

УДК 511.9

РЕАЛИЗАЦИЯ ПАРАЛЛЕЛЬНОГО АЛГОРИТМА ПОИСКА КРАТЧАЙШЕГО ВЕКТОРА В БЛОЧНОМ МЕТОДЕ КОРКИНА — ЗОЛОТАРЕВА

В. С. Усатюк

Предложена параллельная реализация алгоритма Каннана для решения задач поиска кратчайшего и короткого векторов в решётке. Алгоритм может применяться как в составе блочного метода Коркина — Золотарева, так и независимо. Эксперимент показал трёхкратное ускорение работы блочного метода Коркина — Золотарева на четырёхъядерной системе.

Ключевые слова: решётка, проблема поиска кратчайшего вектора, блочный метод Коркина — Золотарева.

Определение 1. Базис $B = \{b_1, b_2, \dots, b_m\}$ решётки $L \subset R^n$ приведён блочным методом Коркина — Золотарева (BKZ, Block Korkin — Zolotarev method [1]) с блоком β , если:

- 1) базис B приведён по длине;
- 2) $\|b_i^\perp\| = \lambda_1(L_i)$, $i = 1, \dots, m$, где $\lambda_1(L_i)$ — длина кратчайшего вектора в обратной (сопряжённой) решётке L_i , образованной ортогональным дополнением векторного пространства с базисом $b_i, \dots, b_{\min(i+\beta-1, m)}$.

BKZ-метод содержит две основные процедуры, которые могут быть распараллелены: ортогонализация базиса решётки и поиск кратчайшего вектора. Вопрос распараллеливания алгоритмов ортогонализации базиса рассматривался в работе [2].

Алгоритм поиска кратчайшего вектора представляет собой вариант метода ветвей и границ и заключается в переборе линейных комбинаций базисных векторов решётки, дающих вектор с нормой, ограниченной сверху некоторым положительным числом A , которое может уменьшаться в процессе поиска.

На начальном этапе можно принять $A = \min \left\{ \sqrt{\gamma_m} \cdot (\det L)^{\frac{1}{m}}, \|b_*\| \right\}$, где γ_m — константа Эрмита; b_* — наименьший по норме вектор в исходном базисе решётки.

Можно показать [3, 4], что координаты кратчайшего вектора удовлетворяют следующей системе неравенств:

$$\begin{cases} x_m^2 \|b_m^\perp\|^2 \leq A^2, \\ (x_{m-1} + \mu_{m,m-1}x_m) \|b_{m-1}^\perp\|^2 \leq A^2 - x_m^2 \|b_m^\perp\|^2, \\ \dots \\ (x_1 + \sum_{i=2}^m x_i \mu_{i,j})^2 \|b_1^\perp\|^2 \leq A^2 - \sum_{j=2}^m l_j, \end{cases} \quad (1)$$

где $\{b_j^\perp\}_{j=1}^m$ — ортогональный базис решётки, полученный из исходного базиса, например в результате процедуры ортогонализации Грама — Шмидта (через μ_{ij} обозначены коэффициенты Грама — Шмидта), $l_j = \left(x_j + \sum_{i=j+1}^m x_i \mu_{i,j} \right)^2 \|b_j^\perp\|^2$.

Для решения системы (1) используем метод ветвей и границ, то есть организуем поиск решения в виде дерева. Корень дерева помечен переменной x_m . Из корня выходит N ветвей, каждая из которых соответствует конкретному решению первого неравенства в (1). Пусть α_m — произвольное решение этого неравенства. Ветвь дерева

поиска, соответствующую данному решению, будем называть α_m -ветвью. Следующая вершина α_m -ветви помечается переменной x_{m-1} . Данная вершина является корнем дерева поиска для системы неравенств, полученной из (1) подстановкой $x_m = \alpha_m$. Если хотя бы одно из неравенств в (1) при этом не выполняется, то рассматриваемая ветвь отсекается (поскольку заведомо не содержит решения, дающего меньшую верхнюю границу, чем текущая). Описанный процесс по аналогии продолжается далее. Если найден вектор со значением нормы, меньшим текущей верхней границы, то значение верхней границы (рекорд) обновляется.

Описанный алгоритм реализован с использованием потоковой модели NPTL (Native POSIX Thread Library [5]) под CentOS 6.3. Каждый из потоков осуществляет вычисление своей α_m -ветви, исходящей из корня дерева.

На задаче приведения 103-мерной решётки BKZ-методом с размером блока $\beta = 52$ на четырёх потоках, выполняемых на AMD Phenom 965/8 Gb DDR2-800, он продемонстрировал трёхкратное ускорение в сравнении с последовательным BKZ-решателем `fp111-4.0.1` [6]. Предложенный алгоритм применялся в составе решателя, который занял 1-е и 6-е места на международных конкурсах поиска коротких векторов [7] для норм $A = m \cdot \det(L)^{1/m}$ и $A = 1,05 \frac{\Gamma(m/2 + 1)^{1/m}}{\sqrt{\pi}} \det(L)^{1/m}$ соответственно.

ЛИТЕРАТУРА

1. Schnorr C. P. Block reduced lattice bases and successive minima // *Combinatorics, Probability and Computing*. 1994. V. 3. P. 507–522.
2. Усатюк В. С. Реализация параллельных алгоритмов ортогонализации в задаче поиска кратчайшего базиса целочисленной решетки // *Прикладная дискретная математика. Приложение*. 2012. № 5. С. 120–122.
3. Kannan R. Improved algorithms for integer programming and related lattice problems // *Proc. STOC'83*. New York, NY, USA, 1983. P. 193–206.
4. Hanrot G. and Stehle D. Improved analysis of Kannan's shortest lattice vector algorithm // *LNCS*. 2007. V. 4622. P. 170–186.
5. Kerrisk M. *The Linux programming interface: a Linux and UNIX system programming handbook*. San Francisco, USA: No Starch Press, 2010. 1552 p.
6. <http://perso.ens-lyon.fr/damien.stehle/fp111/index.html> — Приложение fp111. 2013.
7. <http://www.latticechallenge.org/ideallattice-challenge/index.php> — Ideal lattice challenge (SVP, Approx-SVP). 2012.

УДК 004.627

РАСПАРАЛЛЕЛИВАНИЕ АЛГОРИТМА ДЕКОДИРОВАНИЯ СТАНДАРТА СЖАТИЯ ВИДЕОДАННЫХ H.265/HEVC

Р. И. Черняк

Рассматривается возможность параллельной реализации декодера в новом стандарте сжатия цифровых видеопоследовательностей H.265/HEVC. Предложены два способа параллелизации декодера, эффективность которых обоснована теоретически и показана экспериментально.

Ключевые слова: видеокодирование, сжатие цифрового видео, распараллеливание алгоритмов декодирования.