УДК 681.325

А. А. КОЛЯДА, М. Ю. СЕЛЯНИНОВ

# УМНОЖЕНИЕ ДРОБЕЙ В МОДУЛЯРНОЙ СИСТЕМЕ СЧИСЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНТЕРВАЛЬНОГО ИНДЕКСА

Важнейшей операцией модулярной арифметики является умножение дробей типа Свободы [1]. Ее выполнение обычно осуществляется путем расширения модулярного кода на основания дополнительного диапазона [2]; при этом используются сложноформируемые интегральные характеристики кода: ранг, ядро, коэффициенты полиадического представления чисел. Такой подход сопряжен с существенными аппаратурными затратами. В этой связи большой интерес представляют собой алгоритмы умножения чисел, не требующие введения дополнительных модулей [3—5].

В настоящей работе рассматривается один из методов умножения указанного класса, базирующийся на использовании интервального индекса числа, вычисление которого значительно проще, чем традиционно применяемых интегральных характеристик. Предлагается алгоритм, имеющий конвейерную структуру и обладающий высоким уровнем параллелизма.

Излагаемый нами метод базируется на следующей теореме, вытекающей из работы [6].

**Теорема.** В модулярной системе счисления (МСС) с попарно простыми модулями $m_1, m_2, \ldots, m_k$ для интервального номера $N_k(X) = \left[\frac{X}{M_k}\right]$ произвольного целого числа $X$ справедливо соотношение

$$N_k(X) = J_k(X) + \Theta_k(X), \quad k = 2, 3, \ldots, n, \qquad (1)$$

где $J_k(X)$ — главный интервальный индекс числа $X$; $\Theta_k(X)$ — поправка Амербаева, соответствующая числу $X$ [6—8], через $[y]$ обозначается целая часть действительного числа $y$.

Пусть требуется перемножить две дроби $\frac{A}{M_k^2}$ и $\frac{B}{M_k^2}$, где $A, B \in D = \{-\underset{k}{p} \cdot M_{n-1}, \; -p \cdot M_{n-1} + 1, \ldots, \; p \cdot M_{n-1} - 1\}$, а $M_k^2 > 2 \cdot p \cdot M_{n-1}$, где $M_k = \prod_{i=1} m_i$.

Используя лемму Евклида из теории делимости [9], представим числители исходных дробей в виде

$$A = |A|_{M_k} + N_k(A) \cdot M_k, \quad B = |B|_{M_k} + N_k(B) \cdot M_k, \qquad (2)$$

через $|Y|_p$ обозначается наименьший неотрицательный вычет, сравнимый с величиной $Y$ по модулю $p$.

Тогда искомое произведение дробей формируется в соответствии с формулой

$$\frac{A}{M_k^2}\cdot\frac{B}{M_k^2}=\frac{1}{M_k^2}\left(\frac{|A|_{M_k}\cdot|B|_{M_k}}{M_k^2}+N_k(A)\cdot N_k(B)+\frac{N_k(A)\cdot|B|_{M_k}+N_k(B)\cdot|A|_{M_k}}{M_k}\right).\quad(3)$$

Первый член выражения в скобках $\frac{|A|_{M_k}\cdot|B|_{M_k}}{M_k^2}<1$ отбрасывается и в алгоритме не используется, а третий член заменяется на антье. В результате окончательно получаем следующее расчетное соотношение для произведения дробей:

$$\frac{A}{M_k^2}\cdot\frac{B}{M_k^2}\approx\frac{1}{M_k^2}\cdot(N_k(A)\cdot N_k(B)+N_k(C)),\quad(4)$$

где $C=N_k(A)\cdot|B|_{M_k}+N_k(B)\cdot|A|_{M_k}$.

Из соотношения (4) следует, что базовой операцией при умножении дробей является операция округления чисел, состоящая в получении величин вида $N_k(X)$, $X\in D$.

Обозначим через $(\chi_1, \chi_2, \ldots, \chi_{k-1}, I_k(X))$ интервально-модулярный код числа $X$ в системе с модулями $m_1, m_2, \ldots, m_{k-1}$ [6], где $\chi_i=|X|_{m_i}$, $I_k(X)$ — интервальный индекс числа $X$. Используя интервально-модулярное представление чисел [6], найдем модулярный код интервального индекса $I_k(X)$ $(\xi_k, \xi_{k+1}, \ldots, \xi_n)$ по модулям $m_k, m_{k+1}, \ldots, m_n$ в виде

$$\xi_j=\left|\sum_{i=1}^{k-1}\left|-\frac{|\chi_i\cdot M_{i,k-1}^{-1}|_{m_j}}{m_i}\right|_{m_j}+\frac{\chi_j}{M_{k-1}}\right|_{m_j},\quad(5)$$

где $M_{i,k-1}=M_{k-1}/m_i$, $i=1, 2, \ldots, k-1$, $j=k, k+1, \ldots, n$.

Тогда $j$-ая цифра $g_j$ модулярного кода главного интервального индекса $J_k(X)$ запишется в виде

$$g_j=\left|\frac{\xi_j-\xi_k}{m_k}\right|_{m_j},\quad j=k+1, \ldots, n.\quad(6)$$

Для получения остальных цифр модулярного кода числа $J_k(X)$ осуществим его расширение на модули $m_1, m_2, \ldots, m_k$. С этой целью предварительно вычисляется интервальный индекс $H$ числа $J_k(X)$ в системе с модулями $m_k, m_{k+1}, \ldots, m_n$ и затем применяется формула

$$g_i=\left|\sum_{j=1}^{n-k-1}C_j\cdot g_{k+j}+H\cdot\frac{M_n}{M_k}\right|_{m_j},\quad i=1, 2, \ldots, k,\quad(7)$$

где $C_j=\frac{M_n}{M_k\cdot m_j}$, $j=1, 2, \ldots, n-k-1$.

Для получения окончательного результата производится формирование поправки Амербаева $\Theta_k(X)$ [8] и добавление ее к цифрам модулярного кода числа $J_k(X)$. В результате находим модулярный код $(\widehat{\chi}_1, \widehat{\chi}_2, \ldots, \widehat{\chi}_n)$ числа $N_k(X)$ в заданной МСС.

Изложенное позволяет сформулировать следующий алгоритм умножения дробей $\frac{A}{M_k^2}$ и $\frac{B}{M_k^2}$ в МСС с модулями $m_1, m_2, \ldots, m_n$ $(A, B\in D)$.

1. По модулярным кодам $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ и $(\beta_1, \beta_2, \ldots, \beta_n)$ соответственно чисел $A$ и $B$, согласно выражениям (5)—(7), (1), определяются модулярные коды интервальных номеров $N_k(A)$ и $N_k(B)$ в исходной МСС.

2. Находятся модулярные коды остатков

$$|A|_{M_k}=A-N_k(A)\cdot M_k,\quad |B|_{M_k}=B-N_k(B)\cdot M_k.$$

3. Формируются модулярные коды величин $N_k(A)\cdot N_k(B)$, $C=N_k(A)\times\times|B|_{M_k}+N_k(B)\cdot|A|_{M_k}$.

4. В соответствии с соотношениями (5)—(7), (1) определяется модулярный код интервального номера $N_k(C)$ числа $C$ в заданной МСС.

5. Формируется модулярный код числителя $N_k(A) \cdot N_k(B) + N_k(C)$ искомой дроби.

Нетрудно проверить, что абсолютная погрешность сформулированного алгоритма не превышает величины $\frac{3}{2 \cdot M_k^2}$.

Если формирование поправки Амербаева осуществляется с помощью конвейерных устройств типа [8], то при соответствующей структуре умножителя, реализующего приведенный алгоритм, произведение двух дробей может быть получено за $T_{\text{ум.}} = 8 + 4 \cdot ]\log_2 k[$ модульных тактов при пропускной способности: одна операция умножения за $4 + 2 \cdot ]\log_2 k[$ тактов ($]\log_2 k[$ — наименьшее целое число, не меньшее $\log_2 k$).

Наиболее быстродействующий из известных алгоритмов умножения дробей в МСС позволяет выполнить рассматриваемую операцию за $T_{\text{ум.}} = 16 + 4 \cdot ] \log_2 k [$ модульных тактов [4]. При $n = 8$, что соответствует мощности диапазона МСС порядка $2^{32}$, $T_{\text{ум.}} = 16$ тактам, а $T'_{\text{ум.}} = 24$ тактам. Следует при этом подчеркнуть, что для реализации известного алгоритма [4] необходимо использовать два формирователя ранга, каждый из которых сложнее формирователя поправки Амербаева. Так как указанные блоки составляют главную часть оборудования соответствующих умножителей, можно заключить, что предлагаемый метод позволяет уменьшить объем аппаратурных затрат для выполнения операции умножения дробей примерно в два раза.

## Список литературы


1. Свобода А. // Кибернетический сборник.—1964.— № 8.— С. 115.
2. Торгашев В. А. Система остаточных классов и надежность ЦВМ.— 1973.— С. 24.
3. Евстигнеев В. Г., Горская В. В., Филиппова Н. В. // Науч. труды по проблемам микроэлектроники.—1972.— Вып. 9.— С. 200.
4. Акушский И. Я., Бурцев В. М., Дуйсенов Б. Е., Пак И. Т. Устройство для умножения: А. с. 579617 СССР // БИ.—1977.— № 41.
5. Белова Р. С., Евстигнеев В. Г., Новожилов А. С., Сведе-Швец В. Н. Устройство для умножения в системе остаточных классов: А. с. 962942 СССР // БИ.—1982.— № 36.
6. Коляда А. А. // Вестн. Белорусского ун-та. Сер. 1, физ., мат. и мех.—1986.— № 1.— С. 46.
7. Коляда А. А. // Кибернетика.—1982.— № 3.— С. 124.
8. Коляда А. А. Устройство для формирования позиционных характеристик непозиционного кода: А. с. 968802 СССР // БИ.— 1982.— № 39.
9. Виноградов И. М. Основы теории чисел.—1972.— С. 8.


*Поступила в редакцию 26.10.84.*

*УДК 519.1*

*А. Г. ЛЕВИН*

# *NP*-ПОЛНОТА ЗАДАЧИ РЕАЛИЗАЦИИ ГИПЕРГРАФОВ ГРАФАМИ С ЗАДАННОЙ ЧЕТНОСТЬЮ СТЕПЕНЕЙ ВЕРШИН

В последние годы внимание исследователей привлекают вопросы реализации гиперграфов графами с заданными свойствами [1—10]; тем самым естественно возникает вопрос об *NP*-полноте этих задач. В данной работе покажем, что задача выяснения существования реализации графом с заданной четностью степеней вершин является *NP*-полной.

*Определение* [5]. Граф $R = (V, E)$ называется реализацией гиперграфа $G = (V, W)$, если

1) для каждого $[u, v] \in E$ существует $H \in W$ такое, что $\{u, v\} \subseteq H$;

2) для каждого $H \in W$ порожденный множеством вершин $H$ подграф $R(H)$ графа $R$ связен. Пусть $\Gamma(G, \delta)$ — множество всех реализаций