Title: Quantum algorithms for matrix multiplication and product verification
Name: Robin Kothari[1], Ashwin Nayak[2]
Affil./Addr. 1: David R. Cheriton School of Computer Science, and Institute for Quantum Computing, University of Waterloo
Affil./Addr. 2: Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo
Keywords: Quantum algorithms; Matrix product verification; Boolean matrix multiplication
SumOriWork: 2006; Buhrman, Špalek
2012; Jeffery, Kothari, Magniez

Quantum algorithms for matrix multiplication and product verification

Robin Kothari[1], Ashwin Nayak[2]

[1] David R. Cheriton School of Computer Science, and Institute for Quantum Computing, University of Waterloo

[2] Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo

Years aud Authors of Summarized Original Work

2006; Buhrman, Špalek
2012; Jeffery, Kothari, Magniez

Keywords

Quantum algorithms; Matrix product verification; Boolean matrix multiplication

Problem Definition

Let S be any algebraic structure over which matrix multiplication is defined, such as a field (e.g., real numbers), a ring (e.g., integers), or a semiring (e.g., the Boolean semiring). If we use $+$ and $\cdot$ to denote the addition and multiplication operations over S, then the matrix product C of two $n \times n$ matrices A and B is defined as $C_{ij} := \sum_{k=1}^{n} A_{ik} \cdot B_{kj}$ for all $i, j \in \{1, 2, \ldots, n\}$. Over the Boolean semiring, the addition and multiplication operations are the logical OR and logical AND operations respectively, and thus the matrix product C is defined as $C_{ij} := \bigvee_{k=1}^{n} (A_{ik} \wedge B_{kj})$. In this article we consider the following problems.

Problem 1 (Matrix multiplication).
INPUT: Two $n \times n$ matrices A and B with entries from S.
OUTPUT: The matrix $C := AB$.

Problem 2 (Matrix product verification).
INPUT: Three $n \times n$ matrices A, B, and C with entries from S.
OUTPUT: A bit indicating whether or not $C = AB$.

The matrix multiplication problem is a well-studied problem in classical computer science. The straightforward algorithm for matrix multiplication that computes each entry separately using its definition uses $O(n^3)$ operations. In 1969, Strassen [17] presented an algorithm that multiplies matrices over any ring using only $O(n^{2.807})$ operations, showing that the straightforward approach was suboptimal. Since then there have been many improvements and the complexity of matrix multiplication remains an area of active research.

Surprisingly, the matrix product verification problem can be solved faster. In 1979, Freivalds [6] presented an optimal $O(n^2)$ time bounded-error probabilistic algorithm to solve the matrix product verification problem over any ring using a randomized fingerprinting technique, which has found numerous other applications in theoretical computer science (see, e.g., Ref. [15]).

In the quantum setting, these problems are traditionally studied in the model of quantum query complexity, where we assume the entries of the input matrices are provided by a black box or an oracle. The query complexity of an algorithm is the number of queries made to the oracle. The bounded-error quantum query complexity of a problem is the minimum query complexity of any quantum algorithm that solves the problem with bounded error, i.e., it outputs the correct answer with probability greater than (say) 2/3. The time complexity of an algorithm refers to the time required to implement the remaining non-query operations. In this article we only consider bounded-error quantum algorithms.

Key Results

It is not known if quantum algorithms can improve the time complexity of the general matrix multiplication problem compared to classical algorithms. Improvements are possible for matrix product verification and special cases of the matrix multiplication problem, as described below.

Matrix product verification over rings

According to Buhrman and Špalek [3], matrix product verification was first studied (in an unpublished paper) by Ambainis, Buhrman, Høyer, Karpinski, and Kurur. Using a recursive application of Grover's algorithm [7], they gave an $O(n^{7/4})$ query algorithm for the problem. The first published work on the topic is due to Buhrman and Špalek [3], who gave an $O(n^{5/3})$ query algorithm for matrix product verification over any ring using a generalization of Ambainis' element distinctness algorithm [1]. This algorithm also achieves the same query complexity over semirings and more general algebraic structures. The algorithm can easily be cast in the quantum walk search framework of Magniez, Nayak, Roland, and Santha [14] as explained in the survey by Santha [16]. More interestingly, they presented an algorithm with time complexity $\tilde{O}(n^{5/3})$ for the problem over fields and integral domains. Their algorithm uses the same technique used by Freivalds [6] and is therefore also time efficient over arbitrary rings. Buhrman and

Špalek also proved a lower bound showing that any bounded-error quantum algorithm must make at least $\Omega(n^{3/2})$ queries to solve the problem over the field $\mathbb{F}_2$. This lower bound can be extended to all rings [10].

Theorem 1 (Matrix product verification over rings). *The matrix product verification problem over any ring can be solved by a quantum algorithm with query complexity $O(n^{5/3})$ and time complexity $\tilde{O}(n^{5/3})$. Furthermore, any quantum algorithm must make $\Omega(n^{3/2})$ queries to solve the problem over a ring.*

Buhrman and Špalek also studied the relationship between the complexity of their algorithm and the number of incorrect entries in the purported product, C, and showed that their algorithm performs better when C has a large number of incorrect entries [3].

Matrix multiplication over rings

The quantum query complexity of multiplying two $n \times n$ matrices is easy to characterize in terms of the input size. Clearly the query complexity is upper bounded by the input size, $O(n^2)$. On the other hand if A equals the identity matrix, then $C = B$ and in this case the matrix multiplication problem is equivalent to learning all the bits of an input of size n^2, which requires $\Omega(n^2)$ queries. This follows, for example, from the fact that computing the parity of n^2 bits requires $\Omega(n^2)$ queries [2, 5]. This shows that the quantum query complexity of matrix multiplication is $\Theta(n^2)$, which is the same as the classical query complexity. Similarly, no quantum algorithm is known to improve the time complexity of matrix multiplication over rings compared to classical algorithms.

Buhrman and Špalek [3] studied the matrix multiplication problem in terms of n and an additional parameter ℓ, the number of nonzero entries in the output matrix C, and showed the following result.

Theorem 2. *The matrix multiplication problem over any ring can be solved by a quantum algorithm with query and time complexity upper bounded by*

$$\begin{array}{ll} \tilde{O}(n^{5/3}\ell^{2/3}) & \textit{when } 1 \leq \ell \leq \sqrt{n}, \\ \tilde{O}(n^{3/2}\ell) & \textit{when } \sqrt{n} \leq \ell \leq n, \textit{ and} \\ \tilde{O}(n^2\sqrt{\ell}) & \textit{when } n \leq \ell \leq n^2, \end{array}$$

where ℓ is the number of nonzero entries in the output matrix C.

When ℓ is small, this algorithm achieves subquadratic time complexity and when ℓ approaches n^2, its time complexity is close to $O(n^3)$, which is trivial and slower than known classical algorithms. A detailed comparison of this quantum algorithm with classical algorithms may be found in Ref. [3].

Boolean matrix product verification

Buhrman and Špalek [3] also studied the matrix product verification problem over the Boolean semiring and showed that the problem can be solved with query and time complexity $O(n^{3/2})$. On the other hand, the best known lower bound is only $\Omega(n^{1.055})$ queries due to Childs, Kimmel, and Kothari [4].

Theorem 3 (Boolean matrix product verification). *The Boolean matrix product verification problem can be solved by a quantum algorithm with query complexity $O(n^{3/2})$ and time complexity $\tilde{O}(n^{3/2})$. Furthermore, any quantum algorithm must make $\Omega(n^{1.055})$ queries to solve the problem.*

Boolean matrix multiplication

As before, the quantum query complexity of multiplying two $n \times n$ Boolean matrices is $\Theta(n^2)$, since it is at least as hard as learning n^2 input bits. The time complexity of Boolean matrix multiplication can be improved to $\tilde{O}(n^{2.5})$ by observing that the inner product of two Boolean vectors of length n can be computed with $O(\sqrt{n})$ queries using Grover's algorithm [7]. This observation also speeds up matrix multiplication over some other semirings.

Similar to the matrix multiplication problem over rings, Boolean matrix multiplication can be studied in terms of an additional parameter ℓ, the number of nonzero entries in the output matrix. Indeed, the problem has been extensively studied in this setting.

Buhrman and Špalek [3] observed that two Boolean matrices can be multiplied with query complexity $O(n^{3/2}\sqrt{\ell})$. This upper bound was improved by Vassilevska Williams and Williams [18], who presented an algorithm with query complexity $\tilde{O}(\min\{n^{1.3}\ell^{17/30}, n^2 + n^{13/15}\ell^{47/60}\})$, which was then improved by Le Gall [11]. Finally, Jeffery, Kothari, and Magniez [8] presented a quantum algorithm for Boolean matrix multiplication that makes $\tilde{O}(n\sqrt{\ell})$ queries. These upper bounds are depicted in Figure 1. The log factors present in their algorithm were later removed to yield an algorithm with query complexity $O(n\sqrt{\ell})$ [9]. Jeffery, Kothari, and Magniez [8] also proved a matching lower bound of $\Omega(n\sqrt{\ell})$ when $\ell \leq \epsilon n^2$ for any constant $\epsilon < 1$. Their algorithm can also be modified to achieve time complexity $\tilde{O}(n\sqrt{\ell} + \ell\sqrt{n})$ [12].

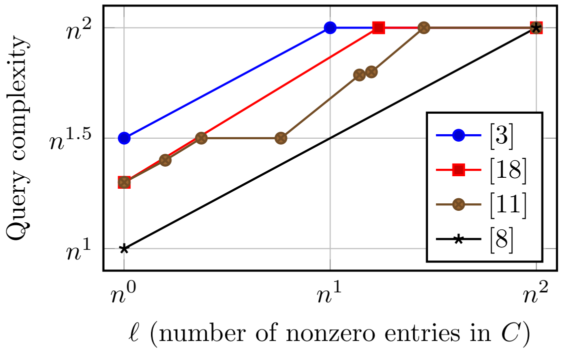

Fig. 1. Upper bounds on the quantum query complexity of Boolean matrix multiplication.

Theorem 4 (Boolean matrix multiplication). *The Boolean matrix multiplication problem can be solved by a quantum algorithm with query complexity $O(n\sqrt{\ell})$. Furthermore, any quantum algorithm that solves the problem must make $\Omega(n\sqrt{\ell})$ queries when $\ell \leq \epsilon n^2$ for any constant $\epsilon < 1$. Boolean matrix multiplication can be solved in time $\tilde{O}(n\sqrt{\ell} + \ell\sqrt{n})$.*

Recently the problem has also been studied in terms of the sparsity of the input matrix. Le Gall and Nishimura [13] present algorithms with improved time complexity in this case. Their algorithm's time complexity is a complicated function of the parameters and the reader is referred to Ref. [13] for details.

Matrix multiplication over other semirings

Le Gall and Nishimura [13] recently initiated the study of matrix multiplication over semirings other than the Boolean semiring and presented algorithms with improved time complexity for the (max, min)-semiring and related semirings.

Open Problems

Several open problems remain in the time and query complexity settings. In the time complexity setting, a major open problem is whether quantum algorithms can solve the matrix multiplication problem faster than classical algorithms over any ring. In the query complexity setting, the complexity of matrix product verification over rings and the Boolean semiring remains open. The best upper and lower bounds are presented in Theorem 1 and Theorem 3. A more comprehensive survey of the quantum query complexity of matrix multiplication and its relation to other problems studied in quantum query complexity such as triangle finding and graph collision can be found in the first author's PhD thesis [10], which also contains additional open problems.

Cross-References

Quantization of Markov Chains
Quantum Algorithm for Element Distinctness
Quantum Search

Recommended Reading

1. Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.
2. Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001.
3. Harry Buhrman and Robert Špalek. Quantum verification of matrix products. In *Proceedings of 17th ACM-SIAM Symposium on Discrete Algorithms*, pages 880–889, 2006.
4. Andrew M. Childs, Shelby Kimmel, and Robin Kothari. The quantum query complexity of read-many formulas. In *Algorithms — ESA 2012*, volume 7501 of *Lecture Notes in Computer Science*, pages 337–348. Springer, 2012.
5. Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Limit on the speed of quantum computation in determining parity. *Physical Review Letters*, 81(24):5442–5444, 1998.
6. Rūsiņš Freivalds. Fast probabilistic algorithms. In *Mathematical Foundations of Computer Science*, volume 74 of *Lecture Notes in Computer Science*, pages 57–69. Springer, 1979.
7. Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th ACM Symposium on Theory of Computing (STOC 1996)*, pages 212–219, 1996.
8. Stacey Jeffery, Robin Kothari, and Frédéric Magniez. Improving Quantum Query Complexity of Boolean Matrix Multiplication Using Graph Collision. In *Automata, Languages, and Programming*, volume 7391 of *Lecture Notes in Computer Science*, pages 522–532. Springer, 2012.
9. Robin Kothari. An optimal quantum algorithm for the oracle identification problem. In *Proceedings of the 31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014)*, volume 25 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 482–493, 2014.
10. Robin Kothari. *Efficient algorithms in quantum query complexity.* PhD thesis, University of Waterloo, 2014.
11. François Le Gall. Improved output-sensitive quantum algorithms for Boolean matrix multiplication. In *Proceedings of the 23rd ACM-SIAM Symposium On Discrete Algorithms (SODA 2012)*, pages 1464–1476, 2012.
12. François Le Gall. A time-efficient output-sensitive quantum algorithm for Boolean matrix multiplication. In *Algorithms and Computation*, volume 7676 of *Lecture Notes in Computer Science*, pages 639–648. Springer, 2012.
13. François Le Gall and Harumichi Nishimura. Quantum algorithms for matrix products over semirings. In *Algorithm Theory — SWAT 2014*, volume 8503 of *Lecture Notes in Computer Science*, pages 331–343. Springer, 2014.
14. Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha. Search via quantum walk. *SIAM Journal on Computing*, 40(1):142–164, 2011.

15. Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms.* Cambridge University Press, 1995.
16. Miklos Santha. Quantum walk based search algorithms. In *Theory and Applications of Models of Computation*, volume 4978 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2008.
17. Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13:354–356, 1969.
18. Virginia Vassilevska Williams and Ryan Williams. Subcubic equivalences between path, matrix and triangle problems. In *Proceedings of the 51st IEEE Symposium on Foundations of Computer Science (FOCS 2010)*, pages 645–654, 2010.