УДК 681.142

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

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД ОПРЕДЕЛЕНИЯ АЛЬТЕРНАТИВНОЙ СОВОКУПНОСТИ ЧИСЕЛ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Введение

Современный этап развития науки и техники отличается все более сложными задачами, которые требуют быстрого решения. Однако сложность решаемых задач опережает темпы нарастания мощности универсальных компьютеров. В этом аспекте основным направлением совершенствования вычислительной системы обработки данных реального времени является повышение ее производительности. Известно, что одним из возможных направлений в разработке высокопроизводительных вычислительных систем является распараллеливание решаемых задач и алгоритмов на уровне арифметических микроопераций. Одним из вариантов распараллеливания является переход к вычислениям в нетрадиционной машинной арифметике с нетрадиционным представлением операндов. Из множества нетрадиционных арифметик наибольшее практическое применение в вычислительных системах нашла непозиционная система счисления остаточных классов (СОК) [1 – 3].

Совокупность положительных свойств СОК определяет следующие классы задач, в которых она существенно эффективнее позиционной арифметики: криптографические и модульные преобразования (реализация криптопреобразований в группе точек эллиптической кривой, а также для реализации алгоритма хеширования и генератора псевдослучайных чисел [4, 5]), обработка сигналов, обработка (сжатие) изображений, целочисленная обработка данных большой (сотни бит) разрядности в реальном времени, векторная и матричная обработка больших массивов информации, нейрокомпьютерная обработка информации, реализация алгоритмов БПФ и ДПФ и оптоэлектронная табличная обработка информации.

Известно, что в СОК существует необходимость определения альтернативной совокупности (АС) $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ неправильных $\tilde{A} = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ чисел. Под понятием АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ неправильного (искаженного) числа $\tilde{A} = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ понимается совокупность $\left\{ m_{l_\kappa} \right\}$ $(\kappa = \overline{1, \rho})$ из ρ оснований СОК, по которым правильное (неискаженное) число (кодовое слово) $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ может отличаться от данной совокупности $\left\{ \tilde{A} \right\}$ возможных производных неправильных чисел. При этом предполагается, что может возникнуть только однократная (по одному из остатков m_i $(i = \overline{1, n+1})$ числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ ошибка (искажение одного из (n+1)-го остатка) в правильном числе A.

Отметим, что АС рассматривается при введении в кодовую структуру СОК минимальной информационной избыточности путем добавления к n информационным одного (k=1) дополнительного (контрольного) основания m_{n+1} СОК, при условии, что $m_i < m_{n+1}$ $(i = \overline{1, n})$. В этом случае общее количество кодовых слов в СОК $N_{OK} = \prod_{i=1}^{n+1} m_i$. Количество правильных кодовых слов $N_{ПК} = \prod_{i=1}^{n} m_i$, а количество неправильных

(искаженных) кодовых слов $N_{HK} = N_{OK} - N_{ПК} = N_{ПК} \cdot (m_{n+1} - 1)$.

Необходимость определения АС может возникать в следующих основных случаях. Во-первых, при необходимости проведения процесса контроля, диагностики и коррекции ошибок данных в СОК. Во-вторых, при организации процедур контроля, диагностики и исправлении ошибок данных в СОК в процессе решения задачи в динамике вычислительного процесса (ДВП) (в реальном времени, т.е. без останова вычислений) при введении минимальной информационной избыточности [1]. Одним из основных требований к процедуре определения АС в СОК является требование уменьшения времени определения данного набора оснований. Особенно это требование критично для второго случая – при решении вычислительных задач в ДВП [6 – 9].

Таким образом, актуальной и важной научно-технической задачей является разработка новых и совершенствование существующих методов быстрого определения АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ чисел в СОК.

Основная часть

Все существующие методы определения АС чисел основываются на процедуре последовательного определения искомых оснований АС чисел в СОК [1].

Первый метод. АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ неправильного числа $\tilde{A} = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ может быть установлена последовательной проверкой каждого из оснований m_i $(i = \overline{1, n})$ СОК следующим образом. Определяется совокупность чисел, имеющих одинаковое значение остатков по всем основаниям СОК, что и число $\tilde{A}$, кроме
одного определенного основания, и отличающихся лишь значениями возможных остатков по этому основанию. Среди этой совокупности чисел может не быть ни одного правильного числа, либо может быть только одно правильное число. В последнем случае полученное число входит в АС проверяемого неправильного числа $\tilde{A}$. Рассматриваемый метод предполагает последовательное проведение аналогичных проверок для каждого из информационных оснований СОК (контрольное основание всегда входит в состав оснований АС). Результат таких последовательных проверок полностью определяет АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$. Недостатки данного метода определения АС: высокая вычислительная трудоемкость и значительное время определения АС.

Второй метод определения АС основан на вычислении всех возможных проекций $\tilde{A}_i = (a_1, a_2, ..., a_{i-1}, a_{i+1}, ..., a_n)$ неправильного числа $\tilde{A}$, и последующем их сравнении со значением величины информационного диапазона заданной СОК. В [1] доказано, что необходимым и достаточным условием вхождения основания СОК в АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ числа $\tilde{A} = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ является правильность его проекции $\tilde{A}_i$. Рассмотрим пример определения АС чисел в СОК на основе использования второго метода.

Пусть необходимо определить АС числа $A_{COK} = (0 \| 0 \| 0 \| 0 \| 5)$, заданного в СОК информационными $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_5 = 7$ и контрольным $m_k = m_5 = 11$

основаниями. При этом $M = \prod_{i=1}^{n} m_i = \prod_{i=1}^{4} m_i = 420$ и $M_0 = M \cdot m_{n+1} = 420 \cdot 11 = \quad = 4620$.

Ортогональные базисы B_i $(i = \overline{1, n+1})$ для данной СОК даны в табл. 1.

Таблица 1

$B_1 = (1\square 0\square 0\square 0\square 0) = 1540, \quad \bar{m}_1 = 1$
$B_2 = (0\square 1\square 0\square 0\square 0) = 3465, \quad \bar{m}_2 = 3$
$B_3 = (0\square 0\square 1\square 0\square 0) = 3696, \quad \bar{m}_3 = 4$
$B_4 = (0\square 0\square 0\square 1\square 0) = 2640, \quad \bar{m}_4 = 4$
$B_5 = (0\square 0\square 0\square 0\square 1) = 2520, \quad \bar{m}_5 = 6$

Предварительно проведем контроль данных $A_{COK} = (0, 0, 0, 0, 5)$. В соответствии с процедурой контроля [1, 4] определим значение исходного числа в позиционной десятичной системе счисления (ПСС)

$$A_{ПСС} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 =$$

$$= (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 + a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 +$$
$$+5 \cdot 2520) \bmod 4620 = (5 \cdot 2520) \bmod 4620 = 12600 (\bmod 4620) = 3360 > 420.$$

Таким образом, в процессе контроля определено, что $A_{ПСС} = 3360 > M = 420$. В этом случае при возможности возникновений только однократных ошибок делается вывод о том, что рассматриваемое число $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ неправильное. Далее осуществим процедуру определения АС числа $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. В соответствии со вторым методом определения АС составим возможные проекции $\tilde{A}_j$ числа $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$: $\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 5)$ и $\tilde{A}_5 = (0 \| 0 \| 0 \| 0)$.

Формула для вычисления значений $\tilde{A}_{j\,ПСС}$ проекций числа в ПСС имеет вид [1]

$$\tilde{A}_{j\,ПСС} = \left(\sum_{\substack{i=\overline{1;} \\ j=\overline{1, n+1.}}}^{n} a_i \cdot B_{ij} \right) \bmod M_j = (a_1 \cdot B_{1j} + a_2 \cdot B_{2j} + \ldots + a_n \cdot B_{nj}) \bmod M_j. \qquad (1)$$

В соответствии с формулой (1) вычислим все значения $A_{j\,ПСС}$. Далее проводим $(n+1)$-о сравнение чисел $\tilde{A}_{j\,ПСС}$ и числа $M = M_0 / m_{n+1}$. Если среди проекций $\tilde{A}_{i\,ПСС}$ есть числа, не находящиеся внутри информационного $[0, M)$ числового интервала (т.е. $\tilde{A}_{k\,ПСС} \geq M$), содержащего k правильных чисел, то делается вывод о том, что эти k остатков числа $\tilde{A}_{COK}$ не искажены. Ошибочными могут быть только остатки, находящиеся среди остальных $[(n+1)-k]$ остатков числа $\tilde{A}_{COK}$. Наборы рассчитанных в [8] частных рабочих
оснований и частных B_{ij} ортогональных базисов для заданных СОК представлены соответственно в табл. 2 и 3. В этом случае имеем, что

$$\tilde{A}_{1ПСС} = \left(\sum_{i=1}^{4} a_i \cdot B_{i1} \right) \bmod M_1 = (a_1 \cdot B_{11} + a_2 \cdot B_{21} +$$

$$+a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 = (0 \cdot 385 + 0 \cdot 616 + 0 \cdot 1100 + 5 \cdot 980) \bmod 1540 = 280 < 420 .$$

Делаем вывод, что $\bar{a}_1$ – возможно искаженный остаток;

$$\tilde{A}_{2ПСС} = \left(\sum_{i=1}^{4} a_i \cdot B_{i2} \right) \bmod M_2 = (a_1 \cdot B_{12} + a_2 \cdot B_{22} +$$

$$+a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 = (0 \cdot 385 + 0 \cdot 231 + 0 \cdot 330 + 5 \cdot 210) \bmod 1155 = 1050 > 420 .$$

Таким образом, получим, что a_2 достоверно не искаженный остаток;

$$\tilde{A}_{3ПСС} = \left(\sum_{i=1}^{4} a_i \cdot B_{i3} \right) \bmod M_3 = (a_1 \cdot B_{13} + a_2 \cdot B_{23} +$$

$$+a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 = (0 \cdot 616 + 0 \cdot 693 + 0 \cdot 792 + 5 \cdot 672) \bmod 924 = 588 > 420 .$$

Получим, что a_3 достоверно не искаженный остаток;

$$\tilde{A}_{4ПСС} = \left(\sum_{i=1}^{4} a_i \cdot B_{i4} \right) \bmod M_4 = (a_1 \cdot B_{14} + a_2 \cdot B_{24} +$$

$$+a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 = (0 \cdot 220 + 0 \cdot 165 + 0 \cdot 369 + 5 \cdot 540) \bmod 660 = 60 < 420 .$$

Вывод: $\bar{a}_4$ – возможно искаженный остаток; $\tilde{A}_{5ПСС} = \left(\sum_{i=1}^{4} a_i \cdot B_{i5} \right) \bmod M_5$. Так как $M_5 = M = 420$, то остаток $\bar{a}_5$ по модулю $m_k = m_5$ всегда будет в совокупности возможных искаженных остатков числа в СОК.

Таблица 2

j \ i	m_1	m_2	m_3	m_4	M_j
1	4	5	7	11	1540
2	3	5	7	11	1155
3	3	4	7	11	924
4	3	4	5	11	660
5	3	4	5	7	420

Таблица 3

B_{ij} j \ i	1	2	3	4
1	385	616	1100	980
2	385	231	330	210
3	616	693	792	672
4	220	165	396	540
5	280	105	336	120

Таким образом, для числа $\tilde{A}_{COK} = (0, 0, 0, 0, 5)$ определились точно не искаженные остатки. Это $a_2 = 0$ и $a_3 = 0$. Ошибочными могут быть остатки по основаниям m_1, m_4 и m_5, т.е. остатки $a_1 = 0$, $a_4 = 0$ и $a_5 = 5$. В этом случае для числа $\tilde{A}_{COK} = (0, 0, 0, 0, 5)$ АС равна следующей совокупности оснований СОК: $W(\tilde{A}) = \{1, 4, 5\}$. Применение второго метода позволяет несколько ускорить процесс определения АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ за счет возможности параллельно во времени определять значения возможных проекций $\tilde{A}_j$ неправильного числа. Данное обстоятельство

снижает временную сложность определения АС. Однако отметим, что процедура определения АС числа содержит такие основные операции: перевод числа $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n)$ из СОК в ПСС; перевод проекций $\tilde{A}_i$ неправильного числа $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n)$ из СОК в ПСС и операцию сравнения чисел. В СОК перечисленные операции относятся к непозиционным операциям, требующим больших временных и аппаратных затрат на ее реализацию. Недостатки данного метода определения АС такие же, как и при первом методе: высокая вычислительная трудоемкость и значительное время определения АС. Таким образом, остается задача совершенствования второго рассмотренного метода в плане уменьшения времени определения АС.

Совершенствование известного второго метода состоит в снижении времени определения АС. Суть предложенного в статье метода определения АС чисел в СОК заключается в предварительном формировании M таблиц соответствия (таблиц первой ступени) $A=\Phi_1(\tilde{A})$ каждого правильного $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n)$ числа (из числового диапазона $0\div M-1$), возможной совокупности $\{\tilde{A}\}$ неправильных чисел (из числового диапазона $M\div M_0-1$) при возникновении в числе А однократных (в одном остатке) ошибок. На основе анализа содержимого данных таблиц первой ступени составляется таблица второй ступени, в которой приведено соответствие $\tilde{A}=\Phi_2(A)$ каждого неправильного $\tilde{A}$ числа из числового диапазона $M\div M_0-1$ возможным значениям исправленных (правильных) $A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n)$ чисел. Количество правильных A чисел соответствует количеству оснований СОК, содержащихся в АС $W(\tilde{A})=\{m_{l_1},m_{l_2},...,m_{l_\rho}\}$ числа A. Целесообразно рассмотреть использование предлагаемого метода определения АС для конкретной СОК, заданной информационными $m_1=2$, $m_2=3$ и контрольным основаниями $m_k=m_3=m_{n+1}=5$ ($M=2\cdot3=6$; $M_0=30$). Совокупность кодовых слов в позиционной (десятичной) системе счисления (ПСС) и в СОК представлена в табл. 4.

Таблица 4

A в ПСС	m_1	m_2	m_3	A в ПСС	m_1	m_2	m_3
0	0	0	0	15	1	0	0
1	1	1	1	16	0	1	1
2	0	2	2	17	1	2	2
3	1	0	3	18	0	0	3
4	0	1	4	19	1	1	4
5	1	2	0	20	0	2	0
6	0	0	1	21	1	0	1
7	1	1	2	22	0	1	2
8	0	2	3	23	1	2	3
9	1	0	4	24	0	0	4
10	0	1	0	25	1	1	0
11	1	2	1	26	0	2	1
12	0	0	2	27	1	0	2
13	1	1	3	28	0	1	3

14	0	2	4	29	1	2	4

Исходя из содержимого табл. 4 по числу правильных кодовых слов 0 – 5 составляются табл. 5 – 10 соответствий $A = \Phi_1(\tilde{A})$ первой ступени.

Таблица 5

0	0	0	0
15	1	0	0
10	0	1	0
20	0	2	0
6	0	0	1
12	0	0	2
18	0	0	3
24	0	0	4

Таблица 6

1	1	1	1
16	0	1	1
21	1	0	1
11	1	2	1
25	1	1	0
7	1	1	2
13	1	1	3
19	1	1	4

Таблица 7

2	0	2	2
17	1	2	2
12	0	0	2
22	0	1	2
20	0	2	0
26	0	2	1
8	0	2	3
14	0	2	4

Таблица 8

3	1	0	3
18	0	0	3
13	1	1	3
23	1	2	3
15	1	0	0
21	1	0	1
27	1	0	2
9	1	0	4

Таблица 9

4	0	1	4
19	1	1	4
24	0	0	4
14	0	2	4
10	0	1	0
16	0	1	1
22	0	1	2
28	0	1	3

Таблица 10

5	1	2	0
20	0	2	0
15	1	0	0
25	1	1	0
11	1	2	1
17	1	2	2
23	1	2	3
29	1	2	4

На основании этих таблиц формируется табл. 11 второй $\tilde{A} = \Phi_2(A)$ ступени. В табл. 8 приведено соответствие $\tilde{A} = \Phi_2(A)$ каждого неправильного $\tilde{A}$ числа из числового диапазона 6 – 29 возможным значениям исправленных (правильных) A чисел. В табл. 11 дан алгоритм определения АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ чисел в СОК.

Таблица 11

Неправильное $\tilde{A}$ число	Правильное A число	Значение АС $W(\tilde{A})$
$\tilde{A}_6 = (0\,0\,1)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_6) = \{m_3\}$
$\tilde{A}_7 = (1\,1\,2)$	$A_1 = (1\,1\,1)$	$W(\tilde{A}_7) = \{m_3\}$
$\tilde{A}_8 = (0\,2\,3)$	$A_2 = (0\,2\,3)$	$W(\tilde{A}_8) = \{m_3\}$
$\tilde{A}_9 = (1\,0\,4)$	$A_3 = (1\,0\,3)$	$W(\tilde{A}_9) = \{m_3\}$
$\tilde{A}_{10} = (0\,1\,0)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_{10}) = \{m_2, m_3\}$
	$A_4 = (0\,1\,4)$	
$\tilde{A}_{11} = (1\,2\,1)$	$A_1 = (1\,1\,1)$	$W(\tilde{A}_{11}) = \{m_2, m_3\}$
	$A_5 = (1\,2\,0)$	
$\tilde{A}_{12} = (0\,0\,2)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_{12}) = \{m_2, m_3\}$
	$A_2 = (0\,2\,2)$	
$\tilde{A}_{13} = (1\,1\,3)$	$A_1 = (1\,1\,1)$	$W(\tilde{A}_{13}) = \{m_2, m_3\}$
	$A_3 = (1\,0\,3)$	
$\tilde{A}_{14} = (0\,2\,4)$	$A_2 = (0\,2\,2)$	$W(\tilde{A}_{14}) = \{m_2, m_3\}$
	$A_4 = (0\,1\,4)$	
$\tilde{A}_{15} = (1\,0\,0)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_{15}) = \{m_1, m_2, m_3\}$
	$A_3 = (1\,0\,3)$	
	$A_5 = (1\,2\,0)$	
$\tilde{A}_{16} = (0\,1\,1)$	$A_1 = (1\,1\,1)$	$W(\tilde{A}_{16}) = \{m_1, m_3\}$
	$A_4 = (0\,1\,4)$	
$\tilde{A}_{17} = (1\,2\,2)$	$A_2 = (0\,2\,2)$	$W(\tilde{A}_{17}) = \{m_1, m_3\}$
	$A_5 = (1\,2\,0)$	
$\tilde{A}_{18} = (0\,0\,3)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_{18}) = \{m_1, m_3\}$
	$A_3 = (1\,0\,3)$	
$\tilde{A}_{19} = (1\,1\,4)$	$A_1 = (1\,1\,1)$	$W(\tilde{A}_{19}) = \{m_1, m_3\}$
	$A_4 = (0\,1\,4)$	
$\tilde{A}_{20} = (0\,2\,0)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_{20}) = \{m_1, m_2, m_3\}$
	$A_2 = (0\,2\,2)$	
	$A_5 = (1\,2\,0)$	
$\tilde{A}_{21} = (1\,0\,1)$	$A_1 = (1\,1\,1)$	$W(\tilde{A}_{21}) = \{m_2, m_3\}$
	$A_3 = (1\,0\,3)$	
$\tilde{A}_{22} = (0\,1\,2)$	$A_2 = (0\,2\,2)$	$W(\tilde{A}_{22}) = \{m_2, m_3\}$
	$A_4 = (0\,1\,4)$	
$\tilde{A}_{23} = (1\,2\,3)$	$A_3 = (1\,0\,3)$	$W(\tilde{A}_{23}) = \{m_2, m_3\}$
	$A_5 = (1\,2\,0)$	
$\tilde{A}_{24} = (0\,0\,4)$	$A_0 = (0\,0\,0)$	$W(\tilde{A}_{24}) = \{m_2, m_3\}$

	$A_4 = (0 \square 1 \square 4)$	
$\tilde{A}_{25} = (1 \square 1 \square 0)$	$A_1 = (1 \square 1 \square 1)$	$W(\tilde{A}_{25}) = \{m_2, m_3\}$
	$A_5 = (1 \square 2 \square 0)$	
$\tilde{A}_{26} = (0 \square 2 \square 1)$	$A_2 = (0 \square 2 \square 2)$	$W(\tilde{A}_{26}) = \{m_3\}$
$\tilde{A}_{27} = (1 \square 0 \square 2)$	$A_3 = (1 \square 0 \square 3)$	$W(\tilde{A}_{27}) = \{m_3\}$
$\tilde{A}_{28} = (0 \square 1 \square 3)$	$A_4 = (0 \square 1 \square 4)$	$W(\tilde{A}_{28}) = \{m_3\}$
$\tilde{A}_{29} = (1 \square 2 \square 4)$	$A_5 = (1 \square 2 \square 0)$	$W(\tilde{A}_{29}) = \{m_3\}$

Рассмотрим пример определения АС чисел в СОК предложенным в статье табличным методом. Пусть дано неправильное число $\tilde{A}_{15} = (1 \square 0 \square 0)$ (табл. 4). Необходимо определить АС этого числа. Первоначально формируются 6 таблиц (табл. 5 – 10) соответствия первой ступени каждого правильного $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ числа (из числового диапазона 0 – 5), возможной совокупности неправильных чисел (из числового диапазона 6 – 29) при возникновении в числе А однократных (в одном остатке) ошибок (табл. 4). На основе анализа содержимого данных таблиц первой ступени составляется таблица второй ступени, в которой приведено соответствие каждого неправильного числа из числового диапазона 6 – 29 возможным значениям исправленных (правильных) $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ чисел. Количество правильных А чисел соответствует количеству оснований СОК, содержащихся в АС $W(\tilde{A}) = \left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$ числа А. При воздействии однократных ошибок неправильное число $\tilde{A}_{15} = (1 \square 0 \square 0)$ может быть образовано из следующих правильных А чисел.

Во-первых, правильное число $A_0 = (0 \square 0 \square 0)$ (табл. 5) может быть искажено в первом остатке $a_1 = 0$ $(\tilde{a}_1 = 1)$. Во-вторых, правильное число $A_3 = (1 \square 0 \square 3)$ (табл. 8) может быть искажено в третьем остатке $a_3 = 3$ $(\tilde{a}_3 = 0)$. И, наконец, в-третьих, правильное число $A_5 = (1 \square 2 \square 0)$ (табл. 10) может быть искажено во втором остатке $a_2 = 2$ $(\tilde{a}_2 = 0)$. Таким образом, АС $W(\tilde{A}) = \left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$ неправильного числа $\tilde{A}_{15} = (1 \square 0 \square 0)$ будет равна значению $W(\tilde{A}_{15}) = \{m_1, m_2, m_3\}$ (табл. 11).

Выводы

Предложен усовершенствованный метод определения АС чисел в СОК. Совершенствование известного метода состоит в снижения времени определения АС. Суть предложенного в статье метода определения АС чисел в СОК заключается в предварительном формировании *M* таблиц соответствия (таблиц первой ступени) $A = \Phi_1(\tilde{A})$ каждого правильного $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ числа (из числового диапазона $0 \div M - 1$), возможной совокупности неправильных чисел (из числового диапазона $M \div M_0 - 1$) при возникновении в числе A однократных ошибок. Далее на основе анализа содержимого данных таблиц первой ступени составляется таблица второй ступени, в которой приведено соответствие $\tilde{A} = \Phi_2(A)$ каждого неправильного $\tilde{A}$ числа из числового диапазона $M \div M_0 - 1$ возможным значениям исправленных (правильных) $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ чисел. Применение данного метода, по сравнению с существующими методами, позволяет сократить время определения АС чисел. Это достигается, во-первых, за счет уменьшения количества последовательно проверяемых оснований СОК, по которым возможно искажение остатков правильного числа

$A=(a_1,a_2,...,a_{i-1},a_i,a_{i+1},...,a_n)$. И, во-вторых, за счет организации процесса быстрой (табличной) выборки предварительно рассчитанных данных значений АС $W(\tilde{A})=\left\{m_{l_1},m_{l_2},...,m_{l_\rho}\right\}$. Уменьшение времени определения АС $W(\tilde{A})=\left\{m_{l_1},m_{l_2},...,m_{l_\rho}\right\}$ чисел позволит в дальнейшем, при необходимости, повысить быстродействие процесса диагностики и коррекции ошибок данных в СОК.

Список литературы: 1. *Акушский, И. Я., Юдицкий, Д. И.* Машинная арифметика в остаточных. – Москва : Сов. радио, 1968. – 440с. 2. *Krasnobayev, V. A.* Method for Realization of Transformations in Public-Key Cryptography // Telecommunications and Radio Engineering. USA. – 2007. – Vol. 66, Issue 17. – PP. 1559 – 1572. 3. *Краснобаев, В.А., Кошман, С. А., Маврина, М. А.* Метод исправления однократных ошибок данных, представленных кодом класса вычетов // Электронное моделирование. – 2013. – Т. 35, № 5. – С. 43–56. 4. *Кузнецов, О. О., Горбенко, Ю. І., Колованова, Є. П.* Періодичні властивості шифргами у режимі Output Feedback // Прикладная радиоэлектроника. –Харьков : ХНУРЭ, 2014. – Т. 13, №3. – С. 239 – 251. 5. *Кузнецов, А. А., Швагер, А. С., Фесенко, Д. А.* Сокрытие данных в кластерных файловых системах // Радиотехника. – 2015. – Вып. 181. – С. 86–100. 6. *Мороз, С. А., Краснобаев, В.А.* Методы контроля, диагностики и коррекции ошибок данных в информационно-телекоммуникационной системе, функционирующей в классе вычетов // Інформаційно-керуючі системи на залізничному транспорті. – 2012. – № 2. – С. 60 – 78. 7. *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. Volume 50, Issue 6. pp 969-976.
8. *Krasnobayev, V. A., Yanko, A. S., Koshman, S. A.* A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. January 2016. Volume 52, Issue 1. pp. 145-150. 9. *Материалы* Междунар. науч.-техн. конф. "50 лет модулярной арифметике" // МИЭТ. Зеленоград, Моск. обл. 23-25 ноября 2005г. – С. 101-130.

Харьковский национальный университет имени В.Н.Каразина

Поступила в редколлегию 20.04.2017