УДК 004.36 DOI: 10.17587/it.26.570-576

С. А. Инютин, д-р техн. наук, профессор,e-mail: inyutin_int@mail.ru,
Московский авиационный институт (национальный исследовательский университет) (МАИ)

Метрики в модулярном векторном пространстве

Модулярные представления числовых величин в форме кортежей вычетов по взаимно простым модулям из некоторой конечной совокупности можно рассматривать как множество модулярных векторов. Множество модулярных векторов рассматривается как линейное подпространство в векторном пространстве, содержащем векторы с компонентами, имеющими ограниченное значение, его кольцевая структура не учитывается. Анализируются свойства линейного модулярного подпространства, способы определения новых скалярных произведений, что позволяет ввести новые метрики. Введенные алгебраические конструкции предназначены для анализа сходимости многоразрядных параллельных вычислительных процессов в больших компьютерных диапазонах, оперирующих с числовыми величинами в модулярном представлении. Введенные числовые векторные представления ориентированы на применение в модулярных реконфигурируемых вычислительных системах SIMD-архитектуры.

Ключевые слова: *модулярное векторное подпространство, модулярные скалярные произведения, модулярные метрики, параллельный модулярный вычислительный процесс, многопроцессорная реконфигурируемая система*

Введение

В модулярной компьютерной системе счисления числовые величины $A(\mathrm{mod}\,P) \in \{0,1,2,\ldots P-1\}$, принадлежащие полной системе вычетов по модулю P, представлены векторами с компонентами — наименьшими неотрицательными вычетами (абсолютно наименьшими) по простым (взаимно простым) модулям:

$$A(\mathrm{mod}\,P) \leftrightarrow \\ \leftrightarrow (a_1(\mathrm{mod}\,p_1),\ldots, a_i(\mathrm{mod}\,p_i),\ldots a_n(\mathrm{mod}\,p_n)), \quad (1)$$

где $a_i \equiv A(\mathrm{mod}\,p_i), a_i \in \{0,1,\ldots,p_i-1\}$ — вычет по модулю числовой величины A по одному из модулей $p_i \in \{p_1,\ldots p_n\}$, принадлежащих полной упорядоченной системе оснований модулярной системы: $p_1 < p_2 \ldots < p_i < \ldots p_n$.

Векторы, определяемые соотношением (1), назовем модулярными.

Для анализа сходимости модулярных вычислительных процессов, в частности процессов, в которых входные, промежуточные и выходные числовые величины представлены в модулярной системе счисления (без выхода за ее пределы), рассмотрим свойства метрического векторного подпространства, элементами которого являются n-мерные модулярные векторы.

1. Свойства модулярного векторного подпространства

Введем n-мерное линейное векторное пространство V^n, элементы которого — векторы с компонентами, имеющими ограниченное значение. Для ограничения значения компонент используется операция вычисления наименьших неотрицательных или абсолютно наименьших вычетов по некоторому фиксированному модулю g, в частности по модулю максимального модулярного основания $g = p_n$:

$$A(\mathrm{mod}\,p_n^n) \leftrightarrow \\ \leftrightarrow (a_1(\mathrm{mod}\,p_n),\ldots,a_i(\mathrm{mod}\,p_n),\ldots a_n(\mathrm{mod}\,p_n)).$$

Компоненты таких векторов будем считать цифрами представления некоторой числовой величины A в позиционной системе с основанием p_n.

Векторное пространство V^n является линейным. Для его элементов выполняются условия однородности и аддитивности:

$$\forall k \in Z\ kA(\mathrm{mod}\,p_n^n) \leftrightarrow (ka_1(\mathrm{mod}\,p_n),\ldots, \\ \ldots, ka_i(\mathrm{mod}\,p_n),\ldots, ka_n(\mathrm{mod}\,p_n));$$

$$(A+B)\,(\mathrm{mod}\,p_n^n) \leftrightarrow ((a_1+b_1)(\mathrm{mod}\,p_n),\ldots, \\ \ldots,(a_i+b_i)(\mathrm{mod}\,p_n),\ldots.(a_n+b_n)(\mathrm{mod}\,p_n)).$$

В этом n-мерном векторном пространстве V^n введем подпространство W^n модулярных векторов, компоненты которых принадлежат полным системам вычетов по модулям соответствующих модулярных оснований. Векторное подпространство W^n назовем модулярным, его кольцевая структура при такой трактовке не учитывается. Элементами подпространства являются модулярные векторы, значения компонент которых ограничены результатами операций вычисления наименьших неотрицательных или абсолютно наименьших вычетов по отдельным модулям выбранной модулярной системы счисления. После определения скалярного произведения в векторном пространстве можно ввести ортогональное подпространство.

Модулярное подпространство W^n является линейным. Для его элементов

$$A(\mathrm{mod}\, P) \leftrightarrow$$
$$\leftrightarrow (a_1(\mathrm{mod}\, p_1),\ldots,a_i(\mathrm{mod}\, p_i),\ldots.a_n(\mathrm{mod}\, p_n));$$
$$B(\mathrm{mod}\, P) \leftrightarrow$$
$$\leftrightarrow (b_1(\mathrm{mod}\, p_1),\ldots,b_i(\mathrm{mod}\, p_i),\ldots.b_n(\mathrm{mod}\, p_n))$$

выполняются условия однородности и аддитивности:

$$\forall k \in Z\ kA(\mathrm{mod}\, P) \leftrightarrow (ka_1(\mathrm{mod}\, p_1),\ldots,$$
$$\ldots, ka_i(\mathrm{mod}\, p_i),\ldots,ka_n(\mathrm{mod}\, p_n));$$
$$(A+B)\ (\mathrm{mod}\, P) \leftrightarrow ((a_1+b_1)(\mathrm{mod}\, p_1),\ldots,$$
$$\ldots,(a_i+b_i)(\mathrm{mod}\, p_i),\ldots,(a_n+b_n)(\mathrm{mod}\, p_n)).$$

Операции над модулярными векторами — умножение на число и сложение — выполняются посредством вычислений вычетов компонент модулярных векторов по соответствующим модулям [1, 2].

2. Модулярные скалярные произведения

Для введения в подпространстве W^n модулярных векторов понятий ортогональности и базиса рассмотрим скалярные произведения.

Сформируем требования, которым должно удовлетворять модулярное скалярное произведение (A, B) двух векторов A, B, принадлежащих векторному модулярному подпространству W^n, учитывающее особенности модулярной системы счисления:

- симметричность, равенство $(A, B) = (B, A)$ должно выполняться для наименьших неотрицательных и абсолютно наименьших вычетов по модулю;
- умножение на число скалярного произведения $k(A, B)$ является произведением двух чисел;
- для выполнения аддитивности $((A + B)C) = (A, C) + (B, C)$ сумму векторов в модулярном пространстве определим следующим образом:

$$((A+B-kP),C) = (A,C)+(B,C)-k(P,C) =$$
$$= (A,C)+(B,C)+0;$$

- для выполнения условия неотрицательности модуля вектора используются наименьшие неотрицательные вычеты по модулю:

$$\forall A \in M\ (A,A) \geqslant 0,\ (A,A) = 0 \text{ при } A = \theta,$$

где θ — нулевой модулярный вектор.

Введем скалярные произведения векторов с модулярными компонентами, принадлежащих W^n.

Определение. В общем случае скалярное произведение следующего вида есть сумма скалярных произведений:

$$\left(\left(\sum_{i=1}^{k} A_i - kP\right), C\right) =$$
$$= \sum_{i=1}^{k}(A_i,C) + k(P,C) = \sum_{i=1}^{k}(A_i,C).$$

Определение. Скалярное произведение (первое) двух модулярных векторов A, $B \in W^n$ является числом:

$$(A,B) = \sum_{i=1}^{n} |a_i|_{p_i} |b_i|_{p_i}, \qquad (2)$$

где $|a_i|_{p_i}$ — обозначена бинарная операция вычисления вычета по модулю p_i в инфиксной записи.

Замечание $(A,B) < n(p_n - 1)^2$.

Введем модуль (первый) модулярного вектора как сумму квадратов вычетов по соответствующим модулям:

$$(A,A) = \sum_{i=1}^{n} |a_i|^2_{p_i},\ |A| = \sqrt{\sum_{i-1}^{n} |a_i|^2_{p_i}},$$
$$|A|^2 = \left(\sqrt{\sum_{i-1}^{n} |a_i|^2_{p_i}}\right)^2 = \sum_{i-1}^{n} |a_i|^2_{p_i}.$$

Замечание. В этих соотношениях и далее используется арифметическое значение квадратного корня.

Для вычисления скалярного произведения (2) возможно использование наименьших неотрицательных или абсолютно-наименьших вычетов по модулю.

Теорема Т-1. Для скалярного произведения (2) неравенство Коши—Буняковского имеет следующий вид:

$$\sum_{i-1}^{n}|a_i|_{p_i}|b_i|_{p_i} \leqslant \sqrt{\sum_{i-1}^{n}|a_i|_{p_i}^2}\sqrt{\sum_{i-1}^{n}|b_i|_{p_i}^2}.$$

Доказательство.

Сформируем выражение $C = |A|^2B - (A,B)A$, которое возведем в квадрат:

$$|C|^2 = (|A|^2B - (A,B)A)^2 =$$
$$= (|A|^2)^2|B|^2 - 2(A,B)^2|A|^2 + (A,B)^2|A|^2 =$$
$$= |A|^2(|A|^2|B|^2 - (A,B)^2).$$

Выполняется неравенство $|C|^2 \geqslant 0$. Следовательно, выполняются неравенства

$$(|A|^2|B|^2 - (A,B)^2) \geqslant 0,\ |A|^2|B|^2 \geqslant (A,B)^2 \text{ или}$$

$$|A||B| \geqslant (A,B) \text{ или } \sum_{i-1}^{n}|a_i|_{p_i}|b_i|_{p_i} \leqslant \sqrt{\sum_{i-1}^{n}|a_i|_{p_i}^2}\sqrt{\sum_{i-1}^{n}|b_i|_{p_i}^2}.$$

Неравенство выполняется при использовании наименьших неотрицательных вычетов или абсолютно наименьших вычетов по модулю.

Теорема Т-2. Для скалярного произведения (2) выполняется неравенство треугольника

$$\sqrt{\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}^2} + \sqrt{\sum_{i=1}^{n}|(z_i - y_i)|_{p_i}^2} \geqslant \sqrt{\sum_{i=1}^{n}|(x_i - y_i)|_{p_i}^2}.$$

Доказательство.

Выполняются следующие модульные соотношения:

$$|x_i - y_i|_{p_i} = ||x_i - z_i|_{p_i} + |z_i - y_i|_{p_i}|_{p_i} =$$
$$= |x_i - z_i|_{p_i} + |z_i - y_i|_{p_i} - 0|p_i,$$

где символом $0|p_i$ обозначены альтернативные варианты "или".

Следовательно,

$$|x_i - z_i|_{p_i} + |z_i - y_i|_{p_i} \geqslant |x_i - y_i|_{p_i}.$$

Возведем обе части неравенства в квадрат и просуммируем:

$$\sum_{i=1}^{n}(|(x_i - z_i)|_{p_i}^2 + 2|(x_i - z_i)|_{p_i}|(z_i - y_i)|_{p_i} +$$
$$+ |(z_i - y_i)|_{p_i}^2) \geqslant \sum_{i=1}^{n}|(x_i - y_i)|_{p_i}^2$$

Применим неравенство Коши—Буняковского, которое для модульных соотношений в данном случае имеет вид

$$\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}|(z_i - y_i)|_{p_i} \leqslant$$
$$\leqslant \sqrt{\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}^2}\sqrt{\sum_{i=1}^{n}|(z_i - y_i)|_{p_i}^2}.$$

Получим

$$\left(\sqrt{\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}^2}\right)^2 + 2\sqrt{\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}^2}\sqrt{\sum_{i=1}^{n}|(z_i - y_i)|_{p_i}^2} +$$
$$+\left(\sqrt{\sum_{i=1}^{n}|(z_i - y_i)|_{p_i}^2}\right)^2 \geqslant \sum_{i=1}^{n}|(x_i - y_i)|_{p_i}^2$$

или

$$\left(\sqrt{\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}^2} + \sqrt{\sum_{i=1}^{n}|(z_i - y_i)|_{p_i}^2}\right)^2 \geqslant \sum_{i=1}^{n}|(x_i - y_i)|_{p_i}^2$$

или

$$\sqrt{\sum_{i=1}^{n}|(x_i - z_i)|_{p_i}^2} + \sqrt{\sum_{i=1}^{n}|(z_i - y_i)|_{p_i}^2} \geqslant \sqrt{\sum_{i=1}^{n}|(x_i - y_i)|_{p_i}^2}.$$

Теорема доказана.

В символике векторной алгебры скалярное произведение (2) имеет вид

$$(A,B) = (a_1(\mathrm{mod}\ p_1),\ldots,a_n(\mathrm{mod}\ p_n))\times$$
$$\times(b_1(\mathrm{mod}\ p_1),\ldots,b_n(\mathrm{mod}\ p_n))^{\mathrm{T}},$$

где $^{\mathrm{T}}$ — символ транспонирования матрицы, вектора.

Введем модулярное (второе) скалярное произведение векторов $A,\ B \in W^n$.

Определение. Модулярное (второе) скалярное произведение двух модулярных векторов $A,\ B \in W^n$ есть число

$$(A,B)' = \sum_{i=1}^{n}|a_ib_i|_{p_i}. \qquad (3)$$

Замечание. $(A,B)' < n(p_n - 1)$.

Для модулярного скалярного произведения (3), учитывая взаимно однозначное соответствие, возможно использование наименьших неотрицательных и абсолютно наименьших вычетов по модулю.

Определим второй модуль модулярного вектора $A(\mathrm{mod}P)$ как сумму квадратичных вычетов по соответствующим модулям:

$$(A,A)' = \sum_{i=1}^{n}|a_ia_i|_{p_i} = \sum_{i-1}^{n}|a_i^2|_{p_i};$$

$$|A| = \sqrt{\sum_{i-1}^{n}|a_i^2|_{p_i}};\ |A|^2 = \left(\sqrt{\sum_{i-1}^{n}|a_i^2|_{p_i}}\right)^2 = \sum_{i-1}^{n}|a_i^2|_{p_i}.$$

Для вычисления модулей модулярных векторов используются наименьшие неотрица-

тельные вычеты, что не нарушает условие для скалярного произведения:

$$\forall A\ (A, A) \geqslant 0,\ (A, A) = 0 \text{ при } A = 0.$$

Теорема Т-3. Для модулярного скалярного произведения (3) неравенство Коши—Буняковского имеет следующий вид:

$$\sum_{i-1}^{n} |a_i b_i|_{p_i} \leqslant \sqrt{\sum_{i-1}^{n} |a_i^2|_{p_i}} \sqrt{\sum_{i-1}^{n} |b_i^2|_{p_i}}.$$

Доказательство.

Сформируем следующее выражение:

$$C = |A|^2 B - (A, B)' A.$$

Возведя выражение в квадрат, получим

$$|C|^2 = (|A|^2 B - (A, B)' A)^2 =$$
$$= (|A|^2)^2 |B|^2 - 2(A, B)'^2 |A|^2 + (A, B)'^2 |A|^2 =$$
$$= |A|^2 (|A|^2 |B|^2 - (A, B)'^2).$$

Учитывая, что $|C|^2 \geqslant 0$, можно заметить, что для второго числового сомножителя, записанного в виде разности квадрата модуля модулярного вектора и квадрата скалярного произведения (3), должно выполняться условие

$$(|A|^2 |B|^2 - (A, B)'^2) \geqslant 0,$$

следовательно,

$$|A|^2 |B|^2 \geqslant (A, B)'^2 \text{ и } (A, B)' \leqslant |A||B|$$
$$\text{или } \sum_{i-1}^{n} |a_i b_i|_{p_i} \leqslant \sqrt{\sum_{i-1}^{n} |a_i^2|_{p_i}} \sqrt{\sum_{i-1}^{n} |b_i^2|_{p_i}}.$$

Неравенство выполняется при использовании в левой части наименьших неотрицательных вычетов или абсолютно наименьших вычетов по модулю. В правой части неравенства возможно использование только наименьших неотрицательных вычетов по модулю, иначе нарушается соответствующее условие для скалярного произведения.

Теорема Т-4. Для модулярного скалярного произведения (3) выполняется неравенство треугольника

$$\sqrt{\sum_{i=1}^{n} |(x_i - z_i)^2|_{p_i}} + \sqrt{\sum_{i=1}^{n} |(z_i - y_i)^2|_{p_i}} \geqslant$$
$$\geqslant \sqrt{\sum_{i=1}^{n} |(x_i - y_i)^2|_{p_i}}.$$

Доказательство.

Выполняются следующие модульные соотношения:

$$|x_i - y_i|_{p_i} = \| x_i - z_i |_{p_i} + | z_i - y_i |_{p_i} |_{p_i} =$$
$$= |x_i - z_i|_{p_i} + |z_i - y_i|_{p_i} - 0|p_i,$$

где символом $0|p_i$ обозначены альтернативные варианты "или". Следовательно,

$$|x_i - z_i|_{p_i} + |z_i - y_i|_{p_i} \geqslant |x_i - y_i|_{p_i}.$$

Возведем в квадрат обе части неравенства

$$(|x_i - z_i|_{p_i} + |z_i - y_i|_{p_i})^2 \geqslant (|x_i - y_i|_{p_i})^2,$$

получим

$$|x_i - z_i|_{p_i}^2 + |x_i - z_i|_{p_i} |z_i - y_i|_{p_i} + |x_i - z_i|_{p_i} |z_i - y_i|_{p_i} + \\ + |z_i - y_i|_{p_i}^2 \geqslant (|x_i - y_i|_{p_i})^2. \quad (4)$$

Возьмем вычеты по модулю от каждого слагаемого в обеих частях неравенства (4) и выполним преобразования по модулю в левой части неравенства:

$$\| (x_i - z_i)^2 |_{p_i} + |(x_i - z_i)(z_i - y_i)|_{p_i} +$$
$$+ |(x_i - z_i)(z_i - y_i)|_{p_i} + |(z_i - y_i)^2|_{p_i} |_{p_i} \geqslant$$
$$\geqslant \left| (|x_i - y_i|_{p_i})^2 \right|_{p_i};$$
$$\| (x_i - z_i)(x_i - z_i + z_i - y_i) |_{p_i} +$$
$$+ |(x_i - z_i + z_i - y_i)(z_i - y_i)|_{p_i} |_{p_i} \geqslant$$
$$\geqslant \left| (|x_i - y_i|_{p_i})^2 \right|_{p_i}.$$

В результате получим соотношение, которое показывает, что левая часть не меньше правой части:

$$\| (x_i - y_i) |_{p_i} (x_i - y_i) |_{p_i} |_{p_i} \geqslant \left| (x_i - y_i)^2 \right|_{p_i}.$$

Заметим, что при $z = 0$ нестрогое неравенство превращается в равенство.

После возведения в квадрат обеих частей неравенства (4) и вычисления вычетов по модулю окончательно получим слева сумму четырех вычетов по модулю, которая не меньше правой части, содержащей одиночный вычет по модулю:

$$|(x_i - z_i)^2|_{p_i} + |(x_i - z_i)(z_i - y_i)|_{p_i} +$$
$$+ |(x_i - z_i)(z_i - y_i)|_{p_i} + |(z_i - y_i)^2|_{p_i} \geqslant \left| (x_i - y_i)^2 \right|_{p_i}.$$

После суммирования в обеих частях неравенства получим

$$\sum_{i=1}^{n} (|(x_i - z_i)^2|_{p_i} + 2|(x_i - z_i)(z_i - y_i)|_{p_i} +$$
$$+ |(z_i - y_i)^2|_{p_i}) \geqslant \sum_{i=1}^{n} |(x_i - y_i)^2|_{p_i}.$$

Применим неравенство Коши—Буняковского, которое для данного случая имеет вид

$$\sum_{i=1}^{n}|(x_i - z_i)(z_i - y_i)|_{p_i} \leqslant$$
$$\leqslant \sqrt{\sum_{i=1}^{n}|(x_i - z_i)^2|_{p_i}}\sqrt{\sum_{i=1}^{n}|(z_i - y_i)^2|_{p_i}}.$$

В результате получим:

$$\left(\sqrt{\sum_{i=1}^{n}|(x_i - z_i)^2|_{p_i}}\right)^2 + 2\sqrt{\sum_{i=1}^{n}|(x_i - z_i)^2|_{p_i}}\times$$
$$\times\sqrt{\sum_{i=1}^{n}|(z_i - y_i)^2|_{p_i}} + \left(\sqrt{\sum_{i=1}^{n}|(z_i - y_i)^2|_{p_i}}\right)^2 \geqslant$$
$$\geqslant \sum_{i=1}^{n}|(x_i - y_i)^2|_{p_i}$$

или

$$\left(\sqrt{\sum_{i=1}^{n}|(x_i - z_i)^2|_{p_i}} + \sqrt{\sum_{i=1}^{n}|(z_i - y_i)^2|_{p_i}}\right)^2 \geqslant$$
$$\geqslant \sum_{i=1}^{n}|(x_i - y_i)^2|_{p_i}$$

или

$$\sqrt{\sum_{i=1}^{n}|(x_i - z_i)^2|_{p_i}} + \sqrt{\sum_{i=1}^{n}|(z_i - y_i)^2|_{p_i}} \geqslant$$
$$\geqslant \sqrt{\sum_{i=1}^{n}|(x_i - y_i)^2|_{p_i}}.$$

Теорема доказана.

Определение. Модулярный оператор линейной свертки $S(A \cdot B(\mathrm{mod}\, P))$ двух модулярных векторов $A,\ B \in W^n$ вычисляется следующим образом:

$$S(A \cdot B(\mathrm{mod}\, P)) \leftrightarrow$$
$$\leftrightarrow \begin{pmatrix} a_1 \ldots & a_i \ldots & a_n \\ . & . & . \\ a_1 \ldots & a_i \ldots & a_n \ldots \end{pmatrix} \cdot (b_1, \ldots, b_i, \ldots, b_n)^{\mathrm{T}} = \qquad (5)$$
$$= \left(\sum_{i=1}^{n}|a_i b_i|_{p_i}(\mathrm{mod}\, p_1), \ldots, \sum_{i=1}^{n}|a_i b_i|_{p_i}(\mathrm{mod}\, p_n)\right)^{\mathrm{T}}.$$

Рассмотрим вопрос базиса в модулярном векторном подпространстве W^n. В векторном модулярном подпространстве W^n существует как минимум один ортонормированный базис, состоящий из базисных векторов модулярной системы счисления:

$$\forall i = 1, \ldots, n\ B_i(\mathrm{mod}\, P) \leftrightarrow (0(\mathrm{mod}\, p_1), \ldots,$$
$$\ldots, m_i \frac{P}{p_i}(\mathrm{mod}\, p_i), \ldots, 0(\mathrm{mod}\, p_n)) =$$
$$= (0(\mathrm{mod}\, p_1), \ldots, 1(\mathrm{mod}\, p_i), \ldots, 0(\mathrm{mod}\, p_n)),$$

где $\forall i = 1, \ldots, n\ \ m_i = \left|\frac{P}{p_i}\right|_{p_i}^{-1}$.

Базис ортонормированный, скалярные произведения (2) и (3) взятых попарно базисных векторов равны нулю [3, 4]:

$$(B_i, B_j) = (B_i, B_j)' =$$
$$= (0, \ldots, 1(\mathrm{mod}\, p_i), \ldots, 0) \cdot (0, \ldots, 1(\mathrm{mod}\, p_j), \ldots, 0)^{\mathrm{T}} = 0.$$

Базисом в векторном пространстве является любая совокупность линейно независимых векторов, он может быть найден стандартными методами. Решение неоднородной системы линейных алгебраических уравнений, столбцами которой являются базисные векторы, дает разложение по этому базису произвольного вектора, записываемого в правой части системы уравнений.

3. Метрики в векторном модулярном подпространстве

Для анализа сходимости модулярных вычислительных процессов введем два вида расстояний или метрик (аналогов евклидового расстояния) на множестве n-мерных модулярных векторов из подпространства W^n через их скалярные произведения.

Определение. Модулярное расстояние между двумя модулярными величинами — векторами $A,\ B \in W^n$ — на основе скалярного произведения (2) есть число

$$l^1(A, B) = \sqrt{\sum_{i=1}^{n}|a_i - b_i|_{p_i}^2}.$$

Определение. Модулярный вес модулярного вектора A на основе скалярного произведения (2) есть модулярное расстояние между произвольным модулярным вектором и нулевым:

$$w^1(A) = l^1(A, \theta) = \sqrt{\sum_{i=1}^{n}|a_i|_{p_i}^2} = \sqrt{(A, A)}.$$

Модулярный вес, полученный на основе скалярного произведения (2), совпадает с первым модулем вектора в модулярном векторном подпространстве W^n.

Теорема Т-5. Модулярное расстояние $l^1(A, B)$ между двумя модулярными векторами

$A, B \in W^n$ на основе скалярного произведения (2) является метрикой.

Доказательство.

Используя арифметическое значение квадратного корня, можно получить:

1. $l^1(A, B) \geqslant 0$.
2. $l^1(A, B) = 0$, если $A \equiv B(\mathrm{mod}\, P)$.
3. $l^1(A, B) = l^1(B, A)$.
4. Выполнение неравенства треугольника установлено в теореме *Т-2*.

Определение. Модулярное расстояние между двумя модулярными величинами — векторами $A, B \in W^n$ — на основе модулярного скалярного произведения (3) есть число

$$l^2(A, B) = \sqrt{\sum_{i=1}^{n} |(a_i - b_i)^2|_{p_i}}.$$

Определение. Модулярный вес модулярного вектора A на основе модулярного скалярного произведения (3) есть модулярное расстояние между произвольным модулярным вектором и нулевым:

$$w^2(A) = l^2(A, \theta) = \sqrt{\sum_{i=1}^{n} |a_i^2|_{p_i}} = \sqrt{(A, A)'}.$$

Модулярный вес, полученный на основе модулярного скалярного произведения (3), совпадает со вторым модулем вектора в модулярном векторном подпространстве W^n.

Модулярные веса, полученные на основе скалярных произведений (2) и (3), не равны в общем случае.

Теорема Т-6. Модулярное расстояние $l^2(A, B)$ между двумя модулярными векторами $A, B \in W^n$ на основе модулярного скалярного произведения (3) является метрикой.

Доказательство.

Используя арифметическое значение квадратного корня, можно получить:

1. $l^2(A, B) \geqslant 0$.
2. $l^2(A, B) = 0$, если $A \equiv B(\mathrm{mod}\, P)$.
3. $l^2(A, B) = l^2(B, A)$.
4. Выполнение неравенства треугольника установлено в теореме *Т-4*.

Приведем для полноты обзора, кроме выше введенных метрик, остаточное расстояние (аналог метрики Хэмминга), применимое для задач помехозащитного модулярного кодирования дискретной информации и учитывающее характер модульной ошибки канала передачи, хранения и обработки для векторов с модулярными компонентами [5,6].

Определение. Остаточное расстояние $d(A, B)$ между двумя модулярными векторами $A, B \in W^n$ есть остаточный вес модульной разности двух модулярных векторов

$$d(A, B) = \sum_{i=1}^{n} \delta(|a_i - b_i|_{p_i}),$$

где символ Кронекера

$$\delta(|a_i - b_i|_{p_i}) = \begin{cases} 1, \text{ при } a_i \neq b_i; \\ 0, \text{ при } a_i = b_i. \end{cases}$$

Остаточное расстояние является метрикой, так как для него выполняются соответствующие аксиомы [6].

Остаточный вес определяется как остаточное расстояние между произвольным модулярным вектором и нулевым.

Введем модулярный аналог расстояния и веса Ли, предназначенный для помехозащитного кодирования дискретной информации в системах передачи данных с фазовой модуляцией несущего сигнала.

Определение. Модулярный вес Ли $|a_i|_L$ одиночной компоненты a_i модулярного вектора равен:

$$|a_i|_L = a_i \text{ при } 0 \leqslant a_i \leqslant \frac{p_i - 1}{2};$$

$$|a_i|_L = p_i - a_i \text{ при } \frac{p_i - 1}{2} < a_i \leqslant p_i - 1.$$

Определение. Модулярное расстояние Ли между двумя модулярными векторами $A, B \in W^n$ есть сумма модулярных весов Ли разности их компонент:

$$t(A, B) = \sum_{i=1}^{n} ||a_i - b_i|_{p_i}|_L.$$

В вычислительных экспериментах для ускорения вычислений нормированных компонент модулярных векторов, а также ряда функций, например оператора линейной свертки, необходимые для этих процедур константы хранятся в специальных областях кэш-памяти моделируемой модулярной вычислительной системы [7].

Заключение

Известны классы вычислительных процессов, оперирующих с числовыми величинами и называемых многоразрядными процессами или процессами в больших компьютерных диапазонах. В этих процессах операнды, промежуточные результаты операций и результаты вычислительных процессов являются модулярными числовыми величинами, т.е. представленными в компьютерной моду-

лярной системе счисления [3, 8]. Модулярные представления для целых числовых величин и правильных рациональных дробей при соответствующих алгоритмах позволяют организовать эффективное распараллеливание вычислительного процесса [8, 9]. Технической базой таких параллельных процессов являются вычислительные системы с SIMD-архитектурой, лежащей в основе большинства современных многопроцессорных систем, содержащих кроме центральных процессоров CPU множество графических ускорителей GPU, используемых для распараллеливания вычислений [2, 9].

По оценкам ряда исследователей модулярная машинная арифметика имеет преимущества именно в области параллельных многоразрядных вычислений, она позволяет организовывать высокопроизводительные модулярные вычислительные процессы в больших компьютерных диапазонах [9, 10].

Анализ особенностей модулярного векторного подпространства, введенные модулярные скалярные произведения позволяют определить метрики в векторном модулярном пространстве W^n, предназначенные для оценки сходимости модулярных вычислительных процессов.

Список литературы

1. **Амербаев В. М.** Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 320 с.
2. **Ахо А.** и др. Построение и анализ вычислительных алгоритмов. М.: Мир, 2011. 536 с.
3. **Инютин С. А.** Основы модулярной алгоритмики. Ханты-Мансийск: Полиграфист, 2009. 237 с.
4. **Inutin S.** Parallel Square Modular Computer Algebra. Transaction of Parallel Processing and Applied Mathematics. Poland-Denmark: Springer, LNCS 3019, 2003. P. 539—547.
5. **Инютин С. А**. Проблема метрик в модулярном помехозащитном кодировании // Труды СурГУ. 2008. Вып. 12. С. 84—93.
6. **Торгашев В. А.** Система остаточных классов и надежность ЦВМ. М.: Советское радио, 1973. 120 с.
7. **Столярский Е. З., Шилов В. В.** Организация и работа кэш-памяти // Информационные технологии. 2000. № 7. С. 2—8.
8. **Инютин С. А.** Анализ сложности многоразрядных вычислительных процессов // Научные труды МАТИ. 2014. Вып. 22 (94). С. 154—159.
9. **Инютин С. А**. Комплексирование систем счисления для многоразрядных вычислительных процессов // Информационные технологии.2018. Т. 24, № 12. С. 343—347.
10. **Ноден П., Китте К.** Алгебраическая алгоритмика. М.: Мир, 1999. 720с.

S. A. Inyutin, Doctor Technical Science (PhD), Full Professor, e-mail: inyutin_int@mail.ru,
Moscow Aviation Institute (Nation Research University) (MAI), Moscow, Russian Federation

Metrics for Modular Vectors Space

Modular representations of numerical quantities in the form of residue vectors by prime modules from a finite set can be considered as a set of modular vectors. The set of modular vectors is considered as a linear subspace in a vector space containing vectors with components of limited size; its ring structure is not taken into account. The properties of a linear modular subspace, methods for determining new scalar products are analyzed, which allows us to introduce new metrics. The introduced algebraic constructions are designed to analyze the convergence of multi-bit parallel computing processes in large computer ranges that operate with numerical values in the modular representation. The introduced numerical vector representations are oriented for application in modular reconfigurable computing systems of SIMD architecture.

Keywords: *modular vector subspace, modular scalar products, modular metrics, parallel modular computing process, multiprocessor reconfigurable system*

DOI: 10.17587/it.26.570-576

References

1. **Amerbaev V. M.** Theoretic base computer arithmetic, Alma-Ata, Nauka, 1976, 320 p.
2. **Aho A., Hopcroft J., Ullman J.** The design and analysis of computer algorithms, Moscow, Mir, 2011, 536 p.
3. **Inyutin S. A.** Base at modular algorithmic, Hanty-Mansiysk, Poligrafist, 2009, 237 p.
4. **Inutin S.** Parallel Square Modular Computer Algebra. Transaction of Parallel Processing and Applied Mathematics, Poland-Denmark, Springer, LNCS 3019, 2003, pp. 539—547.
5. **Inyutin S. A.** The problem of metrics in modular error control-codes, *Transactions of SUSU*, vol. 12, Surgut, RIO, 2008, pp. 84—93.
6. **Torgashev V. A.** The system of residual classes and the reliability of the computer, Moscow, Soviet Radio, 1973, 120 p.
7. **Stolyarskiy E. Z., Shilov V. V.** Cache organization and operation, *Informatsionnyie Tehnologii*, 2000, no. 7, pp. 2—8.
8. **Inyutin S. A.** Analysis of many digital calculation process, *Nauchnye trudy MATI,* 2014, vol. 22 (94), pp. 154—159.
9. **Inyutin S. A.** Integration of number systems for multi-digit computing processes, *Informatsionnyie Tehnologii*, 2018, no. 12, vol. 26, pp. 343—347.
10. **Noden P., Kitte K.** Algebraic algorithmic, Moscow, Mir, 1999, 720 p.