Quantum Algorithms for Matrix Multiplication

François Le Gall[1] *

[1] *Department of Computer Science*
Graduate School of Information Science and Technology
The University of Tokyo, Japan

Abstract. This talk will describe recent progresses in the development of quantum algorithms for matrix multiplication. I will start with the case of Boolean matrices, and discuss the time complexity and query complexity of Boolean matrix multiplication in the quantum setting. I will then focus on other kinds of matrix products, in particular matrix products over algebraic structures known as semirings (such as the distance matrix product or the max-min matrix product), and describe new quantum algorithms, which are faster than the best known classical algorithms, for some of these products. Finally I will present several open problems related to the complexity of matrix multiplication. Part of this talk will be based on a recent joint work with Harumichi Nishimura.

Keywords: quantum algorithms, matrix multiplication, graph algorithms

1 Boolean Matrix Multiplication

Multiplying two Boolean matrices, where addition is interpreted as a logical OR and multiplication as a logical AND, is a fundamental problem that have found applications in many areas of computer science, and in particular in the design of graph algorithms. The product of two $n \times n$ Boolean matrices can be trivially computed in time $O(n^3)$. The best known algorithm is obtained by seeing the input matrices as integer matrices, computing the product, and converting the product matrix to a Boolean matrix. This gives a classical algorithm for Boolean matrix multiplication with time complexity $\tilde{O}(n^\omega)$, where ω denotes the exponent of square matrix multiplication over a ring (the best known upper bound on ω is $\omega < 2.3727$, by Vassilevska Williams [9]).

In the quantum setting, there exists a straightforward $\tilde{O}(n^2\sqrt{p})$-time algorithm that computes the product of an $n \times p$ Boolean matrix A by a $p \times n$ Boolean matrix B: for each pair of indexes $(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$, check if there exists an index $k \in \{1,\ldots,p\}$ such that $A[i,k] = B[k,j] = 1$ in time $\tilde{O}(\sqrt{p})$ using Grover's quantum search algorithm. While for square matrices (i.e., $n = p$) this algorithm does not give any improvement over the $\tilde{O}(n^\omega)$-time classical algorithm mentioned above, for rectangular matrices (e.g., for $p \geq n^3$) this already outperforms the best known classical algorithm for rectangular matrix multiplication [5]. Even for square matrices, Buhrman and Špalek [1] observed that a similar approach leads to a quantum algorithm that computes the Boolean product AB in $\tilde{O}(n^{3/2}\sqrt{\ell})$ time, where ℓ denotes the number on non-zero entries in AB, which is better than the complexity of the best known classical algorithms when ℓ is small enough (concretely, when $\ell \leq n^{1.60}$). This bound has been further improved recently: Jeffery, Kothari and Magniez [3] showed that the quantum query complexity of computing the product of two $n \times n$ Boolean matrices with ℓ non-zero entries in the product is $\tilde{O}(n\sqrt{\ell})$, and gave a matching (up to polylogarithmic factors) lower bound $\Omega(n\sqrt{\ell})$, while Le Gall [4, 6] obtained the upper bound $\tilde{O}(n\sqrt{\ell} + \ell\sqrt{n})$ in the time complexity setting.

Instead of assuming that the output matrix is sparse, it is also natural to consider the case where the input matrices are sparse. In this setting quantum algorithms faster than the best known classical algorithms can be constructed as well, as stated in the following theorem.

Theorem 1 ([7]) *Let A and B be two $n \times n$ Boolean matrices each containing at most m non-zero entries. There exists a quantum algorithm that computes, with high probability, the Boolean matrix product AB and has time complexity*

$$\begin{cases} \tilde{O}(n^2) & \text{if } m \leq n^{1.1514}, \\ \tilde{O}\left(m^{0.5168} n^{1.4049}\right) & \text{if } n^{1.1514} \leq m \leq n^{\omega-1/2}, \\ \tilde{O}(n^\omega) & \text{if } n^{\omega-1/2} \leq m \leq n^2. \end{cases}$$

The complexity of the algorithm of Theorem 1 is the function of $\log_n(m)$ represented in Figure 1, along with the complexity of the best known classical algorithm by Yuster and Zwick [10]. This quantum algorithm performs better whenever $n^{1.1514} < m < n^{\omega-1/2}$.

2 Matrix Products over other Semirings

The straightforward $\tilde{O}(n^{5/2})$-time quantum algorithm for Boolean matrix multiplication described in the previous section can actually be generalized to compute matrix products over several other algebraic structures known as semirings. For instance, let us consider the $(\max, \min)$-product and the distance product defined as follows.

Definition 2 *Let A and B be two $n \times n$ matrices with entries in $\mathbb{Z}$. The $(\max, \min)$-product of A and B is the $n \times n$ matrix C defined as*

$$C[i,j] = \max_{k \in \{1,\ldots,n\}} \{\min(A[i,k], B[k,j])\}$$

for all $(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$.

*legall@is.s.u-tokyo.ac.jp

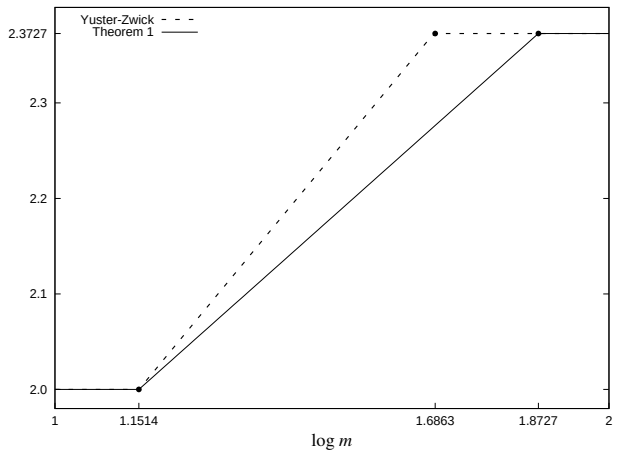

Figure 1: The upper bounds of Theorem 1 (in solid lines). The horizontal axis represents the logarithm of m with respect to basis n (i.e., the value $\log_n(m)$). The vertical axis represents the logarithm of the complexity with respect to basis n. The dashed lines represent the upper bounds of the classical algorithm obtained in [10].

Definition 3 *Let A and B be two $n \times n$ matrices with entries in $\mathbb{Z} \cup \{\infty\}$. The distance product of A and B is the $n \times n$ matrix C defined as*

$$C[i,j] = \min_{k \in \{1,\ldots,n\}} \{A[i,k] + B[k,j]\}$$

for all $(i,j) \in \{1,\ldots,n\} \times \{1,\ldots,n\}$.

The $(\max, \min)$-product has mainly been studied in the field in fuzzy logic under the name *composition of relations* and in the context of computing the all-pairs bottleneck paths of a graph (i.e., computing, for all pairs (s,t) of vertices in a graph, the maximum flow that can be routed between s and t). The distance product has a multitude of applications in the design of graph algorithms, mostly related to computations of all-pairs shortest paths problems. It is straightforward to construct $\tilde{O}(n^{5/2})$-time quantum algorithms computing these two products by using variants of quantum search (more precisely, by using a $\tilde{O}(\sqrt{n})$-time quantum algorithm to find the minimal or maximal element in a list of size n).

This exponent $5/2$ can actually be improved. For the $(\max, \min)$-product, in particular, a significant improvement can be obtained.

Theorem 4 ([7]) *There exists a quantum algorithm that computes, with high probability, the $(\max, \min)$-product of two $n \times n$ matrices in time $O(n^{2.4728})$.*

In comparison, the best known classical algorithm for the $(\max, \min)$-product, by Duan and Pettie [2], has time complexity $\tilde{O}(n^{(3+\omega)/2}) = O(n^{2.6864})$. As an application of Theorem 4, a $O(n^{2.4728})$-time quantum algorithm computing the all-pairs bottleneck paths of a graph of n vertices can be immediately obtained, while classically the best upper bound for this task is $O(n^{2.6864})$, again from [2]. Similar techniques can be used to speed up the computation of the distance product as well [7]. Namely, it is possible to construct a quantum algorithm computing the ℓ most significant bits of each entry of the distance product of two $n \times n$ matrices with time complexity

$$\tilde{O}\left(2^{0.6397\ell} n^{(5+\omega)/3}\right) \leq O(2^{0.6397\ell} n^{2.4576}).$$

In comparison, the best known classical algorithm for the same problem by Vassilevska and Williams [8] has complexity $\tilde{O}\big(2^{\ell} n^{(3+\omega)/2}\big) \leq O(2^{\ell} n^{2.6864})$.

These results are, to the best of our knowledge, the first quantum algorithms for matrix multiplication over semirings other than the Boolean semiring improving over the straightforward $\tilde{O}(n^{5/2})$-time quantum algorithm, and the first nontrivial quantum algorithms offering a speedup with respect to the best classical algorithms for matrix multiplication when no assumptions are made on the sparsity of the matrices involved. This shows that, while it is still open whether quantum algorithms can outperform the classical $\tilde{O}(n^{\omega})$-time algorithm for matrix multiplication of (dense) matrices over a ring, quantum computation can offer a speedup for matrix multiplication over other algebraic structures.

References

[1] H. Buhrman and R. Špalek. Quantum verification of matrix products. In *Proc. of SODA'06*, pp. 880–889.

[2] R. Duan and S. Pettie. Fast algorithms for $(\max, \min)$-matrix multiplication and bottleneck shortest paths. In *Proc. of SODA'09*, pp. 384–391.

[3] S. Jeffery, R. Kothari and and F. Magniez. Improving quantum query complexity of Boolean matrix multiplication using graph collision. In *Proc. of ICALP'12, Part I*, pp. 522–532.

[4] F. Le Gall. Improved output-sensitive quantum algorithms for Boolean matrix multiplication. In *Proc. of SODA'12*, pp. 1464–1476.

[5] F. Le Gall. Faster algorithms for rectangular matrix multiplication. In *Proc. of FOCS'12*, pp. 514–523.

[6] F. Le Gall. A time-efficient output-sensitive quantum algorithm for Boolean matrix multiplication. In *Proc. of ISAAC'12*, pp. 639–648.

[7] F. Le Gall and H. Nishimura. Quantum Algorithms for Matrix Products over Semirings. *Submitted*.

[8] V. Vassilevska and R. Williams. Finding a maximum weight triangle in $n^{3-\delta}$ time, with applications. In *Proc. of STOC'06*, pp. 225–231.

[9] V. Vassilevska Williams. Multiplying matrices faster than Coppersmith-Winograd. In *Proc. of STOC'12*, pp. 887–898.

[10] R. Yuster and U. Zwick Fast sparse matrix multiplication. *ACM Transactions on Algorithms*, 1(1), pp. 2–13, 2005.