УДК 621.391

ПРИБЛИЖЕННЫЙ МЕТОД ВЫПОЛНЕНИЯ НЕМОДУЛЬНЫХ ОПЕРАЦИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Червяков Н.И., Авербух В.М., Бабенко М.Г., Ляхов П.А., Гладков А.В., Гапочкин А.В.

ФГБОУ ВПО «Ставропольский государственный университет», Ставрополь, e-mail: Ljahov@mail.ru

Основным препятствием для широкого применения системы остаточных классов в вычислительной технике является сложность выполнения немодульных операций, то есть таких операций, для которых требуется знание о величине числа в целом. Известные методы нахождения позиционных характеристик числа в модулярной форме: метод ортогональных базисов, метод функций Эйлера, метод перевода в обобщенную позиционную систему счисления – обладают такими существенными недостатками, как высокая вычислительная сложность и большие аппаратурные затраты на их реализацию. В статье предлагается новый метод вычисления позиционной характеристики числа в системе остаточных классов, основанный на использовании относительной величины анализируемого числа к полному диапазону. Предложенный метод обладает низкой вычислительной сложностью и малыми аппаратурными затратами. Показано, как можно применять предложенный метод для выполнения основных немодульных операций и приведены примеры.

Ключевые слова: система остаточных классов, приближенный метод, позиционная характеристика, немодульная операция

APPROXIMATE METHOD OF IMPLEMENTATION NON-MODULAR OPERATIONS IN THE RESIDUE NUMBER SYSTEM

Chervyakov N.I., Averbukh V.M., Babenko M.G., Lyakhov P.A., Gladkov A.V., Gapochkin A.V.

Stavropol State University, Stavropol, e-mail: Ljahov@mail.ru

The main obstacle to widespread use of the residue number system in computer science is the complexity of the non-modular operations, that is of such operations, which require knowledge of the magnitude of the whole. The known methods for finding the positional characteristics of the number in a modular form, the method of orthogonal bases, the method of the Euler functions, mixed radix conversion method – have major drawbacks such as high computational complexity and large hardware expenses for their realization. In this paper we propose a new method for calculating the positional characteristics in the system of residual classes, based on the use of the relative magnitude of the sample to the full range. The proposed method has low computational complexity and low instrumental cost. We show how to apply the proposed method to perform basic non-modular operations and examples are given.

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

Современное состояние развития инфокоммуникационных технологий в области обработки и передачи данных характеризуется интенсивным внедрением новых принципов и подходов к обработке информации. Результаты теоретических и практических разработок отечественных и зарубежных специалистов со всей определенностью указывают на то, что одним из перспективных многообещающих путей решения задач сокращения времени обработки данных и повышения надежности вычислительных средств является применение различных форм параллельной обработки данных, в том числе и на основе числовых систем с параллельной структурой. Одним из магистральных направлений среди современных подходов к созданию отказоустойчивых высокопроизводительных средств обработки данных является использование системы остаточных классов (СОК).

Арифметика СОК долгое время привлекала интерес только на теоретическом уровне из-за сложности архитектур, определяемых использованием представляемых данных. Однако быстрый рост технологий вычислительной базы делает СОК удобным для многих приложений цифровой обработки данных, криптографии, систем передачи данных, основанных на множественном доступе с кодовым разделением каналов и др.

Главным преимуществом СОК является разложение динамического диапазона на параллельные каналы с меньшими динамическими диапазонами, определяемыми выбором оснований СОК, которые приводят к операциям без переноса между каналами с различными основаниями и сокращению задержек сигналов.

В качестве недостатка СОК можно отметить трудность выполнения немодульных операций.

Система остаточных классов

Основной теоретико-числовой базой системы остаточных классов является теория сравнений. Полной системой вычетов по модулю p называется совокупность p целых чисел, содержащая точно по одному представителю из каждого класса вычетов

по модулю p. Каждый класс вычетов по модулю p содержит в точности одно из чисел совокупности всех возможных остатков от деления на p: {0, 1, ..., p – }. Множество {0, 1, ..., p – } также называется полной системой наименьших неотрицательных вычетов по модулю p.

Один из методов выполнения арифметических операций над длинными целыми числами основан на простых положениях теории чисел. Представление чисел в СОК позволяет заменить операции с большими числами на операции с малыми числами, которые представлены в виде остатков от деления больших чисел на заранее выбранные взаимно-простые модули $p_1, p_2, ..., p_n$. Пусть

$$A \equiv \alpha_1 \left(\mathrm{mod}\, p_1\right), \quad A \equiv \alpha_2 \left(\mathrm{mod}\, p_2\right),$$

$$A \equiv \alpha_n \left(\mathrm{mod}\, p_n\right). \qquad (1)$$

Тогда целому числу A можно поставить в соответствие кортеж (α_1, α_2, ..., α_n) наименьших неотрицательных вычетов по одному из соответствующих классов. Данное соответствие будет взаимно однозначным, пока $A < p_1, p_2, ..., p_n$, в силу Китайской Теоремы об Остатках (КТО). Кортеж (α_1, α_2, ..., α_n) можно рассматривать как один из способов представления целого числа A в ЭВМ – модулярное представление или представление в СОК.

Основным преимуществом такого представления является тот факт, что выполнение операций сложения, вычитания и умножения реализуется очень просто, по формулам:

$$\begin{aligned} A \pm B &= (\alpha_1, \alpha_2, ..., \alpha_n) \pm (\beta_1, \beta_2 ..., \beta_n) = \\ &= ((\alpha_1 \pm \beta_1) \mathrm{mod}\, p_1, (\alpha_2 \pm \beta_2) \mathrm{mod}\, p_2, ..., (\alpha_n \pm \beta_n) \mathrm{mod}\, p_n); \\ AB &= (\alpha_1, \alpha_2, ..., \alpha_n) \times (\beta_1, \beta_2 ..., \beta_n) = \\ &= ((\alpha_1 \times \beta_1) \mathrm{mod}\, p_1, (\alpha_2 \times \beta_2) \mathrm{mod}\, p_2, ..., (\alpha_n \times \beta_n) \mathrm{mod}\, p_n). \end{aligned} \qquad (2)$$

Эти операции носят название модульных, так как для их выполнения в СОК достаточно одного такта обработки численных значений, причем эта обработка происходит параллельно и значения информации в каждом разряде не зависят от других разрядов.

Основной недостаток модулярного представления чисел состоит в том, что трудно упорядочить множество всех целочисленных кортежей длины n так, чтобы этот порядок соответствовал естественному порядку на множестве целых чисел. Как следствие этого факта, трудно установить, является ли кортеж (α_1, α_2, ..., α_n) большим (меньшим), чем (β_1, β_2, ..., β_n). Трудно также проверить, возникло ли переполнение допустимого диапазона чисел $P = p_1 p_2 ... p_n$ в результате выполнения операций сложения или умножения, но еще труднее выполнить операцию деления. Эти и некоторые другие операции носят название немодульных, так как для их выполнения требуется знание о величине числа в целом, которое называется позиционной характеристикой числа.

Модель целочисленной модулярной арифметики можно задать следующей сигнатурой

$$\left\langle \left|P\right|, \left|\bullet\right|_{p_i}^{+}, MO, HO \right\rangle,$$

где $\left|P\right|$ – полная система вычетов по модулю полного динамического диапазона; $\left|\bullet\right|_{p_i}^{+}$ – вычет чисел по модулю p_i; МО – множество модульных операций, к которым относятся арифметические операции сложения, вычитания, умножения и деления нацело или умножение на обратный элемент, НО – множество немодульных операций, к которым относятся операции определения знаков чисел и переполнения динамического диапазона, сравнение, определение интервалов чисел, определение и локализация ошибочного разряда и др.

Немодульные операции обусловлены знанием числового значения модулярной величины, которая определенным образом связана со значениями компонент модулярного представления. Эти операции являются медленными, что снижает эффективность применения модулярной алгебры. Для реализации немодульных операций используются специальные функционалы, которые определяют количественные характеристики отношения порядка над множеством модулярных векторов. Одно из устоявшихся названий функционалов – позиционная характеристика (ПХ) модулярной величины или числовой величины в модулярном коде. В основе алгоритмов выполнения немодульных операций лежат методы вычисления ПХ, сложность которых непосредственно влияет на скорость выполнения немодульных операций в модулярной алгебре. Поиск эффективных и универсальных ПХ важен для теоретических основ модулярных вычислительных структур и вычислительных средств на их основе.

В настоящее время известны следующие методы определения позиционных характеристик модулярного представления чисел [1–3]:

– метод ортогональных базисов;

– метод интервальных оценок;

– метод с использованием коэффициентов обобщенной позиционной системы счисления (ОПСС) и другие.

С целью повышения эффективности вычисления позиционной характеристики предлагается новый приближенный метод определения позиционной характеристики, который позволяет реализовать практически все немодульные процедуры модулярного кода.

Исторически так сложилось, что поиск некоторого компромисса в удовлетворении требований, предъявляемых к ПХ, привел исследователей к введению таких характеристик модулярной алгебры, как ранг, след, нормированный ранг, неточный ранг, ядро числа и другие [1, 2, 3, 6]. Анализ этих ПХ показал, что значение модулярной величины по ним определяется сложно и не всегда однозначно. Кроме того, при выполнении некоторых НО нет необходимости в точном их определении, а достаточно знать значения в пределах каких-то интервалов, то есть при определении этих характеристик появляется избыточная информация, которая не используется. Эта идея и подтолкнула к поиску такой позиционной характеристики, которая бы не содержала избыточной информации, на нахождение которой требуются дополнительные вычислительные ресурсы.

Приближенный метод вычисления позиционной характеристики числа на основе использования относительных величин

Анализ немодульных операций показал, что их можно представить точно или приближенно, поэтому методы вычисления позиционных характеристик можно разделить на две группы:

– методы точного вычисления позиционных характеристик;

– методы приближенного вычисления позиционных характеристик.

Методы точного вычисления позиционных характеристик рассмотрены в [1–3]. В данной работе исследуются приближенные методы вычисления позиционных характеристик, которые позволяют существенно сократить аппаратные и временные затраты, обусловленные операциями, выполняемыми над позиционными кодами уменьшенной разрядности. В связи с этим возникает задача использования приближенного метода при вычислении определенного ряда немодульных процедур: определения интервалов чисел, знака числа, сравнения чисел, в том случае когда не требуется знания точного значения, насколько одно число больше или меньше другого.

Суть приближенного метода вычисления позиционных характеристик основан на использовании относительных величин анализируемых чисел к полному диапазону

$$\frac{A}{P}=\left|\sum_{i=1}^{n}\frac{\left|P_i^{-1}\right|_{p_i}}{p_i}\alpha_i\right|_1\approx\left|\sum_{i=1}^{n}K_i\alpha_i\right|_1, \qquad (4)$$

где A – исследуемое число; p_i – модули СОК; $\left|P_i^{-1}\right|_{p_i}$ – мультипликативная инверсия P_i относительно p_i;

$$P_i=\frac{P}{p_i}=p_1p_2\ldots p_{i-1}p_{i+1}\ldots p_n;$$

$K_i=\dfrac{\left|P_i^{-1}\right|}{p_i}$ – константы выбранной системы;

α_i – разряды числа, представленного в СОК,

$|*|_1$ – означает дробную часть числа.

Приближенный метод вычисления позиционной характеристики описывается такой последовательностью действий [4, 5]:

1. Вычисление констант СОК $k_i=\dfrac{\left|P_i^{-1}\right|_{p_i}}{p_i}$ с требуемой точностью.

2. Вычисление приближенных значений $\alpha_i k_i$ и запись их в LUT-память вычислительной системы, где k_i – константы, найденные в п. 1, $1\le\alpha_i\le p_i-1$. Адресами выборки значений $\alpha_i k_i$ являются разряды СОК α_i, где $i = 1, ..., n$.

3. Вычисление приближенного значения позиционной характеристики $\left|\sum_{i=1}^{n}k_i\alpha_i\right|_1$ в интервале [0, 1). Конечный результат определяется после суммирования и отбрасывания целой части числа с сохранением дробной части суммы. Тогда позиционная характеристика определяется в виде относительного значения величины

$$\frac{A}{P}=\left|\sum_{i=1}^{n}\frac{\left|P_i^{-1}\right|_{p_i}}{p_i}\alpha_i\right|_1\approx\left|\sum_{i=1}^{n}k_i\alpha_i\right|_1.$$

4. Конструируются некоторые правила Ψ_i, $i = 1, ..., 4$ согласно которым вычисляется i-я немодульная операция (определение знака числа, сравнение чисел, обнаружение

ошибки и переполнения, а также локализация ошибочного разряда).

Правило Ψ_1. Определение знака числа, в случае, если $p_1 = 2$:

– Если $\frac{A}{P} < \frac{1}{2}$, то число положительное;

– Если $\frac{A}{P} > \frac{1}{2}$, то число отрицательное.

Правило Ψ_2. Сравнение модулярных чисел A и B:

– Если $\frac{A}{P} - \frac{B}{P} = 0$, то $A = B$;

– Если $\frac{A}{P} - \frac{B}{P} > 0$, то $A > B$;

– Если $\frac{A}{P} - \frac{B}{P} < 0$, то $A < B$.

Правило Ψ_3. Обнаружение ошибки и переполнения динамического диапазона:

– Если $\frac{\overline{A}}{P_{\text{изб}}} < \frac{M}{P_{\text{изб}}}$, тогда ошибки нет, где $\overline{A}$ – искаженное число; $P_{\text{изб}} = p_{n+1}p_{n+2}P$ – избыточный диапазон при двух избыточных модулях p_{n+1} и p_{n+2}; $M = P = \prod_{i=1}^{n} p_i$ – рабочий диапазон.

– Если $\frac{\overline{A}}{P_{\text{изб}}} \geq \frac{M}{P_{\text{изб}}}$, тогда есть ошибка и установлено переполнение динамического диапазона.

Правило Ψ_4. Локализация неисправного канала:

– Если $\frac{\overline{A_i}}{P_i} < \frac{M_i}{P_i}$, то в разряде i нет ошибки;

– Если $\frac{\overline{A_i}}{P_i} \geq \frac{M_i}{P_i}$, то в разряде i есть ошибка, где

$$\overline{A_i} = (\alpha_1, \alpha_2, ..., \alpha_{i-1}, \alpha_{i+1}, ..., \alpha_n, \alpha_{n+1}, \alpha_{n+2})$$

– проекция искаженного числа $\overline{A}$;

$$M_i = (m_1, m_2, ..., m_{i-1}, m_{i+1}, ..., m_n, m_{n+1}, m_{n+2})$$

– проекция рабочего диапазона.

Пример. Пусть дана система оснований $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, объем диапазона $P = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Допустим, что в заданной СОК будут представлены только положительные числа. Величины

$$P_1 = \frac{P}{p_1} = 105, \quad P_2 = \frac{P}{p_2} = 70,$$

$$P_3 = \frac{P}{p_3} = 42, \quad P_4 = \frac{P}{p_4} = 30.$$

Сравним два числа $A_1 = 25$ и $A_2 = 30$, представленные в СОК по основаниям p_1, p_2, p_3, p_4, так $A_1 = (1,1,0,4)$, $A_2 = (0,0,0,2)$. Для этого найдем константы $k_i = \frac{\left|P_i^{-1}\right|_{p_i}}{p_i}$:

$$k_1 = \frac{\left|\frac{1}{105}\right|_2}{2} = \frac{1}{2} = 0{,}5;$$

$$k_2 = \frac{\left|\frac{1}{70}\right|_3}{3} = \frac{1}{3} \approx 0{,}3333;$$

$$k_3 = \frac{\left|\frac{1}{42}\right|_5}{5} = \frac{3}{5} = 0{,}6;$$

$$k_4 = \frac{\left|\frac{1}{30}\right|_7}{7} = \frac{4}{7} \approx 0{,}5714.$$

По выражению (4) получим

$$\frac{A_1}{P} \approx \left|1 \cdot 0{,}5 + 1 \cdot 0{,}3333 + 0 \cdot 0{,}6 + 4 \cdot 0{,}5714\right|_1 \approx 0{,}1189;$$

$$\frac{A_2}{P} \approx \left|0 \cdot 0{,}5 + 0 \cdot 0{,}3333 + 0 \cdot 0{,}6 + 2 \cdot 0{,}5714\right|_1 \approx 0{,}1428.$$

Так как $\frac{A_2}{P} > \frac{A_1}{P}$ то есть $0{,}1428 > 0{,}1189$, то $A_2 > A_1$, и действительно $30 > 25$.

Проблема синтеза немодульных устройств на основе предложенного приближенного метода побуждает к разработке таких правил Ψ_i, которые бы минимизировали число операций и вместе с тем могли быть достаточно просто реализованы на современной элементной базе.

В зависимости от типа немодульной операции, применяются либо точные, либо приближенные методы, или их комбинация. При необходимости можно использовать приближенные методы и для точных вычислений. В первую очередь необходимо исследовать возможность использования данного приближенного метода для восстановления остаточного кода.

Заключение

1. Противоречие между вычислительной сложностью определения основных проблемных процедур в СОК и их быстродействием разрешена путем замены абсолютных величин их относительными значениями и простотой их вычисления, которая сохраняет адекватную связь числовых значений модулярных величин с их представлениям в СОК и позволяет повысить скорость выполнения немодульных операций. Благодаря этому, применение системы остаточных классов может дать значительные преимущества не только в тех приложениях, в которых основная доля вычислений приходится на точное умножение, возведение в степень больших чисел в сочетании со сложением и вычитанием, но и в которых часто появляется необходимость в делении либо сравнении и определении знака числа, а также при проверке не «выходят» ли результаты за пределы допустимых значений и другие.

2. Решена фундаментальная проблема реализации основных проблемных операций в СОК, которые ранее определяли наибольший вклад в алгоритмическую сложность и сдерживали широкое применение СОК при разработке новых классов вычислительных систем. Внедрение полученных результатов позволяет снять это ограничение и расширить область применения модулярной арифметики.

3. Разработанные методы и алгоритмы самых проблемных процедур, характеризующихся простотой и высокой скоростью выполнения операций, дополняют известный универсальный базис СОК на основе обобщенной позиционной системы счисления и позволяют разделить выполнения всех немодульных процедур на два класса: процедуры точного вычисления (вычисления остатка, округления числа, деления, масштабирования, расширения модулярной величины на дополнительные основания и коррекция ошибок) и процедуры приблизительного вычисления (сравнения модулярных чисел, вычисления ранга числа, определения знака числа и переполнения диапазона, обнаружение и локализация ошибок при кодировании помехоустойчивым кодом). Перечисленные классы процедур являются важнейшими для машинной модулярной обработки и требуют глубокого дальнейшего исследования для определения границ их эффективного применения.

4. Полученные новые результаты эффективного выполнения немодульных процедур являются развитием теории математических основ разработки и проектирования высокопроизводительных и надежных вычислительных систем, функционирующих в системе остаточных классов.

Работа выполнена при поддержке гранта РФФИ 12-07-00482-а.

Список литературы

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

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

3. Нейрокомпьютеры в остаточных классах / Н.И. Червяков, П.А. Сахнюк, А.В. Шапошников, А.Н. Макоха; под ред. А.И. Галушкина. – М.: Радиотехника, 2003. – 272 с.

4. Червяков Н.И. Методы, алгоритмы и техническая реализация основных проблемных операций, выполняемых в системе остаточных классов // Инфокоммуникационные технологии. – 2011. – №4. – С. 4–12.

5. Приближенный метод ускоренного обнаружения и локализации неисправного вычислительного канала ЭВМ, функционирующей в системе остаточных классов / Н.И. Червяков, М.Г. Бабенко, П.А. Ляхов, И.Н. Лавриненко // Нейрокомпьютеры: разработка, применение. – 2011. – №10. – С. 13–19.

6. Амербаев В.М. Теоретические основы машинной арифметики. – Алма-Ата.: Наука, 1976. – 324 с.

References

1. Akushskiy I.Ya., Yuditskiy D.I. *Mashinnaya arifmetika v ostatochnykh klassakh* [Machine arithmetic in residue classes] Moskow, «Sovetskoe radio», 1968. 440 p.

2. Chervyakov N.I., Sakhnyuk P.A., Shaposhnikov A.V., Ryadnov S.A. *Modulyarnye parallel'nye vychislitel'nye struktury neyroprotsessonykh sistem* [Modular parallel computing structures of neural processing systems] Moskow, FIZMATLIT, 2003. 288 p.

3. Chervyakov N.I., Sakhnyuk P.A., Shaposhnikov A.V., Makokha A.N. *Neyrokomp'yutery v ostatochnykh klassakh* [Neurocomputers in residue classes] Moskow, Radiotekhnika, 2003. 272 p.

4. Chervyakov N.I. *Metody, algoritmy i tekhnicheskaya realizatsiya osnovnykh problemnykh operatsiy, vypolnyaemykh v sisteme ostatochnykh klassov* – Methods, algorithms and technical implementation of the basic problematic operations performed in the residue number system. *Infokommunikatsionnye tekhnologii* – Infocommunication Technology. 2011, no. 4. pp. 4–12.

5. Chervyakov N.I., Babenko M.G., Lyakhov P.A., Lavrinenko I.N. *Priblizhennyy metod uskorennogo obnaruzheniya i lokalizatsii neispravnogo vychislitel'nogo kanala EVM, funktsioniruyushchey v sisteme ostatochnykh klassov* – An approximate method for rapid detection and localization of a faulty computer channel computer operating system of residual classes. *Neyrokomp'yutery: razrabotka, primenenie* – Neurocomputers: development, application. 2011, no. 10. pp. 13–19.

6. Amerbaev V.M. *Teoreticheskie osnovy mashinnoy arifmetiki* [Theoretical foundations of computer arithmetic]. Alma-Ata, Nauka, 1976. 324 p.

Рецензенты:

Мочалов В.П., д.т.н., профессор, зав. кафедрой автоматизированных систем обработки информации и управления СевКавГТУ, г. Ставрополь;

Калмыков И.А., д.т.н., профессор, профессор кафедры защиты информатизации СевКавГТУ, г. Ставрополь.

Работа поступила в редакцию 13.04.2012.