УДК 681.142:681.3

МЕТОД КОНТРОЛЯ ДАННЫХ, ПРЕДСТАВЛЕННЫХ КОДОМ НЕПОЗИЦИОННОЙ СИСТЕМЫ СЧИСЛЕНИЯ КЛАССА ВЫЧЕТОВ

МОРОЗ С. А., КРАСНОБАЕВ В. А.

Рассматривается метод контроля цифровой информации, представленной в виде данных. Данные кодируются в непозиционной системе счисления класса вычетов (КВ). Приводятся примеры конкретной реализации метода контроля данных в КВ.

1. Введение

Известно, что использование свойств непозиционной системы счисления класса вычетов (КВ) обеспечивает высокую пользовательскую производительность реализации в системе обработки данных (СОД) вычислительных алгоритмов, состоящих из арифметических операций. Наибольшая эффективность от применения КВ достигается в случае, когда реализуемые алгоритмы состоят из совокупности таких арифметических операций, как сложение, умножение и вычитание [1-2].

Необходимость обеспечения отказоустойчивого функционирования СОД требует разработки и внедрения в КВ новых методов контроля и коррекции ошибок информации, отличных от методов, используемых в обычных двоичных позиционных системах счисления (ПСС) [3].

Отметим, что, во-первых, все методы контроля и коррекции данных в КВ основываются на специфике реализации позиционных операций в данной системе счисления, требующей знания величины (возможно знака) числа, представленного данной непозиционной кодовой структурой. Во-вторых, методы контроля в КВ являются дальнейшим развитием контроля по модулю в ПСС (арифметические AN-коды). Действительно, с точки зрения информационного резервирования коды являются дальнейшим совершенствованием известных арифметических многоостаточных кодов. Известно, что многоостаточный код представляется в виде:

$$A'_k = (A_k, A_k(\bmod m_1), A_k(\bmod m_2), \ldots,$$
$$A_k(\bmod m_k), \ldots, A_k(\bmod m_{n-1}), A_k(\bmod m_n))$$

т.е. $A'_k = (A_k, a_1, a_2, \ldots, a_n)$,

где $a_i = A_k - [A_k / m_i] m_i$.

В этом случае для $\prod_{i=1}^{n} m_i \geq A_k$ совокупность остатков $\{a_i\}$ однозначно определяет операнд $A'_к$ и численное значение $A_к$ становится вообще не нужным. Многоостаточный код принимает вид непозиционного кода КВ $A_k^{'} = (a_1, a_2, ..., a_n)$, что позволяет реализовать модульные операции по отдельным независимым трактам, оперируя только с остатками $\{a_i\}$. Такое кодирование чисел позволяет построить СОД, в котором обработка всех остатков a_i числа производится параллельно во времени. В этом случае обобщенная структурная схема СОД в КВ представляет собой набор отдельных микро-ЭВМ, функционирующих независимо друг от друга и параллельно во времени, причем каждая по своему определенному модулю m_i [4].

2. Основная часть

Процесс коррекции (обнаружения и исправления) ошибок в информационной кодовой структуре Г данных состоит из следующих основных этапов:

– контроль данных (процесс обнаружения факта наличия ошибки в числе А);

– диагностика (локализация места ошибок с заданной глубиной диагностирования);

– исправление ошибок в кодовой структуре данных (восстановление искаженных остатков $\tilde{a}_j (j = \overline{1, n})$ числа $\tilde{A}$ и получение правильного числа А).

Число $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ в КВ представляется совокупностью $\{a_i\} (i = \overline{1, n})$ остатков $a_i \equiv A(\bmod m_i)$ по выбранной системе информационных оснований (модулей) $\{m_i\}$ в рабочем (информационном) числовом интервале [0, M) (где $M = \prod_{i=1}^{n} m_i$ – общее количество информационных кодовых слов). При этом НОД $(m_i, m_j) = 1$, при $i, j = \overline{1, n}\ (i \neq j)$.

Для того чтобы код КВ обладал корректирующими свойствами необходимо, чтобы он содержал определенную информационную избыточность. При этом, во-первых, необходимо определить (выявить) и, по возможности, количественно оценить имеющуюся (естественную) в исходной информационной кодовой структуре избыточность. Во-вторых, при необходимости обеспечения данных дополнительными корректирующими способностями ввести дополнительную (искусственную) информационную избыточность (применить методы информационного резервирования) за счет введения дополнительных (контрольных) оснований $\{m_k\}$ КВ. Без потери общности рассуждений будем полагать, что к n информационным основаниям КВ добавлено одно $m_k = m_{n+1}$ контрольное основание взаимно-простое с любым из имеющихся информационных оснований. В этом случае число $A = (a_1, a_2, ..., a_n, a_{n+1})$ в КВ представляется посредством совокупности $\{m_j\}\ (j = \overline{1, n+1})$ оснований в полном числовом $[0, M_0)$ интервале, где $M_0 = M$ • m_{n+1} – общее количество кодовых слов для данного КВ.

Известно [1], что для непозиционных кодовых структур в КВ минимальное кодовое расстояние определяется выражением $d_{\min} = K + 1$, т.е. оно зависит как от числа К контрольных оснований, так и от величины каждого из них. Если для контрольных оснований m_{z_t} выполняется условие $\prod_{t=1}^{k} m_{z_t} \le m_k$, тогда введение в систему оснований КВ одного контрольного $m_k = m_{n+1}$ основания эквивалентно наличию К контрольных оснований. С учетом того, что все числа, принимающие участие в обработке данных (передача и обработка информации), а также результат операции данными находится в интервале [0, M), то очевидно, что если в результате обработки данных получен окончательный результат $A \ge M$, это означает, что полученное число $\tilde{A}$ искаженное (неправильное).

Таким образом, если в результате обработки данных определено, что $\tilde{A} \ge M$, то делается вывод, что число Г неправильное. На этом принципе (принципе сравнения) основываются все методы сравнения данных в КВ. Если A < M, то делается вывод, что число А правильное, а если $A \ge M$, то число $\tilde{A}$ неправильное. При этом предполагаются только однократные (в одном из остатков $\{a_i\}$ числа А) ошибки, либо пачка ошибок длинною не более $k = [\log_2(m_i - 1)] + 1$ двоичных разрядов.

Для рассмотрения метода контроля (метод прямого сравнения) данных в КВ на основе изложенного выше принципа, который используется также при разработке методов диагностики и коррекции ошибок, воспользуемся результатами доказательства известного [1] научного утверждения.

Утверждение. Пусть информационное основание $\{m_i\}\ (i = \overline{1, n})$ КВ с одним контрольным $m_k = m_{n+1}$ основанием упорядочено ($m_i < m_{i+1}$), и пусть результат $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ выполнения операции является правильным числом, т.е. $A < M\ (M = \prod_{i=1}^{n} m_i)$. Тогда утверждается, что число $\tilde{A} = (a_1, a_2, ..., a_{i-1}, \tilde{a}_i, a_{i+1}, ..., a_n, a_{n+1})$, в котором искажен один остаток $\tilde{a}_i \neq a_i$ по основанию m_i, является неправильным, т.е. $\tilde{A} \ge M$.

Покажем это. На основе принципа сравнения правильность числа А определяется исходя из соотношения

$$A < M = M_0 / m_{n+1}\ (M_0 = \prod_{i=1}^{n+1} m_i).$$

С другой стороны, очевидно выполнение условия $M_0 / m_i > M_0 / m_{n+1}$ для упорядоченного КВ при $i = \overline{1, n}$. В этом случае выполняется следующее неравенство $A < M_0 / m_i$. Отметим, что остаток

$a_i \equiv A(\bmod m_i)$ числа А по модулю m_i может принимать значение $a_i = \overline{0, m_i - 1}$. В соответствии с условием утверждения, что $\tilde{a}_i \neq a_i$, и учитывая, что остальные значения остатков $a_j\,(j = \overline{1, n+1}$ и $i \neq j)$ неправильного $\tilde{A}$ числа остаются без изменений, то в интервале $[0, M_0/m_i)$ не могут одновременно находиться оба числа А и $\tilde{A}$. Тогда, так как число $A < M_0/m_{n+1}$ правильное (находится в рабочем [0, M] интервале), то число Г находится вне интервала $[0, M_0/m_i)$, и тем более находится вне интервала [0, M). В этом случае число Г, для которого выполняется условие $\tilde{A} \geq M$, является неправильным. Таким образом показано, что число

$$A = (a_1, a_2, ..., a_{i-1}, \tilde{a}_i, a_{i+1}, ..., a_n, a_{n+1})$$

является искаженным (рис 1,2).

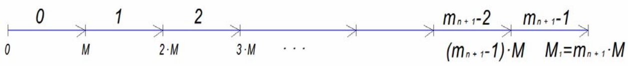

Рис. 1. Числовые интервалы для $m_k = m_{n+1}$

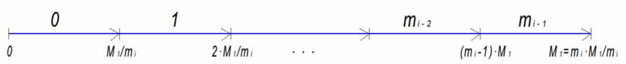

Рис. 2. Числовые интервалы для произвольного модуля m_i

3. Анализ метода контроля данных

Рассмотрим метод контроля данных в КВ, основанный на результатах и выводах рассмотренного научного утверждения.

В основе контроля лежит базовая операция – сравнение результата А операции с числом $M = M_0/m_{n+1}$. Для сравнения чисел $A = (a_1, a_2, ..., a_n, a_{n+1})$ и M необходимо перевести значение А в позиционную двоичную систему счисления (ПСС). Для этого можно использовать ортогональные базисы $B_i\,(i = \overline{1, n+1})$, которые представляются в виде [1]:

$$\begin{cases} B_1 = (1, 0, ..., 0, ..., 0, 0), \\ B_2 = (0, 1, ..., 0, ..., 0, 0), \\ B_i = (0, 0, ..., 1, ..., 0, 0), \\ B_n = (0, 0, ..., 0, ..., 1, 0), \\ B_{n+1} = (0, 0, ..., 0, ..., 0, 1). \end{cases} \quad (1)$$

Ортогональные базисы B_i определяются для каждого

$$B_i = \overline{m}_i \cdot M_0 / m_i \equiv 1(\bmod m_i). \quad (2)$$

Значение веса $\overline{m}_i$ ортогонального базиса B_i определяется как одно из решений системы сравнений:

$$\begin{cases} \overline{m}_i = 1, \quad 1 \cdot M_i \equiv \rho_1 (\bmod m_i), \\ \overline{m}_i = 2, \quad 2 \cdot M_i \equiv \rho_2 (\bmod m_i), \\ \qquad \qquad \dots \\ \overline{m}_i = m_i - 2, \quad (m_i - 2) \cdot M_i \equiv \rho_{m-2} (\bmod m_i), \\ \overline{m}_i = m_i - 1, \quad (m_i - 1) \cdot M_i \equiv \rho_{m-1} (\bmod m_i). \end{cases} \quad (3)$$

Значение $\overline{m}_i$, для которого выполняется условие (2), определяется путем подстановки возможных значений $\overline{m}_i = \overline{1, m_i - 1}$ методом простого перебора.

Значение А в ПСС определяется в соответствии с формулой $A_{ПСС} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_0$.

4. Примеры конкретной реализации метода контроля данных в КВ

Рассмотрим примеры реализации метода контроля данных для упорядоченного КВ, заданного информационными $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ и контрольным $m_k = m_5 = 11$ основаниями (рис. 3). Данный КВ обеспечивает информационный интервал [0, M) для однобайтовой (l=1) СОД, где $M = \prod_{i=1}^{4} m_i = 420$. Полный числовой интервал представления чисел в КВ определяется как $[0, M_0)$, где $M_0 = M \bullet m_{n+1} = 4620$ (рис.3).

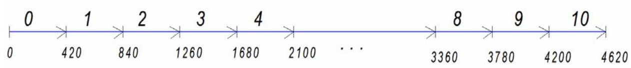

Рис. 3. Числовые интервалы для l = 1 ($m_k = m_{n+1} = 11$)

В табл. 1–5 представлены процедуры определения значений $\overline{m}_i\,(i = \overline{1,5})$, а в табл. 6 даны рассчитанные значения ортогональных базисов $B_i\,(i = \overline{1,5})$.

Таблица 1. Процедура определения $\overline{m}_1$

$\overline{m}_1 = 3$, $M_1 = 4 \cdot 5 \cdot 7 \cdot 11 = 1540$	
$\overline{m}_1 = 1$	$\overline{m}_1 \cdot M_1 = 1540 \equiv 1(\bmod m_1)$
$\overline{m}_2 = 2$	$\overline{m}_1 \cdot M_1 = 3080 \equiv 2(\bmod m_1)$
$\overline{m}_1 = 1$, $B_1 = (1{,}0{,}0{,}0{,}0) = 1540$	

Таблица 2. Процедура определения $\overline{m}_2$

$m_2 = 4$, $M_2 = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$	
$\overline{m}_2 = 1$	$1 \cdot M_2 = 1155 \equiv 3(\bmod m_2)$
$\overline{m}_2 = 2$	$2 \cdot M_2 = 2310 \equiv 2(\bmod m_2)$
$\overline{m}_2 = 3$	$3 \cdot M_2 = 3465 \equiv 1(\bmod m_2)$
$\overline{m}_2 = 3$	$B_2 = (0{,}1{,}0{,}0{,}0) = 3465$

Таблица 3. Процедура определения $\overline{m}_3$

$m_3 = 5$, $M_3 = 3 \cdot 4 \cdot 7 \cdot 11 = 924$	
$\overline{m}_3 = 1$	$1 \cdot M_3 = 924 \equiv 4(\bmod m_3)$
$\overline{m}_3 = 2$	$2 \cdot M_3 = 1848 \equiv 3(\bmod m_3)$
$\overline{m}_3 = 3$	$3 \cdot M_3 = 2772 \equiv 2(\bmod m_3)$
$\overline{m}_3 = 4$	$4 \cdot M_2 = 3696 \equiv 1(\bmod m_3)$
$\overline{m}_3 = 4$, $B_3 = (0{,}0{,}1{,}0{,}0) = 3696$	

Таблица 4. Процедура определения $\overline{m}_4$

$m_4 = 7, M_4 = 3 \cdot 4 \cdot 5 \cdot 11 = 660$	
$\overline{m}_4 = 1$	$1 \cdot M_4 = 660 \equiv 2(\bmod m_4)$
$\overline{m}_4 = 2$	$2 \cdot M_4 = 1320 \equiv 4(\bmod m_4)$
$\overline{m}_4 = 3$	$3 \cdot M_4 = 1980 \equiv 6(\bmod m_4)$
$\overline{m}_4 = 4$	$4 \cdot M_4 = 2640 \equiv 1(\bmod m_4)$
$\overline{m}_4 = 5$	$5 \cdot M_4 = 3300 \equiv 3(\bmod m_4)$
$\overline{m}_4 = 6$	$6 \cdot M_4 = 3960 \equiv 5(\bmod m_4)$
$\overline{m}_4 = 4,\ B_4 = (0,0,0,1,0) = 2640$	

Таблица 5. Процедура определения $\overline{m}_5$

$m_5 = 11, M_5 = 3 \cdot 4 \cdot 5 \cdot 7 = 420$	
$\overline{m}_5 = 1$	$1 \cdot M_5 = 420 \equiv 2(\bmod m_5)$
$\overline{m}_5 = 2$	$2 \cdot M_5 = 840 \equiv 4(\bmod m_5)$
$\overline{m}_5 = 3$	$3 \cdot M_5 = 1260 \equiv 6(\bmod m_5)$
$\overline{m}_5 = 4$	$4 \cdot M_5 = 1680 \equiv 8(\bmod m_5)$
$\overline{m}_5 = 5$	$5 \cdot M_5 = 2100 \equiv 10(\bmod m_5)$
$\overline{m}_5 = 6$	$6 \cdot M_5 = 2520 \equiv 1(\bmod m_5)$
$\overline{m}_5 = 7$	$7 \cdot M_5 = 2940 \equiv 3(\bmod m_5)$
$\overline{m}_5 = 8$	$8 \cdot M_5 = 3360 \equiv 5(\bmod m_5)$
$\overline{m}_5 = 9$	$9 \cdot M_5 = 3780 \equiv 7(\bmod m_5)$
$\overline{m}_5 = 10$	$10 \cdot M_5 = 4200 \equiv 9(\bmod m_5)$
$\overline{m}_5 = 6,\ B_5 = (0,0,0,0,1) = 2520$	

Таблица 6. Ортогональные базисы B_i КВ

$B_1 = (1,0,0,0,0) = 1540$
$B_2 = (0,1,0,0,0) = 3465$
$B_3 = (0,0,1,0,0) = 3696$
$B_4 = (0,0,0,1,0) = 2640$
$B_5 = (0,0,0,0,1) = 2520$

Пусть задано правильное $A_{400} = (1,0,0,1,4)$ число в КВ.

Пример 1. Определить правильность числа $\tilde{A} = (1,0,0,1,4)$, искаженного по основанию $m_1 = 3$ ($\tilde{a}_1 = 0$). Переводим число $\tilde{A}$ в ПСС и сравниваем его с величиной M = 420:

$$\tilde{A} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_1 = (\sum_{i=1}^{5} a_i \cdot B_i) \bmod 4620 =$$

$$= (1540 \cdot 0 + 3465 \cdot 0 + 3696 \cdot 0 + 2640 \cdot 1 + 2520 \cdot 4)$$

$$\bmod 4620 = 12720,$$

$\bmod(4620) = 3480 > 420$. Таким образом, операнд $\tilde{A}$ содержит ошибку в одном из пяти остатков.

Пример 2. Пусть число $A_{400} = (1,0,0,1,4)$ неискаженно. В этом случае получим $A = (1540 \cdot 1 + 3465 \cdot 0 + 3696 \cdot 0 + 2640 \cdot 1 + 2520 \cdot 4)$ $\bmod 4620 = 14260 (\bmod 4620) = 400 < 420.$

Число А правильное.

5. Выводы

1. Анализ свойств непозиционных кодовых структур показал, что коды в КВ являются арифметическими кодами (некоторый аналог этих кодов в ПСС – арифметические AN-коды), пригодны к использованию как для передачи, так и для обработки информации. Для кодов КВ контрольные основания включены в общую кодовую структуру данных, содержащих совокупность информационных оснований. В этом случае остатки, которыми представляются операции в КВ по информационным и контрольным основаниям, одновременно и независимо участвуют в процессе обработки информации. Результат обработки информации, представленный кодом КВ, может контролироваться либо поэтапно, либо по окончанию всех вычислений, так как ошибка, возникшая в каком-либо остатке a_i числа

$$A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1}),$$

не распространяется (не «размножается») в остальные остатки $a_j\,(j = \overline{1, n+1}$ и $i \neq j)$ числа А (в соседние тракты обработки информации СОД). Важное значение имеет факт определения количества и величин (по количеству реализуемых операций) каждого их этих этапов. Например, величина каждого этапа обработки информации (этапа вычислений) может быть определена либо по определяемому законченному циклу обработки алгоритма, либо в соответствии с возможным значением вероятности возникновения однократной (в одном остатке числа в КВ) ошибки.

2. Для произвольной упорядоченной ($m_i < m_{i+1}$) системы оснований КВ, с одним контрольным m_k основанием искажение одного произвольного остатка a_j по модулю m_j однозначно превращает правильное (неискаженное) число А в неправильное Г. В этом случае система контроля в КВ достоверно определяет факт искажения числа А. Корректирующие способности помехоустойчивого кода в КВ зависят от количества и величины контрольных $\{m_k\}$ оснований. Если для некоторого количества r информационных оснований данного КВ выполняется условие

$$\prod_{i=1}^{r} m_{z_i} \le m_k \ (m_{z_i} \in M),$$

то искажения в одновременно нескольких или даже во всех этих r остатках не превращают правильное число А в неправильное. При этом считается, что СОД функционирует безотказно. Однако при этом система контроля СОД не определяет номера отказавших трактов обработки данных.

3. Предложенный метод контроля, основанный на принципе сравнения, в дальнейшем создает предпосылки для разработки эффективных методов диагностики и коррекции ошибок в КВ. Недостатком предложенного метода является относительно низкая оперативность контроля. Этот недостаток обусловлен значительными временными затратами на операции перевода числа А из КВ в ПСС и сравнения чисел А и М в ПСС. Кроме этого, если контролю подвергается промежуточный результат вычислений, то возможно потребуется дополнительная операция перевода числа А из ПСС в КВ. Данное обстоятельство обуславливает необходимость повышения оперативности контроля СОД в КВ за счет уменьшения времени выполнения перечисленных выше операций путем разработки и использования, например, методов и средств реализации позиционных признаков непозиционного кода КВ.

Литература: **1.** *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. М.: Сов. радио, 1968. 440с. **2.** *Барсов В.И., Краснобаев В.А., Сиора А.А., Авдеев И.В.* Методы многоверсионной обработки информации в модулярной арифметике: Монография. Х.: МОН, УИПА, 2008. 460с. **3.** *Сиора А.А., Краснобаев В.А., Харченко В.С.* Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: Монография. Х.: МОН, НАУ им. Н.Е. Жуковского (ХАИ), 2009. 320с. **4.** *Барсов В.И., Сорока Л.С., Краснобаев В.А.* Методология параллельной обработки информации в модулярной системе счисления: Монография. Х.: МОН, УИПА, 2009. 268с.

Поступила в редколлегию 02.03.2011

Рецензент: д-р техн. наук, проф. Фурман И.А.

Мороз Сергей Александрович, аспирант кафедры автоматизации и компьютерно-интегрированных технологий Харьковского национального технического университете сельского хозяйства им. Петра Василенка. Научные интересы: создание отказоустойчивого спецпроцессора быстрой и достоверной обработки данных на основе использования непозиционной системы счисления в классе вычетов. Адрес: Украина, 61052, Харьков, ул. Кацарская, 9, тел. 712-35-37.

Краснобаев Виктор Анатольевич, д-р техн. наук, профессор кафедры автоматизации и компьютерно-интегрированных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенка. Научные интересы: теоретическое обоснование и практическое создание быстродействующих и отказоустойчивых вычислительных структур в модулярной системе счисления. Адрес: Украина, 61052, Харьков, ул. Кацарская, 9, тел. 712-35-37.