



МОДУЛЯРНАЯ АРИФМЕТИКА

Авторы: С. А. Инютин

МОДУЛЯРНАЯ АРИФМЕТИКА (система остаточных классов), базируется на известном в теории чисел частном виде отношения эквивалентности – понятии сравнения целого числа по натуральному модулю и возникающему при этой операции вычету. Непозиционная система счисления, в дальнейшем получившая название модулярной или системы остаточных классов, возникает при использовании множества вычетов от одного целого числа (числовой величины в терминологии А. Н. [Колмогорова](#)) по конечному множеству взаимнопростых чисел – модулей, называемых основаниями непозиционной системы счисления. Следовательно, модулярная арифметика содержит модулярную систему счисления для представления целых числовых величин в виде упорядоченной совокупности наименьших неотрицательных вычетов от отображаемой числовой величины по множеству простых или взаимнопростых модулей, что даёт векторные модулярные образы скалярных числовых величин. Для задания модулярной арифметики необходимо задать математические соотношения, позволяющие взаимнооднозначно отображать значение числовой величины в компоненты векторного представления и обратно, а также алгоритмы выполнения машинных операций над компонентами векторного модулярного представления.

Различные модулярные системы счисления позволяют сформировать множество оснований – простых (взаимнопростых) целых чисел: $\left\{ \{p_1, \dots, p_i, \dots, p_n\} \right\}, \forall i, j = 1, \dots, n, \gcd(p_i, p_j) = 1$ и метод их использования. Произведение оснований задаёт вычислительный диапазон $P = \prod_{i=1}^n p_i$, замкнутый относительно результатов операций сложения и умножения, а также учитывающий знак числовой величины.

В математическом смысле целые числа – основания модулярной системы являются модулями, по которым вычисляются наименьшие неотрицательные вычеты, являющиеся компонентами модулярного вектора при отображении значения числовой величины в модулярное представление.

В основе модулярного способа представления данных лежит известная «китайская теорема об остатках», в которой доказывается существование биективного отображения целых числовых величин из некоторого числового подмножества на множество векторов модулярного представления: $(\{\alpha_1, \alpha_2, \dots, \alpha_n\}) \mapsto A \in [0, \dots, \prod_{i=1}^n p_i]$, где $\alpha_i = \left\{ \left\lfloor \frac{A}{p_i} \right\rfloor \right\}$, – наименьший неотрицательный вычет по модулю p_i от целой числовой величины $A \in [0, \dots, P]$.

Для машинной модулярной арифметики, кроме собственно системы счисления, необходимо задать отображение числовых величин в различные компьютерные модулярные форматы данных, а также алгоритмы выполнения машинных операций над модулярными форматами данных в вычислительных устройствах. К таким машинным операциям относятся алгебраическое сложение, умножение по модулю, возведение в степень, вычисление обратной величины по модулю, целочисленного деления и др. Формирование модулярного вычислительного диапазона необходимо для взаимнооднозначного отображения результатов преобразования в соответствии с

вычислительным алгоритмом векторов модулярных представлений и значений числовых величин. Для учёта знака числа вычислительный диапазон удваивается, что позволяет оперировать с модулярными образами положительных и отрицательных чисел. Для применения в вычислительной технике вводятся компьютерные модулярные форматы данных в виде одномерных массивов. Связь значения числовой величины и компонент модулярного векторного представления задаётся следующей формулой: $A = \sum_{j=1}^n \left(\frac{\alpha_j}{p_j} \right) P \left| \frac{P}{p_i} \right|_{p_i^{-1}} - \{R_A\}P$, где $\{R_A\} = \left| \sum_{j=1}^n \left(\frac{\alpha_j}{p_j} \right) \left| \frac{1}{p_i} \right|_{p_i^{-1}} \right|$ – характеристический функционал модулярного представления [2]. От векторного модулярного представления числовых величин можно перейти к нормированному векторному модулярному представлению: $(\alpha_1, \alpha_2, \dots, \alpha_n) \rightarrow (\beta_1, \beta_2, \dots, \beta_n) \rightarrow A \in [0, \dots, P]$, где $\beta_i = \left| \alpha_i \right|_{\left| \frac{1}{p_i} \right|_{p_i^{-1}} P} \left| \frac{1}{p_i} \right|_{p_i^{-1}} < p_i$. Для нормированного модулярного представления характеристический функционал принимает более простой вид $\tilde{R}_A = \left| \sum_{j=1}^n \beta_j \right|$.

Характеристические функционалы необходимы для выполнения отдельных машинных операций над модулярными компьютерными форматами данных. Важнейшей проблемой в модулярной арифметике является поиск методов вычисления характеристических функционалов от компонент модулярного представления с наименьшей (почти линейной) сложностью, позволяющих эффективно вычислять предикаты выполнимости отношения линейного порядка на множестве векторных модулярных представлений.

Декартово произведение полных систем вычетов по простым (взаимнопростым) модулям является составным кольцом, что позволяет арифметические кольцевые операции выполнять независимо (в параллельных вычислительных трактах процессора SIMD архитектуры) над компонентами векторных модулярных представлений операндов. Это обуславливает основное преимущество в скорости вычислений над операндами компьютерного алгоритма для процессора, использующего модулярную арифметику.

Наиболее исследованным является способ модулярного представления целых чисел. Для рациональных чисел модулярный способ представления числовых величин может быть введён следующим образом: $\left| \frac{A}{B} \right|_{P/Q} = \frac{A}{B} - \left| \frac{AQ}{BP} \right| \frac{P}{Q} = \frac{AQ}{BQ} - \left| \frac{AQ}{BP} \right| \frac{P}{Q} = \frac{\left| \frac{AQ}{BP} \right|_{PB}}{BQ} = C \in R$.

В модулярной арифметике введены машинные модулярные коды:

– дополнительный (по модулю) $(p_1 - \alpha_1, \dots, p_n - \alpha_n) \rightarrow P - A \in (0, \dots, P]$

– обратный (по модулю): $(\alpha_1 \left| \frac{1}{p_1} \right|_{p_1^{-1}} - 1, \dots, \alpha_n \left| \frac{1}{p_n} \right|_{p_n^{-1}} - 1) \rightarrow A \left| \frac{1}{P} \right|_{P^{-1}} \in [1, \dots, P] \backslash \{D_i\}$, где D_i – множество числовых величин, кратных основаниям модулярной системы. При использовании простых оснований в модулярной арифметике обратный код существует для всех ненулевых компонент.

Введена модулярная логарифметика, в которой в компонентах векторного модулярного представления вместо вычетов применяются индексы по модулю на основе первообразных корней $(\text{ind}_{g_1} \alpha_1, \dots, \text{ind}_{g_n} \alpha_n) \rightarrow A \in [1, \dots, P]$, где для всех вычетов по модулю выполняются соотношения, аналогичные логарифмическим: $\forall i = 1, \dots, n, \alpha_i \equiv g_i^{\text{ind}_{g_i} \alpha_i}$

$(\text{bmod } \{p_i\})$. Использование в модулярных форматах упорядоченного множества пар – вычет по модулю и индекс вычета по модулю даёт перспективный подход для конструированию цифровых модулярных фильтров и процессоров обработки сигналов.

В специализированной вычислительной технике известны сочетания способов представления данных, в частности для формата с плавающей запятой: мантисса – модулярная, порядок – позиционный. Для модулярной арифметики построены помехозащитные арифметические коды введением дополнительных избыточных компонент в модулярное векторное представление. Модулярный помехозащитный код позволяет контролировать процесс арифметической обработки компьютерных данных, наряду с процессами их передачи по каналам связи и хранения в оперативной памяти и на носителях информации. Помехозащитные свойства модулярного кода задаются условиями: дополнительный вычет позволяет обнаруживать любую одиночную ошибку (в одной компоненте вектора представления), дополнительная пара вычетов позволяет корректировать любую одиночную ошибку. Построены эффективные синдромные алгоритмы обнаружения и коррекции арифметических ошибок в этих кодах.

Историческая справка

В 1955 Миро Валах и Антонин Свобода (оба Чехословакия) опубликовали работу, в которой предложили для кодирования целых чисел в машинах для распараллеливания математических расчётов использовать кольцо вычетов по составному модулю с попарно взаимно-простыми основаниями. Перспективная идея получила широкую поддержку мировой компьютерной общественности, что привело к большому объёму научных публикаций, часть которых была закрытой. Просматривались хорошие перспективы для реализации такого способа представления и обработки данных в специализированных вычислителях с параллельной структурой задолго до появления SIMD и MIMD архитектур суперкомпьютеров. Можно выделить начальные этапы в становлении модулярной арифметики. Свободы и Валах, работающие в США (1954–58) исследовали и опубликовали базовые принципы модулярной арифметики; Г. Айкен и У. Симон (США, 1957–59) доказали её преимущества для параллельного выполнения основных машинных арифметических операций; Х. Л. Гарнер (Канада, 1959) показал возможность арифметической самокоррекции для оперативного контроля вычислений с использованием модулярных кодов; П. Чейни (Англия, 1959–61) сконструировал нашедший широкое применение цифровой коррелятор на модулярных принципах; Р. Танака (Япония) и Э. Шапиро (США) в 1962–64 исследовали принципы организации параллельных вычислений и способы введения знака числовой величины в модулярном представлении. В СССР первые открытые публикации по системе остаточных классов (модулярной арифметике) появились в 1964 в «Кибернетическом сборнике» № 8 под редакцией академиков А. А. Ляпунова и О. Б. Лупанова серией статей ведущих отечественных и зарубежных специалистов. Для разработки отечественной ЭВМ 5Э53 на модулярных принципах, предназначенной для управления сложными объектами в режиме реального времени, в 1964 был создан специализированный Вычислительный центр (НИИ – СВЦ) Зеленоградского научного центра Министерства электронной промышленности. В нём под руководством И. Я. Акушского и Д. И. Юдицкого ведущие разработчики специализированных ЭВМ В. М. Амербаев, Е. С. Андрианов совместно с большим коллективом учёных и инженеров исследовали и разрабатывали параллельные методы реализации важнейших немодульных операций и блоки спецЭВМ. В Ленинграде В. А. Торгашев исследовал вопросы влияния разных типов модулярных представлений компьютерных данных на надёжность ЭВМ параллельной архитектуры. Под руководством Акушского и Юдицкого в Зеленоградском СВЦ были созданы ряд ЭВМ, в частности

экспериментальная модулярная ЭВМ Т-340А для отработки перспективных проектных решений, в дальнейшем нашедших широкое применение в серийно выпускаемой ЭВМ К-340А, прошедшей специальное тестирование и показавшей уникальное для своего времени быстроедействие и надёжность. Важнейшие научные результаты в этой области были обобщены в широко известной монографии Акушского и Юдицкого, представленной на соискание Госпремии СССР. В ней впервые появилось отечественное название модулярной тематики. Монография в 1968 дала импульс дальнейшим исследованиям по этой тематике в научных организациях Ленинграда, Минска, Киева, Алма-Аты под руководством авторитетных специалистов в области цифровой вычислительной техники. Исследования различных проблем в области модулярной арифметики получили развитие в изданных в разные годы монографиях. В разные годы за работы по тематике модулярных вычислений и специализированных параллельных вычислительных устройств были получены три Государственные премии СССР.

Литература

Лит.: Акушский И. Я., Юдицкий Д. И. Машинная арифметика в системе остаточных классов. М., 1968; Акушский И. Я., Амербаев В. М., Пак И. Т. Основы машинной арифметики комплексных чисел. Алма-Ата, 1970; Амербаев В. М. Теоретические основы машинной арифметики. Алма-Ата, 1976; Амербаев В. М., Пак И. Т. Параллельные вычисления в комплексной плоскости. Алма-Ата, 1984; Евстигнеев В. Г. Недвоичная машинная арифметика и специализированные процессоры. М., МИФИ, 1992; Коляда А. А., Пак И. Т. Модулярные структуры конвейерной обработки цифровой информации. Минск, 1992; Финько О. А. Модулярная арифметика параллельных логических вычислений. Краснодар, 2003; Нейрокомпьютеры в остаточных классах / Под. ред. А.И. Галушкина, Н.И. Червякова. М., 2003; 50 лет модулярной арифметики / Юбилейная международная конференция: сборник докладов. М., 2006; Инютин С. А. Основы модулярной алгоритмики. Ханты – Мансийск, 2008; Стемковский А. Л., Амербаев В. М., Соловьев Р. А. Принципы рекурсивных модулярных вычислений // Информационные технологии. № 2, 2013; Инютин С. А. Моделирование вычислений характеристик отношения порядка для модулярных представлений // Информационные технологии, № 9, 2013.

Processing math: 0%