Eliminating Intermediate Measurements in Space-Bounded Quantum Computation

Bill Fefferman and Zachary Remscrim*
Department of Computer Science, The University of Chicago

While fully scalable, fault-tolerant quantum computers may still be far from fruition, we have now entered an exciting period in which impressive but resource constrained quantum experiments are being implemented in many academic and industrial labs. As the field transitions from "proof of principle" demonstrations of provable quantum advantage to solving useful problems on near-term experiments, it is particularly critical to characterize the algorithmic power of feasible models of quantum computations that have restrictive resources such as "time" (i.e., the number of gates in the circuit) and "space" (i.e., the number of qubits on which the circuit operates) and to understand how these resources can be traded-off.

A foundational question in this area asks if it is possible to *space-efficiently* eliminate intermediate measurements in a quantum computation (see e.g., [11,14,19,22,26,30–32]). While a classic result known as the "principle of safe storage" states that it is always possible to *time-efficiently* defer intermediate measurements to the end of a computation [1, 21], this procedure uses extra ancilla qubits, and so is not generally space efficient. More specifically, if a quantum circuit Q acts on s qubits and performs m intermediate measurements, the circuit Q' constructed using this principle operates on $s + poly(m)$ qubits; if, for example, $s = O(\log t)$ and $m = \Theta(t)$, this entails an *exponential blowup* in the amount of needed *space*.

Our main result solves this problem. We show that every problem solvable by a "general" quantum algorithm, which may make arbitrary use of quantum measurements, can also be solved, using the same amount of space, by a "unitary" quantum algorithm, which may not perform any intermediate measurements. As an immediate corollary, this shows that, in the space-bounded setting, unitary quantum algorithms are at least as powerful as probabilistic algorithms, resolving a longstanding open problem [19, 31].

In the process of proving this result, we also obtain the following result, which is likely of independent interest: approximating the solution of the "well-conditioned" versions of various standard linear-algebraic problems, such as the determinant problem, the matrix inversion problem, or the matrix powering problem, is complete for the class of bounded-error logspace quantum algorithms. These are a new class of natural problems on which quantum computers seem to outperform their classical counterparts.

1 Eliminating Intermediate Measurements

Before proceeding further, it is worthwhile to briefly discuss why it is desirable to be able to eliminate intermediate measurements. Firstly, quantum measurements are a natural resource, much as time and space are. In addition to the general desirability of using as few resources as possible in any sort of computational task, it is especially desirable to avoid intermediate measurements, due to the technical challenges involved in implementing such measurements and resetting qubits to their initial states [8]. Secondly, unitary computations are *reversible*, whereas quantum measurement is an inherently irreversible process. The ability to "undo" a unitary subroutine, by running it in reverse, is routinely used in the design and analysis of quantum algorithms [3, 10, 11, 18, 20, 25, 33]. Moreover, reversible computations may be performed without generating heat [16]. Thirdly, by demonstrating that unitary quantum space and general quantum space are equivalent in power, we show that the definition of quantum space is quite *robust*. Allowing intermediate measurements, or even general quantum operations, does not provide any additional power in the space-bounded setting.

*Corresponding author, remscrim@uchicago.edu

Let $\mathsf{BQ_U SPACE}(s(n))$ (resp. $\mathsf{BQSPACE}(s(n))$) denote the class of promise problems recognizable with two-sided bounded-error by a uniform family of unitary (resp. general) quantum circuits, where, for each input of length n, there is a corresponding circuit that operates on $O(s(n))$ qubits and has $2^{O(s(n))}$ gates. Note that it is standard to require that the running time of a computation is at most exponential in its space bound; see, for instance, [19, 23, 30, 32] for the importance of this restriction in quantum and/or probabilistic space-bounded computation. Furthermore, let $\mathsf{QMASPACE}(s(n))$ denote those promise problems recognized by a quantum Merlin-Arthur protocol that operates in space $O(s(n))$ and time $2^{O(s(n))}$. Our main result is:

Theorem 1. *For any space-constructible function $s : \mathbb{N} \to \mathbb{N}$, where $s(n) = \Omega(\log n)$, we have*

$$\mathsf{BQ_U SPACE}(s(n)) = \mathsf{BQSPACE}(s(n)) = \mathsf{QMASPACE}(s(n)).$$

We also study the one-sided (bounded-error and unbounded-error) analogues of the aforementioned two-sided bounded-error space-bounded quantum complexity classes. We establish analogous results concerning the relationship between the unitary and general versions of these classes.

2 Exact and Approximate Linear Algebra

Let intDET denote the problem of computing the determinant of an $n \times n$ integer-valued matrix, and, following its original definition by Cook [6], let DET^* denote the class of problems NC^1 (Turing) reducible to intDET. Let $\mathsf{BQ_U L} = \mathsf{BQ_U SPACE}(\log(n))$, $\mathsf{BQL} = \mathsf{BQSPACE}(\log(n))$, and $\mathsf{BPL} = \mathsf{BPSPACE}(\log(n))$ denote the bounded-error quantum and probabilistic logspace classes. Before our work, the following relationships were known [30, 32]: $\mathsf{BQ_U L} \subseteq \mathsf{BQL} \subseteq \mathsf{DET}^*$ and $\mathsf{BPL} \subseteq \mathsf{BQL}$. Many natural linear-algebraic problems are complete for DET^*, including intDET, $\mathsf{intMATINV}$ (the problem of computing a single entry of the inverse of a matrix), and $\mathsf{intITMATPROD}$ (the problem of computing a single entry of the product of polynomially-many matrices). It seems rather unlikely that any such DET^*-complete problem is in the class BQL, as this would imply $\mathsf{BQL} = \mathsf{DET}^*$, and, therefore, $\mathsf{NL} \subseteq \mathsf{BQL}$.

We next consider the problem of *approximating* the answer to such linear-algebraic problems. In particular, let *poly*-conditioned-MATINV denote the promise problem of approximating, to additive $1/poly(n)$ accuracy, a single entry of the inverse of an $n \times n$ matrix A with *condition number* $\kappa(A) = poly(n)$. Ta-Shma [26], building on the landmark result of Harrow, Hassidim, and Lloyd [13], showed *poly*-conditioned-$\mathsf{MATINV} \in \mathsf{BQL}$. Fefferman and Lin [11] improved upon this result by presenting a *unitary* quantum logspace algorithm and proving a matching $\mathsf{BQ_U L}$-hardness result, thereby exhibiting the first known natural $\mathsf{BQ_U L}$-complete (promise) problem. We further extend this line of research by proving the following theorem, which demonstrates an intriguing relationship between $\mathsf{BQ_U L}$ and DET^*:

Theorem 2. *(Informal) All of the poly-conditioned versions of the "standard" DET^*-complete problems are $\mathsf{BQ_U L}$-complete.*

This shows that several natural linear-algebraic problems are in $\mathsf{BQ_U L}$, and, moreover, are not in BPL (unless $\mathsf{BQ_U L} = \mathsf{BPL}$). In particular, the above theorem shows *poly*-conditioned-$\mathsf{ITMATPROD} \in \mathsf{BQ_U L}$. We also show that this problem is BQL-hard, which implies $\mathsf{BQL} = \mathsf{BQ_U L}$; Theorem 1, which states the more general equivalence for any larger space bound, then follows from a standard padding argument.

We next exhibit several other applications of this theorem. Firstly, we consider *fully logarithmic approximation schemes*, whose study was initiated by Doron and Ta-Shma [9]. Using the preceding theorem, we show that the BQL vs. BPL question is equivalent to several distinct questions involving the relative power of quantum and probabilistic fully logarithmic approximation schemes. Secondly, consider $\kappa(n)$-conditioned-DET, the problem of approximating, to within a *multiplicative* factor $1 + 1/poly(n)$, the determinant of an $n \times n$ matrix with condition number $\kappa(n)$. Boix-Adserà, Eldar, and Mehraban [5] recently showed that $\kappa(n)$-conditioned-$\mathsf{DET} \in \mathsf{DSPACE}(\log(n)\log(\kappa(n))poly(\log\log n))$. They also raised the following question: is *poly*-conditioned-DET BQL-complete? As an immediate consequence of Theorem 2, we answer their question in the affirmative.

Corollary 2.1. *poly-conditioned-DET is $\mathsf{BQ_U L}$-complete (and, therefore, BQL-complete).*

To see the significance of the previous corollary, recall the well-known "dequantumization" result given by Watrous [32]: $\mathsf{BQL} \subseteq \mathsf{DSPACE}(\log^2 n)$. It is natural to ask if a stronger upper bound on BQL can be established. We note that the strongest currently known "derandomization" result of this type, given by Saks and Zhou [24], states $\mathsf{BPL} \subseteq \mathsf{DSPACE}(\log^{\frac{3}{2}} n)$. Note that the statement $\mathsf{BQL} \subseteq \mathsf{DSPACE}(\log^{2-\epsilon} n)$ would follow from either a small improvement in the result of Boix-Adserà, Eldar, and Mehraban (i.e., proving a stronger upper bound on the needed amount of deterministic space in terms of $\kappa(n)$) or from a small improvement in our result (i.e., proving $\kappa(n)$-conditioned-DET remains BQL-hard for *subpolynomial* $\kappa(n)$). Therefore, if $\mathsf{BQL} \not\subseteq \mathsf{DSPACE}(\log^{2-\epsilon} n)$, $\forall \epsilon > 0$, then both our result and their result are essentially optimal.

Next, we study well-conditioned versions of the "standard" $\mathsf{C_{=}L}$-complete problems. We establish a result, very much analogous to Theorem 2, which shows that these problems are complete for the *one*-sided error versions of space-bounded quantum complexity classes. This enables us to prove results, analogous to Theorem 1, concerning the relative power of unitary and general quantum space in the one-sided error cases. Finally, we establish the $\mathsf{BQ_UL}$-completeness of "scaled-down" versions of certain QMA-complete problems and certain $\mathsf{DQC1}$-complete [15] problems, thereby showing that the *space*-bounded analogues of $\mathsf{DQC1}$, BQP, and QMA all coincide. This result is especially intriguing as each of the inclusions $\mathsf{DQC1} \subseteq \mathsf{BQP} \subseteq \mathsf{QMA}$ of *time*-bounded classes are generally believed to be proper.

3 Techniques

We now briefly discuss the techniques used to prove Theorem 2, which states that the *poly*-conditioned versions of the "standard" DET^*-complete problems are $\mathsf{BQ_UL}$-complete. As discussed earlier, Fefferman and Lin [11] showed that *poly*-conditioned-MATINV is $\mathsf{BQ_UL}$-complete. In order to establish the $\mathsf{BQ_UL}$-completeness of the other *poly*-conditioned problems, we exhibit a long cycle of reductions through these problems. We note that reductions between the standard versions of these problems (i.e., where there is no assumption of being well-conditioned) are well-known [2,4,6,7,17,27–29]. However, these reductions, generally, *do not* preserve the property of being *poly*-conditioned. Therefore, we must exhibit reductions that are rather different from the "standard" reductions.

As a motivating example, consider *poly*-conditioned-DET^+ and *poly*-conditioned-$\mathsf{SUMITMATPROD}$. Note that, while Berkowitz's algorithm [4] provides a reduction from DET^+ to $\mathsf{SUMITMATPROD}$, this reduction does not preserve the property of being *poly*-conditioned. We now provide a brief sketch of a reduction which does preserve this property. Consider a positive definite $n \times n$ matrix H, with $\sigma_1(H) \leq 1$ and $\kappa(H) = \mathit{poly}(n)$. We wish to obtain an additive $1/\mathit{poly}(n)$ approximation of $\ln(\det(H))$. By Jacobi's formula, $\ln(\det(H)) = \mathrm{tr}(\ln(H))$, where $\ln(H)$ denotes the matrix logarithm. We have $\sigma_1(I - H) \leq 1 - 1/\mathit{poly}(n) < 1$, which implies that the series $-\sum_{k=1}^{\infty} \frac{(I-H)^k}{k}$ converges to $\ln(H)$. Therefore, $\ln(\det(H)) = -\sum_{k=1}^{\infty} \frac{\mathrm{tr}((I-H)^k)}{k}$. Moreover, as $\sigma_1(I - H) \leq 1 - 1/\mathit{poly}(n)$, the aforementioned series converges "quickly," which implies that, for some $m = \mathit{poly}(n)$, the quantity $-\sum_{k=1}^{m} \frac{\mathrm{tr}((I-H)^k)}{k}$ is a sufficiently good approximation of $\ln(\det(H))$. Estimating this quantity corresponds to an instance of *poly*-conditioned-$\mathsf{SUMITMATPROD}$.

4 Related Work

Simultaneously and independently of our work, Girish, Raz, and Zhan [12] proved the following weaker version of our Theorem 2: *contraction*-$\mathsf{MATPOW} \in \mathsf{BQ_UL}$, where *contraction*-$\mathsf{MATPOW}$ is a special case of our *poly*-conditioned-MATPOW. We note that the techniques used in their proof differed substantially from ours. As a consequence of this result, they then obtain the following weaker version of our Theorem 1: $\mathsf{BQ_UL} = \mathsf{BQ_QL}$, where $\mathsf{BQ_QL} \subseteq \mathsf{BQL}$ is a version of quantum logspace that allows a special type of intermediate measurements to be performed, but does not allow using the (classical) result of earlier measurements to control (in a general fashion) later steps of the computation.

References

[1] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 20–30, 1998.

[2] Eric Allender and Mitsunori Ogihara. Relationships among pl, #l, and the determinant. *RAIRO-Theoretical Informatics and Applications*, 30(1):1–21, 1996.

[3] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997.

[4] Stuart J Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information processing letters*, 18(3):147–150, 1984.

[5] Enric Boix-Adserà, Lior Eldar, and Saeed Mehraban. Approximating the determinant of well-conditioned matrices by shallow circuits. *arXiv preprint arXiv:1912.03824*, 2019.

[6] Stephen A Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64(1-3):2–22, 1985.

[7] C Damm. Det= l# l. informatik-preprint 8. *Fachbereich Informatik der Humboldt-Universitat zu, Berlin*, 1991.

[8] David P DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik: Progress of Physics*, 48(9-11):771–783, 2000.

[9] Dean Doron and Amnon Ta-Shma. On the de-randomization of space-bounded approximate counting problems. *Information Processing Letters*, 115(10):750–753, 2015.

[10] Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, and Harumichi Nishimura. Space-efficient error reduction for unitary quantum computations. In *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[11] Bill Fefferman and Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. In *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[12] Uma Girish, Ran Raz, and Wei Zhan. Quantum logspace algorithm for powering matrices with bounded norm. *arXiv preprint arXiv:2006.04880*, 2020.

[13] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[14] Richard Jozsa, Barbara Kraus, Akimasa Miyake, and John Watrous. Matchgate and space-bounded quantum computations are equivalent. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 466(2115):809–830, 2010.

[15] Emanuel Knill and Raymond Laflamme. Power of one bit of quantum information. *Physical Review Letters*, 81(25):5672, 1998.

[16] Rolf Landauer. Irreversibility and heat generation in the computing process. *IBM journal of research and development*, 5(3):183–191, 1961.

[17] Meena Mahajan and V Vinay. Determinant: Combinatorics, algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, 1997.

[18] Chris Marriott and John Watrous. Quantum arthur–merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[19] Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory of Computing*, 8(1):1–51, 2012.

[20] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of qma. *Quantum Information & Computation*, 9(11):1053–1068, 2009.

[21] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[22] Simon Perdrix and Philippe Jorrand. Classically controlled quantum computation. *Mathematical Structures in Computer Science*, 16(4):601–620, 2006.

[23] Michael Saks. Randomization and derandomization in space-bounded computation. In *Proceedings of Computational Complexity (Formerly Structure in Complexity Theory)*, pages 128–149. IEEE, 1996.

[24] Michael Saks and Shiyu Zhou. Bphspace (s)/spl sube/dspace (s3/2). *Journal of computer and system sciences*, 58(2):376–403, 1999.

[25] Peter W Shor and Stephen P Jordan. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Information & Computation*, 8(8):681–714, 2008.

[26] Amnon Ta-Shma. Inverting well conditioned matrices in quantum logspace. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 881–890, 2013.

[27] Seinosuke Toda. Counting problems computationally equivalent to the determinant, 1991.

[28] Leslie G Valiant. Why is boolean complexity theory difficult. *Boolean Function Complexity*, 169:84–94, 1992.

[29] V Vinay. Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits. In *1991 Proceedings of the Sixth Annual Structure in Complexity Theory Conference*, pages 270–284. IEEE.

[30] John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999.

[31] John Watrous. Quantum simulations of classical random walks and undirected graph connectivity. *Journal of computer and system sciences*, 62(2):376–391, 2001.

[32] John Watrous. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12(1-2):48–84, 2003.

[33] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.