

On the Satisfiability of Quantum Circuits of Small Treewidth

Mateus de Oliveira Oliveira

Institute of Mathematics - Academy of Sciences of the Czech Republic
mateus.oliveira@math.cas.cz

November 26, 2014

Abstract

It has been known since long time that many NP-hard optimization problems can be solved in polynomial time when restricted to structures of constant treewidth. In this work we provide the first extension of such results to the quantum setting. We show that given a quantum circuit C with n uninitialized inputs, $\text{poly}(n)$ gates, and treewidth t , one can compute in time $(\frac{n}{\delta})^{\exp(O(t))}$ a classical witness $y \in \{0, 1\}^n$ that maximizes the acceptance probability of C up to a δ additive factor. In particular our algorithm runs in polynomial time if t is constant and $1/\text{poly}(n) \leq \delta < 1$. For unrestricted values of t this problem is known to be hard for the complexity class QCMA, a quantum generalization of NP. In contrast, we show that the same problem is already NP-hard if $t = O(\log n)$ even when δ is constant. Finally, we show that for $t = O(\log n)$ and constant δ , it is QMA-hard to find a quantum witness $|\varphi\rangle$ that maximizes the acceptance probability of a quantum circuit of treewidth t up to a δ additive factor.

Keywords: Treewidth, Satisfiability of Quantum Circuits, Tensor Networks

1 Introduction

The notions of tree decomposition and treewidth of a graph [12] play a central role in algorithmic theory. On the one hand, many natural classes of graphs have small treewidth. For instance, trees have treewidth at most 1, series-parallel graphs and outer-planar graphs have treewidth at most 2, Halin graphs have treewidth at most 3, and k -outerplanar graphs for fixed k have treewidth $O(k)$. On the other hand, many problems that are hard for NP on general graphs, and even problems that are hard for higher levels of the polynomial hierarchy, may be solved in polynomial time when restricted to graphs of constant tree-width [4, 7, 3].

In this work, we identify for the first time a natural quantum optimization problem that becomes feasible when restricted to graphs of constant treewidth. More precisely, we show how to find in polynomial time a classical assignment that maximizes, up to an inverse polynomial additive factor, the acceptance probability of a quantum circuit of constant treewidth. For quantum circuits of unrestricted treewidth this problem is hard for QCMA, a quantum generalization of MA [2]. Before stating our main result, we fix some notation. If C is a quantum circuit acting on n d -dimensional qudits, and $|\psi\rangle$ is a quantum state in $(\mathbb{C}^d)^{\otimes n}$, then we denote by $Pr(C, |\psi\rangle)$ the probability that the state of the output of C collapses to $|1\rangle$ when the input of C is initialized with $|\psi\rangle$ and the output is measured in the standard basis $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$. If y is a string in $\{0, \dots, d-1\}^n$ then we let $|y\rangle = \otimes_{i=1}^n |y_i\rangle$ denote the basis state corresponding to y . We let $Pr^{cl}(C) = \max_{y \in \{0, \dots, d-1\}^n} Pr(C, |y\rangle)$ denote the maximal acceptance probability of C among all classical input strings in $\{0, \dots, d-1\}^n$. The treewidth of a quantum circuit is defined as the treewidth of its underlying undirected graph.

Theorem 1 (Main Theorem). *Let C be a quantum circuit with n uninitialized inputs, $\text{poly}(n)$ gates and treewidth t . For any δ with $1/\text{poly}(n) < \delta < 1$ one may find in time $(\frac{n}{\delta})^{\exp(O(t))}$ a classical string $y \in \{0, \dots, d-1\}^n$ such that $|\text{Pr}(C, |y\rangle) - \text{Pr}^{\text{cl}}(C)| \leq \delta$.*

The use of treewidth in quantum algorithmics was pioneered by Markov and Shi [11] who showed that quantum circuits of logarithmic treewidth can be simulated in polynomial time with exponentially high precision. Note that the simulation of quantum circuits [11, 8, 1, 14, 15, 9] deals with the problem of computing the acceptance probability of a quantum circuit when all inputs are already initialized, and thus may be regarded as a generalization of the classical CIRCUIT-VALUE problem. On the other hand, Theorem 1 deals with the problem of finding an initialization that maximizes the acceptance probability of a quantum circuit, and thus may be regarded as a generalization of the classical CIRCUIT-SAT problem. Therefore, Theorem 1 is the first result showing that a quantum *optimization* problem can be solved in polynomial time when restricted to structures of constant treewidth.

It is interesting to determine whether the time complexity of our algorithm can be substantially improved. To address this question, we first introduce the *online-width* of a circuit, a width measure for DAGs that is at least as large as the treewidth of their underlying graphs. If $G = (V, E)$ is a directed graph and $V_1, V_2 \subseteq V$ are two subsets of vertices of V with $V_1 \cap V_2 = \emptyset$ then we let $E(V_1, V_2)$ be the set of all edges with one endpoint in V_1 and another endpoint in V_2 . If $\omega = (v_1, v_2, \dots, v_n)$ is a total ordering of the vertices in V , then we let $\mathbf{cw}(G, \omega) = \max_i |E(\{v_1, \dots, v_i\}, \{v_{i+1}, \dots, v_n\})|$. The *cutwidth* of G [13] is defined as $\mathbf{cw}(G) = \min_{\omega} \mathbf{cw}(G, \omega)$ where the minimum is taken over all possible total orderings of the vertices of G . If G is a DAG, then the *online-width* of G is defined as $\mathbf{ow}(G) = \min_{\omega} \mathbf{cw}(G, \omega)$ where the minimum is taken only among the *topological orderings* of G . Below we compare online-width with other width measures. We write $\mathbf{pw}(G)$ for the pathwidth of G and $\mathbf{tw}(G)$ for the treewidth of G .

$$\mathbf{tw}(G) \leq \mathbf{pw}(G) \leq \mathbf{cw}(G) \leq \mathbf{ow}(G) \tag{1}$$

Theorem 2 below states that finding a classical witness that maximizes the acceptance probability of quantum circuits of logarithmic online-width is already NP-hard even when δ is constant. Since $\mathbf{tw}(C) \leq \mathbf{ow}(C)$ for any quantum circuit C , the same hardness result holds with respect to quantum circuits of logarithmic treewidth.

Theorem 2. *For any constant $0 < \delta < 1$, the following problem is NP-hard. Given a quantum circuit C of online width $O(\log n)$ with n uninitialized inputs and $\text{poly}(n)$ gates, determine whether $\text{Pr}^{\text{cl}}(C) = 1$ or whether $\text{Pr}^{\text{cl}}(C) \leq \delta$.*

An analog hardness result holds when the verifier is restricted to have logarithmic online-width and the witness is allowed to be an arbitrary quantum state. It was shown by Kitaev [10] that finding an δ -optimal quantum witness for a quantum circuit of unrestricted width is hard for the complexity class QMA for any constant δ . Interestingly, Kitaev's hardness result is preserved when the quantum circuits are restricted to have logarithmic online-width. If C is a quantum circuit with n inputs, then we let $\text{Pr}^{\text{qu}}(C) = \max_{|\varphi\rangle} \text{Pr}^{\text{qu}}(C)$ be the maximum acceptance probability among all n -qudit quantum states $|\psi\rangle$.

Theorem 3. *For any $0 < \delta < 1$ the following problem is QMA-Hard. Given a quantum circuit C of online-width $O(\log n)$ with n uninitialized inputs and $\text{poly}(n)$ gates, determine whether $\text{Pr}^{\text{qu}}(C) \geq 1 - \delta$ or whether $\text{Pr}^{\text{qu}}(C) \leq \delta$.*

We analyse the implications of theorems 2 and 3 to quantum generalizations of Merlin-Arthur protocols. In this setting Arthur, a polynomial sized quantum circuit, must decide the

membership of a string x to a given language \mathcal{L} by analysing a quantum state $|\psi\rangle$ provided by Merlin. In the case that $x \in \mathcal{L}$, there is always a quantum state $|\psi\rangle$ that is accepted by Arthur with probability at least $2/3$. On the other hand if $x \notin \mathcal{L}$ then no state is accepted by Arthur with probability greater than $1/3$. The class of all languages that can be decided via some quantum Merlin-Arthur game is denoted by QMA. The importance of QMA stems from the fact that this class has several natural complete problems [6, 10]. Additionally, the oracle version of QMA contains problems, such as the group non-membership problem [16] which are provably not in the oracle version of MA and hence not in the oracle version of NP [5]. The class QCMA is defined analogously, except for the fact that the witness provided by Merlin is a product state encoding a classical string. Below we define width parameterized versions of QMA.

Definition 1. A language $\mathcal{L} \subseteq \{0, 1\}^*$ belongs to the class $f(n)$ -Online-QMA ($f(n)$ -treewidth-QMA) if there exists a polynomial time constructible family of quantum circuits $\{C_x\}_{x \in \{0, 1\}^*}$ such that for every $x \in \{0, 1\}^*$, C_x has online-width (treewidth) at most $f(|x|)$ and

- if $x \in \mathcal{L}$ then there exists a quantum state $|\psi\rangle$ such that C_x accepts $|\psi\rangle$ with probability at least $2/3$,
- if $x \notin \mathcal{L}$ then for any quantum state $|\psi\rangle$, C_x accepts $|\psi\rangle$ with probability at most $1/3$.

The class $f(n)$ -Online-QCMA ($f(n)$ -Treewidth-QCMA) is defined analogously, except that the witness $|y\rangle$ is required to be a classical string y encoded into a basis state $|y\rangle$.

Corollary 1.i below follows from Theorem 1. Corollary 1.ii is a consequence of the hardness result stated in Theorem 2 together with Markov and Shi's result [11] stating that quantum circuits of logarithmic treewidth can be simulated in polynomial time. Notice that by Equation 1, the results in [11] also imply that circuits of logarithmic online-width can be simulated in polynomial time. Corollary 1.iii follows directly from Theorem 3. We notice that the classes QMA and QCMA are respectively equal to $poly(n)$ -Online-QMA and $poly(n)$ -Online-QCMA.

Corollary 1.

- i) $O(1)$ -Treewidth-QCMA $\subseteq P$.
- ii) $O(\log n)$ -Treewidth-QCMA = $O(\log n)$ -Online-QCMA = NP.
- iii) $O(\log n)$ -Treewidth-QMA = $O(\log n)$ -Online-QMA = QMA,

Thus, assuming that $QMA \neq NP$, Corollary 1 implies that, whenever Arthur is restricted to have logarithmic treewidth, quantum Merlin-Arthur protocols differ in power with respect to whether the witness provided by Merlin is classical or quantum. We observe that obtaining a similar separation between the power of classical and quantum witnesses when Arthur is allowed to have polynomial treewidth is equivalent to determining whether $QMA \neq QCMA$. This question remains widely open.

References

- [1] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *CoRR*, quant-ph/0406196, 2004.
- [2] D. Aharonov and T. Naveh. Quantum NP - A survey, 2002. Comment: 23 pages.

- [3] S. Arnborg, J. Lagergren, and D. Seese. Easy problems for tree-decomposable graphs. *Journal of Algorithms*, 12(2):308–340, 1991.
- [4] S. Arnborg and A. Proskurowski. Linear time algorithms for np-hard problems restricted to partial k-trees. *Discrete Applied Mathematics*, 23(1):11–24, 1989.
- [5] Babai. Bounded round interactive proofs in finite groups. *SIJDM: SIAM Journal on Discrete Mathematics*, 5, 1992.
- [6] A. Bookatz. QMA complete problems. 2013.
- [7] B. Courcelle. The monadic second-order logic of graphs. i. recognizable sets of finite graphs. *Information and computation*, 85(1):12–75, 1990.
- [8] D. Gottesman. The heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006*, 1998.
- [9] R. Jozsa and N. Linden. On the role of entanglement in quantum computational speed-up. *Proc. R. Soc. Lond. A*, 459:2011–2032, June 2003.
- [10] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. 2002.
- [11] I. L. Markov and Y. Shi. Simulating quantum computation by contracting tensor networks. *SIAM Journal on Computing*, 38(3):963–981, 2008.
- [12] N. Robertson and P. D. Seymour. Graph minors. iii. planar tree-width. *Journal of Combinatorial Theory, Series B*, 36(1):49–64, 1984.
- [13] D. M. Thilikos, M. Serna, and H. L. Bodlaender. Cutwidth i: A linear time fixed parameter algorithm. *Journal of Algorithms*, 56(1):1–24, 2005.
- [14] Valiant. Quantum circuits that can be simulated classically in polynomial time. *SICOMP: SIAM Journal on Computing*, 31, 2002.
- [15] G. Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91:147902, Oct 2003.
- [16] Watrous2000. Succinct quantum proofs for properties of finite groups. In *FOCS 2000 - IEEE Symposium on Foundations of Computer Science*, 2000.