
6. *Овчаренко Л.А. Вариант реализации основных операций в модулярном арифметическом устройстве // Телекоммуникации. – 2001. – №3.*

Поступила 25.10.2002

***ЛОПАТИН Дмитрий Сергеевич**, адъюнкт Военного института радиоэлектроники (г. Воронеж). В 1999 году окончил Военный институт радиоэлектроники. Область научных интересов – высокопроизводительные и отказоустойчивые вычислительные структуры цифровой обработки сигналов.*

***ОВЧАРЕНКО Леонид Александрович**, канд. техн. наук, ст. науч. сотрудник, докторант Военного института радиоэлектроники (г. Воронеж). В 1983 году окончил Череповецкое высшее военное инженерное училище радиоэлектроники. Область научных интересов – высокопроизводительные и отказоустойчивые вычислительные структуры цифровой обработки сигналов.*