2. *Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
3. *Jarvisalo M. and Junttila T.* Limitations of restricted branching in clause learning // Constraints. 2009. V. 14. No. 3. P. 325–356.
4. *Семенов А. А.* Декомпозиционные представления логических уравнений в задачах обращения дискретных функций // Изв. РАН. Теория и системы управления. 2009. № 5. С. 47–61.
5. *Ignatiev A. S. and Semenov A. A.* DPLL+ROBDD derivation applied to inversion of some cryptographic functions // LNCS. 2011. V. 6695. P. 76–89.
6. *Bryant R. E.* Graph-Based Algorithms for Boolean Function Manipulation // IEEE Trans. Comput. 1986. V. 35. No. 8. P. 677–691.

УДК 004.056.5:512.545

РЕАЛИЗАЦИЯ ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ ОРТОГОНАЛИЗАЦИИ В ЗАДАЧЕ ПОИСКА КРАТЧАЙШЕГО БАЗИСА ЦЕЛОЧИСЛЕННЫХ РЕШЁТОК

В. С. Усатюк

Целью работы является демонстрация увеличения производительности алгоритмов приведения базиса целочисленных решёток за счёт замены рекуррентного алгоритма Грама — Шмидта параллельными алгоритмами ортогонализации.

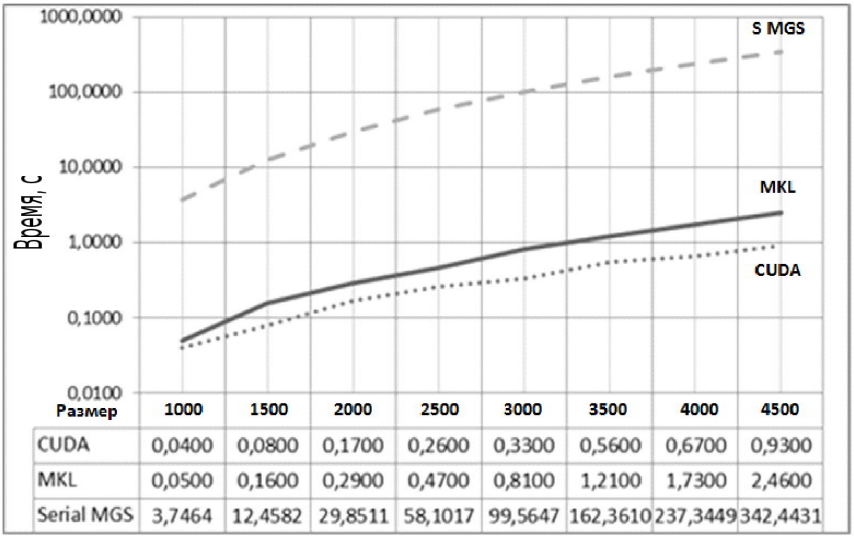
Для приведения базиса решётки с экспоненциальной точностью $\gamma = 2^{(n-1)/2}$ достаточно привести базис к $(\delta - LLL)$-редуцированному базису, применив полиномиальный по временной сложности алгоритм Ленстра — Ленстра — Ловаса (LLL) [1]. Для приведения базиса решётки с точностью $\gamma \in \left[2^{(n-1)/2} - \varepsilon, 1\right]$ достаточно привести подмножество базиса решётки, состоящее из $\beta \leqslant n$ векторов, к базису Коркина — Золотарева, применив блочный алгоритм Коркина — Золотарева (BKZ), чья временная сложность зависит от размера блока, изменяясь от полиномиальной до экспоненциальной [1].

Ключевой частью алгоритмов приведения базиса решёток является этап ортогонализации, осуществляемый при помощи алгоритмов, вычисляющих QR-разложение матрицы базисных векторов. Традиционно, в силу своей геометрической наглядности и простоты, для ортогонализации используется рекуррентный алгоритм Грама — Шмидта или его вычислительно устойчивый аналог — модифицированный алгоритм Грама — Шмидта [2]. Однако рекуррентная природа данного алгоритма препятствует его распараллеливанию и делает его «узким местом» процедуры приведения базиса решётки. Алгоритм Грама — Шмидта может быть заменён другими алгоритмами, осуществляющими QR-разложение, а именно алгоритмом отражения Хаусхолдера или алгоритмом вращения Гивенса [3]. Их применение теоретически позволяет ускорить процесс ортогонализации $(n \times n)$-матрицы базиса решётки в n раз.

В основе метода Гивенса лежит идея поворота векторов матрицы базиса с целью последовательного обнуления координат векторов ортогонализуемого базиса. Одной из ключевых особенностей алгоритма Гивенса является необходимость вычисления квадратного корня и в два раза большее число операций по сравнению с алгоритмом Хаусхолдера. Однако этот недостаток компенсируется отсутствием ветвления, что приводит к высокой эффективности исполнения данного алгоритма на векторных вычислительных устройствах, в частности на видеокартах. Последнее обстоятельство привело к реализации именно этого алгоритма в библиотеке CUBLAS [4].

Алгоритм Хаусхолдера основан на использовании линейного преобразования ортогонализуемой матрицы, которое осуществляет «отражение» векторов относительно гиперплоскости, проходящей через начало координат. Каждое преобразование обнуляет часть строки и столбца ортогонализуемого базиса. При распараллеливании алгоритма Хаусхолдера возникает необходимость взаимодействия процессов, осуществляющих ортогонализацию, что в целом накладывает ограничения на реализацию данного метода на устройствах с SIMD-архитектурой.

В настоящей работе представлена библиотека, содержащая реализацию модифицированного алгоритма Грама — Шмидта, а также алгоритмов Хаусхолдера и Гивенса и предназначенная специально для решения задач приведения базисов целочисленных решёток в рамках созданного ранее приложения LRT [5]. В процессе создания библиотеки реализован специальный менеджер памяти, обеспечивающий устойчивую работу приложения в целом. Полученное приложение апробировано на конкурсных задачах из тестовых библиотек для алгоритмов приведения базиса решёток [6]. На рис. 1 приведено сравнение времени выполнения различных алгоритмов ортогонализации при решении задачи приведения базиса решётки размера n. Последовательная реализация метода Грама — Шмидта (S MGS) выполнялась на одном ядре CPU Phenom II X4 965, метод Гивенса — на GPU GeForce Ti 550 1GB (NVIDIA CUDA), алгоритм Хаусхолдера — на четырёх ядрах CPU Phenom II X4 965 (Intel Math Kernel Library). Из представленного графика видно, что применение параллельных методов ортогонализации обеспечило 300-кратный прирост (устойчиво растущий с ростом размера решётки) производительности по сравнению с последовательной реализацией метода Грама — Шмидта. В классе параллельных методов ортогонализации метод Гивенса, исполняемый на GPU, продемонстрировал незначительное преимущество перед методом Хаусхолдера.



Размер	1000	1500	2000	2500	3000	3500	4000	4500
CUDA	0,0400	0,0800	0,1700	0,2600	0,3300	0,5600	0,6700	0,9300
MKL	0,0500	0,1600	0,2900	0,4700	0,8100	1,2100	1,7300	2,4600
Serial MGS	3,7464	12,4582	29,8511	58,1017	99,5647	162,3610	237,3449	342,4431

Рис. 1. Зависимость времени (в секундах) выполнения алгоритмов ортогонализации базиса решётки от её размера (однократная точность вычислений)

ЛИТЕРАТУРА

1. *Schnorr C. P. and Euchner M.* Lattice basis reduction: Improved practical algorithms and solving subset Sum Problems // Fundamentals of Computation Theory. Gosen, Germany, 1991. P. 68–85.
2. *Longley J. W.* Modified Gram — Schmidt process vs. classical Gram — Schmidt // Commun. Stat. — Simul. Comp. 1981. No. 10(5). P. 517–527.
3. *Press W. H., Teukolsky S. A., and Vetterling W. T.* Numerical Recipes: The Art of Scientific Computing. New York: Cambridge University Press, 2007. 1262 p.
4. `http://goo.gl/85KwD` — CUDA Toolkit 4.1 CUBLAS Library. January 2012. 99 p.
5. `http://www.lcrypto.com/lsolv` — Программы для приведения базиса решёток. 2012.
6. `http://www.latticechallenge.org/` — Lattice SVP and SBP challenge. 2011.