2. СИСТЕМА ЗАЛИШКОВИХ КЛАСІВ

Результати досліджень, що проводились різними групами вчених з метою пошуків шляхів підвищення продуктивності обчислювальних засобів, методів організації ефективної системи виявлення та виправлення помилок, а також побудови надійних обчислювальних комплексів, дають можливість стверджувати, що в межах позиційних систем числення не можна очікувати принципових зрушень в даних напрямках без суттєвого збільшення робочих частот і ускладнення апаратної частини. Причина полягає в тому, що позиційні системи числення, в яких представляється і обробляється інформація в сучасних ЕОМ, мають важливий недолік – наявність міжрозрядних зв'язків. Таким чином ефективним є використання непозиційних систем числення, які позбавлені даного недоліку.

З огляду на сучасний рівень розвитку обчислювальних засобів використання непозиційних систем числення дозволяє збільшити надійність та швидкість цифрової обробки даних, ввести методи контролю за правильністю виконання операцій без подальшого ускладнення апаратної частини та забезпечувати необхідну точність обчислень без збільшення розрядності шини. Сучасні обчислювальні потужності дозволяють розв'язувати задачі оптимального вибору модулів системи та розрахунку відповідних вагових коефіцієнтів та базисних чисел, що відкриває нові можливості застосування непозиційних систем числення.

Нехай задано набір із k взаємопростих натуральних чисел $p_i \in N$, $i = \overline{1, k}$, тоді під СЗК будемо розуміти таку систему, в якій ціле число представляється у вигляді невід'ємних залишків по вибраних модулях p_i.

$$b_i = res\, N \,(\mathrm{mod}\, p_i),\ i = \overline{1, k}. \qquad (1)$$

Даний вираз відповідає системі діофантових рівнянь:

$$N = c_i \cdot p_i + b_i,\ i = \overline{1, k}, \qquad (2)$$

де N – вихідна величина; p_i – набір модулів; b_i – набір залишків по відповідних модулях; c_i – ранг числа N по модулю p_i.

В теорії чисел доведено, що система рівнянь (2) має єдиний розв'язок при взаємопростих модулях. Діапазон чисел, що може бути представлений за допомогою набору модулів ($p_1, p_2, \ldots, p_{k-1} p_k$) становить $[0, \wp]$, $\wp = \prod_{i=1}^{k} p_i$.

Нехай у десятковій системі числення задано число N=13, вибираємо взаємно прості модулі: $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, добуток яких

$$\wp = \prod_{i=1}^{3} p_i = 3 \cdot 5 \cdot 7 = 105 .$$

Враховуючи, що $N < \wp$ можна використовувати даний набір модулів для перетворення заданого числа.

Спосіб 1.

При невеликому діапазоні представлених даних найбільш ефективним є табличний метод кодування та перетворення даних в СЗК .

Таблиця 2.1 – Таблиця кодування даних в СЗК.

Число в десятковій системі числення	$p_1 = 3$	$p_2 = 5$	$p_3 = 7$
0	0	0	0
1	1	1	1
2	2	2	2
3	0	3	3
4	1	4	4
5	2	0	5
6	0	1	6
7	1	2	0
8	2	3	1
9	0	4	2
10	1	0	3
11	2	1	4
12	0	2	5
13	1	3	6
14	2	4	0
15	0	0	1
…	…	….	….
…	…	….	….
100	1	0	2
101	2	1	3
102	0	2	4
103	1	3	5
104	2	4	6
105	0	0	0

Отже, згідно таблиці 2.1: $13_{10} = (1, 3, 6)_{(3, 5, 7)}$.

Спосіб 2. Нехай у десятковій системі числення задано число N=103. Використовуючи рівняння (1) маємо:

$$b_1 = res\ 103\ (\ \mathrm{mod}\ 3) = 1;$$

$$b_2 = res\ 103\ (\ \mathrm{mod}\ 5) = 3\ ;$$

$$b_2 = res\ 103\ (\ \mathrm{mod}\ 5) = 5\ .$$

Отже $103_{10} = (1, 3, 5)_{(3, 5, 7)}$.

Спосіб 3. Задано число N=103.

Число N представлено в позиційній системі числення з основою $d = 10$. Представлення степенів основи d в СЗК буде мати вигляд:

$$d^0 = 1 = (1,1,1)_{(3, 5, 7)}\ \text{б}$$

$$d^1 = 10 = (1, 0,3)_{(3, 5, 7)}\ ,$$

$$d^2 = 100 = (1, 0, 2)_{(3, 5, 7)}\ .$$

Отримаємо представлення коефіцієнтів полінома (2.4).

$$a_0 = 3 = (0,3,3)_{(3, 5, 7)}\ ,$$

$$a_1 = 0 = (0, 0, 0)_{(3, 5, 7)}\ ,$$

$$a_2 = 1 = (1,1,1)_{(3, 5, 7)}\ .$$

Згідно формули (5):

$103_{10} = (0 \cdot 1 + 0 \cdot 1 + 1 \cdot 1,\ 3 \cdot 1 + 0 \cdot 0 + 1 \cdot 0,\ 3 \cdot 1 + 0 \cdot 3 + 1 \cdot 2) = (1, 3, 5)_{(3,5,7)}$.

Представлення числа $N = 103_{10}$ отримані за допомогою різних методів аналогічні, що підтверджує достовірність отриманих результатів.

Переведення числа з системи залишкових класів в десяткову систему числення

Переведення числа з системи залишкових класів в десяткову систему числення здійснюється за формулою

$$N = \sum_{i=1}^{k} b_i \cdot B_i \pmod{\wp}\ . \qquad (3)$$

Згідно визначення ортогональних базисів, вони можуть бути обчислені:

$$B_i = m_i \cdot \frac{\wp}{p_i}\ ,\ i = \overline{1, k}\ ; \qquad (4)$$

де $1 \le m_i \le p_i - 1$ – вага ортогонального елементу.

При чому

$$m_i \cdot \frac{\wp}{p_i} = 1 \pmod{p_i}. \quad (5)$$

Рівняння (5) еквівалентне наступному діафантовому рівнянню:

$$m_i \cdot \frac{\wp}{p_i} = 1_i \cdot p_i + 1, \; 1_i \in N. \quad (6)$$

Для обчислення m_i використовується формула (5). Застосування операції визначення залишку по заданому модулю обумовлює обмежений діапазон можливих значень вагових коефіцієнтів: $m_i \in [1, p-1]$.

Позначимо $\wp_i = \frac{\wp}{p_i}$. В результаті ділення $\wp_i$ на p_i отримаємо певний залишок δ_i, згідно рівняння (5):

$$m_i \cdot \delta_i = 1 \cdot (\mathrm{mod}\, \wp). \quad (7)$$

З огляду на порівняно невеликі значення величини p_i можемо скласти таблицю розв'язків рівняння (7), за допомогою якої згідно величини δ_i знаходиться відповідне значення m_i. Припускаючи, що основи p_i вибираються з множини простих чисел, приведемо таблицю розв'язків рівняння (7), для $p_i < 25$ (таблиця 2.2).

Згідно (5):

$$B_1 + B_2 + ... + B_k = (1,0,...,0) + (0,1,...,0) + ... + (0,0,...,1) = (1,1,...,1). \quad (8)$$

Оскільки сумування проводиться в СЗК:

$$\sum_{i=1}^{k} B_i = 1 \pmod{\wp}. \quad (9)$$

Таблиця 2.2 – Розв’язки рівняння $m \cdot \delta = 1 (\mathrm{mod}\ p)$ для множини простих чисел $p_i < 25$

δ	P								
	2	3	5	7	11	13	17	19	23
1	1	1	1	1	1	1	1	1	1
2		2	3	4	6	7	9	10	12
3			2	5	4	9	6	13	8
4			4	2	3	10	13	5	6
5				3	9	8	7	4	14
6				6	2	11	3	16	4
7					8	2	5	11	10
8					7	5	15	12	3
9					5	3	2	17	18
10					10	4г	12	2	7
11						6	14	7	21
12						12	10	8	2
13							4	3	16
14							11	15	5
15							8	14	20
16							16	6	13
17								9	19
18								18	9
19									17
20									15
21									11
22									22

Рівняння (9) можна використати для перевірки достовірності знаходження базисів системи.

Розглянемо приклад зворотного перетворення для значень отриманих вище

$$P_1 = 3,\ P_2 = 5,\ P_3 = 7.$$

$$a_1 = 1,\ a_2 = 3,\ a_3 = 5.$$

$$\delta_1 = 35(\text{mod}3) = 2,$$

$$\delta_2 = 21(\text{mod}5) = 1,$$

$$\delta_3 = 15(\text{mod}7) = 1.$$

Використовуючи означення базисних чисел та таблицю

$$2.2:\ m_1 = 2\ ;\ m_2 = 1;\ m_3 = 1;$$

$$B_1 = \frac{105}{3}\cdot 2 = 70\ ;\ B_2 = \frac{105}{5}\cdot 1 = 21;\ B_3 = \frac{105}{7}\cdot 1 = 15\ .$$

Перевіримо достовірність обчислення базисних чисел згідно формули (9):

$$(70 + 21 + 15) = 106 = 1 \pmod{105}\ .$$

Згідно формули (3):

$$N_{10} = res\ (1\cdot 70 + 3\cdot 21 + 5\cdot 15) \pmod{105} = 103_{10}$$

В результаті послідовного застосування прямого та зворотного перетворень для цілочисельної форми СЗК отримаємо вихідне число в позиційній системі числення.

Представлення даних в системі залишкових класів дає змогу здійснювати розпаралелювання обробки інформації без значного ускладнення обчислювальних засобів. Використання СЗК спрощує побудову систем збору інформації, а також дозволяє вирішувати клас задач, що є невизначеними в позиційних системах числення. Особливістю СЗК залишається простота реалізації прямого та зворотного перетворень.

2.2 Математичні операції в СЗК

Розглянемо правила виконання операцій додавання і множення в СЗК при умові, що обидва числа і результат операції знаходяться в діапазоні $[0, \wp]$.

Нехай операнди A і B представлені відповідно залишками α_i і β_i по модулю P_i при i = 1, 2,. . . , n.

Результат операцій додавання і множення $A + B$ і $A \cdot B$ представлені відповідними залишками γ_i і δ_i по тих же модулях P_i , тобто

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n)\ ,$$

$$B = (\beta_1 , \beta_2 , \ldots , \beta_n) ,$$
$$A + B = (\gamma_1 , \gamma_2 , \ldots , \gamma_n) ,$$
$$A \cdot B = (\delta_1 , \delta_2 , \ldots , \delta_n) ,$$

і при цьому мають місце співвідношення:

$$A < \wp , B < \wp , A + B < \wp , A \cdot B < \wp .$$

Припускається, що γ_i дорівнює $\alpha_i + \beta_i$ по модулю P_i , а δ_i дорівнює $\alpha_i \cdot \beta_i$ також по модулю P_i .

$$\gamma_i \equiv \alpha_i + \beta_i \ (\mathrm{mod} P_i) ,$$
$$\delta_i \equiv \alpha_i \cdot \beta_i \ (\mathrm{mod} P_i) .$$

При цьому в якості цифри результату береться відповідно

$$\gamma_i = \alpha_i + \beta_i - [\frac{\alpha_i + \beta_i}{P_i}] \cdot P_i \qquad (10)$$

$$\delta_i = \alpha_i \cdot \beta_i - [\frac{\alpha_i \cdot \beta_i}{P_i}] \cdot P_i . \qquad (11)$$

Отже, можна записати для додавання

$$\gamma_i = A + B - [\frac{A + B}{P_i}] \cdot P_i ,$$

для i = 1, 2,. . . , n.

$$A + B \ (\mathrm{mod} P) = \begin{cases} \alpha_i + \beta_i , & \text{ÿêùî} \quad \alpha_i + \beta_i < P_i ; \\ \alpha_i + \beta_i - P, & \text{ÿêùî} \quad \alpha_i + \beta_i \geq P_i . \end{cases}$$

Для множення

$$\delta_i = A \cdot B - [\frac{A \cdot B}{P_i}] \cdot P_i .$$

Приклад: нехай основою системи є $P_1 = 3$, $P_2 = 5$, $P_3 = 7$.

Діапазон представлення чисел за допомогою вибраних модулів визначається, як $\wp = P_1 \cdot P_2 \cdot P_3 = 105$.

Приклад. Додати числа A=17 і B=63. Переведемо числа A і B в систему залишкових класів по заданих модулях

$$A = 17 = (2, 2, 3)_{(3, 5, 7)} ,$$
$$B = 63 = (0, 3, 0)_{(3, 5, 7)} .$$

В відповідності з (2.10) отримаємо

$$A + B = (2, 0, 3)_{(3, 5, 7)} .$$

Легко перевірити, що число $(2, 0, 3)_{(3,5 , 7)}$ в десятковій системі числення є 80 і дорівнює сумі операндів.

Приклад. Помножити число A=17 на число B=6. В СЗК числа A і B будуть представлені як

$$A = 17 = (2, 2, 3)_{(3, 5, 7)}$$
$$B = 6 = (0, 1, 6)_{(3, 5, 7)} .$$

В відповідності з (11) отримаємо $A \cdot B = (0, 2, 4)_{(3, 5, 7)}$.

Легко перевірити, що число $(0, 2, 4)_{(3,5 , 7)}$ в СЗК дорівнює десятковому числу 102 в десятковій системі числення і рівне добутку операндів.

Правила виконання операції віднімання в СЗК в випадку, якщо два числа і результат операції знаходяться в діапазоні $[0, \wp]$.

Нехай операнди A і B представлені відповідними залишками α_i і β_i по модулях P_i при i = 1, 2,. . . , n.

Результат операції віднімання A-B представлений відповідними залишками γ_i по тих же модулях P_i .

Тобто

$$A = (\alpha_1 , \alpha_2 , . . , \alpha_n) ,$$
$$B = (\beta_1 , \beta_2 , . . , \beta_n) ,$$
$$A - B = (\gamma_1 , \gamma_2 , . . , \gamma_n) ,$$

і при цьому виконуються умови:

$$A < \wp , B < \wp , 0 \le A - B < \wp .$$

Аналогічно з (10) отримаємо вираз для віднімання

$$\gamma_i = \alpha_i - \beta_i - [\frac{\alpha_i - \beta_i}{P_i}] \cdot P_i ,$$
$$\gamma_i = \alpha_i - \beta_i (P_i) , i = 1, 2,. . . , n.$$

Операція віднімання в тих випадках, коли її результат додатній, виконується відніманням відповідних цифр розрядів, при цьому завжди в результаті приводиться найменший додатній залишок, так як це випливає із визначення СЗК. Якщо різниця цифр від'ємна, то береться її доповнення до відповідного модуля.

Тобто

$$A - B \ (\mathrm{mod}\ P) = \begin{cases} \alpha_i - \beta_i , & \text{ÿêùî} \quad \alpha_i - \beta_i \ge 0; \\ \alpha_i - \beta_i + P, & \text{ÿêùî} \quad \alpha_i - \beta_i < 0. \end{cases}$$

Приклад. Виконати віднімання двох чисел в СЗК. C=A-B.

$A = 17 = (2, 2, 3)_{(3, 5, 7)}$,

$B = 6 = (0, 1, 6)_{(3, 5, 7)}$,

$C = (2 - 0, 2 - 1, 3 - 6 + 7) = (2, 1, 4)_{(3, 5, 7)}$.

$C = 11 = (2, 1, 4)_{(3, 5, 7)}$.

В результаті послідовного застосування прямого та зворотного перетворень для цілочисельної форми СЗК отримаємо вихідне число в позиційній системі числення.

Представлення даних в системі залишкових класів дає змогу здійснювати розпаралелювання обробки інформації без значного ускладнення обчислювальних засобів. Використання СЗК спрощує побудову систем збору інформації, а також дозволяє вирішувати клас задач, що є невизначеними в позиційних системах числення. Особливістю СЗК залишається простота реалізації прямого та зворотного перетворень.

Контрольні запитання

1. Назвіть переваги та недоліки СЗК ?
2. Переведіть задані числа з десяткової СЧ в СЗК.
3. Переведіть задані числа з СЗК в десяткову СЧ.
4. Виконайте арифметичні операції в СЗК.