УДК 004.04

АЛГОРИТМ ВЫЧИСЛЕНИЯ ИНТЕРВАЛЬНО-ПОЗИЦИОННОЙ ХАРАКТЕРИСТИКИ ДЛЯ ВЫПОЛНЕНИЯ НЕМОДУЛЬНЫХ ОПЕРАЦИЙ В СИСТЕМАХ ОСТАТОЧНЫХ КЛАССОВ

К.С. Исупов

Рассматривается метод выполнения и оценки достоверности немодульных операций в системах остаточных классов на основе новой интервально-позиционной характеристики значений модулярных чисел. Предлагается высокоскоростной алгоритм вычисления интервально-позиционной характеристики с априорно задаваемой точностью, приводятся результаты экспериментального исследования его быстродействия.

Ключевые слова: система остаточных классов, интервально-позиционная характеристика, немодульная операция.

Введение

Система остаточных классов (СОК, модулярная система) – непозиционная система счисления [1, 2], определяемая набором взаимно простых модулей $\{p_1, p_2, \ldots, p_n\}$. Числовой диапазон ограничен произведением $\mathrm{P} = \prod p_i$, при этом всякое целое число $\tilde{x}$ из интервала [0, P – 1], многоразрядное в позиционной системе, представляется в виде нескольких малоразрядных позиционных остатков (модулярных разрядов): $\tilde{x} = \langle x_1, x_2, ..., x_n \rangle$, $x_i = |\tilde{x}|_{p_i} \equiv \tilde{x} \bmod p_i$. Число, представленное в такой форме, называется модулярным числом. Все модульные операции (сложение, умножение и пр.) над остатками по каждому основанию СОК выполняются отдельно и независимо, следовательно, в связи с их малой разрядностью, легко и быстро. Поэтому модулярные системы являются перспективной основой для высокоскоростной обработки чисел большой разрядности.

Однако сложность выполнения немодульных операций (сравнение, вычисление знака, оценка переполнения допустимого диапазона представления чисел, масштабирование и пр.) ограничивает область эффективного применения СОК классом узкоспециализированных задач, сводимых к массовому умножению и сложению. Немодульные операции требуют на порядок больше времени, чем модульные и вносят основной вклад в результатную сложность алгоритма. Позиционная величина модулярного числа определяется суммой $|x_1B_1 + \ldots + x_nB_n|_{\mathrm{P}}$, где B_i – ортогональный базис СОК. Прямое вычисление этой суммы затруднено в связи с многоразрядностью ортогональных базисов. Поэтому для выполнения немодульных операций используются различные позиционные характеристики, дающие оценку значения модулярного числа: представление в системе со смешанными основаниями (MRC), ранг, ядро, диагональная функция (SQT) и пр. [1–4]. Однако алгоритмы их вычисления обладают высокой сложностью, поэтому актуальны исследования, направленные на создание эффективных методов выполнения немодульных процедур в СОК.

Целью данной работы является дальнейшее развитие метода выполнения и оценки достоверности операций сравнения, вычисления знака и контроля переполнения допустимого диапазона в СОК, основанного на использовании интервально-позиционных характеристик модулярных чисел [5].

1. Метод интервально-позиционных характеристик для выполнения немодульных операций

Определение. Пусть $E(\tilde{x}/\mathrm{P})$ – функция с областью значений [0, 1), определяющая точное отношение позиционной величины модулярного числа $\tilde{x} = \langle x_1, x_2, ..., x_n \rangle$ к произведению P модулей СОК. Интервально-позиционная характеристика (ИПХ) – замкнутый вещественный интервал $I(\tilde{x}/\mathrm{P}) := \left[\underline{\tilde{x}/\mathrm{P}}, \overline{\tilde{x}/\mathrm{P}} \right]$ с направленно округленными границами, которые удовлетворяют условию включения: $\underline{\tilde{x}/\mathrm{P}} \le I(\tilde{x}/\mathrm{P}) \le \overline{\tilde{x}/\mathrm{P}}$.

ИПХ отображает модулярный числовой диапазон на единичный отрезок (рис. 1) и ставит в соответствие каждому модулярному числу вещественный интервал, локализующий его относительное позиционное, в общем случае многоразрядное, значение $E(\tilde{x}/\mathrm{P}) = \left|\sum_{i=1}^{n} x_i B_i\right|_{\mathrm{P}} \Big/ \mathrm{P}$.

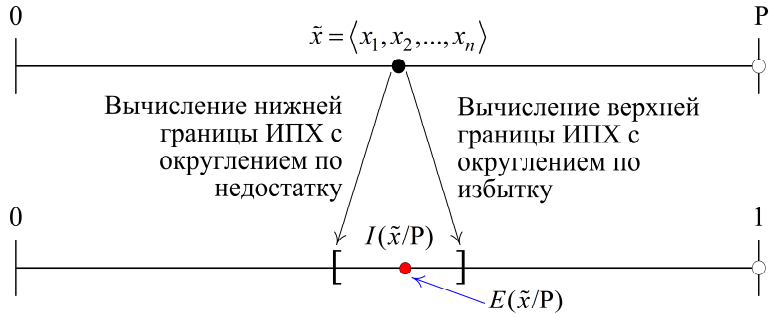

Рис. 1. Интервально-позиционная характеристика модулярного числа

Границы ИПХ могут быть вычислены по формулам [5]

$$\underline{\tilde{x}/\mathrm{P}} = \left| \sum_{i=1}^{n} \downarrow \left(\frac{\left| x_i \cdot \left| \mathrm{P}_i^{-1} \right|_{p_i} \right|_{p_i}}{p_i} \right) \right|_1, \quad \overline{\tilde{x}/\mathrm{P}} = \left| \sum_{i=1}^{n} \uparrow \left(\frac{\left| x_i \cdot \left| \mathrm{P}_i^{-1} \right|_{p_i} \right|_{p_i}}{p_i} \right) \right|_1, \tag{1}$$

где $\left|\mathrm{P}_i^{-1}\right|_{p_i}$ – мультипликативная инверсия от P / p_i (вес ортогонального базиса СОК), x_i – разряды модулярного числа $\tilde{x}$, $|\ |_1$ – дробная часть аргумента, $\downarrow$ и $\uparrow$ – операторы округления «вниз» и «вверх» соответственно. Все $\left|\mathrm{P}_i^{-1}\right|_{p_i}$ являются константами, поэтому последовательное вычисление формул (1) выполняется за время $O(n)$, а параллельное – за время $O(\log n)$. При знании $I(\tilde{x}/\mathrm{P})$ и $I(\tilde{y}/\mathrm{P})$ выполнение немодульных операций над $\tilde{x}$ и $\tilde{y}$ сводится к анализу их границ. Например, сравнения модулярных чисел $\tilde{x}$ и $\tilde{y}$ достаточно проверить условия: если $\underline{\tilde{x}/\mathrm{P}} > \overline{\tilde{y}/\mathrm{P}}$, то $\tilde{x} > \tilde{y}$ и наоборот, если $\overline{\tilde{x}/\mathrm{P}} < \underline{\tilde{y}/\mathrm{P}}$, то $\tilde{x} < \tilde{y}$.

Интервальный учет погрешностей округления, возникающих при вычислении формул (1) в арифметике ограниченной разрядности, обеспечивает достоверность получаемых результатов путем анализа формальных признаков корректности немодульной операции. Например, пересечение $I(\tilde{x}/\mathrm{P}) \cap I(\tilde{y}/\mathrm{P}) \neq \varnothing$ сигнализирует о нарушении достаточного условия достоверности сравнения чисел $\tilde{x}$ и $\tilde{y}$, что позволяет использовать другой метод либо вычислить $I(\tilde{x}/\mathrm{P})$ и $I(\tilde{y}/\mathrm{P})$ с большей точностью. Аналогичным образом формулируются и другие правила выполнения немодульных операций: вычисление знака, оценка переполнения допустимого диапазона и пр. Таким образом, метод интервально-позиционных характеристик позволяет при достаточной точности вычисления ИПХ быстро и достоверно выполнить оценивание значения модулярного кода.

2. Оценка погрешностей вычисления ИПХ

При вычислении ИПХ с ограниченным числом разрядов происходит накопление ошибки округления. Мажорантой абсолютной ошибки является диаметр

$$\operatorname{diam} I(\tilde{x}/\mathrm{P}) = \overline{\tilde{x}/\mathrm{P}} - \underline{\tilde{x}/\mathrm{P}}. \tag{2}$$

Чем меньше $\operatorname{diam} I(\tilde{x}/\mathrm{P})$, тем точнее $I(\tilde{x}/\mathrm{P})$ локализует значение модулярного числа $\tilde{x}$. При вычислении по формулам (1) значение диаметра прямо пропорционально количеству модулей СОК и обратно пропорционально количеству представимых разрядов границ ИПХ. Однако диаметр не отражает в полной мере точность вычисления ИПХ. Если произведение СОК большое, а значение модулярного числа лежит вблизи левой границы диапазона представления, то $E(\tilde{x}/\mathrm{P}) \to 0$, что приводит к накоплению значительной относительной ошибки ИПХ. Результатом этого является снижение информативности ИПХ и затрудняет использование таких «неточных» характеристик для выполнения немодульных операций. Повышению точности способствует вычисление ИПХ средствами длинной арифметики. Однако такой подход приводит к росту времени вычислений,

нивелируя основные преимущества рассматриваемого метода выполнения немодульных операций по сравнению с аналогами. Поэтому далее рассматривается алгоритмический способ разрешения поставленной проблемы.

Относительная ошибка ИПХ определяется максимумом ошибки ее границ:

$$\delta I(\tilde{x}/\mathrm{P}) = \max\left\{\delta\left(\underline{\tilde{x}/\mathrm{P}}\right), \delta\left(\overline{\tilde{x}/\mathrm{P}}\right)\right\}, \qquad (3)$$

где

$$\delta\left(\underline{\tilde{x}/\mathrm{P}}\right) = \left(E(\tilde{x}/\mathrm{P}) - \underline{\tilde{x}/\mathrm{P}}\right)/E(\tilde{x}/\mathrm{P}), \quad \delta\left(\overline{\tilde{x}/\mathrm{P}}\right) = \left(\overline{\tilde{x}/\mathrm{P}} - E(\tilde{x}/\mathrm{P})\right)/E(\tilde{x}/\mathrm{P}).$$

Положим $E(\tilde{x}/\mathrm{P}) = \underline{\tilde{x}/\mathrm{P}}$. Тогда ошибка (3) будет определяться выражением

$$\delta I(\tilde{x}/\mathrm{P}) = \delta\left(\overline{\tilde{x}/\mathrm{P}}\right) = \operatorname{diam} I(\tilde{x}/\mathrm{P})/E(\tilde{x}/\mathrm{P}).$$

Зафиксируем ε – предел допустимой относительной ошибки ИПХ. Минимальное модулярное число $\tilde{x}$, для которого $\delta I(\tilde{x}/\mathrm{P}) \le \varepsilon$, определяется условиями $\tilde{x} \ge \operatorname{diam} I(\tilde{x}/\mathrm{P})\cdot \mathrm{P}/\varepsilon$. Пусть k – количество представимых двоичных разрядов границ, n – количество модулей СОК. Тогда при вычислении по формулам (1) диаметр (2) не превышает $n2^{-k}$. Обозначив $\psi = n2^{-k}/\varepsilon$, получим условие

$$\tilde{x} \ge \psi\cdot\mathrm{P}, \text{ при } \psi < 1. \qquad (4)$$

Таким образом, формулы (1) позволяют вычислить ИПХ с ошибкой, не превышающей ε, только для чисел из поддиапазона $[\psi\mathrm{P}, \mathrm{P}-1]$ и не пригодны для чисел, лежащих в промежутке $[1, \psi\mathrm{P}-1]$. Например, если $\mathrm{P} = 2^{128}$, $n = 8$, $k = 53$, то ИПХ числа $\tilde{x} = 1{,}5\cdot 2^{86}$ будет вычислена с погрешностью $\delta I(\tilde{x}/\mathrm{P}) \approx 0{,}0026 < 2^{-8}$. Взяв меньшее модулярное число, например $\tilde{x} = 1{,}5\cdot 2^{85}$, получим $\delta I(\tilde{x}/\mathrm{P}) \approx 0{,}0052 > 2^{-8}$. Следовательно, для заданного предела ошибки $\varepsilon = 2^{-8}$ значение модулярного числа должно быть не меньше 2^{86}.

3. Итеративный алгоритм вычисления ИПХ

На рис. 2 представлен алгоритм, позволяющий вычислить ИПХ с относительной ошибкой, не превышающей априорно задаваемого предела ε, не прибегая при этом к использованию чисел большой разрядности. Алгоритм основан на предположении, что границы ИПХ представлены в одном из стандартных двоичных форматов с плавающей точкой [6], т. е. в виде

$$\underline{\tilde{x}/\mathrm{P}} = \underline{m}\cdot 2^{e}, \qquad \overline{\tilde{x}/\mathrm{P}} = \overline{m}\cdot 2^{e}, \qquad (5)$$

где $\underline{m}$ и $\overline{m}$ – двоичные k-разрядные мантиссы, а e – порядок (экспонента), что позволяет в пределах числового диапазона безошибочно выполнять их деление на натуральные степени двойки.

Основные принципы работы алгоритма состоят в следующем.

1. Заранее фиксируется максимальная относительная ошибка ε и вычисляется значение ψ, константное при заданном числе модулей и разрядности границ ИПХ. Кроме этого, вычисляется вектор смещающих степеней двойки

$$\mathbf{V} = \left(2^{v_1}, 2^{v_2}, \ldots, 2^{v_g}\right), \forall j = 1, 2, \ldots, g-1 : v_j < v_{j+1},$$

и матрица $g\times n$ смещенных весов ортогональных базисов СОК

$$\mathbf{M} = \begin{pmatrix} \left|2^{v_1}\cdot\left|\mathrm{P}_1^{-1}\right|_{p_1}\right|_{p_1} & \cdots & \left|2^{v_1}\cdot\left|\mathrm{P}_n^{-1}\right|_{p_n}\right|_{p_n} \\ \vdots & \ddots & \vdots \\ \left|2^{v_g}\cdot\left|\mathrm{P}_1^{-1}\right|_{p_1}\right|_{p_1} & \cdots & \left|2^{v_g}\cdot\left|\mathrm{P}_n^{-1}\right|_{p_n}\right|_{p_n} \end{pmatrix}.$$

Для определения элементов V_j вектора $\mathbf{V}$ и $M_{j,i}$ матрицы $\mathbf{M}$ задается упорядоченный g-набор натуральных чисел $\{v_1, v_2, \ldots, v_g\}$, где $v_1 = \lfloor \log_2\{(\mathrm{P}-1)/(\psi\mathrm{P}-1)\}\rfloor$, $v_g = \lceil \log_2\psi\mathrm{P}\rceil$, $v_{j+1} = v_j + v_1$. При этом обеспечивается существование пары соседей (v_{j-1}, v_j) таких, что если $\tilde{x}\cdot 2^{v_{j-1}} < \psi\mathrm{P}$, то $\psi\mathrm{P} \le \tilde{x}\cdot 2^{v_j} \le \mathrm{P}-1$ для всех $\tilde{x}$ из полного диапазона СОК.

2. В процессе работы алгоритма вначале по второй формуле в (1) вычисляется верхняя граница ИПХ, которая сравнивается с ψ. Если $\overline{\tilde{x}/\mathrm{P}} \ge \psi$, то условие (4) выполняется, и тогда вычисляется нижняя граница по первой формуле в (1).

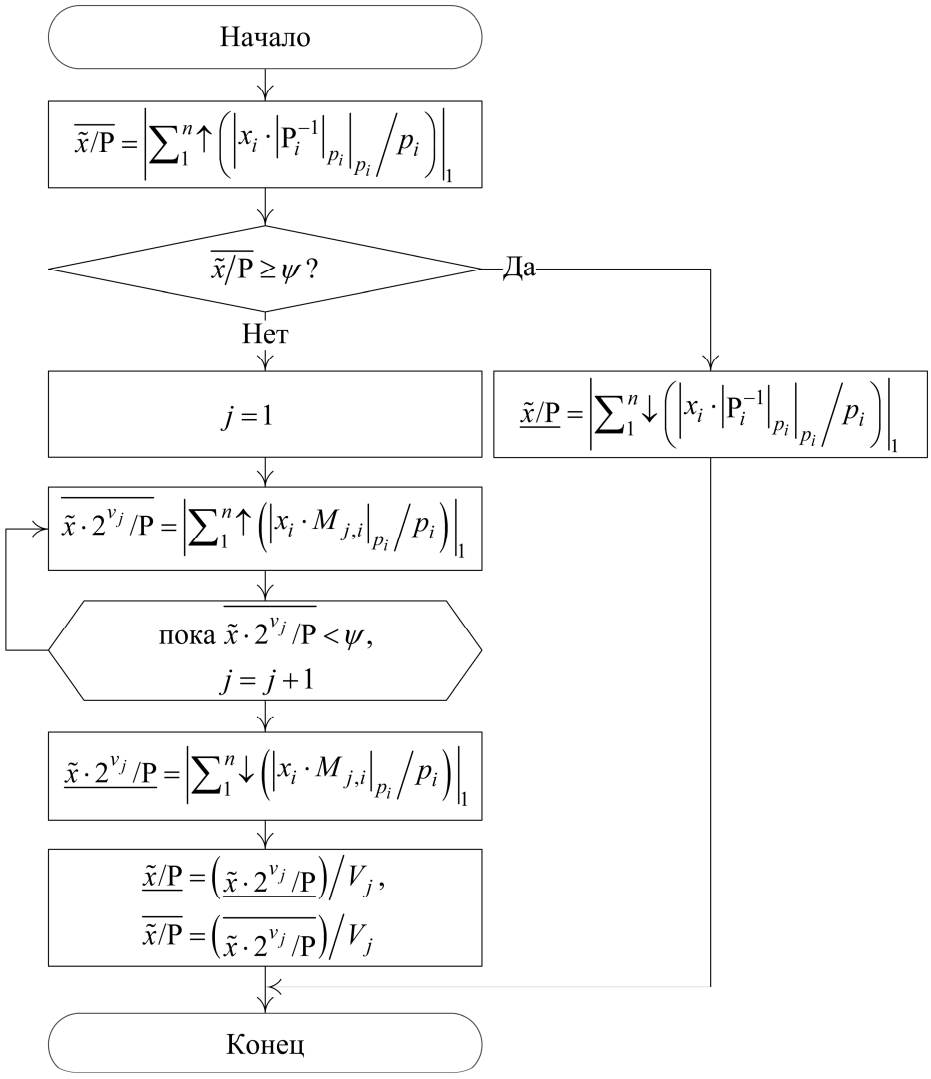

Рис. 2. Алгоритм высокоточного вычисления ИПХ модулярного числа

3. В противном случае для вычисления ИПХ используются формулы

$$\underline{\tilde{x}/\mathrm{P}} = \frac{\left|\sum\limits_{i=1}^{n} \downarrow \left(\dfrac{\left|x_i \cdot M_{j,i}\right|_{p_i}}{p_i}\right)\right|_1}{V_j}, \qquad \overline{\tilde{x}/\mathrm{P}} = \frac{\left|\sum\limits_{i=1}^{n} \uparrow \left(\dfrac{\left|x_i \cdot M_{j,i}\right|_{p_i}}{p_i}\right)\right|_1}{V_j}, \tag{6}$$

где $M_{j,i}$ – элемент, стоящий на пересечении j-й строки и i-го столбца матрицы **M**, а V_j – j-й элемент вектора **V**. Числители в формулах (6) – это границы смещенной ИПХ, т. е. ИПХ для модулярного числа $\tilde{x} \cdot 2^{v_j}$ (рис. 3).

4. Для определения индекса j, по которому выбираются строка из матрицы **M** и смещающая константа V_j из вектора **V**, используемые в формулах (6), поочередно фиксируется $j = 1, 2, 3, \ldots$ и т. д. до тех пор, пока смещенная верхняя граница не будет $\geq \psi$. Выполнение этого условия означает, что требуемая точность вычислений достигнута, т. е. $\delta I(\tilde{x} \cdot 2^{v_j}/\mathrm{P}) \leq \varepsilon$.

5. Деление вычисленной смещенной ИПХ на степень двойки $V_j = 2^{v_j}$ при условии, что ее границы представлены в двоичном формате с плавающей точкой, т. е. в виде (5), состоит в отыскании разности порядков $e - v_j$ и выполняется без потери точности при $e - v_j \geq e_{\min}$. Таким образом, переход от $I(\tilde{x} \cdot 2^{v_j}/\mathrm{P})$ к $I(\tilde{x}/\mathrm{P})$ выполняется без увеличения относительной ошибки с пропорциональным уменьшением диаметра diam $I(\tilde{x}/\mathrm{P})$ в V_j раз, и после деления: $\delta I(\tilde{x}/\mathrm{P}) \leq \varepsilon$.

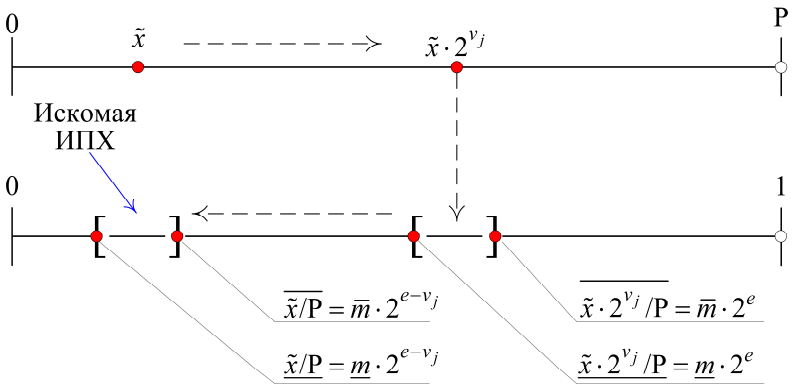

Рис. 3. Смещенная схема вычисления ИПХ

Техническим пределом эффективного использования рассмотренного алгоритма является (помимо очевидного условия $\psi < 1$) лишь ограничение минимального порядка $e_{\min}$ в машинном формате с плавающей точкой, используемом для представления границ ИПХ. В частности, для формата двойной точности binary64 (IEEE-754): $e_{\min} = -1022$, для формата binary80: $e_{\min} = -16382$. Оба этих формата поддерживаются в большинстве универсальных аппаратных вычислительных платформ. Рассмотрим примеры применения алгоритма.

Пример 1. Пусть СОК задана модулями {7, 9, 11, 13}, для которых веса ортогональных базисов: {6, 5, 9, 10}. Требуется вычислить в четырехзначной арифметике ИПХ для числа $\tilde{x} = \langle 4, 7, 3, 12 \rangle$ с ошибкой $\varepsilon \le 1$ %. Для наглядности все вычисления будут выполняться в десятичной системе, поэтому приведенные выше положения имеют соответствующую десятичную интерпретацию.

1. Вначале вычислим $I(\tilde{x}/\mathrm{P})$ в соответствии с формулами (1):

$$\underline{\tilde{x}/\mathrm{P}} = \left| \downarrow \frac{|4\cdot 6|_7}{7} + \downarrow \frac{|7\cdot 5|_9}{9} + \downarrow \frac{|3\cdot 9|_{11}}{11} + \downarrow \frac{|12\cdot 10|_{13}}{13} \right|_1 =$$

$$= |0{,}4285 + 0{,}8888 + 0{,}4545 + 0{,}2307|_1 = 0{,}0025,$$

$$\overline{\tilde{x}/\mathrm{P}} = \left| \uparrow \frac{|4\cdot 6|_7}{7} + \uparrow \frac{|7\cdot 5|_9}{9} + \uparrow \frac{|3\cdot 9|_{11}}{11} + \uparrow \frac{|12\cdot 10|_{13}}{13} \right|_1 =$$

$$= |0{,}4286 + 0{,}8889 + 0{,}4546 + 0{,}2308|_1 = 0{,}0029.$$

Таким образом, $I(\tilde{x}/\mathrm{P}) = [0{,}0025,\ 0{,}0029]$. Точное значение относительной величины для числа $\tilde{x}$ составляет $E(\tilde{x}/\mathrm{P}) = 0{,}002775$, поэтому $\delta\, I(\tilde{x}/\mathrm{P}) = 9{,}91$ %. Воспользуемся итеративным алгоритмом.

2. Необходимые константы для выбранной системы модулей:

$$\psi = 4\cdot 10^{-4}/0{,}01 = 0{,}04, \quad \mathbf{V} = (10^1,\ 10^2,\ 10^3), \quad \mathbf{M} = \begin{pmatrix} 4 & 5 & 2 & 9 \\ 5 & 5 & 9 & 12 \\ 1 & 5 & 2 & 3 \end{pmatrix}.$$

3. Примем $j = 1$ и вычислим смещенную верхнюю границу ИПХ:

$$\overline{\tilde{x}\cdot 10^1/\mathrm{P}} = \left| \uparrow \frac{|4\cdot 4|_7}{7} + \uparrow \frac{|7\cdot 5|_9}{9} + \uparrow \frac{|3\cdot 2|_{11}}{11} + \uparrow \frac{|12\cdot 9|_{13}}{13} \right|_1 =$$

$$= |0{,}2858 + 0{,}8889 + 0{,}5455 + 0{,}3077|_1 = 0{,}0279.$$

Условие (4) не выполняется, поэтому принимаем $j = 2$:

$$\overline{\tilde{x}\cdot 10^2/\mathrm{P}} = \left| \uparrow \frac{|4\cdot 5|_7}{7} + \uparrow \frac{|7\cdot 5|_9}{9} + \uparrow \frac{|3\cdot 9|_{11}}{11} + \uparrow \frac{|12\cdot 12|_{13}}{13} \right|_1 =$$

$$= |0{,}8572 + 0{,}8889 + 0{,}4546 + 0{,}0770|_1 = 0{,}2777.$$

Полученная смещенная граница отвечает условию (4).

4. Вычисляем смещенную нижнюю границу: $\underline{\tilde{x}\cdot 10^2/\mathrm{P}} = 0{,}2773$.

5. Делением смещенных границ на второй элемент вектора **V** получается результатная ИПХ $I(\tilde{x}/\mathrm{P}) = [0{,}002773,\ 0{,}002777]$ (ведущие нули не хранятся в регистрах ЭВМ). Ее относительная ошибка (3) составляет 0,072 %.

Пример 2. В системе с модулями из предыдущего примера даны числа $\tilde{x} = \langle 6,2,9,7 \rangle$ и $\tilde{y} = \langle 2,5,1,10 \rangle$, требуется сравнить их по величине.

1. Вычисляем ИПХ операндов в соответствии с итеративным алгоритмом:

$$\underline{\tilde{x}/\mathrm{P}} = \left|0{,}2857 + 0{,}1111 + 0{,}3636 + 0{,}4615\right|_1 / 10^2 = 0{,}002219,$$

$$\overline{\tilde{x}/\mathrm{P}} = \left|0{,}2858 + 0{,}1112 + 0{,}3637 + 0{,}4616\right|_1 / 10^2 = 0{,}002223,$$

$$\underline{\tilde{y}/\mathrm{P}} = \left|0{,}4285 + 0{,}7777 + 0{,}8181 + 0{,}2307\right|_1 / 10^2 = 0{,}002550,$$

$$\overline{\tilde{y}/\mathrm{P}} = \left|0{,}4286 + 0{,}7778 + 0{,}8182 + 0{,}2308\right|_1 / 10^2 = 0{,}002554.$$

2. ИПХ не пересекаются, причем $I(\tilde{x}/\mathrm{P}) < I(\tilde{y}/\mathrm{P})$, поэтому $\tilde{x} < \tilde{y}$.

3. Выполним проверку переводом в десятичную систему: $\tilde{x} = 20$, $\tilde{y} = 23$.

4. Результаты экспериментов

Были проведены эксперименты, в ходе которых исследовались скорость работы итеративного алгоритма относительно аналогов, а также эффективность метода интервально-позиционных характеристик для выполнения немодульных операций. СОК бала задана 32 16-битными модулями с диапазоном $\mathrm{P} \approx 2^{480}$. В качестве тестовой платформы выступала система Pentium® Dual-Core T4400 2.2 GHz / 2 core / 3 Gb RAM / Intel C++ Compiler v13.0.

1. Исследование быстродействия итеративного алгоритма. Для реализации смещенной схемы был определен 11-элементный вектор $\mathbf{V} = (2^{41}, \ldots, 2^{410}, 2^{440})$ и матрица **M** смещенных весов ортогональных базисов СОК размера 11×32. Рассматривались три алгоритма вычисления ИПХ: классический, основанный на вычислении формул (1) в стандартной 64-битной арифметике (тип Double языка C), итеративный, также использующий тип Double, и многоразрядный, основанный на вычислении формул (1) с использованием 490-битной арифметики библиотеки MPFR [7]. Результаты представлены на рис. 4.

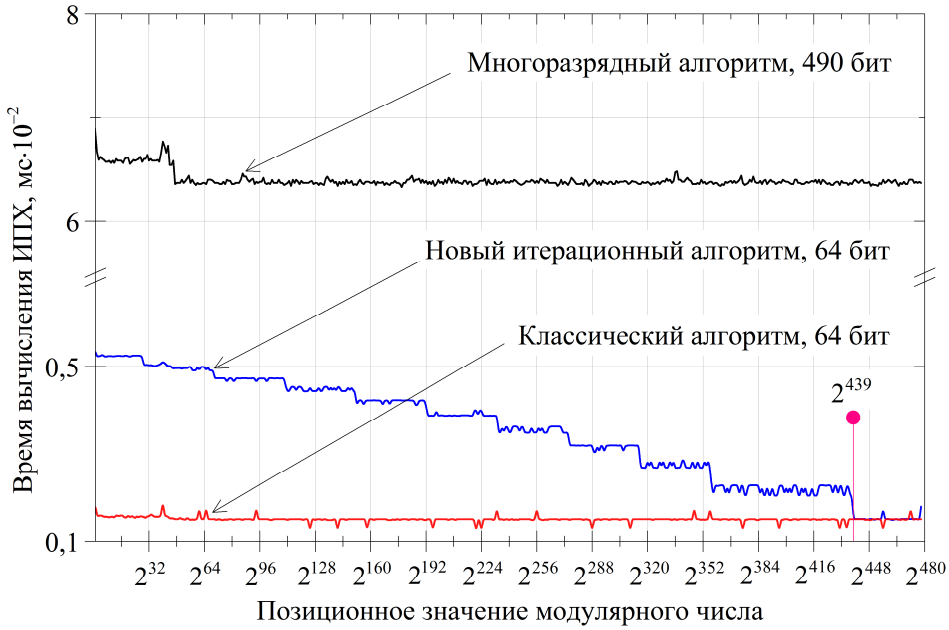

Рис. 4. Время работы алгоритмов вычисления ИПХ

Меткой на рис. 4 отмечена граница области значений модулярных чисел, в пределах которой классический 64-битный алгоритм приводит к вычислению неправильных ИПХ из-за антипереполнения [5] нижней границы. При этом итерационный и многоразрядный алгоритмы позволили

на всем числовом диапазоне $[1, 2^{478}]$ получить корректные ИПХ с относительной ошибкой $\varepsilon < 1$ %. При одинаковой точности результатов время работы нового алгоритма меньше от 11 до 50 раз по сравнению с 490-битным алгоритмом.

Таким образом, разработанный алгоритм, благодаря учету конструктивных особенностей машинного представления ИПХ в виде чисел с плавающей точкой, обеспечивает высокую скорость их высокоточного вычисления, что позволяет эффективно оценивать значения модулярных чисел при выполнении немодульных операций над ними.

2. Исследование быстродействия метода интервально-позиционных характеристик (ИПХ) для выполнения немодульных операций в СОК. В ходе эксперимента выполнялись операции модулярного сравнения, вычисления знака, оценки переполнения допустимого диапазона представления чисел. Сравнение производилось с двумя аналогами: с алгоритмом потактового перехода от СОК к коду смешанной системы (MRC) [8] и с многоразрядным методом ортогональных базисов, основанным на преобразовании модулярных чисел из СОК в позиционную систему с использованием китайской теоремы об остатках (КТО). Цель экспериментов состояла в исследовании скорости последовательного выполнения основных немодульных операций перечисленными методами. ИПХ вычислялись с использованием итерационного алгоритма с установленным пределом относительной ошибки $\varepsilon < 1$ %. Для реализации алгоритмов на основе КТО использовалась длинная арифметика библиотеки GMP [9]. Результаты экспериментов представлены на рис. 5.

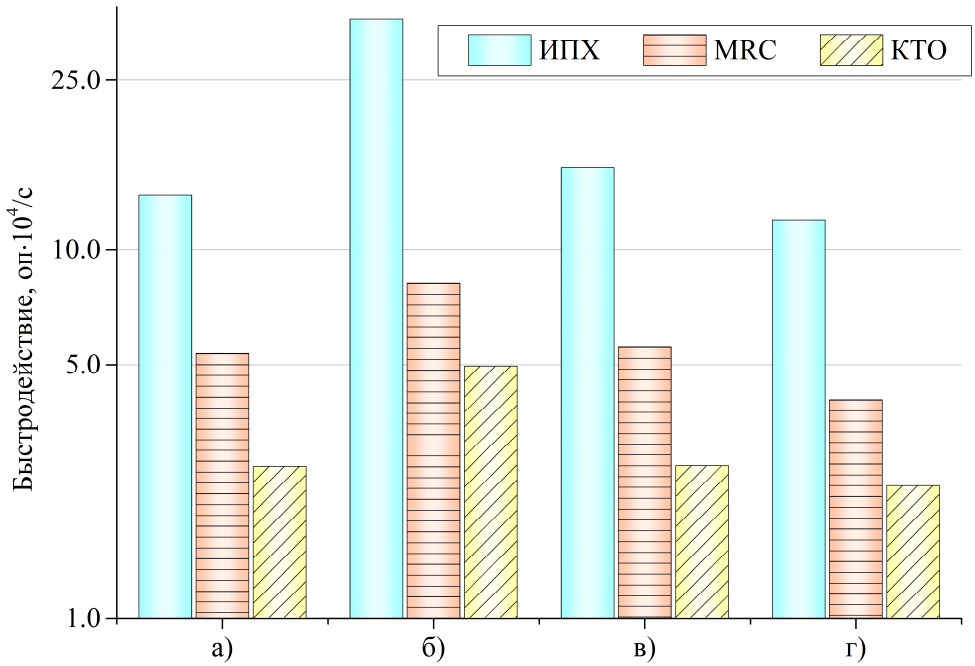

Рис. 5. Быстродействие методов выполнения немодульных операций

Заключение

Исследован новый метод выполнения и оценки достоверности немодульных операций сравнения, вычисления знака и контроля переполнения допустимого диапазона представления чисел в системах остаточных классов, основанный на использовании интервально-позиционной характеристики для оценки значения модулярного кода. Данный метод не требует работы с многоразрядными числами и позволяет в общем случае выполнить перечисленные операции за время $O(n)$ и $O(\log n)$ при параллельной и параллельной реализации соответственно, что на порядок ниже, по сравнению с известными аналогами на основе преобразования чисел из СОК в позиционные (смешанные) системы.

Разработан новый итеративный алгоритм высокоскоростного вычисления интервально-позиционной характеристики. Разработанный алгоритм учитывает конструктивные особенности машинного представления границ вычисляемой ИПХ в виде двоичных чисел с плавающей точкой, заключающиеся в возможности их безошибочного деления на натуральные степени двойки в пределах целевого формата. За счет этого обеспечивается получение результата с априорно задаваемой точностью без использования многоразрядной арифметики, что позволяет быстро и успешно оценивать значения модулярных чисел при выполнении немодульных операций над ними. При вычислениях в 32-модульной СОК с полным диапазоном $P \approx 2^{480}$ время работы алгоритма при одинаковой точности результатов ниже в среднем от 11 до 50 раз по сравнению с 490-битным аналогом.

Данные эксперимента показывают, что скорость выполнения немодульных операций с использованием метода интервально-позиционных характеристик выше в среднем в 3,22 раза по сравнению с MRC-методом, и в 5,93 раза по сравнению с многоразрядным методом на основе китайской теоремы.

Литература

1. Акушский, И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. Радио, 1968. – 440 с.

2. Omondi, A. Residue Number Systems: Theory and Implementation / A. Omondi, B. Premkumar. – London: Imperial College Press, 2007. – 312 p.

3. Модулярные параллельные вычислительные структуры нейропроцессорных систем / Н.И. Червяков, П.А. Сахнюк, А.В. Шапошников, С.А. Ряднов. – М.: Физматлит, 2003. – 288 с.

4. Dimauro, G. A New Technique for Fast Number Comparison in the Residue Number System / G. Dimauro, S. Impedovo, G. Pirlo // IEEE Transactions on Computers. – 1993. – Vol. 42, no. 5. – P. 608–612.

5. Исупов, К. С. Методика выполнения базовых немодульных операций в модулярной арифметике с применением интервальных позиционных характеристик / К.С. Исупов // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2013. – № 3. – С. 31–45.

6. IEEE Standard for Floating-Point Arithmetic . – Introduced 2008-08-29. – New York: Institute of Electrical and Electronics Engineers, 2008. – 70 p.

7. The GNU MPFR Library. – Electronic text data. – Mode of access: http://www.mpfr.org/. – The title from the screen.

8. А. с. 608155 СССР, М. Кл2 G 06 F 7/04. Устройство для сравнения чисел, выраженных в системе остаточных классов / М.Г. Факторович, Ю.Д. Полисский. – № 2317604/18-24; заявл. 19.01.26; опубл. 25.05.78, Бюл. № 19. – 3 с.

9. The GNU Multiple Precision Arithmetic Library. – Electronic text data. – Mode of access: http://gmplib.org/. – The title from the screen.

Исупов Константин Сергеевич, преподаватель кафедры электронных вычислительных машин, Вятский государственный университет (г. Киров); isupov.k@gmail.com.

Bulletin of the South Ural State University
Series "Computer Technologies, Automatic Control, Radio Electronics"
2014, vol. 14, no. 1, pp. 89–97

CALCULATION INTERVAL-POSITIONAL CHARACTERISTIC ALGORITHM FOR IMPLEMENTATION NON-MODULAR OPERATIONS IN RESIDUE NUMBER SYSTEMS

***K.S. Isupov**, Vyatka State University, Kirov, Russian Federation,*
isupov.k@gmail.com

This paper describes the method of implementation and reliability evaluation of non-modular operations in Residue Number Systems which based on the new interval-positional characteristics values of modular numbers. High-speed iterative algorithm for interval-positional characteristic with a priori defined accuracy calculating is proposed, the results of experimental analysis of its performance is given.

Keywords: residue number system, interval-positional characteristic, non-modular operation.

References

1. Akushskiy I.Ya., Yuditskiy D.I. Machine Arithmetic in Residual Classes [*Mashinnaya arifmetika v ostatochnykh klassakh*]. Moscow, Sovetskoe radio, 1968. 440 p.

2. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation. London, Imperial College Press, 2007. 312 p.

3. Chervyakov N.I., Sakhnyuk P.A., Shaposhnikov A.V., Ryadnov S.A. Modular Parallel Computing Structures of Neuroprocessor Systems [*Modulyarnye parallel'nye vychislitel'nye struktury neyroprotsessornykh sistem*]. Moscow, Fizmatlit, 2003. 288 p.

4. Dimauro G., Impedovo S., Pirlo G. "A New Technique for Fast Number Comparison in the Residue Number System". IEEE Transactions on Computers, 1993, vol. 42, no. 5, pp. 608−612.

5. Isupov K.S. The Method for Implementation Non-Modular Operations in Modular Arithmetic with Use of Interval Positional Characteristics [Metodika vypolneniya bazovykh nemodul'nykh operatsiy v modulyarnoy arifmetike s primeneniem interval'nykh pozitsionnykh kharakteristik]. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki* [*News of Higher Educational Institutions. Povolzhsky Region. Technical Science*], 2013, no. 3, pp. 31–45.

6. IEEE Standard for Floating-Point Arithmetic. Introduced 2008-08-29. New York, Institute of Electrical and Electronics Engineers. 2008, 70 p.

7. The GNU MPFR Library. Available at: http://www.mpfr.org/.

8. Faktorovich M.G., Polisskiy Yu.D. Device to Compare Numbers Expressed in Residue Number System [*Ustroystvo dlya sravneniya chisel, vyrazhennykh v sisteme ostatochnykh klassov*]. USSR Patent No. 608155, Byull. Izobret., no. 19 (1978).

9. The GNU Multiple Precision Arithmetic Library. Available at: http://gmplib.org/.

Поступила в редакцию 30 ноября 2013 г.