Проблемы организации параллельных многоразрядных вычислительных процессов

С.А. Инютин

МАТИ –РГТУ им. К.Э. Циолковского

При математическом моделировании тонких технологических процессов в ряде отраслей производства, в прикладной теории чисел появляются вычислительные задачи, для которых требуется специальная организация вычислительных процессов. В них значения операндов целочисленных операций на сто, тысячу, … порядков превышают максимум типового компьютерного диапазона серийной вычислительной техники. Типовой компьютерный диапазон связан с длиной машинного слова, в котором отображаются данные во внутренних форматах и обрабатываются в операционных регистрах процессора с аппаратной и микропрограммной поддержкой. Машинная арифметика для их обработки имеет наибольшее быстродействие.

Для анализа вычислительных процессов с превышением типового компьютерного диапазона введем специальную терминологию. Назовем диапазонными числовые величины, для отображения которых типовой диапазон достаточен. В зависимости от длины машинного слова вычислительной системы типовой диапазон 16, 32 или 64 разрядный (бинарные разряды). Для диапазонных величин, отображаемых в беззнаковом целочисленном формате для $n = 16 \mid 32 \mid \ 64$ выполняются неравенства $0 \le A \le 2^n - 1$, а для числовых величин, отображаемых в целочисленном формате со знаком выполняются неравенства $-2^{n-1} \le A \le 2^{n-1} - 1$. Компьютерные форматы данных с двойной точностью, условно относятся к диапазонным, в регистрах процессора обработка этих форматов имеет микропрограммную и аппаратную поддержку. Назовем сверхдиапазонными (многоразрядными) числовые величины, для отображения которых типовой и удвоенный диапазоны недостаточны. Для них введем производные беззнаковый и знаковый целочисленные форматы. Для сверхдиапазонных числовых величин, отображаемых в беззнаковом формате, для $n = 16 \mid 32 \mid \ 64$ -разрядного процессора выполняются неравенства $2^{2n} - 1 < C \le D$, а для величин, отображаемых в формате со знаком, выполняются неравенства $-D \le C < -2^{2n-1}$ *и* $2^{2n-1} - 1 < C \le D$, где D – константа, зависящая от предельных возможностей программно эмулируемой многоразрядной арифметики, операционных ресурсов и объема памяти вычислительной системы. Множество многоразрядных числовых величин назовем большим диапазоном *W*, для которого $D = \max W$.

Задачи тестирования и факторизации больших числовых величин называют вычислительными проблемами из-за большой временной сложности. В частности, это проблема тестирования на простоту при больших показателях степени чисел Мерсенна $M_q = 2^q - 1$, где $q \in N$ – множество натуральных чисел, $q>2$. Современные методы ориентированы на тестирование чисел Мерсенна при $q>300000$, а числовые величины для таких процессов содержат более миллиона десятичных разрядов позиционного представления. Программная реализация эффективных методов вычислений в больших диапазонах позволяет решать задачи, требующих вычислений в сверхбольших диапазонах, появляющихся при вычислении функций от многоразрядных величин. Для ряда задач вычислительной теории чисел максимум сверхбольшого компьютерного диапазона должен достигать значения константы Виноградова - Гольбаха $3^{3^{15}}$. Такие задачи возникают, при вычислении выражений вида:

$$C = \sum_{i=1}^{k} A_i^{f(B)} - [\sum_{i=1}^{k} A_i^{f(B)} / B] \cdot B,$$

где A_i , *B,* а также область значений функции *f(B)* принадлежат большому диапазону ***W*.**

Для эффективного решения таких задач предлагается использование распараллеливаемой модулярной программно-эмулируемой арифметики и производных форматов данных.