$\alpha: C \to C$ — автоморфизм сдвига $(n \to n+1)$. Имеют место аддитивные эквивалентности категорий $C_\alpha[t, t^{-1}] \simeq A$, $C_\alpha[t] \simeq gr(A[t])$, где $A[t]$ — градуированное кольцо многочленов от переменной t степени 1. Категория $NIL(\alpha, C)$ эквивалентна категории $NGR(A)$, поэтому группы $Nil_i(\alpha, C)$ и Ngr_iA изоморфны. Далее, по [4, с. 107] $K_i(gr(A[t])) \simeq K_i(gr(A)) \simeq K_iA_0 \times_Z Z[t, t^{-1}]$ (тензорно), поэтому по теореме 1 $Nil_i(\alpha^{-1}, C) = 0$, $K_iA \simeq X_i \dotplus Ngr_{i-1}A$, причем $X_i = \operatorname{coker}(Id$ — «сдвиг$) \simeq K_iA_0$, откуда и следует утверждение теоремы.

ЛИТЕРАТУРА

1. Gersten S.— Communs Algebra, 1974, v. 1, № 1, p. 39.
2. Прасолов А. В.— УМН, 1977, т. 32, № 5, с. 195.
3. Прасолов А. В.— XV Всесоюзная алгебр. конф.— Красноярск, 1979, ч. 1, с. 124.
4. Quillen D.— Lecture Notes Math., 1973, v. 341, p. 85.

Поступила в редакцию 24.01.80.

Кафедра высшей математики

УДК 681.142.01

М. К. БУЗА

О МУЛЬТИПЛИКАТИВНОМ ПЕРЕПОЛНЕНИИ В КОДЕ ВЫЧЕТОВ

Расширение сферы использования системы кодирования данных с помощью вычетов (СКВ) во многом зависит от эффективности методов обработки информации. Ниже предлагается один метод определения мультипликативного переполнения в СКВ.

Основные обозначения: $P_1, P_2, \ldots, P_n$ — основания СКВ; r_A — ранг числа A; $m_1, m_2, \ldots, m_n$ — веса ортогональных базисов; $b_i = b_i - P_i$, $i = \overline{1, n}$.

Построим метод мультипликативного переполнения применительно к безранговой СКВ (БСКВ) [1]. Система оснований $P_1P_2, \ldots, P_n$ будет безранговой, т. е. любое $A \in [0, M)$ допускает расширенное представление нулевого ранга (РПНР), если $r_A = \sum_{j \in N} m_j$; где N — множество номеров, которые образуют индексы весов ортогональных базисов [2].

Не нарушая общности рассуждений, предположим, что РПНР чисел A и B соответственно: $A' = (\alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_{m+1} - P_{m+1}, \ldots, \alpha_j - P_j, \alpha_{j+1}, \ldots, \alpha_n)$ и $B' = (\beta_1, \beta_2, \ldots, \beta_l, \beta_{l+1} - P_{l+1}, \ldots, \beta_k - P_k, \beta_{k+1}, \ldots, \beta_n)$, т. е. $r_A = \sum_{i=m+1}^{j} m_i$, $r_B = \sum_{i=l+1}^{k} m_i$ в соответствующей классической СКВ [3].

Пусть A' B' в коде вычетов есть $(\gamma_1, \gamma_2, \ldots, \gamma_n)$, где

$$\gamma_i = \alpha_i\beta_i - \left[\frac{\alpha_i\beta_i}{P_i}\right] P_i, \quad i = \overline{1, n}, \tag{1}$$

где α_i и β_i, $i = \overline{1, n}$ «разряды» чисел A' и B' в БСКВ.

Число $A'B'$ не всегда будет иметь РПНР. Чтобы выяснить, возможно ли его представить в РПНР, необходимо вычислить поразрядные переполнения $n_i = l_i + k_i$, где $l_i = \left[\frac{\alpha_i\beta_i}{P_i}\right]$; k_i — число переполнений, потерянных при умножении по формуле (1); $i = \overline{1, n}$.

Схема предлагаемого метода сводится к следующему:

1) определение поразрядных переполнений n_i, $i = \overline{1, n}$;
2) вычисление величины корректировки Q;
3) выяснение возможности представления $A'B'$ в РПНР. Если это

возможно, то произвести корректировку $(\gamma_1, \gamma_2, \ldots, \gamma_n)$, если нет — выдать сигнал о переполнении.

Так как l_i, $i=\overline{1, n}$ можно получить из (1), то для определения Q необходимо вычислить k_i, $i=\overline{1, n}$.

Пусть $\left[\frac{B}{P_i}\right] = S_i$, $i = \overline{1, n}$. Представим S_i в виде

$$S_1 = \{\beta_{1n}^1, \beta_{1n}^2, \ldots, \beta_{1n}^{N_1}\}, S_2 = \{\beta_{2n}^1, \beta_{2n}^2, \ldots, \beta_{2n}^{N_2}\}, \ldots, S_n = \{\beta_{nn}^1, \beta_{nn}^2, \ldots, \beta_{nn}^{N_n}\},$$

где $\beta_{in}^1 = s_i - \left[\frac{s_i}{P_n}\right] P_n$, $\beta_{in}^2 = \Theta_1^i - \left[\frac{\Theta_1^i}{P_n}\right] P_n$, .. ;

$$\beta_{in}^{N_i-1} = \Theta_{N_i-2}^i - \left[\frac{\Theta_{N_i-2}^i}{P_n}\right] P_n, \quad \beta_{in}^{N_i} = \Theta_{N_i-1}^i \Theta_1^i = \left[\frac{s_i}{P_n}\right], \ldots ;$$

$$\Theta_{N_i-1}^i = \left[\frac{\Theta_{N_i-2}^i}{P_n}\right], \quad \Theta_{N_i-1}^i < P_n.$$

Оценим величину N_i для основания P_i. Пусть R — целое, такое что $P_i P_n^{N_i-1} < R < P_i P_n^N$, тогда $N = \left[\frac{\ln \frac{P}{P_i}}{\ln P_n}\right]$. Умножив каждое из s_i, $i = \overline{1,n}$ на A', получим

$$(\sigma_{in}^1, \sigma_{in}^2, \ldots, \sigma_{in}^{N_i}) = \{\beta_{in}^1, \beta_{in}^2, \ldots, \beta_{in}^{N_i}\} \alpha_i, \quad i = \overline{1, n}, \tag{2}$$

где $\sigma_{in}^k = \beta_{in}^k \alpha_i - a_k P_n$, $a_k = \left[\frac{\beta_{in}^k \alpha_i}{P_n}\right]$, $k = \overline{1, N}$; $i = \overline{1, n}$. В каждой из N_i компонент в (2), начиная с первой, выделяем переполнения и переносим в следующую. Получим

$$\{\xi_{1n}^1, \xi_{1n}^2, \ldots, \xi_{1n}^{N_i}\}, \{\xi_{2n}^1, \xi_{2n}^2, \ldots, \xi_{2n}^{N_i}\}, \ldots, \{\xi_{nn}^1, \xi_{nn}^2, \ldots, \xi_{nn}^{N_i}\}, \tag{3}$$

где $\xi_{in}^k = \xi_{in}^k + a_{k-1} - b_k P_n$, $b_k = \left[\frac{\sigma_{in}^k + a_{k-1}}{P_n}\right]$; $\xi_{in}^{k+1} = \sigma_{in}^{k+1} + a_k + b_k - b_{k+1} P_n$, $b_{k+1} = \left[\frac{\sigma_{in}^{k+1} + a_k + b_k}{P_n}\right]$, $k = \overline{1, N_i}$.

Отсюда

$$k_i = \{[(\xi_{in}^{N_i} P_n) + \xi_{in}^{N_i-1}] P_n + \xi_{in}^{N_i-2}\} P_n + \ldots + \xi_{in}^1. \tag{4}$$

Теперь можем определить

$$Q = \sum_{i=1}^{n} (k_i + l_i) m_i. \tag{5}$$

Ясно, что величина Q коррекции числа $A'B'$ равна $\sum_{i=1}^{n} n_i m_i$.

При этом, если

$$Q = \sum_{j \in N} m_j, \tag{6}$$

то $A'B'$ имеет РПНР в виде $(\gamma_1, \gamma_2, \ldots, \gamma_j, \gamma_{j+1}, \ldots, \gamma_{j+l}, \gamma_{j+l+1}, \ldots, \gamma_n)$, где $j+1$, $j+2$, ... , $j+l$ индексы m_j, вошедших в (6). Если же условие (6) не выполняется, т. е. корректировка $A'B'$ невозможна, то при определении $A'B'$ произошло мультипликативное переполнение.

Подсчитаем количество модульных операций, необходимых для выполнения операции мультипликативного переполнения. Для вычисления

разрядов $\beta_{in}^{N_i}$ потребуется $2+\log_2(k-1)$ модульных операций, для получения выражений (2) — 1 модульная операция, для выражения (3) — $\log_2 N$ модульных операций, для (4) — $2N-2$ и для (5) — $1+\log_2 n$ модульных операций. Итого: $2+\log_2(k-1)+2N+\log_2 N+2\log_2 n$ модульных операций, где $N=\max\{N_1, N_2, \ldots, N_n\}$; k — разрядность s_t.

Следует отметить, что предложенный метод определения мультипликативного переполнения легко перенести как на классическую, так и на нормированную СКВ и систему типа Сасаки.

ЛИТЕРАТУРА

1. Буза М. К.— В сб.: Вопросы кибернетики и математики.— Минск, 1970.
2. Буза М. К., Поснов Н. Н.— Вестн. Белорусского ун-та. Сер. 1, мат., физ., мех., 1970, № 3, с. 23.
3. Торгашев В. А. Система остаточных классов и надежность.— М., 1973.

Поступила в редакцию 25.01.79.

Кафедра МО ЭВМ

УДК 518:512.25

Л. М. ГОРОДЕЦКИЙ

КВАЗИОБРАТНЫЕ МАТРИЦЫ И РЕШЕНИЕ СИСТЕМ ЛИНЕЙНЫХ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ

Пусть L_k — некоторое k-мерное подпространство линейного пространства, элементами которого являются векторы-столбцы размерности n, и A — невырожденная $n\times n$-матрица.

Обозначим через M_k множество невырожденных матриц H_k, удовлетворяющих соотношениям

$$(AH_k-I)F_k=0,\ (H_kA-I)F_k=0, \tag{1}$$

где F_k — матрица размерности $n\times k$, столбцы которой образуют базис пространства L_k. Очевидно, что множество M_k не зависит от выбора базиса в L_k и содержит, по крайней мере, матрицу A^{-1}.

Элементы множества M_k назовем квазиобратными матрицами к A над пространством L_k. В свою очередь, матрица A является квазиобратной к любой $H_k\in M_k$, т. е. введенное соотношение симметрично.

Теорема 1. Если матрица A_k квазиобратна над L_k к некоторой $H_k\in M_k$, то она является квазиобратной к любой матрице из M_k.

Таким образом, операция квазиобращения разбивает все множество невырожденных матриц на пары подмножеств со взаимно квазиобратными элементами.

Пусть $L_k^{\perp}=\{x: x^{\top}y=0,\ \forall y\in L_k\}$ и $AL_k=\{x: x=Ay,\ y\in L_k\}$.

Теорема 2. Для того, чтобы невырожденная матрица H_k являлась квазиобратной к A, необходимо и достаточно, чтобы существовала матрица W_k, столбцы которой ортогональны проекции AL_k на $L_k^{\perp}$, такая что

$$H_k=A^{-1}+W_k^{\top}(I-F_kF_k^{+}). \tag{2}$$

Здесь через F_k^{+} обозначена псевдообратная [1] к F_k матрица.

Если $AL_k=L_k$, то множество M_k соответствует множеству невырожденных линейных операторов, сужение которых на L_k совпадает с A^{-1} и, в силу этого [2], все квазиобратные матрицы имеют, по крайней мере, k одинаковых собственных значений.

Рассмотрим итерационный процесс

$$x_{k+1}=x_k-H_kf_k,\ f_k=f(x_k) \tag{3}$$

решения системы линейных уравнений

$$f(x)=Ax-b=0. \tag{4}$$

Если невырожденные матрицы H_k удовлетворяют условиям

$$H_0=I,\ H_k\Delta f_j=\Delta x_j,\ 0\leqslant j<k\leqslant n, \tag{5}$$