



Табличная реализация операций модулярной арифметики

*(Международный институт компьютерных технологий,
г. Воронеж)*

В статье проведен анализ алгоритмов проведения модульных операций в табличном исполнении. Получены граничные оценки аппаратных затрат

Одним из важных достоинств модулярной арифметики является малоразрядность операндов и результата операции. Это обстоятельство позволяет применять табличные методы, при которых бинарные операции превращаются в одноктактовые, осуществляемые простой выборкой из таблиц.

Недостатком данного подхода, препятствующему внедрению его в практику, является существенный рост аппаратных затрат при увеличении разрядности операндов, ввиду того, что сами операции выполняются в однопозиционном коде. Рассмотрим ряд алгоритмов, позволяющих оптимизировать структуру таблиц путем преобразования исходных данных.

Применительно к операции модульного умножения $|A \cdot B|_m$ (A, B

– операнды; m модуль операции) известно [1], что ее таблица Кэли обладает симметрией диагоналей, а также вертикали и горизонтали, проходящих между величинами $\lfloor m/2 \rfloor$ и $\lceil m/2 \rceil$. Обозначив индекс операнда $g_A(g_B)$, получим

$$g_A(g_B) = \begin{cases} 0, & \text{если } 0 \leq A(B) < \lfloor m/2 \rfloor \\ 1, & \text{если } \lceil m/2 \rceil \leq A(B) < m \end{cases}$$

Определим значения $A'(B') = m - A(B)$, если операнды принадлежат диапазону $\lfloor (m+1)/2, m-1 \rfloor$. При $g_A = g_B$ $|A \cdot B|_m = |A' \cdot B'|_m$, а в противном случае ($g_A \neq g_B$) $|A \cdot B|_m = m - |A' \cdot B'|_m$ [1].

Аналогичным образом выведем подобные соотношения для операций модульного сложения и вычитания, сохраняя принятые обозначения. Полученные результаты сведены в таблицу.

g_A, g_B	$ A + B _m$	$ A - B _m$
$g_A = g_B = 0$	$ A + B _m$	$ A - B _m$
$g_A = 0, g_B = 1$	$ A - B' _m$	$ A + B' _m$
$g_A = 1, g_B = 0$	$m - A' - B _m$	$m - A' + B _m$
$g_A = g_B = 1$	$m - A' + B' _m$	$m - A' - B' _m$

Следовательно, при реализации базового набора операций модульной арифметики можно использовать 1/8 часть полной таблицы, инвертируя по модулю полученный результат в зависимости от соотношений g_A и g_B . Возможность достижения этого объясняется тем, что паре входных операндов A и B соответствует определенный элемент таблицы, который можно интерпретировать как

результат произвольной модульной операции. Данное обстоятельство позволяет проводить одновременно несколько бинарных операций на одной таблице с использованием симметричного матричного вычислителя [2] и половинными значениями входных операндов.

Таким образом, реализация всех осей симметрии таблицы Кэли для модульных операций предполагает построение таблицы с общим числом элементов (узлов) N равным $m^2/8$, что примерно на порядок уменьшает аппаратные затраты.

Дальнейшее сокращение числа элементов таблицы возможно путем применения двухуровневых табличных методов.

Рассмотрим алгоритм сокращения таблицы, обеспечивающий ее деление на функционально законченные части с коэффициентом деления d . Приняв следующие обозначения: $D = \lceil m/d \rceil$ и $a(b) = |A(B)|_\Delta$, имеем

$$|A \pm B|_m = |(a \pm b) + (g'_A \pm g_B) \cdot \Delta|_m,$$

где $g_{A(B)} = \overline{0}$, d в отличие от (1) является обобщенным индексом операнда. Для реализации соотношения (2) с последующим восстановлением результата операции по модулю используется схема, представленная на рис. 1.

В этой схеме имеются три таблицы (T_1 и T_2 для получения промежуточных результатов) и T_3 – для заключительного, однако общее число узлов их меньше, чем в одноуровневой структуре. Умножение на величину D согласно (2) в однопозиционном коде выполняется простой перекоммутацией выходных шин таблицы T_2 . Определим минимальное число всех табличных элементов

$$N = \frac{1}{2}(m/d)^2 + \frac{1}{2}d^2 + (m/d) \cdot d.$$

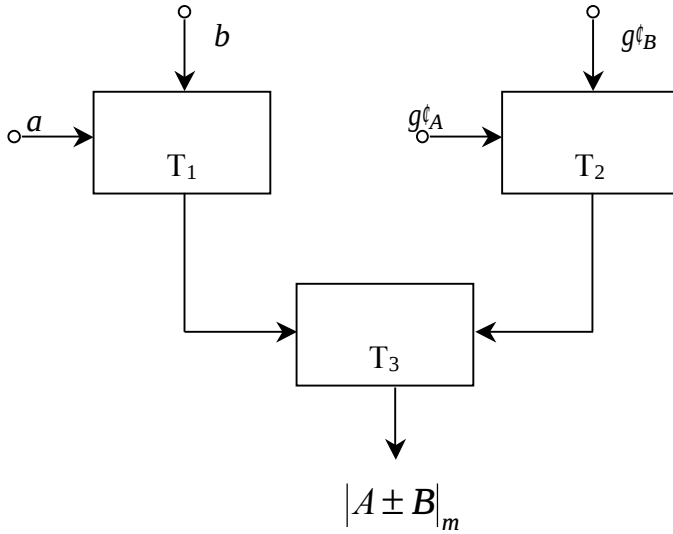


Рис. 1. Двухуровневая табличная структура

Тогда
$$\frac{\partial N}{\partial d} = -m^2 d^{-3} + d = 0,$$

откуда $d_{opt} = \sqrt{m}$ и $N_{min} = 2m$.

Следовательно, при выборе $d = \sqrt{m}$ число табличных узлов обладает не квадратичной, а линейной зависимостью от величины модуля m , что позволяет использовать табличные методы выполнения операций модулярной арифметики с операндами $A(B)$ более значительными по величине.

Другой алгоритм, соответствующий реализации двухуровневой структуры (рис. 1), использует понятие внутреннего модуля устройства K . В этом случае

$$|A \pm B|_m = |K(a \pm b) + (\Delta_A \pm \Delta_B)|_m,$$

где $a(b) = [A(B)/K]$, $D_{A(B)} = |A(B)|_K$.

Число табличных узлов N при этом будет равно

$$N = \frac{1}{2} (m/K)^2 + \frac{1}{2} K^2 + (m/K) \cdot K, \quad \text{откуда} \quad \text{следует}$$

$$K_{opt} = \sqrt{m} \text{ и } N_{min} = 2m.$$

Отметим, что выражения (2) и (4) инвариантны, вследствие чего оптимальные параметры и величины N_{min} одинаковы. При использовании схемы на рис.1 отличие заключается в формировании операндов для таблиц T_1 и T_2 , а также в восстановлении результата операции по модулю m .

Следующим этапом сокращения табличного оборудования является таблично-групповой метод [3]. Сущность его состоит в последовательном использовании группы таблиц при проведении модульной операции. Отличие его от известных в позиционных системах счисления алгоритмов заключается в том, что величина разряда $t \gg 2$ и разрядная операция выполняется табличным путем. Модульная операция производится таблично-групповым методом в t -ичной системе счисления. Соответствующая этому методу структура для числа разрядов, равных трем представлена на рис. 2.

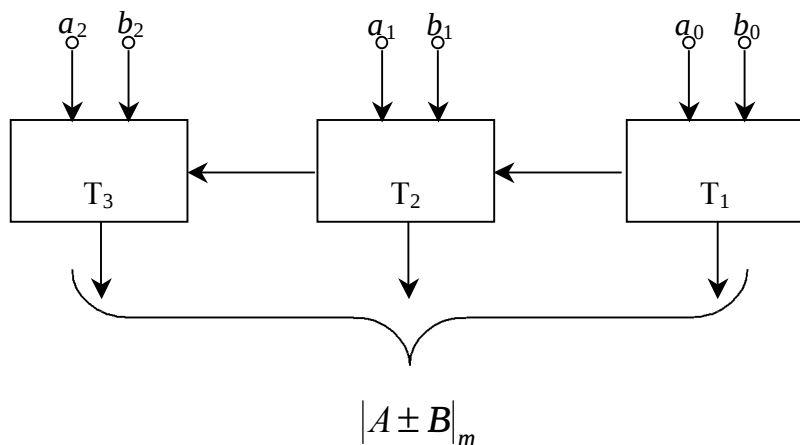


Рис. 2. Структурная схема реализации таблично-группового метода

При этом $A = (a_2, a_1, a_0)$ и $B = (b_2, b_1, b_0)$ – представление

операндов в t -ичной системе счисления. Число табличных узлов N при исполнении трехразрядной схемы с учетом диагональной симметрии составляет

$$N = \frac{1}{2} \left(m/t^2 \right)^2 + \frac{1}{2} t^2 + \frac{1}{2} t^2.$$

Тогда $t_{ОПТ} = \sqrt[3]{m}$, а $N_{мин} = \frac{3}{2} \sqrt{m^3}$. При величине t равной степени числа два результат модульной операции представляется в двоичной системе счисления. Следует отметить, что $m \leq t^3 - 1$, а выбором соответствующего значения t можно обеспечить условие $t^3 - m < t$, при этом получение результата операции реализуется коррекцией только в нулевом разряде.

Ввиду того, что данный метод занимает промежуточное положение между сумматорным и табличным вариантами, то при его использовании можно регулировать соотношение между аппаратными затратами и быстродействием проведения модульной операции.

Дальнейшее развитие этого метода, связанное с увеличением разрядности операндов $A(B)$ позволяет довести величину N до значе-

ния $N = \frac{n}{2} m^{\frac{2}{n}}$, где n – разрядность операндов $A(B)$, откуда получаем $n_{ОПТ} = 2 \ln m$, $N_{мин} = e \ln m$.

Полученная логарифмическая зависимость числа узлов таблицы от величины модуля определяет нижнюю границу, так как анализ проводился без учета восстановления результата операции по модулю m , когда t не равно степени числа 2. Расчеты, проведенные для предельных оценок N при многоуровневой табличной реализации, показывают, что в этом случае $N_{мин} = 2 \cdot e \cdot \ln m$ [3].

Выбор конкретного метода сокращения табличного оборудования должен производиться исходя из требований к элементной базе операционного устройства модулярной арифметики. Предлагаемые алгоритмы могут быть использованы в вычислительных трактатах непозиционных спецпроцессов, основанных на других принципах

выполнения модульных операций для повышения их быстродействия.

Полученные предельные оценки оборудования табличных вычислительных структур могут найти применение при анализе и сравнительной оценке перспективных алгоритмов для проведения операций модулярной арифметики.

Литература

- 1 Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968.
- 2 А.с. 1775721 СССР. Арифметическое устройство по модулю / В.П. Ирхин и др. – Оpubл. в Б.И. №42, 1992.
- 3 Ирхин В.П. Проектирование непозиционных специализированных процессов. – Воронеж: Изд-во Воронежского госуниверситета, 1999.