

Занятие № 3 (Лекции 5, 6).

Методы перевода чисел из ПСС в СОК и обратно

Методы перевода чисел из ПСС в СОК

Первый метод. Метод основан на использовании формулы

$$a_i = A - \left[\frac{A}{m_i} \right] \cdot m_i \quad \text{для } i = \overline{1, n}.$$

В этом случае из исходного числа A для набора оснований СОК $\{m_i\}$ получаем совокупность остатков $\{a_i\}$, $i = \overline{1, n}$. Число в СОК представится в виде $A = (a_1, a_2, \dots, a_n)$.

Второй метод. Метод осуществляется с помощью набора констант, являющихся эквивалентами оснований P ПСС, которые представляются в СОК.

Пусть задано число A в ПСС

$$A = (a_r \cdot P^r + a_{r-1} \cdot P^{r-1} + \dots + a_1 \cdot P + a_0) = \sum_{i=0}^r a_i \cdot P_i,$$

$$a_i = \overline{1, P-1},$$

пусть основание ПСС представляется в СОК по основаниям

m_1, m_2, \dots, m_n

$$P^{(i)} = [\beta_1^{(i)}, \beta_2^{(i)}, \dots, \beta_n^{(i)}], \quad i = \overline{1, r}.$$

Величины $a_i = [\alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_n^{(i)}]$ представлены также в СОК.

Число $A = (Q_1, Q_2, \dots, Q_n)$ (1) представляется в СОК, где

$$Q_j = \sum_{i=0}^r (\alpha_j^{(i)} \cdot \beta_j^{(i)}) \quad (2), \quad j = \overline{1, n}.$$

Для образования числа A в СОК требуется r констант, являющихся степенями оснований P ПСС и $(P-1)$ констант, соответствующих возможным значениям коэффициентов a_i , т.е. в общем случае необходимо всего $(r + P - 1)$ констант.

Пример реализации второго метода преобразования чисел из ПСС в СОК.

Перевести число $A = 102$ из десятичной ПСС в СОК с основаниями $m_1 = 3$, $m_2 = 5$, $m_3 = 7$.

Константы для значений r и P представляются в следующем виде

$$P^0 = 1 = (1, 1, 1), P^1 = 10 = (1, 0, 3), P^2 = 100 = (1, 0, 2);$$

$$a_0 = 2 = (2, 2, 2), a_1 = 0 = (0, 0, 0), a_2 = 1 = (1, 1, 1).$$

Тогда в соответствии с выражениями (1, 2 слайд 3) имеем, что

$$A = \left[\begin{array}{c} \underbrace{(2 \boxtimes 1 \boxplus 0 \cdot 1 + 1 \boxtimes 1)}_{m_1=3}, \underbrace{(2 \boxtimes 1 \boxplus 0 \cdot 0 + 1 \cdot 0)}_{m_2=5}, \underbrace{(2 \boxtimes 1 \boxplus 0 \cdot 3 + 1 \cdot 2)}_{m_1=7} \end{array} \right] = (0, 2, 4)$$

Проверка: $A = 102 = (0, 2, 4)$.

Метод перевода чисел из СОК в ПСС

Пусть задана СОК основаниями m_1, m_2, \dots, m_n . Зададим n чисел B_1, B_2, \dots, B_n в СОК, где $B_j = [b_1^{(j)}, b_2^{(j)}, \dots, b_n^{(j)}]$, $j = \overline{1, n}$, которые называются базисами СОК.

Это одни из основных констант СОК. Они рассчитываются заранее по основаниям СОК и хранятся в ПЗУ в СОК и в ПСС.

Пусть необходимо перевести число $A = (a_1, a_2, \dots, a_n)$ из СОК в ПСС. Задача перевода заключается в том, что необходимо определить числа $\mu_1, \mu_2, \dots, \mu_n$, такие, что

$$\mu_1 \cdot B_1 + \mu_2 \cdot B_2 + \dots + \mu_n \cdot B_n = A. \quad (1)$$

Перепишем выражение (1) в СОК

$$\mu_1 \cdot [b_1^{(1)}, b_2^{(1)}, \dots, b_n^{(1)}] + \mu_2 \cdot [b_1^{(2)}, b_2^{(2)}, \dots, b_n^{(2)}] + \dots \\ \dots \mu_n \cdot [b_1^{(n)}, b_2^{(n)}, \dots, b_n^{(n)}] = [a_1, a_2, \dots, a_n].$$

Для определения величины μ_i , $i = \overline{1, n}$, необходимо решить систему линейных алгебраических уравнений

$$\begin{cases} \mu_1 \cdot b_1^{(1)} + \mu_2 \cdot b_1^{(2)} + \dots + \mu_n \cdot b_1^{(n)} = a_1, \\ \mu_1 \cdot b_2^{(1)} + \mu_2 \cdot b_2^{(2)} + \dots + \mu_n \cdot b_2^{(n)} = a_2, \\ \dots \\ \mu_1 \cdot b_n^{(1)} + \mu_2 \cdot b_n^{(2)} + \dots + \mu_n \cdot b_n^{(n)} = a_n. \end{cases}$$

Система уравнений будет иметь целые решения, если определитель матрицы будет равен ± 1 , т.е.

$$\begin{vmatrix} b_1^{(1)} & b_1^{(2)} & \dots & b_1^{(n)} \\ b_2^{(1)} & b_2^{(2)} & \dots & b_2^{(n)} \\ & \dots & & \\ b_n^{(1)} & b_n^{(2)} & \dots & b_n^{(n)} \end{vmatrix} = \pm 1.$$

Имеется большой выбор величин b_1, b_2, \dots, b_n , поскольку любая возможная система величин $b_j^{(i)}$ приемлема в качестве базиса. В частности, в качестве базисов СОК предполагаются следующие величины $B_1 = (1, 0, 0, \dots, 0)$, $B_2 = (0, 1, 0, \dots, 0) \dots B_n = (0, 0, 0, \dots, 0, 1)$. Их называют ортогональные базисы. В этом случае для ортогональных базисов получим

$$\left\{ \begin{array}{l} \mu_1 = a_1, \\ \mu_2 = a_2, \\ \boxtimes \\ \mu_n = a_n. \end{array} \right. \quad \left| \begin{array}{cccc} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ & \boxtimes & & & \\ 0 & 0 & 0 & \dots & 1 \end{array} \right| = 1$$

Откуда, $A = (a_1 \cdot B_1 + a_2 \cdot B_2 + \dots + a_n \cdot B_n) \bmod M$, $M = \prod_{i=1}^n m_i$.

Пример

Задана СОК $m_1 = 3$, $m_2 = 5$ и $m_3 = 7$. $M = 3 \cdot 5 \cdot 7 = 105$.

Перевести число $A = (2, 3, 5)$ в десятичную ПСС. Ортогональные базисы имеют вид $B_1 = (1, 0, 0) = 70$, $B_2 = (0, 1, 0) = 21$, $B_3 = (0, 0, 1) = 15$.

$$\begin{aligned} A = (2, 3, 5) &= 2 \cdot B_1 + 3 \cdot B_2 + 5 \cdot B_3 = \\ &= 2 \cdot 70 + 3 \cdot 21 + 5 \cdot 15 = 278 = 68(\text{mod } 105). \end{aligned}$$

Для того чтобы реализовать процедуру перевода чисел из СОК в ПСС необходимо определить B_i ($i = \overline{1, n}$).

По определению ортогональных базисов они могут быть представленными в виде

$$B_i = (0, 0, \dots, 0, 1, 0, \dots, 0, 0), \quad B_i = \frac{\overline{m}_i \cdot M}{m_i}, \quad i = \overline{1, n}, \quad \text{где } \overline{m}_i \text{ – целое}$$

положительное число (вес ортогонального базиса).

Причём \overline{m}_i выбирается таким образом, чтобы имело место сравнение

$$\frac{\overline{m}_i \cdot M}{m_i} \equiv 1 \pmod{m_i} \quad \text{или} \quad \frac{\overline{m}_i \cdot M}{m_i} = l_i m_i + 1. \quad (2)$$

Вариант вычисления веса \overline{m}_i ортогонального базиса.

Введём обозначение $M_i = \frac{M}{m_i}$. Разделим M_i на m_i . Так как значение M_i составлено из множителей взаимно простых с m_i , оно нацело не делится, т.е. будет определенным остаток δ_i . Тогда в соответствии с формулой (2) значение \overline{m}_i округлится как результат решения сравнения

$$\overline{m}_i \cdot \delta_i \equiv 1 \pmod{m_i}.$$

Ввиду малости оснований m_i , δ_i СОК, значение \overline{m}_i выбирается по числу δ_i табличным образом (или перебором).

Общий алгоритм определения B_i .

1. По значениям $\{m_i\}$, определяем $M = \prod_{i=1}^n m_i$.

2. Определяем значения $M_i = \frac{M}{m_i}$.

3. Вычисляем значения $\delta_i \equiv M_i \pmod{m_i}$.

4. По значениям δ_i в выражении $\overline{m_i} \cdot \delta_i \equiv 1 \pmod{m_i}$ подбираем (перебором) значение $\overline{m_i}$.

5. $B_i = \overline{m_i} \cdot M_i$.

Для контроля вычислений ортогональных базисов B_i можно воспользоваться соотношением

$$\sum_{i=1}^n B_i = 1 \pmod{M}.$$

Метод определения ортогональных базисов

В соответствии с общим алгоритмом для СОК заданной основаниями $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ и $m_4 = 17$ ($n = 4$), определим ортогональные базисы B_i ($i = \overline{1, n}$). Провести проверку правильности полученного результата.

1. Определение значения модуля

$$M = \prod_{i=1}^n m_i = \prod_{i=1}^4 m_i = 3 \cdot 5 \cdot 7 \cdot 17 = 1785.$$

2. Определение частных значений модулей M_i ($i = \overline{1, n}$)

$$M_i = M / m_i:$$

$$M_1 = M / m_1 = 5 \cdot 7 \cdot 17 = 595;$$

$$M_2 = M / m_2 = 3 \cdot 7 \cdot 17 = 357;$$

$$M_3 = M / m_3 = 3 \cdot 5 \cdot 17 = 255;$$

$$M_4 = M / m_4 = 3 \cdot 5 \cdot 7 = 105. \quad 13$$

3. Определим значения $\delta_i = M_i \pmod{m_i}$ для $i = \overline{1, 4}$:

$$\delta_1 = M_1 \pmod{m_1} = 595 \pmod{3} = 1;$$

$$\delta_2 = M_2 \pmod{m_2} = 357 \pmod{5} = 2;$$

$$\delta_3 = M_3 \pmod{m_3} = 255 \pmod{7} = 3;$$

$$\delta_4 = M_4 \pmod{m_4} = 105 \pmod{17} = 3.$$

4. Исходя из условия $\overline{m}_i \cdot \delta_i = 1(\text{mod } m_i)$ определим веса \overline{m}_i ($i = \overline{1, 4}$) ортогональных базисов B_i , где $\overline{m}_i = \overline{1, m_i - 1}$.

$$\overline{m}_1 \cdot \delta_1 = 1(\text{mod } m_1); \delta_1 = 1; \overline{m}_1 = \overline{1, 2}; m_1 = 3.$$

$$\overline{m}_1 = 1; \delta_1 = 1; \overline{m}_1 \cdot \delta_1 = (\overline{m}_1 \cdot 1) \text{mod } m_1 = (1 \cdot 1) \text{mod } 3 = 1(\text{mod } 3) = 1;$$

$$\overline{m}_1 = 2; \delta_1 = 1; \overline{m}_1 \cdot \delta_1 = (\overline{m}_1 \cdot 1) \text{mod } m_1 = (2 \cdot 1) \text{mod } 3 = 2(\text{mod } 3) = 2.$$

$$\boxed{\overline{m}_1 = 1}$$

$$\underline{\overline{m_2} \cdot \delta_2 = 1(\text{mod } m_2); \delta_2 = 2; \overline{m_2} = \overline{1, 4}; m_2 = 5.}$$

$$\overline{m_2} = 1; \delta_2 = 1; \overline{m_2} \cdot \delta_2 (\text{mod } m_2) = (1 \cdot 2) \text{mod } 5 = 2(\text{mod } 5) = 2;$$

$$\overline{m_2} = 2; \delta_2 = 1; \overline{m_2} \cdot \delta_2 (\text{mod } m_2) = (2 \cdot 2) \text{mod } 5 = 4(\text{mod } 5) = 4;$$

$$\overline{m_2} = 3; \delta_2 = 2; \overline{m_2} \cdot \delta_2 (\text{mod } m_2) = (3 \cdot 2) \text{mod } 5 = 6(\text{mod } 5) = 1;$$

$$\overline{m_2} = 4; \delta_2 = 2; \overline{m_2} \cdot \delta_2 (\text{mod } m_2) = (4 \cdot 2) \text{mod } 5 = 8(\text{mod } 5) = 3.$$

$$\boxed{\overline{m_2} = 3}$$

$$\underline{\overline{m_3} \cdot \delta_3 = 1(\text{mod } m_3); \delta_3 = 3; \overline{m_3} = \overline{1, 6}; m_3 = 7.}$$

$$\overline{m_3} = 1; \delta_3 = 1; \overline{m_3} \cdot \delta_3(\text{mod } m_3) = (1 \cdot 3) \text{mod } 7 = 3(\text{mod } 7) = 3;$$

$$\overline{m_3} = 2; \delta_3 = 1; \overline{m_3} \cdot \delta_3(\text{mod } m_3) = (2 \cdot 3) \text{mod } 7 = 6(\text{mod } 7) = 6;$$

$$\overline{m_3} = 3; \delta_3 = 3; \overline{m_3} \cdot \delta_3(\text{mod } m_3) = (3 \cdot 3) \text{mod } 7 = 9(\text{mod } 7) = 2;$$

$$\overline{m_3} = 4; \delta_3 = 3; \overline{m_3} \cdot \delta_3(\text{mod } m_3) = (4 \cdot 3) \text{mod } 7 = 12(\text{mod } 7) = 5;$$

$$\overline{m_3} = 5; \delta_3 = 3; \overline{m_3} \cdot \delta_3(\text{mod } m_3) = (5 \cdot 3) \text{mod } 7 = 15(\text{mod } 7) = 1;$$

$$\overline{m_3} = 6; \delta_3 = 3; \overline{m_3} \cdot \delta_3(\text{mod } m_3) = (6 \cdot 3) \text{mod } 7 = 18(\text{mod } 7) = 4.$$

$$\boxed{\overline{m_3} = 5}$$

$$\underline{\overline{m_4} \cdot \delta_4 = 1(\text{mod } m_4); \delta_4 = 3; \overline{m_4} = \overline{1, 16}; m_4 = 17.}$$

$$\overline{m_4} = 1; \delta_4 = 3; (1 \cdot 3) \text{mod } 17 = 3(\text{mod } 17) = 3;$$

$$\overline{m_4} = 2; \delta_4 = 3; (2 \cdot 3) \text{mod } 17 = 6(\text{mod } 17) = 6;$$

$$\overline{m_4} = 3; \delta_4 = 3; (3 \cdot 3) \text{mod } 17 = 9(\text{mod } 17) = 9;$$

$$\overline{m_4} = 4; \delta_4 = 3; (4 \cdot 3) \text{mod } 17 = 12(\text{mod } 17) = 12;$$

$$\overline{m_4} = 5; \delta_4 = 3; (5 \cdot 3) \text{mod } 17 = 15(\text{mod } 17) = 15;$$

$$\overline{m_4} = 6; \delta_4 = 3; (6 \cdot 3) \text{mod } 17 = 18(\text{mod } 17) = 1;$$

$$\overline{m_4} = 7; \delta_4 = 3; (7 \cdot 3) \text{mod } 17 = 21(\text{mod } 17) = 4;$$

$$\overline{m_4} = 8; \delta_4 = 3; (8 \cdot 3) \text{mod } 17 = 24(\text{mod } 17) \stackrel{18}{=} 17;$$

$$\overline{m}_4 = 9; \delta_4 = 3; (9 \cdot 3) \bmod 17 = 27 \bmod 17 = 10;$$

$$\overline{m}_4 = 10; \delta_4 = 3; (10 \cdot 3) \bmod 17 = 30 \bmod 17 = 13;$$

$$\overline{m}_4 = 11; \delta_4 = 3; (11 \cdot 3) \bmod 17 = 33 \bmod 17 = 16;$$

$$\overline{m}_4 = 12; \delta_4 = 3; (12 \cdot 3) \bmod 17 = 36 \bmod 17 = 2;$$

$$\overline{m}_4 = 13; \delta_4 = 3; (13 \cdot 3) \bmod 17 = 39 \bmod 17 = 5;$$

$$\overline{m}_4 = 14; \delta_4 = 3; (14 \cdot 3) \bmod 17 = 42 \bmod 17 = 8;$$

$$\overline{m}_4 = 15; \delta_4 = 3; (15 \cdot 3) \bmod 17 = 45 \bmod 17 = 11;$$

$$\overline{m}_4 = 16; \delta_4 = 3; (16 \cdot 3) \bmod 17 = 48 \bmod 17 = 14.$$

$$\boxed{\overline{m}_4 = 6}$$

5. Определяем значения ортогональных базисов $B_i = \overline{m}_i \cdot M_i$
($i = \overline{1, n}$)

$$B_1 = \overline{m}_1 \cdot M_1 = 1 \cdot 595 = 595;$$

$$B_2 = \overline{m}_2 \cdot M_2 = 3 \cdot 357 = 1071;$$

$$B_3 = \overline{m}_3 \cdot M_3 = 5 \cdot 255 = 1275;$$

$$B_4 = \overline{m}_4 \cdot M_4 = 6 \cdot 105 = 630.$$

Проверка:

$$\begin{aligned}(B_1 + B_2 + B_3 + B_4) \bmod M &= (595 + 1071 + 1275 + 630) \bmod 1785 = \\ &= 3571 \bmod 1785 = 1\end{aligned}$$

Пример.

Перевести число $A_{СОК} = (2, 3, 4, 1)$ из СОК, заданной основаниями $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ и $m_4 = 7$ в десятичную ПСС.

I этап. Необходимо определить значения ортогональных базисов B_i ($i = \overline{1, n}$).

$$1. M = \prod_{i=1}^4 m_i = 3 \cdot 4 \cdot 5 \cdot 7 = 420.$$

2. Определим $M_i = M / m_i$

$$M_1 = M / m_1 = 420 / 3 = 4 \cdot 5 \cdot 7 = 140;$$

$$M_2 = M / m_2 = 420 / 4 = 3 \cdot 5 \cdot 7 = 105;$$

$$M_3 = M / m_3 = 420 / 5 = 3 \cdot 4 \cdot 7 = 84;$$

$$M_4 = M / m_4 = 420 / 7 = 3 \cdot 4 \cdot 5 = 60.$$

3. Определим значения $\delta_i = M_i \pmod{m_i}$

$$\delta_1 = M_1 \pmod{m_1} = 140 \pmod{3} = 2;$$

$$\delta_2 = M_2 \pmod{m_2} = 105 \pmod{4} = 1;$$

$$\delta_3 = M_3 \pmod{m_3} = 84 \pmod{5} = 4;$$

$$\delta_4 = M_4 \pmod{m_4} = 60 \pmod{4} = 4.$$

4. Исходя из условия $\overline{m}_i \cdot \delta_i = 1$ определим веса \overline{m}_i

ортогональных базисов B_i ($i = \overline{1, 4}$).

$$\overline{m}_1 = 1; \delta_1 = 2; (\overline{m}_1 \cdot \delta_1) \bmod m_1 = (1 \cdot 2) \bmod 3 = 2 \pmod{3} = 2;$$

$$\overline{m}_1 = 2; \delta_1 = 2; (\overline{m}_1 \cdot \delta_1) \bmod m_1 = (2 \cdot 2) \bmod 3 = 4 \pmod{3} = 1.$$

$$\boxed{\overline{m}_1 = 2}$$

$$\overline{m_2} = 1; \delta_2 = 1; (\overline{m_2} \cdot \delta_2) \bmod m_2 = (1 \cdot 1) \bmod 4 = 1(\bmod 4) = 1;$$

$$\overline{m_2} = 2; \delta_2 = 1; (\overline{m_2} \cdot \delta_2) \bmod m_2 = (2 \cdot 1) \bmod 4 = 2(\bmod 4) = 2;$$

$$\overline{m_2} = 3; \delta_2 = 1; (\overline{m_2} \cdot \delta_2) \bmod m_2 = (3 \cdot 1) \bmod 4 = 3(\bmod 4) = 3.$$

$$\boxed{\overline{m_2} = 1}$$

$$\overline{m_3} = 1; \delta_3 = 4; (\overline{m_3} \cdot \delta_3) \bmod m_3 = (1 \cdot 4) \bmod 5 = 4(\bmod 5) = 4;$$

$$\overline{m_3} = 2; \delta_3 = 4; (\overline{m_3} \cdot \delta_3) \bmod m_3 = (2 \cdot 4) \bmod 5 = 8(\bmod 5) = 3;$$

$$\overline{m_3} = 3; \delta_3 = 4; (\overline{m_3} \cdot \delta_3) \bmod m_3 = (3 \cdot 4) \bmod 5 = 12(\bmod 5) = 2;$$

$$\overline{m_3} = 4; \delta_3 = 4; (\overline{m_3} \cdot \delta_3) \bmod m_3 = (4 \cdot 4) \bmod 5 = 16(\bmod 5) = 1.$$

$$\boxed{\overline{m_3} = 4}$$

$$\overline{m_4} = 1; \delta_4 = 4; (\overline{m_4} \cdot \delta_4) \bmod m_4 = (1 \cdot 4) \bmod 7 = 4(\bmod 7) = 4;$$

$$\overline{m_4} = 2; \delta_4 = 4; (\overline{m_4} \cdot \delta_4) \bmod m_4 = (2 \cdot 4) \bmod 7 = 8(\bmod 7) = 1;$$

$$\overline{m_4} = 3; \delta_4 = 4; (\overline{m_4} \cdot \delta_4) \bmod m_4 = (3 \cdot 4) \bmod 7 = 12(\bmod 7) = 5;$$

$$\overline{m_4} = 4; \delta_4 = 4; (\overline{m_4} \cdot \delta_4) \bmod m_4 = (4 \cdot 4) \bmod 7 = 16(\bmod 7) = 2;$$

$$\overline{m_4} = 5; \delta_4 = 4; (\overline{m_4} \cdot \delta_4) \bmod m_4 = (5 \cdot 4) \bmod 7 = 20(\bmod 7) = 6;$$

$$\overline{m_4} = 6; \delta_4 = 4; (\overline{m_4} \cdot \delta_4) \bmod m_4 = (6 \cdot 4) \bmod 7 = 24(\bmod 7) = 3.$$

$$\boxed{\overline{m_4} = 2}$$

5. Определяем ортогональные базисы $B_i = \overline{m}_i \cdot M_i$ ($i = \overline{1, n}$)

$$B_1 = \overline{m}_1 \cdot M_1 = 2 \cdot 140 = 280;$$

$$B_2 = \overline{m}_2 \cdot M_2 = 1 \cdot 105 = 105;$$

$$B_3 = \overline{m}_3 \cdot M_3 = 4 \cdot 84 = 336;$$

$$B_4 = \overline{m}_4 \cdot M_4 = 2 \cdot 60 = 120.$$

Проверка:

$$\begin{aligned}(B_1 + B_2 + B_3 + B_4) \bmod M &= (280 + 105 + 336 + 120) \bmod 420 = \\ &= 841 \pmod{420} = 1\end{aligned}$$

II этап. Представим число $A_{СОК} = (2, 3, 4, 1)$ в ПСС

$$A_{ПСС} = (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 + a_4 \cdot B_4) \bmod M =$$

$$= (2 \cdot 280 + 3 \cdot 105 + 4 \cdot 336 + 1 \cdot 120) \bmod 420 =$$

$$= (560 + 315 + 1344 + 120) \bmod 420 = 2339 \pmod{420} = 239 < 420.$$

Проверка: число $A_{ПСС} = 239$ в ПСС представляется в СОК в виде

$$A_{СОК} = (2, 3, 4, 1).$$