ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

УДК 519.6
DOI 10.34822/1999-7604-2020-2-6-11

МЕТОДЫ ВЫБОРА ОСНОВАНИЙ, ПОНИЖАЮЩИХ БИВАЛЕНТНЫЙ ДЕФЕКТ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Н. С. Золотарева✉, С. А. Инютин
Сургутский государственный университет, Сургут, Россия
✉E-mail: zolotareva_ns@surgu.ru

В статье анализируется «бивалентный дефект» модуля в системе остаточных классов, или модулярной арифметике (явление естественной избыточности, возникающее при отображении вычетов модулярного представления числа в двоичных регистрах разрядной сетки специализированного модулярного процессора). Систематизированы методы уменьшения бивалентного дефекта. Рассматривается задача рационального выбора основания системы остаточных классов для уменьшения избыточности от бивалентного дефекта, поскольку основания модулярной арифметики, кроме, возможно, одного, взаимно просты со степенью двух, что приводит к определенной избыточности при отображении вычетов числа по каждому модулю.

Ключевые слова: система остаточных классов, модулярная арифметика, бивалентный дефект, избыточность двоичного регистра, выбор оптимальных оснований.

METHODS FOR SELECTION OF BASES REDUCING BIVALENT DEFECT IN RESIDUE NUMBER SYSTEM

N. S. Zolotareva✉, S. A. Inyutin
Surgut State University, Surgut, Russia
✉E-mail: zolotareva_ns@surgu.ru

The article analyzes the concept of a bivalent defect of modulus in the residue number system or modular arithmetic. This natural redundancy phenomenon occurs when the remainders of the modular representation of a number are displayed in binary registers of the bit grid in a specialized modular processor. Methods for reducing bivalent defects are systematized. The problem of rational choice of the modulus for the residue number system to reduce redundancy from a bivalent defect is analyzed. This choice is connected with the fact that all the moduli of modular arithmetic, except, possibly, for one, are coprime numbers with the power of two, which leads to a certain redundancy when displaying the modulo remainder.

Keywords: residue number system, modular arithmetic, bivalent defect, redundancy of the binary register, choice of optimal bases.

Введение

Компьютерная система счисления – метод отображения (записи) чисел с использованием некоторых символов. Существуют различные способы записи чисел, определяемые типами систем счисления: позиционные, непозиционные, смешанные.

Широко распространенной является позиционная система счисления – способ записи числа, в котором вес цифры напрямую зависит от ее положения в числовой записи.

Любое число в позиционной системе счисления можно записать в виде:

$$A = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p^1 + a_0 p^0 + a_{-1} p^{-1} + \cdots + a_{-m} p^{-m}, \quad (1)$$

где A – произвольное число, записанное в позиционной системе счисления с основанием p;

a_i– цифры числовой записи в системе счисления;

$n+1, m$ – количество целых и дробных разрядов в записи числа.

Выбирая различные основания $p = 2, 3, \ldots, 10, \ldots$, можно получить различные позиционные системы счисления – двоичную, троичную, десятичную и т. п.

В двоичном компьютере для записи машинных кодов удобно использовать двоичную систему счисления, содержащую две цифры – 0 и 1. Для краткости записи и вычислений используются восьмеричная и шестнадцатеричная позиционные системы счисления.

Позиционным системам счисления присуща зависимость между разрядами числа. Это влечет необходимость учета переносов из младших разрядов в старшие при выполнении операций над числами. Зависимость между разрядами позиционного представления усложняет аппаратуру для выполнения компьютерных операций и возможность достижения высокого быстродействия при выполнении вычислительного процесса [1]. Оставаясь в рамках позиционной системы счисления, значительного ускорения выполнения операций добиться практически невозможно.

Устранение указанных недостатков привело к построению машинной арифметики на базе непозиционной системы счисления. В непозиционных системах счисления вес цифры не зависит от ее положения в числе. Отдельные непозиционные системы счисления были известны с древних времен (10–11 тысяч лет до н. э.), в частности и в наши дни используется римская система счисления.

С начала 60-х годов прошлого века исследователи уделяют большое внимание непозиционной системе счисления, названной системой остаточных классов (СОК), или модулярной арифметикой. Для применения в компьютерах эта система счисления была предложена в 1955 г. чешскими учеными М. Валахом и А. Свободой [2]. В Советском Союзе в конце 1950-х годов система остаточных классов получила мощное развитие и техническое воплощение в системах специального назначения благодаря работам Ф. В. Лукина, Д. И. Юдицкого, И. Я. Акушского, удостоенных трех Государственных премий.

Система счисления в остаточных классах – это система, в которой целое положительное число представляется в виде кортежа или вектора с компонентами – вычетами по выбранным модулям (основаниям):

$$N = (\alpha_1, \alpha_2, \ldots, \alpha_n), \quad (2)$$

где $\alpha_i = N - \left[\frac{N}{p_i}\right] p_i$, для $i = 1, 2, \ldots, n$;

$p_1, p_2, \ldots, p_n$ – ряд взаимно-простых, положительных целых чисел, называемых основаниями непозиционной системы счисления;

$\Re = p_1 p_2 \ldots p_n$ – операционный диапазон представимых чисел [3–4].

Арифметические операции сложения, вычитания и умножения выполняются с отдельными вычетами (остатками от деления на модули) α_i параллельно и независимо друг от друга по простым алгоритмам.

Операции сложения и умножения в СОК реализуются следующим образом.

Пусть операнды A и B представлены остатками α_i и β_i по основаниям системы счисления p_i:

$$\begin{aligned} A &= (\alpha_1, \alpha_2, \ldots, \alpha_n), \\ B &= (\beta_1, \beta_2, \ldots, \beta_n). \end{aligned} \quad (3)$$

Результаты операций сложения и умножения $A + B$ и AB представлены остатками γ_i и δ_i по тем же основаниям системы счисления p_i:

$$\begin{gathered} A + B = (\gamma_1, \gamma_2, \dots, \gamma_n), \\ AB = (\delta_1, \delta_2, \dots, \delta_n), \end{gathered} \tag{4}$$

где γ_i сравнимо с $\alpha_i + \beta_i$ по модулю p_i, δ_i сравнимо с $\alpha_i\beta_i$ по тому же модулю, выполняются соотношения:

$$\begin{gathered} \gamma_i = \alpha_i + \beta_i (mod p_i), \\ \delta_i = \alpha_i\beta_i (mod p_i). \end{gathered} \tag{5}$$

Результатом являются числа [3–4]:

$$\begin{gathered} \gamma_i = \alpha_i + \beta_i - \left[\frac{\alpha_i + \beta_i}{p_i}\right] p_i, \\ \delta_i = \alpha_i\beta_i - \left[\frac{\alpha_i\beta_i}{p_i}\right] p_i. \end{gathered} \tag{6}$$

Как любая система счисления, СОК имеет достоинства и недостатки.

К достоинствам можно отнести: независимость образования разрядов числа; возможность независимой параллельной обработки разрядов числа; малую разрядность остатков, что позволяет организовать табличную реализацию выполнения операций; организацию вычислений, при которой возникает возможность обнаруживать и исправлять сбои и отказы отдельных блоков и узлов, не прерывая вычислений и не теряя производительности в целом [5].

Недостатками являются: невозможность отслеживания переполнения, т. е. выхода результата за пределы диапазона; запись числа не дает представления о его величине; использование только целых положительных чисел; возникновение квадратичной сложности реализации операций определения знака числа, сравнения, деления, масштабирования и др.

Бивалентный дефект

Современные технологии проектирования и производства вычислительных средств биваленты, т. е. ориентированы на двоичный элементный базис. В связи с этим возникает трудность при использовании модулярной арифметики, а именно несоизмеримость оснований модулярной арифметики и вычетов в записи числа со степенью двойки. Это явление называется бивалентным дефектом модулярной арифметики, приводящим к избыточности бинарных регистров для отображения компонент вектора отображения числовой величины в СОК. При этом остаются трудности при выполнении неподдающихся полному распараллеливанию немодульных операций, в частности: сравнения чисел по величине; деления в общем случае; обнаружения и исправления ошибок, вероятность появления которых при выполнении вычислительного процесса является малой, но отличной от нуля.

Бивалентным дефектом отдельной компоненты модулярного представления называется величина:

$$\delta_i(p_i) = \lceil log_2 p_i \rceil - log_2 p_i = n_i - log_2 p_i \geq 0, \tag{7}$$

где $\lceil log_2 p_i \rceil$ – целая не меньшая часть, равная бинарной разрядности отдельного регистра для отображения одного вычета по соответствующему модулю [6].

Суммарный бивалентный дефект Δ_n для n-регистровой бинарной разрядной сетки модулярного процессора является суммой бивалентных дефектов отдельных компонент модулярного представления числовой величины:

$$\Delta_n = \sum_{i=1}^{n} \delta_i(p_i) \,. \tag{8}$$

Выбор рационального набора оснований

Для уменьшения избыточности от бивалентного дефекта необходим рациональный выбор набора модулей или оснований системы счисления в остаточных классах. Оптимальный выбор приводит к улучшению параметров арифметического устройства – разрядной сетки процессора (количество оборудования, надежность, быстродействие и др.). Выбор системы оснований связан с областью применения модулярного процессора и определяется конкретными требованиями к разрабатываемому специализированному процессору [7–8]. Оптимальной является система оснований, обеспечивающая минимальную избыточность разрядной сетки при необходимом количестве разрядов. Одним из основных критериев оптимизации набора оснований является условие минимальности количества двоичных разрядов, которые используются при построении арифметического устройства. Важным является понятие ранга непозиционной системы, который определяет количество разрядов, необходимое для отображения чисел из некоторого диапазона $[0, \mathrm{P})$ [9].

Условие минимальности запишем в виде:

$$\mathrm{f}(\mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_\mathrm{n}) = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{f}_\mathrm{i}\,(\mathrm{p}_\mathrm{i}) \to \min, \tag{9}$$

где величина $\mathrm{f}(\mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_\mathrm{n})$ – ранг непозиционной системы с модулями $\mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_\mathrm{n}$.

Основным методом уменьшения бивалентного дефекта является выбор оснований модулярной арифметики, максимально близких к степеням двойки. Например, применение системы оснований вида $p_1 = 2^t - 1, p_2 = 2^t, p_3 = 2^t + 1$или $p_1 = 2^{n1}, p_2 = 2^{n2} - 1, p_3 = 2^{n3} - 1, \dots, p_m = 2^{nm} - 1$ дает небольшую избыточность.

Другой способ уменьшения бивалентного дефекта, сохраняющий ранг системы, может быть представлен в виде:

$$\sum_{i=1}^{n} \mathrm{c}(p_i) < \ln 2, \tag{10}$$

где $\mathrm{c}_i(p_i)$ – степенной дефект модуля p_i, вычисляемый из выражения:

$$p_i = 2^{k_i - \mathrm{c}_i} \approx 2^{k_i} - s_i, \tag{11}$$

где k_i – целое число, $0 \le c_i \le 1$ – правильная рациональная дробь.

На выбор совокупности модулей СОК также влияют специальные требования к модулярной арифметике, зависящие от области применения специализированных процессоров. С минимальной избыточностью строится непозиционная система, если в качестве основания выбираются числа Мерсенна $2^n - 1$ или числа Ферма $2^{2^k} + 1$. Недостаток такого выбора модулей состоит в быстром росте значений чисел Мерсенна и Ферма, что не позволяет использовать только их в качестве модулей системы счисления [10].

Еще одним способом уменьшения бивалентного дефекта является переход от традиционного понимания остатков (вычетов) к использованию логарифметики. Модулярная логарифметика – это система счисления, основанная на системе остаточных классов, в которой числа представлены в виде кортежа дискретных логарифмов от соответствующих вычетов по модулю. При построении логарифметики основания p_i модулярной арифметики являются простыми числами, что позволяет выбрать первообразные корни по модулю и использовать их показатели степени для представления вычетов по каждому простому основанию p_i [11].

Способом уменьшения избыточности от бивалентного дефекта является построение многоступенчатой СОК.

Системы остаточных классов обладают возможностью параллельной обработки векторных компонент модулярного представления числа, представляющих собой вычеты по модулям $p_1, p_2, \dots, p_n$. Диапазон $\Re$ представления чисел растет значительно быстрее, чем позволяет разрядная сетка, необходимая для представления числа, характеризуемая суммой разрядов для представления вычетов по выбранным основаниям. При этом требование взаимной

простоты оснований не позволяет выбрать их компактно на небольшом участке ряда натуральных чисел.

Увеличение разрядности оснований модулярной арифметики для увеличения числового диапазона при стандартном использовании приводит к росту разрядности регистров. Увеличение разрядности регистров, в которых находятся вычеты по модулям чисел рассматриваемого диапазона, приводит к усложнению аппаратуры арифметического устройства и увеличению времени выполнения операций [12–13].

Стремление по возможности уменьшить величину оснований привело к идее создания многоступенчатой СОК.

Пусть главная СОК содержит основания $p_1, p_2, \dots, p_n$ и обеспечивает возможность выполнения операций в заданном диапазоне $[0, \Re)$. Максимальное число, которое может быть получено в этой системе при умножении двух вычетов по старшему модулю, есть $(p_n - 1)^2$ [1].

В непозиционной системе нижнего уровня будем представлять все вычеты главной системы в новой системе с новым набором оснований $\pi_1, \pi_2, \dots, \pi_r$ такими, что $\pi = \pi_1 \pi_2 \dots \pi_r \geq (p_n - 1)^2$.

В этой системе максимальным числом, которое может быть получено при аналогичном умножении ее вычетов, является число $(\pi_r - 1)^2$. В свою очередь, эти последние цифры (в системе $\pi_1, \pi_2, \dots, \pi_r$) можно записывать в системе с основаниями $\rho_1, \rho_2, \dots, \rho_s$ при условии $\rho = \rho_1 \rho_2 \dots \rho_s \geq (\pi_r - 1)^2$и т. д.

Такой итерационный процесс перехода к меньшим основаниям упрощает реализацию элементарного арифметического устройства и сокращает время выполнения отдельной арифметической операции, но значительно увеличивает количество оборудования.

Выводы

Модулярная арифметика по сравнению с позиционной арифметикой обладает неоспоримыми преимуществами, такими как внутренний параллелизм и арифметическая самокоррекция ошибок, возникающих при вычислениях.

Введение избыточности в векторное модулярное представление числа позволяет при определенных условиях обнаруживать и исправлять ошибочные вычеты по модулю.

Анализ научных статей, докладов, монографий, посвященных модулярной тематике, позволяет сделать вывод, что модулярная арифметика находит широкое применение во многих областях, в частности в цифровой обработке сигналов и изображений; беспроводных сенсорных сетях; системах повышения отказоустойчивости, контроля процессов вычислений, обнаружения и исправления ошибок; системах информационной безопасности; облачных вычислениях; высокоэффективных нейрокомпьютерных вычислительных средствах; в астрономии; космологии; сейсмографии; системах связи и ряде других.

Анализ достоинств и недостатков модулярной арифметики приводит к выводу о важности бивалентного дефекта для непозиционной системы. Перечислим ряд методов, позволяющих его уменьшить:

- выбор оснований модулярной арифметики, максимально близких к степеням двойки;
- сохранение ранга системы в виде:

$$\sum_{i=1}^{n} \mathrm{c}(p_i) < \ln 2; \qquad (12)$$

- выбор оснований в виде числа Мерсенна $2^n - 1$ или числа Ферма $2^{2^k} + 1$;
- использование модулярной логарифметики;
- построение многоступенчатой системы остаточных классов.

Литература

1. Тынчеров К. Т. Модулярный мультинейропроцессор для АСУ ТП нефтегазового комплекса // Нефтегазовое дело. 2011. № 6. С. 18–24.

2. Valach M., Svoboda A. Origin of the Code and Number System of Remainder Classes // Stroje Na Zpracovani Informaci. Sbornik. 1955. Vol. 3.

3. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. М. : Советское радио, 1968. С. 439.

4. Амербаев В. М. Теоретические основы машинной арифметики. Алма-Ата : Наука, 1986. 224 с.

5. Амербаев В. М., Тельпухов Д. В., Константинов А. В. Бивалентный дефект модулярных кодов. Выбор технологичных модулей, понижающих бивалентный дефект // Проблемы разработки перспективных микро- и наноэлектронных систем – 2008 : сб. науч. тр. / под общ. ред. акад. А. Л. Стемпковского. М. : ИППМ РАН, 2008. С. 462–465.

6. Инютин С. А. Модулярные процессоры – оценки, история борьбы и победы над бивалентным дефектом // Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы. SoRuCom-2017 : сб. тр. IV Междунар. конф., Зеленоград, 3–5 октября 2017 г. / под ред. д. ф.-м. н. А. Н. Томилина. М. : РЭУ им. Г. В. Плеханова, 2017. С. 72–77.

7. Инютин С. А. Модулярные вычисления для задач большой алгоритмической сложности. URL: https://computer-museum.ru/books/archiv/sokcon06.pdf (дата обращения: 02.05.2020).

8. Инютин С. А. Методы организации многоразрядных вычислений // Вестник кибернетики. 2013. № 12. С. 89–93.

9. Бабенко М. Г. Методы и алгоритмы моделирования вычислительных структур на эллиптических кривых с параллелизмом машинных операций : автореф. дис. … канд. физ.-мат. наук. Ставрополь : 2011. 19 с.

10. Стрекалов Ю. А. Разработка методов моделирования параллельно-конвейерных нейросетевых структур для высокоскоростной цифровой обработки сигналов : автореф. дис. … канд. техн. наук. Ставрополь, 2006. 21 с.

11. Амербаев В. М., Корнилов А. И., Стемпковский А. Л. Модулярная логарифметика – новые возможности для проектирования модулярных вычислителей и преобразователей // Проблемы разработки перспективных микро- и наноэлектронных систем – 2010 : сб. тр. / под общ. ред. акад. А. Л. Стемпковского. М. : ИППМ РАН, 2010. С. 368–373.

12. Эрдниева Н. С. Использование специальных модулей системы остаточных классов для избыточного представления // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2013. № 2. С. 75–84.

13. Магомедов Ш. Г. Преобразование представлений чисел в модулярной арифметике в системах остаточных классов с разными основаниями // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2014. № 4. С. 32–39.