**УДК 681.142**

*В.А. КРАСНОБАЕВ, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук,*
*А.С. ЯНКО, канд. техн. наук*

# ПРИМЕРЫ ОПРЕДЕЛЕНИЯ РАНГА ЧИСЛА, ПРЕДСТАВЛЕННОГО В НЕПОЗИЦИОННОЙ СИСТЕМЕ СЧИСЛЕНИЯ ОСТАТОЧНЫХ КЛАССОВ

## Введение

Для решения вычислительных задач при использовании системы остаточных классов (СОК) часто возникает необходимость реализации немодульных (позиционных) операций, т.е. таких операций, которые требуют знания величин чисел [1, 2]. К таким операциям, прежде всего, относятся следующие: арифметическое и алгебраическое сравнение чисел, определение знака числа, определение местоположения числа на числовой оси, деление чисел, операции с дробной частью чисел, округление чисел, определение переполнения разрядной сетки, контроль данных в СОК и пр. [3, 4].

Для реализации позиционных операций в СОК используются так называемые позиционные признаки непозиционного кода (ППНК) (позиционные характеристики числа в СОК) [4-6]. В частности, в качестве ППНК может служить ранг $r_A$ числа $A=(a_1, a_2, ..., a_n)$ [1]. В СОК существуют две разновидности ранга числа.

*Определение 1.* Истинным рангом $r_A$ числа (или просто – рангом $r_A$ числа) $A$ называют натуральное число, показывающее, сколько раз числовой диапазон $M=\prod_{i=1}^{n} m_i$ системы обработки данных (СОД) был превзойден при переходе от представления числа $A$ в СОК к его представлению в ПСС через систему ортогональных базисов $B_i$.

*Определение 2.* Ранг числа, являющийся результатом арифметической операции, полученный из рангов чисел называется расчетным рангом числа.

В статье рассматривается только методы определения истинного ранга $r_A$ числа в СОК. Рассмотрим два метода определения ранга числа в СОК [1].

*Первый метод.* Пусть задана СОК своими основаниями $m_i$ $(i=\overline{1,n})$. Данной СОК однозначно соответствует система ортогональных базисов, $B_i$ $(i=\overline{1,n})$, при которой выполняется равенство

$$A_{ПСС}=\left\{\sum_{i=1}^{n} a_i \cdot B_i\right\} \bmod M \cdot \tag{1}$$

Соотношение (1) можно представить в виде

$$A_{ПСС}=\sum_{i=1}^{n} a_i \cdot B_i - r_A \cdot M \tag{2}$$

Первый метод определения истинного ранга $r_A$ числа основывается на реализации соотношения (2), т.е. требуется осуществить операцию перехода от непозиционного к позиционному представлению числа.

Недостаток первого метода состоит в следующем. При реализации системой обработки данных (СОД) в СОК предполагается, что величина ранга $r_A$ чисел $A$ будет определяться непосредственно в процессе выполнения машинных операций. В этом аспекте рассмотрен-

ный первый метод определения ранга числа по формуле (2) требует выполнения позиционной операции определения величины числа $A$, что нарушает общую процедуру непозиционной обработки данных СОД (снижается время реализации арифметических операций в СОК).

**Основная часть**

*Второй метод.* Использование этого метода позволяет определить ранг $r_A$ числа в СОК без перехода к позиционному представлению числа.

Предварительно, перед описанием метода определения ранга числа в СОК, рассмотрим следующее утверждение. Если в СОК заданы два числа $A=(a_1, a_2, ..., a_n)$ и $B=(b_1, b_2, ..., b_n)$ с соответствующими рангами $r_A$ и $r_B$, то ранг $r_{A+B}$ суммы двух чисел $A+B$ определится следующим образом:

$$r_{A+B} = r_A + r_B - \sum_{i=1}^{n}\left[\frac{a_i + b_i}{m_i}\right]\cdot \overline{m_i}, \tag{3}$$

где значение $\overline{m_i}$ определяет вес *i*-го ортогонального базиса $B_i$ СОК.

Покажем правильность соотношения (3). Запишем выражения для определения рангов чисел $A_{ПСС}$ и $B_{ПСС}$ в виде (2):

$$A_{ПСС} = \sum_{i=1}^{n} a_i \cdot B_i - r_A \cdot M, \tag{4}$$

$$B_{ПСС} = \sum_{i=1}^{n} b_i \cdot B_i - r_B \cdot M \cdot \tag{5}$$

Сложим два соотношения (4) и (5):

$$A_{ПСС} + B_{ПСС} = \sum_{i=1}^{n} a_i \cdot B_i - r_A \cdot M + \sum_{i=1}^{n} b_i \cdot B_i - r_B \cdot M, \text{ или}$$

$$A_{ПСС} + B_{ПСС} = \sum_{i=1}^{n} (a_i + b_i) \cdot B_i - (r_A + r_B) \cdot M \cdot \tag{6}$$

С другой стороны, на основании правила вычисления суммы двух чисел в СОК для каждого соответствующего основания можно записать

$$A+B = \left\{\left(a_1 + b_1 - \left[\frac{a_1 + b_1}{m_1}\right]\cdot m_1\right), \left(a_2 + b_2 - \left[\frac{a_2 + b_2}{m_2}\right]\cdot m_2\right), ... \right.$$
$$\left. ..., \left(a_n + b_n - \left[\frac{a_n + b_n}{m_n}\right]\cdot m_n\right)\right\}. \tag{7}$$

Выражение (7) можно представить в виде (см. (2)):

$$A+B = \sum_{i=1}^{n}\left(\left\{\left(a_i + b_i\right) - \left[\frac{a_i + b_i}{m_i}\right]\cdot m_i\right\}\right) \times B_i - r_{A+B}\cdot M. \tag{8}$$

Преобразуем выражение (8) с учетом того, что $B_i = \dfrac{\overline{m_i}\cdot M}{m_i}$, и получим

$$A+B=\sum_{i=1}^{n}(a_i+b_i)\cdot B_i-\sum_{i=1}^{n}\left[\frac{a_i+b_i}{m_i}\right]\cdot m_i\cdot B_i-r_{A+B}\cdot M\cdot \tag{9}$$

или
$$A+B=\sum_{i=1}^{n}(a_i+b_i)\cdot B_i-\sum_{i=1}^{n}\left[\frac{a_i+b_i}{m_i}\right]\cdot m_i\cdot\frac{\overline{m_i}\cdot M}{m_i}-r_{A+B}\cdot M\cdot \tag{10}$$

Сравним правые части соотношений (6) и (10) и получим

$$\sum_{i=1}^{n}(a_i+b_i)\cdot B_i-(r_A+r_B)\cdot M=$$

$$=\sum_{i=1}^{n}(a_i+b_i)\cdot B_i-\sum_{i=1}^{n}\left[\frac{a_i+b_i}{m_i}\right]\cdot\overline{m_i}\cdot M-r_{A+B}\cdot M\text{, т.е.}$$

$$r_{A+B}=r_A+r_B-\sum_{i=1}^{n}\left[\frac{a_i+b_i}{m_i}\right]\cdot\overline{m_i}\ . \tag{11}$$

Соотношение (11) является основным аналитическим выражением, позволяющим определить ранг $r_{A+B}$ суммы двух чисел $A$ и $B$ по значениям рангов $r_A$, $r_B$ слагаемых $A$ и $B$.

Очевидно, что

$$a_i+b_i\ge m_i\text{, то }\left[\frac{a_i+b_i}{m_i}\right]=1, \tag{12}$$

$$a_i+b_i<m_i\text{, то }\left[\frac{a_i+b_i}{m_i}\right]=0\cdot \tag{13}$$

Последовательность определения ранга $r_A$ числа состоит в следующем.

К исходному числу $A=(a_1,a_2,...,a_n)$ в СОК, ранг $r_A$ которого необходимо определить, последовательно прибавляются константы $t^{(i)}$ $(i=\overline{1,n})$, представленные в СОК, в виде минимальных чисел типа $t^{(i)}=(0,0,...,0,t_i,t_{i+1},...,t_n)$. В этом случае эта величина в ПСС $t^{(\mathrm{i})}_{ПСС}=m_1\cdot m_2\cdot...\cdot m_{i-1}$

В частности, получим

$$t^{(1)}=\min(t_1,t_2,...,t_n)=(1,1,...,1);$$
$$t^{(2)}=\min(0,t_2',...,t_n')=(0,m_1,m_2,...,m_{i-1});$$
$$t^{(3)}=\min(0,0,t_3'',t_4'',...,t_n'')=\{(0,0,m_1\cdot m_2(\mathrm{mod}\,m_3),$$
$$m_1\cdot m_2(\mathrm{mod}\,m_4),...,m_1\cdot m_2(\mathrm{mod}\,m_n)\}$$

и т.д., где $t^{(n)}=(0,0,...,0,t_n)$. В ПСС это значение равно $t^{(\mathrm{n})}_{ПСС}=m_1\cdot m_2\cdot...\cdot m_{n-1}$. Числа $t^{(i)}$ и их ранги $r_i$ определяются основаниями $m_1,m_2,...m_n$ заданной СОК [3].

Покажем, процедуру получения значения $A_n=(0,0,...,0)$. Вначале процедуры к исходному числу $A$ прибавляем константу $t^{(1)}=(t_1,t_2,...,t_n)$ столько раз, сколько потребуется

для того, чтобы выполнялось условие $a_1 = 0$. Пусть для этого потребуется $k_1$ сложений типа $A + t^{(1)}$. В этом случае получим

$$A_1 = A + k_1 \cdot t^{(1)}.$$

В результате число $A_1$ имеет ранг $r_{A_1}$. По формуле (11) получим, что $r_{A_1} = r_A + w_1$, где $w_1$ – известная величина. Далее производим $k_2$ раз сложений величины константы $t^{(2)} = (0, t'_2, ..., t'_n)$ с числом $A_1$ до получения нулевого остатка по основанию $m_2$, т.е. получим $a_2 = 0$. Имеем число $A_2 = A_1 + k_2 \cdot t^{(2)}$ с рангом $r_{A_2} = r_A + w_2$, где $w_2$ – известная величина. Алгоритм получения числа $A = (0, 0, ..., 0)$ представлен соотношением

$$\begin{cases} A_1 = A + k_1 \cdot t^{(1)}, \\ \Gamma_{A_1} = \Gamma_A + \omega_1; \\ A_2 = A_1 + k_2 \cdot t^{(2)}, \\ \Gamma_{A_2} = \Gamma_{A_1} + \omega_2; \\ \quad ... \\ A_i = A_{i-1} + k_i \cdot t^{(i)}, \\ \Gamma_{A_i} = \Gamma_{A_{i-1}} + \omega_i; \\ \quad ... \\ A_n = A_{n-1} + k_n \cdot t^{(n)}, \\ \Gamma_{A_n} = \Gamma_{A_{n-1}} + \omega_n. \end{cases} \tag{14}$$

Продолжая процедуру по всем остаткам числа $A$, получим число $A = (0, 0, ..., 0) = M$. В этом случае значение $\omega_i$ $(i = \overline{1, n})$ – это известная величина, которая определяется последовательно в процессе преобразования исходного числа $A = (a_1, a_2, ..., a_n)$ в число $A_n = M = (0, 0, ..., 0)$.

В соответствии с выражением (2) имеем:

$$\begin{aligned} A_{ПСС} &= \sum_{i=1}^{n} a_i \cdot B_i - r_A \cdot M, \\ A_n &= \sum_{i=1}^{n} a_i B_i - r_A \cdot M, \\ (0, 0, ..., 0) &= \sum_{i=1}^{n} a_i B_i - r_A \cdot M, \\ M &= 0 - r_A \cdot M, \\ r_A &= -1. \end{aligned} \tag{15}$$

Таким образом, промежуточный ранг числа $A_n = (0, 0, ..., 0)$ – $r_A = -1$. С другой стороны, показано (14), что ранг равен $r_A + w_n$. В этом случае

$$r_A + w_n = -1, \tag{16}$$

$$r_A = -1 - w_n. \tag{17}$$

Тогда ранг $r_A$ числа $A=(a_1, a_2, ..., a_n)$ в СОК определится в соответствии с формулой (17).

Таким образом, суть второго метода определения ранга числа $A=(a_1, a_2, ..., a_n)$ состоит в следующем. К исходному числу $A=(a_1, a_2, ..., a_n)$ в СОК, ранг $r_A$ которого необходимо определить, последовательно прибавляя константы $t^{(i)}$ $(i=\overline{1, n})$ до тех пор, пока в конечном результате не получим число $A_n=(0, 0, ..., 0)$, промежуточный ранг которого $r_A=-1$. Далее, по формуле (17), определяется истинный ранг числа.

Приведем примеры определения ранга числа $A$. В табл. 1 представлены основания СОК $\{m_i\}$, $i=\overline{1, 3}$, ортогональные базисы $B_i$ и их веса $\overline{m_i}$. В табл. 2, для заданной СОК, даны минимальные константы $t^{(i)}$ и их ранги $r_{t^{(i)}}$. В этом случае $M=\prod_{i=1}^{3} m_i = 3\cdot 5\cdot 7 = 105$.

Таблица 1

| | | |
|---|---|---|
| $m_1=3$ | $m_2=5$ | $m_3=7$ |
| $\overline{m_1}=2$ | $\overline{m_2}=1$ | $\overline{m_3}=1$ |
| $B_1=70$ | $B_2=21$ | $B_3=15$ |

Таблица 2

| | | |
|---|---|---|
| $t^{(1)}=(1,1,1)$ | $t^{(2)}=(0,3,3)$ | $t^{(3)}=(0,0,1)$ |
| $r_1=1$ | $r_2=1$ | $r_3=0$ |

Ранги минимальных констант $t^{(i)}$ вычисляются заранее по формуле (2). Так, определим значения минимальных констант для СОК, заданной в табл.1:

$t^{(1)}=(1,1,1)=1\cdot B_1+1\cdot B_2+1\cdot B_3=(70+21+15)\bmod 105=106-r\cdot M==106-1\cdot 105.$

В этом случае $r_{t^{(1)}}=1$ (табл. 2).

$t^{(2)}=(0,3,3)=0\cdot B_1+3\cdot B_2+3\cdot B_3=0\cdot 70+3\cdot 21+3\cdot 15=108==3(\bmod 105)=108-r\cdot 105.$

В этом случае $r_{t^{(2)}}=1$ (табл. 2).

$t^{(3)}=(0,0,1)=0\cdot B_1+0\cdot B_2+1\cdot B_3=15=15-r\cdot 105$. В этом случае $r_{t^{(3)}}=0$ (табл. 2).

*Пример 1.* В соответствии с данными табл. 1, 2 найти ранг $r_A$ числа $A=(2,1,1)=71$.

I этап. Обнуление остатка $a_1=2$ по первому модулю $m_1=3$.

Сложим число $A$ с $t^{(1)}$.

$$A+t^{(1)}=(2,1,1)+(1,1,1)=(0,2,2).$$

Ранг суммы определится по формуле (11)

$$r=(r_A+r_{t^{(1)}})-\sum_{i=1}^{3}\left[\frac{a_i+b_i}{m_i}\right]\cdot\overline{m_i}=$$

$$=(r_A+r_{t^{(1)}})-\left\{\left[\frac{a_1+b_1}{m_1}\right]\cdot\overline{m_1}+\left[\frac{a_2+b_2}{m_2}\right]\cdot\overline{m_2}+\left[\frac{a_3+b_3}{m_3}\right]\cdot\overline{m_3}\right\}=$$

$$= (r_A + 1) - \left\{ \left[ \frac{2+1}{3} \right] \cdot 2 + \left[ \frac{1+1}{5} \right] \cdot 1 + \left[ \frac{1+1}{7} \right] \cdot 1 \right\} =$$
$$= (r_A + 1) - (1 \cdot 2 + 0 \cdot 1 + 0 \cdot 1) = r_A + 1 - 2 = r_A - 1.$$

При этом имел место один переход через первое основании $m_1$ (формулы (12), (13)).

II этап. Обнуление остатка $a_2 = 2$ по второму модулю $m_2 = 5$ числа $(0, 2, 2)$. Сложим два числа

$$(0, 2, 2) + t^{(2)} = (0, 2, 2) + (0, 3, 3) = (0, 0, 5).$$

Ранг суммы двух чисел определяется следующим образом

$$r = (r_A - 1) + r_{t^{(2)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$
$$= (r_A - 1) + r_{t^{(2)}} - \left\{ \left[ \frac{a_1 + b_1}{m_1} \right] \cdot \overline{m_1} + \left[ \frac{a_2 + b_2}{m_2} \right] \cdot \overline{m_2} + \left[ \frac{a_3 + b_3}{m_3} \right] \cdot \overline{m_3} \right\} =$$
$$= (r_A - 1 + 1 - \left\{ \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{2+3}{5} \right] \cdot 1 + \left[ \frac{2+3}{7} \right] \cdot 1 \right\} =$$
$$= r_A - (0 \cdot 2 + 1 \cdot 1 + 0 \cdot 1) = r_A - 1.$$

При этом имел место один переход через второе основание $m_2$.

III этап. Обнуление остатка $a_3 = 5$ числа $(0, 0, 5)$. Сложим два числа

$$(0, 0, 5) + t^{(3)} = (0, 0, 5) + (0, 0, 1) = (0, 0, 6).$$

Ранг суммы двух чисел

$$r = (r_A - 1) + r_{t^{(3)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$
$$= (r_A - 1) + r_{t^{(3)}} - \left\{ \left[ \frac{a_1 + b_1}{m_1} \right] \cdot \overline{m_1} + \left[ \frac{a_2 + b_2}{m_2} \right] \cdot \overline{m_2} + \left[ \frac{a_3 + b_3}{m_3} \right] \cdot \overline{m_3} \right\} =$$
$$= (r_A - 1) + 0 - \left\{ \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{0+0}{5} \right] \cdot 1 + \left[ \frac{5+1}{7} \right] \cdot 1 \right\} =$$
$$= r_A - 1 + 0 - 0 - 0 - 0 = r_A - 1.$$

Так как остаток $a_3 = 5$ числа $(0, 0, 5)$ не обнулился, то добавим еще раз значение $t^{(3)}$. Сложим два числа

$$(0, 0, 6) + t^{(3)} = (0, 0, 6) + (0, 0, 1) = (0, 0, 0).$$

Ранг суммы двух чисел

$$r = (r_A - 1) + r_{t^{(3)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$
$$= (r_A - 1) + r_{t^{(3)}} - \left\{ \left[ \frac{a_1 + b_1}{m_1} \right] \cdot \overline{m_1} + \left[ \frac{a_2 + b_2}{m_2} \right] \cdot \overline{m_2} + \left[ \frac{a_3 + b_3}{m_3} \right] \cdot \overline{m_3} \right\} =$$
$$= r_A - 1 + 0 + 0 + 0 + 1 \cdot 1 = r_A - 2.$$

При этом имел место один переход через третье $m_3$ основание СОК. В соответствии с (13) и (14) имеем

$$r_A - 2 = -1, \text{ или } r_A = 1.$$

Проверка (см.(2)).

$$A = (2,1,1) = 2 \cdot B_1 + 1 \cdot B_2 + 1 \cdot B_3 = 2 \cdot 70 + 1 \cdot 21 + 1 \cdot 15 = 176 - r_A \cdot M =$$
$$= 176 - 1 \cdot 105 = 176 - 105 = 71.$$

*Пример 2.* В соответствии с исходными данными (табл. 1, 2) найти ранг $r_A$ числа $A = (1,1,5) = 61$.

I этап. Обнулим остаток $a_1 = 1$ по первому модулю $m_1$. Сложим два числа (табл. 2):

$$A + t^{(1)} = (1,1,5) + (1,1,1) = (2,2,6).$$

Ранг суммы определится по формуле (11)

$$r = (r_A + r_{t^{(1)}}) - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= (r_A + r_{t^{(1)}}) - \left\{ \left[ \frac{a_1 + b_1}{m_1} \right] \cdot \overline{m_1} + \left[ \frac{a_2 + b_2}{m_2} \right] \cdot \overline{m_2} + \left[ \frac{a_3 + b_3}{m_3} \right] \cdot \overline{m_3} \right\} =$$

$$= (r_A + 1) - \left\{ \left[ \frac{1+1}{3} \right] \cdot 2 + \left[ \frac{1+1}{5} \right] \cdot 1 + \left[ \frac{5+1}{7} \right] \cdot 1 \right\} =$$

$$= (r_A + 1) - 0 \cdot 2 - 0 \cdot 1 + 0 \cdot 1 = r_A + 1.$$

Так как остаток $a_1 = 1$ числа $A = (1,1,5)$ не обнулился, то добавим еще раз значение контакта $t^{(1)}$. Сложим два числа

$$(2,2,6) + t^{(1)} = (2,2,6) + (1,1,1) = (0,3,0).$$

Ранг суммы двух этих чисел

$$r = r_A + 1 + r_{t^{(1)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= r_A + 1 + 1 - \left\{ \left[ \frac{a_1 + b_1}{m_1} \right] \cdot \overline{m_1} + \left[ \frac{a_2 + b_2}{m_2} \right] \cdot \overline{m_2} + \left[ \frac{a_3 + b_3}{m_3} \right] \cdot \overline{m_3} \right\} =$$

$$= r_A + 1 + 1 - 1 \cdot 2 - 0 \cdot 1 - 1 \cdot 1 = (r_A + 1) + 1 - 2 - 1 = r_A - 1.$$

При этом имели место два переходаи – через первое основание $m_1$ и через третье основание $m_3$.

II этап. Обнуление остатка $a_2 = 3$ числа $(0,3,0)$. Сложим два числа

$$(0,3,0) + t^{(2)} = (0,3,0) + (0,3,3) = (0,1,3).$$

Ранг суммы двух чисел определяется так

$$r = (r_A - 1) + r_{t^{(2)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= (r_A - 1) + r_{t^{(2)}} - \left\{ \left[ \frac{a_1 + b_1}{m_1} \right] \cdot \overline{m_1} + \left[ \frac{a_2 + b_2}{m_2} \right] \cdot \overline{m_2} + \left[ \frac{a_3 + b_3}{m_3} \right] \cdot \overline{m_3} \right\} =$$

$$= (r_A - 1) + 1 - \left\{ \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{3+3}{5} \right] \cdot 1 + \left[ \frac{0+3}{7} \right] \cdot 1 \right\} =$$

$$= r_A - 1 + 1 - 0 \cdot 2 - 1 \cdot 1 + 0 \cdot 1 = r_A - 1.$$

Имел место один переход через основание $m_2$.

Так, как остаток $a_2 = 3$ числа $(0, 3, 0)$ не обнулился, то сложим два числа:

$$(0, 1, 3) + t^{(2)} = (0, 1, 3) + (0, 3, 3) = (0, 4, 6).$$

Ранг суммы двух чисел

$$r = (r_A - 1) + r_{t^{(2)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= (r_A - 1) + 1 - \left\{ \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{1+3}{5} \right] \cdot 1 + \left[ \frac{3+3}{7} \right] \cdot 1 \right\} =$$

$$= r_A - 1 + 1 - (0 \cdot 2 + 0 \cdot 1 + 0 \cdot 1) = r_A.$$

Переходов (переполнений) по остаткам (основаниям) нет. Так как остаток $a_2 = 3$ числа $(0, 3, 0)$ не обнулился, то вновь сложим два числа

$$(0, 4, 6) + t^{(2)} = (0, 4, 6) + (0, 3, 3) = (0, 2, 2).$$

Ранг суммы двух чисел

$$r = r_A + r_{t^{(2)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= r_A + 1 - \left\{ \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{4+3}{5} \right] \cdot 1 + \left[ \frac{6+3}{7} \right] \cdot 1 \right\} =$$

$$= r_A + 1 - (0 \cdot 2 + 1 \cdot 1 + 1 \cdot 1) = r_A + 1 - 2 = r_A - 1.$$

Имеют место два перехода (переполнения) через основания $m_2$ и $m_3$.

Так, как остаток $a_2$ не обнулился, то реализуется операция сложения двух чисел:

$$(0, 2, 2) + t^{(2)} = (0, 2, 2) + (0, 3, 3) = (0, 0, 5).$$

Ранг суммы двух чисел

$$r = (r_A - 1) + r_{t^{(2)}} - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= (r_A - 1) + 1 - \left\{ \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{2+3}{5} \right] \cdot 1 + \left[ \frac{2+3}{7} \right] \cdot 1 \right\} =$$

$$= r_A - 1 + 1 - 0 \cdot 2 - 1 \cdot 1 - 0 \cdot 1 = r_A - 1 + 1 - 1 = r_A - 1.$$

Имело место одно переполнение по основанию $m_2$.

III этап. Обнуление остатка $a_3 = 5$ числа $(0, 0, 5)$. Сложим два числа

$$(0, 0, 5) + t^{(3)} = (0, 0, 5) + (0, 0, 1) = (0, 0, 6).$$

Ранг суммы двух чисел

$$r = (r_A - 1) + 0 - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= r_A - 1 + 0 - \left( \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{0+0}{5} \right] \cdot 1 + \left[ \frac{5+1}{7} \right] \cdot 1 \right) =$$

$$= r_A - 1 + 0 - 0 \cdot 2 - 0 \cdot 1 - 0 \cdot 1 = r_A - 1.$$

Переполнений основ не было. Так как остаток $a_3$ не обнулен, то реализуется операция сложения двух чисел:

$$(0, 0, 6) + t^{(3)} = (0, 0, 6) + (0, 0, 1) = (0, 0, 0).$$

Ранг суммы определится следующим образом:

$$r = (r_A - 1) + 0 - \sum_{i=1}^{3} \left[ \frac{a_i + b_i}{m_i} \right] \cdot \overline{m_i} =$$

$$= r_A - 1 + 0 - \left( \left[ \frac{0+0}{3} \right] \cdot 2 + \left[ \frac{0+0}{5} \right] \cdot 1 + \left[ \frac{6+1}{7} \right] \cdot 1 \right) =$$

$$= r_A - 1 + 0 - 0 \cdot 2 - 0 \cdot 1 - 1 \cdot 1 = r_A - 2.$$

Имеется одно переполнение в остатке $a_3$ по основанию $m_3$. В соответствии с (15) и (16)

$$r_A - 2 = -1,\ r_A = 1.$$

Проверка (см. (2)). $A = (1, 1, 5)$. В ПСС имеем, что

$$A = a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 = (1 \cdot 70 + 1 \cdot 21 + 5 \cdot 15) \bmod 105 =$$

$$= 166 - r_A \cdot 105 = 166 - 1 \cdot 105 = 61.$$

**Выводы**

Рассмотрены два метода определения ППНК СОК – ранга числа. Основное внимание уделено примерам реализации второго метода, преимуществом которого является то, что определение ранга числа можно проводить в динамике вычислительного процесса, т.е. без останова вычислений на время выполнения непозиционных операций перевода чисел из СОК в ПСС и обратно. Это дает возможность в полной мере использовать основное свойство СОК – высокое быстродействие выполнения арифметических операций. Сокращается количество оборудования, необходимого для реализации позиционных операций, что особенно важно для бортовых вычислителей баллистических ракет и космических аппаратов.

**Список литературы:**

1. Kuznetsov O., Gorbenko Y., Kolovanova I. Combinatorial properties of block symmetric ciphers key schedule // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016. pp. 55-58. DOI: 10.1109/INFOCOMMST.2016.7905334.

2. Sergey G. Rassomakhin. Mathematical and Physical Nature of Channel Capacity // ISCI'2017: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017. 207 p.

3. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. Москва : Сов. радио, 1968. 440 с.

4. Торгашов В. А. Система остаточных классов и надежность ЦВМ. Москва : Сов. радио, 1973. 118 с.

5. Krasnobayev V. A., Koshman S. A., Mavrina M. A. A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. November 2014. Vol. 50, Issue 6. pp 969-976.

6. Краснобаев В.А., Кошман С. А., Маврина М. А. Метод исправления однократных ошибок данных, представленных кодом класса вычетов // Электрон. моделирование. 2013. Т. 35. № 5. С. 43–56.

*Харьковский национальный*
*университет имени В.Н.Каразина*

*Поступила в редколлегию 07.03.2018*