4. Курбатов П.А., Аринчин С.А. Численный расчет электромагнитных полей. – М: Энергоатомиздат, 1984. – 168 с.
5. Красносельский М.А. и др. Приближенное решение операторных уравнений. – М.: Наука, 1969. - 456 с.
6. Марчук Г.И. Основы вычислительной математики. – М.: Наука, 1989. – 608 с.
7. Молчанов И.Н. Машинные методы решения прикладных задач. – К.: Наукова думка, 1987. – 288 с.
8. Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления. – М.: Наука, 1984. – 320 с.
9. Богачев Ю.К. Практикум на ЭВМ. Методы решения линейных систем и нахождения собственных значений. – М: Наука, 1998. – 138 с.
10. Самарский А.А., Гулин А.В. Численные методы. – М.: Наука, 1989. – 432 с.
11. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. – М.: Наука, 1976. – 544 с.

пост.25.05.2010

Выполнение позиционных операций в непозиционной системе остаточных классов

ПОЛИССКИЙ Ю.Д.

НИИ автоматизации черной металлургии

Розглянутий метод розв'язку завдання визначення виходу числа за робочий діапазон у системі залишкових класів, заснований на відновленні контрольних залишків по відомих робочих залишках. Метод алгоритмічно простий і нескладний для схемної реалізації при створенні ефективних обчислювальних структур високої продуктивності й надійності для перспективних інформаційних технологій.

Рассмотрен метод решения задачи определения выхода числа за рабочий диапазон в системе остаточных классов, основанный на восстановлении контрольных остатков по известным рабочим остаткам. Метод алгоритмически прост и несложен для схемной реализации при создании эффективных вычислительных структур высокой производительности и надежности для перспективных информационных технологий.

The method of decision of task of determination of output of number is considered for a working range in the system of remaining classes, based on renewal of control bits and pieces on the known working bits and pieces. A method is algorithmically simple and simple for scheme realization at creation of effective calculable structures of high yield and reliability for perspective information technologies.

Введение. Выполнение быстрых вычислений в параллельных структурах связано в настоящее время с применением новых принципов на основе представления чисел в системе остаточных классов (СОК) [1].

Достоинства СОК подробно рассмотрены в [2], [3]. Они заключаются в высокой степени параллелизма при выполнении арифметических операций сложения, вычитания и умножения. Сложнее обстоят дела при реализации немодульных операций, требующих знания всего числа в целом. К таким операциям относятся, в частности, определение выхода за диапазон системы в результате сложения, вычитания или умножения двух чисел, а также восстановление остатка числа по известным его остаткам.

Постановка задачи. При изложении статьи будем использовать определения и обозначения, приведенные в [4]. Таким образом, СОК называется система счисления, в которой произвольное число N представляется в виде набора наименьших неотрицательных остатков по модулям $m_1, m_2, \dots, m_n$, т.е. $N = [N(\mathrm{mod}\, m_1), N(\mathrm{mod}\, m_2), \dots, N(\mathrm{mod}\, m_n)]$ или

$$N = (\alpha_1, \alpha_2, \dots, \alpha_n) \tag{1}$$

Здесь $\alpha_i = N(\mathrm{mod}\, m_i)$. При этом, если все целые числа N принадлежат диапазону $[0, M)$, объем которого равен

$$M = m_1 m_2 \dots m_n, \tag{2}$$

а модули m_i взаимно простые, то каждому набору $(\alpha_1, \alpha_2, \dots, \alpha_n)$ соответствует только одно число N из этого диапазона.

Первая задача заключается в том, чтобы установить факт переполнения числового диапазона (2). Решение этой задачи рассмотрено в [5]. В данной работе предлагается другой подход, основанный на расширении диапазона (2) представления чисел, т.е. представление числа в диапазоне $[0, M_1)$

$$M_1 = M m_{n+1} m_{n+2} \dots m_j \dots m_k \tag{3}$$

При этом само число N находится в диапазоне $[0, M)$. Поскольку расширение диапазона основано на восстановлении остатков, вторая задача заключается в том, чтобы восстановить остатки $\alpha_{n+1}\alpha_{n+2}\ldots\alpha_j\ldots\alpha_k$ числа N по его остаткам $\alpha_1,\alpha_2,\ldots,\alpha_n$.

Основная часть. Будем диапазон $[0,M)$ называть рабочим диапазоном чисел (1). Введем дополнительные модули $m_{n+1},m_{n+2},\ldots,m_j,\ldots,m_k$, определяющие контрольный диапазон $\lfloor M+1,M_k)$, объем которого равен

$$M_1 = m_{n+1}m_{n+2}\ldots m_k.$$

В [5] показано, что для однозначного суждения о переполнении диапазона $[0,M)$ необходимо, чтобы $M_1 \ge M-1$.

Будем рассматривать числа (1) рабочего диапазона на всем диапазоне $M_2 = M * M_1$,

$$M_2 = m_1m_2\ldots m_nm_{n+1}m_{n+2}\ldots m_k.$$

В этом случае

$$N=(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1},\alpha_{n+2},\ldots,\alpha_j,\ldots,\alpha_k) \qquad (4)$$

Если системой оснований полиадического кода также является система $M_2 = m_1m_2\ldots m_nm_{n+1}m_{n+2}\ldots m_k$, то число N в полиадическом коде представляется в виде

$$N=\pi_1+\pi_2m_1+\pi_3m_1m_2+\ldots+\pi_im_1m_2\ldots m_{i-1}+$$
$$+\cdots+\pi_nm_1m_2\ldots m_{n-1}+\pi_{n+1}m_1m_2\ldots m_n+\ldots+$$
$$+\pi_jm_1m_2\ldots m_{j-1}+\ldots+\pi_km_1m_2\ldots m_{k-1}$$

где

$$0<\pi_i\le m_i-1 \qquad (5)$$

Пусть $N_1=(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1},\alpha_{n+2},\ldots,\alpha_j,\ldots,\alpha_k)$,

$N_2=(\beta_1,\beta_2,\ldots,\beta_n,\beta_{n+1},\beta_{n+2},\ldots,\beta_j,\ldots,\beta_k)$

и

$$N=(\gamma_1,\gamma_2,\ldots,\gamma_n,\gamma_{n+1},\gamma_{n+2},\ldots,\gamma_j,\ldots,\gamma_k),$$

где

$$\gamma_j=\alpha_j\beta_j \qquad (6)$$

Если переполнения нет, т.е. $N<M$, то $\pi_j=0$. Следовательно,

$$\gamma^в{}_j=(\pi_1+\pi_2m_1+\pi_3m_1m_2+\ldots+$$
$$+\pi_im_1m_2\ldots m_{i-1}+\cdots+ \qquad (7)$$
$$+\pi_nm_1m_2\ldots m_{n-1})(mod\ m_j)$$

Поэтому восстановленное по (7) значение остатка $\gamma_j{}^в$ равно значению остатка γ_j по (6).

Пусть

$A=(\gamma_{n+1},\gamma_{n+2},\ldots,\gamma_j,\ldots,\gamma_k)$ для $\gamma_j=\alpha_j\beta_j$

и

$A^в=\left(\gamma^в{}_{n+1},\gamma^в{}_{n+2},\ldots,\gamma^в{}_j,\ldots,\gamma^в{}_k\right)$ для $\gamma_j{}^в$.

Отсюда, переполнение числового диапазона отсутствует при $A=A^в$.

Если же $N>M$, то $\pi_j\ne 0$, и $\gamma_j=(\alpha_j\beta_j+rM)(\mathrm{mod}\ m_j)$,

где

r - число, показывающее во сколько раз был превзойден диапазон M. В то же время восстановленный остаток $\gamma_j{}^в$ по-прежнему определяется (7). Поэтому $A\ne A^в$ является признаком переполнения диапазона M.

Из (2) в соответствии с (1) получаем

$$\alpha_j=(\pi_1+\pi_2m_1+\pi_3m_1m_2+\ldots+$$
$$+\pi_im_1m_2\ldots m_{i-1}+\cdots+\pi_nm_1m_2\ldots m_{n-1}+ \qquad (8)$$
$$+\pi_{n+1}m_1m_2\ldots m_n)(\mathrm{mod}\ m_j)$$

Следовательно, для получения α_j необходимо знание слагаемых (8).

Из (8)

$\alpha_1=N(mod\ m_1)=\pi_1$ и $\pi_1=\alpha_1$.

$\alpha_2=N(mod\ m_2)=\pi_1+\pi_2m_1$ и

$\pi_2m_1=\alpha_2-\pi_1$.

....

....

$$\alpha_i=(\pi_1+\pi_2m_1+\pi_3m_1m_2+\ldots+$$
$$+\pi_{i-1}m_1m_2\ldots m_{i-2}+\pi_im_1m_2\ldots m_{i-1})(\mathrm{mod}\ m_i)$$

и

$$\pi_im_1m_2\ldots m_{i-1}=\alpha_i-(\pi_1+\pi_2m_1+\pi_3m_1m_2+$$
$$+\ldots+\pi_{i-1}m_1m_2\ldots m_{i-2})(mod m_i) \qquad (9)$$

Из (9) видно, что определение очередного слагаемого возможно только после получения предыдущего.

Таким образом, базовый алгоритм восстановления остатка состоит из следующих итераций.

Начальное значение восстанавливаемого остатка принимается $\alpha_j=0$. На первой итерации по каждому из модулей $m_1,m_2,\ldots,m_n$ определяется разность между остатком по этому модулю и значением $\Delta_1=\pi_1(\mathrm{mod}\ m_1)$, взятая по данному модулю. Назовем такие разности приведенными остатками. Значения Δ_1 по модулям $m_2,m_3,\ldots,m_n,m_j$ выбираются из предварительно рассчитанных таблиц. В результате находится значение $\Delta_2=\pi_2m_1(\mathrm{mod}\ m_2)$. В то же время значение π_1 по $\mathrm{mod}\ m_j$ суммируется с α_j. На второй итерации по каждому из модулей $m_2,\ldots,m_n$ определяется разность между приведенным остатком по этому модулю и значением $\Delta_2=\pi_2m_1$, взятая по данному модулю. Значения Δ_2 по модулям $m_3,\ldots,m_n,m_j$ также выбираются из указанных выше предварительно рассчитанных таблиц. В результате находится значение $\Delta_3=(\pi_3m_1m_2)(\mathrm{mod}\ m_3)$, а значение π_2m_1 суммируется с полученным раннее значением остатка по модулю m_j. После выполнения n итераций получаем восстановленный остаток α_j.

Табличную реализацию алгоритма, выполненную в соответствии с [6], рассмотрим на примере восстановления остатков для контрольных модулей $m_5 = 23, m_6 = 17$ по известным остаткам для рабочих модулей $m_1 = 11, m_2 = 3, m_3 = 2, m_4 = 5$.

В таблицах 1–4 приведены константы каждой итерации, рассчитанные в соответствии с [5].

Таблица 1

Модули					
Раб.				Контр.	
11	***3***	***2***	***5***	***23***	***17***
0	**0**	**0**	**0**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**
2	**2**	**0**	**2**	**2**	**2**
3	**0**	**1**	**3**	**3**	**3**
4	**1**	**0**	**4**	**4**	**4**
5	**2**	**1**	**0**	**5**	**5**
6	**0**	**0**	**1**	**6**	**6**
7	**1**	**1**	**2**	**7**	**7**
8	**2**	**0**	**3**	**8**	**8**
9	**0**	**1**	**4**	**9**	**9**
10	**1**	**0**	**0**	**10**	**10**

Таблица 2

Модули				
Раб.			Контр.	
3	***2***	***5***	***23***	***17***
0	**0**	**0**	**0**	**0**
2	**1**	**1**	**11**	**11**
1	**0**	**2**	**22**	**5**

Таблица 3

Модули			
Раб.		Контр.	
2	*5*	*23*	*17*
0	**0**	**0**	**0**
1	**3**	**10**	**16**

Таблица 4

Модули		
Раб.	Контр.	
5	*23*	*17*
0	**0**	**0**
1	**20**	**15**
2	**17**	**13**
3	**14**	**11**
4	**11**	**9**

Рассмотрим произведение пары чисел

$N^M{}_1 = 13 = (\alpha_1 = 2, \alpha_2 = 1, \alpha_3 = 1, \alpha_4 = 3, \alpha_5 = 13, \alpha_6 = 13)$,

$N^M{}_2 = 19 = (\beta_1 = 8, \beta_2 = 1, \beta_3 = 1, \beta_4 = 4, \beta_5 = 19, \beta_6 = 2)$.

$N^M = N^M{}_1 \times N^M{}_2 =$
$= 247 = (\gamma_1 = 5, \gamma_2 = 1, \gamma_3 = 1, \gamma_4 = 2, \gamma_5 = 17, \gamma_6 = 9)$

$N^M < M$.

$A = (\gamma_5, \gamma_6) = (17, 9)$.

Работа алгоритма восстановления остатков γ_5 и γ_6 по остаткам $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ для определения выхода или невыхода числа N^M за рабочий диапазон системы, выполненная в соответствии с [6], представлена табл. 5

Таблица 5. **Работа алгоритма восстановления остатков**

Модули					
Раб.				Контр.	
1	**3**	**2**	**5**	**23**	**17**
5	1	1	2	0	0
5	2	1	0	5	5
0	2	0	2	5	5
	2	1	1	11	11
	0	1	1	16	16
		1	3	10	16
		0	3	3	15
			3	14	11
			0	***17***	***9***

Восстановленные остатки $\gamma_5 = 17$ и $\gamma_6 = 9$, $A^в = (\gamma^в{}_5, \gamma^в{}_6) = (17, 9)$. Поскольку $A^в = A$, произведение $N^M < M$, т.е. N^M не выходит за рабочий диапазон системы.

Рассмотрим произведение пары чисел

$N^б{}_1 = 27 = (\alpha_1 = 5, \alpha_2 = 0, \alpha_3 = 1, \alpha_4 = 2, \alpha_5 = 4, \alpha_6 = 10)$

$N^б{}_2 = 19 = (\beta_1 = 8, \beta_2 = 1, \beta_3 = 1, \beta_4 = 4, \beta_5 = 19, \beta_6 = 2)$

$N^б = N^б{}_1 \times N^б{}_2 = 513 =$
$= (\gamma_1 = 7, \gamma_2 = 0, \gamma_3 = 1, \gamma_4 = 3, \gamma_5 = 7, \gamma_6 = 3)$

$N^б > M$.

$A = (\gamma_5, \gamma_6) = (7, 3)$.

Работа алгоритма восстановления остатков γ_5 и γ_6 по остаткам $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ для определения выхода или невыхода числа $N^б$ за рабочий диапазон системы, выполненная в соответствии с [6], представлена табл. 6.

Таблица 6. **Работа алгоритма восстановления остатков**

Модули					
Раб.				Контр.	
11	**3**	**2**	**5**	**23**	**17**
7	0	1	3	0	0
7	1	1	2	7	7
0	2	0	1	7	7
	2	1	1	11	11
	0	1	0	18	1
		1	3	10	16
		0	2	5	0
			2	17	13
			0	***22***	***13***