Space-Efficient Error Reduction for Unitary Quantum Computations*

Bill Fefferman[1], Hirotada Kobayashi[2], Cedric Yen-Yu Lin[3], Tomoyuki Morimae[4], and Harumichi Nishimura[5]

1 **Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, USA**
2 **Principles of Informatics Research Division, National Institute of Informatics, Tokyo, Japan**
3 **Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, USA**
4 **Advanced Scientific Research Leaders Development Unit, Gunma University, Kiryu, Gunma, Japan**
5 **Department of Computer Science and Mathematical Informatics, Graduate School of Information Science, Nagoya University, Nagoya, Aichi, Japan**

Abstract

This paper presents a general space-efficient method for error reduction for unitary quantum computation. Consider a polynomial-time quantum computation with completeness c and soundness s, either with or without a witness (corresponding to QMA and BQP, respectively). To convert this computation into a new computation with error at most 2^{-p}, the most space-efficient method known requires extra workspace of $O\left(p \log \frac{1}{c-s}\right)$ qubits. This space requirement is too large for scenarios like logarithmic-space quantum computations. This paper shows an error-reduction method for unitary quantum computations (i.e., computations without intermediate measurements) that requires extra workspace of just $O\left(\log \frac{p}{c-s}\right)$ qubits. This in particular gives the first method of strong amplification for logarithmic-space unitary quantum computations with two-sided bounded error. This also leads to a number of consequences in complexity theory, such as the uselessness of quantum witnesses in bounded-error logarithmic-space unitary quantum computations, the PSPACE upper bound for QMA with exponentially-small completeness-soundness gap, and strong amplification for matchgate computations.

1998 ACM Subject Classification F.1.2 Modes of Computation, F.1.3 Complexity Measures and Classes

Keywords and phrases space-bounded computation, quantum Merlin-Arthur proof systems, error reduction, quantum computing

Digital Object Identifier 10.4230/LIPIcs.ICALP.2016.14

1 Introduction

1.1 Background

A very basic topic in various models of quantum computation is whether computation error can be efficiently reduced within a given model. For polynomial-time bounded error quantum computation, the most standard model of quantum computation, the computation error can

* A full version [3] of this paper is available at arXiv.org e-Print archive, arXiv:1604.08192 [quant-ph].

43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016).
Editors: Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi;
Article No. 14; pp. 14:1–14:14

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

be made exponentially small via a simple repetition followed by a threshold-value decision. This justifies the choice of 2/3 and 1/3 for the completeness and soundness parameters in the definition of the corresponding complexity class BQP. This is also the case for quantum Merlin-Arthur (QMA) proof systems, another central model of quantum computation that models a quantum analogue of NP (more precisely, MA), and the resulting class QMA may again be defined with completeness and soundness parameters 2/3 and 1/3.

An undesirable feature of the simple repetition-based error reduction above is that the necessary workspace enlarges linearly with respect to the number of repetitions. More explicitly, for a given p, the number of repetitions necessary to achieve an error of 2^{-p} is $O\big(\frac{p}{(c-s)^2}\big)$, and thus both the workspace size and the witness size become $O\big(\frac{p}{(c-s)^2}\big)$ times larger. This implies that the simple repetition-based method is no longer useful when either the workspace size or the witness size is required to be logarithmically bounded.

Marriott and Watrous [13] developed a more sophisticated method of error reduction for QMA proof systems that does not increase the witness size at all. For a given p, their method still requires $O\big(\frac{p}{(c-s)^2}\big)$ calls of the original computation and its inverse to achieve the computation error 2^{-p}, but the method reuses both the workspace and the witness every time it calls the original computation and its inverse. Hence, the witness size never increases in their method. This is a strong property that allows them to show the uselessness of logarithmic-size quantum witnesses in QMA proof systems (i.e., $\mathrm{QMA}_{\log} = \mathrm{BQP}$, where $\mathrm{QMA}_{\log}$ is the class of problems having QMA proof systems with logarithmic-size quantum witnesses). Their method is also more efficient in workspace size than the simple repetition-based method, but still requires extra workspace of size $O\big(\frac{p}{(c-s)^2}\big)$, as it must record outcomes of all the calls of the original computation and its inverse.

Nagaj, Wocjan, and Zhang [15] succeeded in reducing to $O\big(\frac{p}{c-s}\big)$ the number of calls of the original computation and its inverse necessary to achieve the computation error 2^{-p} for a given p, while keeping the witness size unchanged. Their method makes use of the phase-estimation algorithm, an essential component of many quantum algorithms including the celebrated factoring algorithm. To achieve error 2^{-p} for a given p, their method must repeat $O(p)$ times the phase-estimation algorithm with precision of at least $O\big(\log \frac{1}{c-s}\big)$ bits and record all these estimated phases. Hence, this phase-estimation-based method uses extra workspace of size $O\big(p \log \frac{1}{c-s}\big)$.

As can be seen from above, both of the Marriott-Watrous method and the phase-estimation-based method are still insufficient for the case where the workspace size must be logarithmically bounded. No efficient error-reduction method is known that keeps the size of additionally necessary workspace logarithmically bounded. This is not limited to the case of QMA proof systems, and in fact almost no efficient error-reduction method is known even in the case of logarithmic-space quantum computations, and in the case of space-bounded quantum computations in general. The study of general space-bounded quantum computations was initiated by Watrous [21] based on quantum Turing machines. Several models of space-bounded quantum computations have been proposed and investigated since then in the literature [22, 23, 24, 9, 14, 18], some considering only logarithmic-space quantum computations and others treating general cases. It is not known whether any of these models are computationally equivalent. It is also not known whether error reduction is possible for logarithmic-space quantum computation defined according to any of these models, except the only known affirmative answer shown by Watrous [22] on computation of one-sided bounded error performed by logarithmic-space quantum Turing machines. As negative evidence in the case where computational resources are too limited, computation error cannot be reduced below a certain constant for one-way quantum finite state automata [1].

1.2 Main result and its consequences

This paper presents a general method of strong and space-efficient error reduction for *unitary* quantum computations. In particular, the method is applicable to logarithmic-space unitary quantum computations and logarithmic-space unitary QMA proof systems. All the results in this paper are model-independent and hold with any model of space-bounded quantum computations as long as it performs *unitary* quantum computations. The unitary model is not the most general in that it does not allow any intermediate measurements (notice that the standard technique of simulating intermediate measurements by unitary gates requires unallowably many ancilla qubits in the case of space-bounded computations), but is arguably one of the most reasonable models of space-bounded quantum computation.

Let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively. Let $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s)$ denote the class of problems having QMA proof systems with completeness c and soundness s, where the verifier performs a *unitary* quantum computation that has no time bound but is restricted to use $l_{\mathsf{V}}(n)$ private qubits and to receive a quantum witness of $l_{\mathsf{M}}(n)$ qubits on every input of length n. The main result of this paper is the following strong and space-efficient error-reduction for such QMA-type computations.

▶ **Theorem 1.1.** *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and for any functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c > s$, there exists a function $\delta \colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}](1 - 2^{-p}, 2^{-p}).$$

As will be found later, the proof is based on a reduction that is in space logarithmic and also in time polynomial with respect to $\frac{p}{c-s}$. Actually, the argument used in the reduction is remarkably simple. Nevertheless, the theorem is very powerful in that it fruitfully leads to many consequences that substantially deepen the understanding on the power of QMA proof systems and quantum computations in general, both in the space-bounded scenario and in the usual polynomial-time scenario. In what follows, a function $f \colon \mathbb{Z}^+ \to \mathbb{N}$ is *polynomially bounded* if f is polynomial-time computable and $f(n)$ is in $O(n^d)$ for some constant $d > 0$, and is *logarithmically bounded* if f is logarithmic-space computable and $f(n)$ is in $O(\log n)$.

Strong amplification for unitary BQL. The first consequence of Theorem 1.1 is a remarkably strong error-reducibility in logarithmic-space unitary quantum computations. Let $\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c, s)$ denote the class of problems solvable by logarithmic-space unitary quantum computations with completeness c and soundness s. The following amplifiability is immediate from Theorem 1.1 by taking a function p to be logarithmic-space computable and polynomially bounded, functions c and s to be logarithmic-space computable and to satisfy $c - s \geq 1/q$ for some polynomially bounded function $q \colon \mathbb{Z}^+ \to \mathbb{N}$, a function l_{V} to be logarithmically bounded, and a function $l_{\mathsf{M}} = 0$.

▶ **Corollary 1.2.** *For any polynomially bounded function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic-space computable and for any logarithmic-space computable functions $c, s \colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q \colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{Q}_{\mathbf{U}}\mathrm{L}(c, s) \subseteq \mathrm{Q}_{\mathbf{U}}\mathrm{L}(1 - 2^{-p}, 2^{-p}).$$

This in particular justifies defining the bounded-error class $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$ of logarithmic-space unitary quantum computations by $\mathrm{BQ}_{\mathbf{U}}\mathrm{L} = \mathrm{Q}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$, employing $2/3$ and $1/3$ for completeness and soundness parameters. Before this work, Watrous [22] showed a similar strong error-reducibility in the case of one-sided bounded error, and Corollary 1.2 extends this to the two-sided bounded error case.

Uselessness of quantum witnesses in logarithmic-space unitary QMA. Let $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s)$ denote the class of problems having logarithmic-space unitary QMA proof systems (i.e., such systems in which a verifier performs a logarithmic-space unitary computation upon receiving a logarithmic-size quantum witness) with completeness c and soundness s. Similarly to Corollary 1.2, the following amplifiability is immediate from Theorem 1.1 by taking a function p to be logarithmic-space computable and polynomially bounded, functions c and s to be logarithmic-space computable and to satisfy $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, and functions l_{V} and l_{M} to be logarithmically bounded.

▶ **Corollary 1.3.** *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic-space computable and for any logarithmic-space computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{L}(c,s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{L}(1-2^{-p}, 2^{-p}).$$

Again this justifies defining the bounded-error class $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ of logarithmic-space unitary QMA proof systems by $\mathrm{QMA}_{\mathbf{U}}\mathrm{L} = \mathrm{QMA}_{\mathbf{U}}\mathrm{L}(2/3, 1/3)$. By a standard technique of replacing a quantum witness by a totally mixed state as a self-prepared witness (to do this in a unitary computation, one can simply prepare sufficiently many EPR pairs and then take a qubit from each pair), Corollary 1.3 together with Corollary 1.2 further implies the equivalence of $\mathrm{QMA}_{\mathbf{U}}\mathrm{L}$ and $\mathrm{BQ}_{\mathbf{U}}\mathrm{L}$.

▶ **Corollary 1.4.** $\mathrm{QMA}_{\mathbf{U}}\mathrm{L} = \mathrm{BQ}_{\mathbf{U}}\mathrm{L}$.

As mentioned before, Marriott and Watrous [13] showed the equivalence $\mathrm{QMA}_{\log} = \mathrm{BQP}$, the uselessness of quantum witnesses of logarithmic size in the standard QMA proof systems with a polynomial-time verifier. In this respect, Corollary 1.4 states that quantum witnesses of logarithmic size do not increase the power of logarithmic-space unitary quantum computations at all, and indeed extends the result of Marriott and Watrous to logarithmic-space case.

Space-efficient amplification for QMA. Let $\mathrm{QMA}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$ be the time-efficient version of $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, i.e., the class of problems having standard polynomial-time QMA proof systems with completeness c and soundness s in which a polynomial-time unitary quantum verifier receives a quantum witness of $l_{\mathsf{M}}(n)$ qubits and uses workspace of $l_{\mathsf{V}}(n)$ qubits on every input of length n. As the reduction is in time polynomial with respect to $\frac{p}{c-s}$ in the proof of Theorem 1.1, the following amplifiability is immediate from Theorem 1.1 by taking functions p, l_{V}, and l_{M} to be polynomially bounded, and functions c and s to be polynomial-time computable and to satisfy $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$.

▶ **Corollary 1.5.** *For any polynomially bounded functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and for any polynomial-time computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with respect to $\frac{p}{c-s}$ such that*

$$\mathrm{QMA}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s) \subseteq \mathrm{QMA}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}](1-2^{-p}, 2^{-p}).$$

Recall that the Marriott-Watrous amplification [13] requires δ to be in $O\big(\frac{p}{(c-s)^2}\big)$ and the phase-estimation-based method by Nagaj, Wocjan, and Zhang [15] requires δ to be in $O\big(p \log \frac{1}{c-s}\big)$, instead of δ in $O\big(\log \frac{p}{c-s}\big)$ of Corollary 1.5. Hence, the method in this paper is most space-efficient among known error-reduction methods for standard QMA proof systems, and also among those for BQP.

Strong amplification for unitary QMAPSPACE. Let $\mathrm{Q_U PSPACE}(c,s)$ denote the class of problems solvable by polynomial-space unitary quantum computations with completeness c and soundness s, and let $\mathrm{QMA_U PSPACE}(c,s)$ denote the class of problems having polynomial-space unitary QMA proof systems (i.e., such systems in which a verifier performs a polynomial-space unitary computation upon receiving a polynomial-size quantum witness) with completeness c and soundness s. The following corollary states the scaled-up versions of Corollaries 1.2 and 1.3, and again is immediate from Theorem 1.1 by taking a function p to be polynomial-space computable and exponentially bounded, functions c and s to be polynomial-space computable and to satisfy $c - s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, and functions l_{V} and l_{M} to be polynomially bounded (or a function $l_{\mathsf{M}} = 0$ in the case of $\mathrm{Q_U PSPACE}(c,s)$).

▶ **Corollary 1.6.** *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and for any polynomial-space computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{Q_U PSPACE}(c,s) \subseteq \mathrm{Q_U PSPACE}\big(1 - 2^{-2^p}, 2^{-2^p}\big), \text{ and}$$
$$\mathrm{QMA_U PSPACE}(c,s) \subseteq \mathrm{QMA_U PSPACE}\big(1 - 2^{-2^p}, 2^{-2^p}\big).$$

Again by a standard technique of replacing a quantum witness by a totally mixed state as a self-prepared witness, the following corollary follows from Corollary 1.6 together with the fact that RevPSPACE = PrQPSPACE = PSPACE [2, 21], where RevPSPACE and PrQPSPACE are the complexity classes corresponding to deterministic polynomial-space reversible computations and unbounded-error polynomial-space quantum computations, respectively.

▶ **Corollary 1.7.** *For any polynomial-space computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QMA_U PSPACE}(c,s) = \mathrm{PSPACE}.$$

Now the PSPACE upper bound immediately follows for the class of problems having standard polynomial-time QMA proof systems with exponentially small completeness-soundness gap. More precisely, for the class $\mathrm{QMA}(c,s)$ of problems having standard polynomial-time QMA proof systems with completeness c and soundness s, the following corollary holds.

▶ **Corollary 1.8.** *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and for any polynomial-time computable functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c - s \geq 2^{-q}$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QMA}(c,s) \subseteq \mathrm{PSPACE}.$$

For QMA proof systems with exponentially small completeness-soundness gap, the PSPACE upper bound was known previously only for the one-sided-error case (following from the result in Ref. [7]), and only the EXP upper bound was known for the two-sided-error case (following from the result in Ref. [10]). Natarajan and Wu [16] independently proved a statement equivalent to Corollary 1.8. In fact, statements equivalent to Corollary 1.8 were also proved with different proofs independently by the first and third authors of the present paper in Ref. [4] (see Ref. [5] also) and by the complement subset of the present authors. The first and third authors of the present paper further proved in Refs. [4, 5] that the converse of Corollary 1.8 also holds, i.e., PSPACE is characterized by QMA proof systems with exponentially small completeness-soundness gap.

Strong amplification for matchgate computations. A matchgate is defined to be a two-qubit gate of the form $G(A, B)$ corresponding to the four-by-four unitary matrix in which the four corner elements form A and the four inner-square elements form B for matrices A and B in SU(2), and all the other elements are 0. A matchgate circuit is a quantum circuit such that: (i) the input state is a computational basis state, (ii) all the gates of the circuit are matchgates which are applied to two neighbor qubits, and (iii) the output is a final measurement in the computational basis on any single qubit. Matchgate computations were introduced and proved classically simulable by Valiant [20]. Terhal and DiVincenzo [19] related them to noninteracting-fermion quantum circuits. Let $\mathrm{MG}(c, s)$ denote the class of problems solvable by polynomial-time matchgate computations with completeness c and soundness s. Using the equivalence of polynomial-time matchgate computations and logarithmic-space unitary computations shown by Jozsa, Kraus, Miyake, and Watrous [9, Corollary 3.3], the following is immediate from Corollary 1.2.

▶ **Corollary 1.9.** *For any polynomially bounded function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic-space computable and for any logarithmic-space computable functions $c, s\colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c - s \geq 1/q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{MG}(c, s) \subseteq \mathrm{MG}(1 - 2^{-p}, 2^{-p}).$$

2 Overview of the proof of main theorem

We assume familiarity with basic quantum formalism (see Refs. [17, 11, 26], for instance). The main theorem can be proved with three different proofs. Due to space limitations, this version presents only one of the three proofs. The other two proofs, as well as precise definitions and technical proofs, are deferred to the full version [3].

Consider any unitary transformation V_x of the verifier on input x, and let p_{acc} be the maximum acceptance probability of it (and thus, $p_{\mathrm{acc}} \geq c(|x|)$ for yes instances, and $p_{\mathrm{acc}} \leq s(|x|)$ for no instances). Then the idea is to guess p_{acc} with *mild* precision $\delta = 2^{-l(|x|)}$, where $\frac{c-s}{2\sqrt{6q}} < 2^{-l} \leq \frac{c-s}{\sqrt{6q}}$ for some appropriately chosen function q and the (integer-valued) function l determined uniquely by given c, s, and q.

For each j in $\{1, \ldots, 2^{l(|x|)}\}$, let $r_j = j\delta$ be a possible guess of p_{acc}. Pick an integer k from $\{1, \ldots, 2^{l(|x|)}\}$ uniformly at random, and reject immediately if $r_k = k\delta < c(|x|)$ (so that no k can result in a good guess at p_{acc} for no instances). Otherwise r_k is used as a guess at p_{acc}. The point is that, for yes instances, there exists a choice of k such that $|r_k - p_{\mathrm{acc}}| < \delta \leq \frac{c(|x|)-s(|x|)}{\sqrt{6\,q(|x|)}}$, while for no instances, it holds that $|r_k - p_{\mathrm{acc}}| > c(|x|) - s(|x|)$ for any choice of k. Hence, by using the Reflection Procedure [12] combined with the additive adjustment of acceptance probability [8], the acceptance probability can be *mildly* amplified to at least $1 - \frac{(c(|x|)-s(|x|))^2}{6\,q(|x|)}$ in the yes-instance case, if the appropriate guess r_k is made. It is stressed that this mild amplification is the key for the efficiency in workspace. For no instances, the acceptance probability is at most $1 - \big(c(|x|) - s(|x|)\big)^2$ for any guess r_k.

Fix an index k of the guess r_k and let $V'_{x,k}$ be the unitary operator corresponding to the procedure constructed so far. Now repeat the following procedure $N(|x|)$ times for a function N defined by $N = \left\lceil \frac{q}{2(c-s)^2} \right\rceil$: One applies $V'_{x,k}$, and then increments a counter by 1 if the state corresponds to a rejection state of it. One further applies $(V'_{x,k})^\dagger$, and then increments a counter by 1 if any of the work qubits of $V'_{x,k}$ is in state $|1\rangle$. After the repetition, one accepts if and only if the counter value remains 0. In short, these repetitions essentially take the AND of the $N(|x|)$ attempts of $V'_{x,k}$ (with each initialization try by $(V'_{x,k})^\dagger$). The rigorous analysis shows that the initialization steps also contribute to taking AND, and this process is exactly

Additive Adjustment Procedure associated with (U, Δ, Π, l, k)

1. Prepare a single-qubit register B and an l-qubit register R, where all the qubits in B and R are initialized to state $|0\rangle$. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. Apply the Hadamard transformation H to each qubit in (B, R), and apply U to Q.
3. Accept either if B contains 0 *and* the state in Q belongs to the subspace corresponding to Π or if B contains 1 *and* the content of R is greater than k (when viewed as an integer in $\{1, \ldots, 2^l\}$), and reject otherwise.

Figure 1 The Additive Adjustment Procedure.

equivalent to taking the AND of $2\,N(|x|)$ attempts of $V'_{x,k}$. The acceptance probability is at least $\frac{1}{2}$ for yes instances when the appropriate guess r_k at p_{acc} is made, while it is at most $e^{-\,q(|x|)} < 2^{-\,q(|x|)}$ for any guess r_k for no instances. Taking into account that the index k of r_k is chosen uniformly at random, this results in a unitary procedure V''_x with acceptance probability at least $2^{-\,l(|x|)} \cdot \frac{1}{2} > \frac{c(|x|)-s(|x|)}{4\sqrt{6\,q(|x|)}}$ for yes instances and at most $2^{-\,q(|x|)}$ for no instances.

Finally, by using a repetition similar to above based on V''_x that takes OR instead of AND, it is clear that the completeness acceptance probability becomes exponentially close to 1 with respect to q, while the soundness acceptance probability is still exponentially small with respect to q. To achieve error below 2^{-p} for a target p, one chooses q to be slightly larger than p when constructing V''_x (more precisely, one can choose a function $q = \lceil 2\big(p + \log \frac{6p}{c-s} + 1\big)\rceil$).

3 Basic procedures

Let $\Sigma = \{0, 1\}$ denote the binary alphabet set. For every positive integer n, let $\mathbb{C}(\Sigma^n)$ denote the 2^n-dimensional complex Hilbert space whose standard basis vectors are indexed by the elements in Σ^n. In this paper, all Hilbert spaces are complex and of dimension a power of two. A quantum register is a set of single or multiple qubits. For a quantum register R, let I_{R} denote the identity operator over the Hilbert space associated with R.

Let $\mathcal{H}$ be any Hilbert space of dimension a power of two. Given a unitary transformation U and two projections Δ and Π, all acting over $\mathcal{H}$, define the Hermitian operator M over $\mathcal{H}$ by

$$M = \Delta U^\dagger \Pi U \Delta,$$

which plays crucial roles in many well-known amplification methods in quantum computation, including the Grover search [6], the Marriott-Watrous amplification for QMA [13], and quantum rewinding for zero-knowledge proofs against quantum attacks [25].

Additive Adjustment Procedure. Consider the procedure described in Figure 1, called the Additive Adjustment Procedure, which uses the additive adjustment technique of acceptance probability proposed in Ref. [8].

The following properties hold with the Additive Adjustment Procedure.

▶ **Proposition 3.1.** *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. For any positive integer l and any integer k in $\{1, \ldots, 2^l\}$, the following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* Additive Adjustment Procedure *associated with (U, Δ, Π, l, k) results in acceptance with probability $\frac{1}{2} + \frac{1}{2}\big(\lambda - \frac{k}{2^l}\big)$ when $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

Reflection Procedure associated with (U, Δ, Π)

1. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. Apply U to Q.
3. Perform a phase-flip (i.e., multiply the phase by -1) if the state in Q belongs to the subspace corresponding to the projection Π. That is, apply the unitary transformation $I_{\mathsf{Q}} - 2\Pi$ to Q.
4. Apply $U^\dagger$ to Q.
5. Reject if the state in Q belongs to the subspace corresponding to Δ, and accept otherwise.

Figure 2 The Reflection Procedure.

(Soundness) *Suppose that all the eigenvalues of M are at most ε for some ε in $[0,1)$. Then, the* Additive Adjustment Procedure *associated with (U, Δ, Π, l, k) results in acceptance with probability at most $\frac{1}{2} + \frac{1}{2}\left(\varepsilon - \frac{k}{2^l}\right)$ regardless of the quantum state received in register Q in Step 1.*

Reflection Procedure. Now consider the procedure described in Figure 2, which is exactly the Reflection Procedure in a general form originally developed in Ref. [12].

The following proposition holds with the Reflection Procedure.

▶ **Proposition 3.2** ([12])**.** *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* Reflection Procedure *associated with (U, Δ, Π) results in acceptance with probability $4\lambda(1-\lambda)$ when $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that none of the eigenvalues of M is in the interval $\left(\frac{1}{2} - \varepsilon, \frac{1}{2} + \varepsilon\right)$ for some ε in $\left(0, \frac{1}{2}\right]$. Then, the* Reflection Procedure *associated with (U, Δ, Π) results in acceptance with probability at most $1 - 4\varepsilon^2$ regardless of the quantum state received in register Q in Step 1.*

AND-Type and OR-Type Repetition Procedures. Given a unitary transformation U and two projections Δ and Π all acting over a Hilbert space, consider the process of applying U to a fixed initial state $|\phi\rangle$ in a quantum register Q that is in the subspace corresponding to Δ and then accepting if and only if the resulting state is projected onto the subspace corresponding to Π by the projective measurement $\{\Pi, I_{\mathsf{Q}} - \Pi\}$. Let p denote the acceptance probability of this process. By running N independent attempts of such a process, the probability clearly becomes p^N for the event that all the attempts result in acceptance, but which requires N copies of the initial state $|\phi\rangle$. When $|\phi\rangle$ is an eigenstate of the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$, the AND-Type Repetition Procedure described in Figure 3 essentially simulates such independent attempts with just one copy of $|\phi\rangle$.

The following proposition holds with the AND-Type Repetition Procedure.

▶ **Proposition 3.3.** *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let N be a positive integer. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

AND-Type Repetition Procedure associated with (U, Δ, Π, N)

1. Let $l = \lceil \log(2N+1) \rceil$, and prepare an l-qubit register C, where all the qubits in C are initialized to state $|0\rangle$. Receive a quantum register Q that contains a state in the subspace corresponding to the projection Δ.
2. For $j = 1$ to N, perform the following:
   - 2.1. Apply U to Q.
   - 2.2. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Pi$, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C, where $U_{+1}(\mathbb{Z}_{2^l})$ is the unitary transformation defined by
   $$U_{+1}(\mathbb{Z}_{2^l}) \colon |j\rangle \mapsto \left|(j+1) \bmod 2^l\right\rangle, \quad \forall j \in \mathbb{Z}_{2^l}.$$
   - 2.3. Apply $U^\dagger$ to Q.
   - 2.4. If the state in Q belongs to the subspace corresponding to the projection $I_{\mathsf{Q}} - \Delta$, apply $U_{+1}(\mathbb{Z}_{2^l})$ to C.
3. Accept if the content of C is 0 (i.e., all the qubits in C are in state $|0\rangle$), and reject otherwise.

Figure 3 The AND-Type Repetition Procedure.

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* AND-Type Repetition Procedure *associated with (U, Δ, Π, N) results in acceptance with probability λ^{2N} when $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that all the eigenvalues of M are at most ε for some ε in $[0, 1)$. Then, the* AND-Type Repetition Procedure *associated with (U, Δ, Π, N) results in acceptance with probability at most ε^{2N} regardless of the quantum state received in register Q in Step 1.*

One can also construct a procedure that essentially simulates the process of taking OR of the N independent attempts mentioned before with just one copy of $|\phi\rangle$. One now applies $U_{+1}(\mathbb{Z}_{2^l})$ to C when the state in Q belongs to the subspace corresponding to the projection Π at Step 2.2, and *rejects* if and only if the content of C is 0 at Step 3. The resulting procedure is called the OR-Type Repetition Procedure, which has the following properties.

▶ **Proposition 3.4.** *Let U be a unitary transformation and Δ and Π be projections, all acting over the same Hilbert space, and let N be a positive integer. Consider the Hermitian operator $M = \Delta U^\dagger \Pi U \Delta$. The following two properties hold:*

(Completeness) *Suppose that M has an eigenstate $|\phi_\lambda\rangle$ with its associated eigenvalue λ. Then, the* OR-Type Repetition Procedure *associated with (U, Δ, Π, N) results in acceptance with probability $1 - (1-\lambda)^{2N}$ when $|\phi_\lambda\rangle$ is received in register Q in Step 1.*

(Soundness) *Suppose that all the eigenvalues of M are at most ε for some ε in $[0, 1)$. Then, the* OR-Type Repetition Procedure *associated with (U, Δ, Π, N) results in acceptance with probability at most $1 - (1-\varepsilon)^{2N}$ regardless of the quantum state received in register Q in Step 1.*

4 Guess-based amplification framework

Consider any QMA-type computation for a problem $A = (A_{\text{yes}}, A_{\text{no}})$ induced by a family $\{V_x\}_{x \in \Sigma^*}$ of a unitary transformation V_x of the verifier on input x in Σ^* that acts over a quantum register $\mathsf{Q} = (\mathsf{V}, \mathsf{M})$, where V is the quantum register consisting of all the private qubits of the verifier, and M is the one for storing a received quantum witness. Let Π_{init} be the projection onto the subspace spanned by the legal initial states of the QMA-type

Mild Completeness Amplification with Guess k associated with (V_x, p)

Define functions l and C by $l = \left\lceil \frac{1}{2} \log \frac{p}{(c-s)^2} \right\rceil$ and $C = \lceil 2^l c \rceil$. Let Π_{init} and Π_{acc} be the projections onto the subspaces spanned by the legal initial states and the accepting states, respectively, in the verification with V_x. Given an integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess, consider the Additive Adjustment Procedure associated with $(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}}, l(|x|), k)$. Let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\text{acc},k}$ be the projection onto the subspace spanned by the accepting states of it.
Reject if $k < C(|x|)$, and continue otherwise by performing the Reflection Procedure associated with $\left(V'_{x,k}, \Pi'_{\text{init}}, \Pi'_{\text{acc},k}\right)$.

Figure 4 The Mild Completeness Amplification with Guess k.

computation induced by V_x (i.e., the subspace spanned by those in which all the qubits in V is in state $|0\rangle$) and let Π_{acc} be the projection onto the subspace spanned by the accepting states of the QMA-type computation associated with V_x (i.e., the subspace spanned by states for which the designated output qubit of V_x is in state $|0\rangle$).

The maximum eigenvalue of the Hermitian operator $M_x = \Pi_{\text{init}} V_x^\dagger \Pi_{\text{acc}} V_x \Pi_{\text{init}}$ exactly corresponds to the maximum acceptance probability of the verifier on input x over all possible quantum witnesses received in M. Hence, M_x has an eigenvalue at least $c(|x|)$ if x is in A_{yes}, while all eigenvalues of M_x are at most $s(|x|)$ if x is in A_{no}, where $c, s \colon \mathbb{Z}^+ \to [0,1]$ are functions that provide completeness and soundness conditions of the QMA-type computation induced by $\{V_x\}_{x \in \Sigma^*}$, respectively.

Mild completeness amplification with a guess. Fix arbitrarily a function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $l, C \colon \mathbb{Z}^+ \to \mathbb{N}$ be functions defined by $l = \left\lceil \frac{1}{2} \log \frac{p}{(c-s)^2} \right\rceil$ and $C = \lceil 2^l c \rceil$. Fix an input x and an integer k in $\{1, \ldots, 2^{l(|x|)}\}$. Given the triplet $(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}})$ and an integer k, one first constructs the Additive Adjustment Procedure associated with $\left(V_x, \Pi_{\text{init}}, \Pi_{\text{acc}}, l(|x|), k\right)$, if k is at least $C(|x|)$ (and automatically rejects otherwise so that no k can result in a good guess at the acceptance probability when the actual value of it is unallowably small). Let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\text{acc},k}$ be the projection onto the subspace spanned by the accepting states of it. Next, from the triplet $\left(V'_{x,k}, \Pi'_{\text{init}}, \Pi'_{\text{acc},k}\right)$, one constructs the Reflection Procedure associated with $\left(V'_{x,k}, \Pi'_{\text{init}}, \Pi'_{\text{acc},k}\right)$, and performs it. The resulting procedure is called the Mild Completeness Amplification with Guess k, and is summarized in Figure 4.

From the properties of the Additive Adjustment Procedure and the Reflection Procedure (Propositions 3.1 and 3.2), one can show the following lemma.

▶ **Lemma 4.1.** *Given functions $l_{\mathsf{V}}, l_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Then, for any function $p \colon \mathbb{Z}^+ \to \mathbb{N}$ and for every x in Σ^*, letting $l = \left\lceil \frac{1}{2} \log \frac{p}{(c-s)^2} \right\rceil$,*

(Completeness) *if x is in A_{yes}, there exists an integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess such that the Mild Completeness Amplification with Guess k associated with (V_x, p) results in acceptance with probability at least $1 - \frac{(c(|x|) - s(|x|))^2}{p(|x|)}$, and*

(Soundness) *if x is in A_{no}, for any integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess, the Mild Completeness Amplification with Guess k associated with (V_x, p) results in acceptance with probability at most $1 - \left(c(|x|) - s(|x|)\right)^2$.*

Soundness Error Reduction with Guess k associated with (V_x, p)

Define functions l and N by $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$ and $N = \left\lceil \frac{p}{2(c-s)^2} \right\rceil$. Given an integer k in $\{1, \ldots, 2^{l(|x|)}\}$, consider the Mild Completeness Amplification with Guess k associated with $(V_x, 6p)$. Let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\text{acc},k}$ be the projection onto the subspace spanned by the accepting states of it.
Perform the AND-Type Repetition Procedure associated with $\left(V'_{x,k}, \Pi'_{\text{init}}, \Pi'_{\text{acc},k}, N(|x|)\right)$.

Figure 5 The Soundness Error Reduction with Guess k.

Soundness error reduction with a guess. Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $l, N\colon \mathbb{Z}^+ \to \mathbb{N}$ be functions defined by $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$ and $N = \left\lceil \frac{p}{2(c-s)^2} \right\rceil$. Fix an input x and an integer k in $\{1, \ldots, 2^{l(|x|)}\}$. Given the pair (V_x, p) and the integer k, consider the Mild Completeness Amplification with Guess k associated with $(V_x, 6p)$. As before, let $V'_{x,k}$ be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let $\Pi'_{\text{acc},k}$ be the projection onto the subspace spanned by the accepting states of it. From the triplet $\left(V'_{x,k}, \Pi'_{\text{init}}, \Pi'_{\text{acc},k}\right)$ and a positive integer $N(|x|)$, one constructs the AND-Type Repetition Procedure associated with $\left(V'_{x,k}, \Pi'_{\text{init}}, \Pi'_{\text{acc},k}, N(|x|)\right)$, and performs it. The resulting procedure is called the Soundness Error Reduction with Guess k, and is summarized in Figure 5.

From the properties of the AND-Type Repetition Procedure and the Mild Completeness Amplification with Guess k (Proposition 3.3 and Lemma 4.1), one can show the following lemma.

▶ **Lemma 4.2.** *Given functions $l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in $\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c,s)$, and let $V = \{V_x\}_{x \in \Sigma^*}$ be the $(l_{\mathsf{V}}, l_{\mathsf{M}})$-space-bounded quantum verifier witnessing this membership. Then, for any function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and for every x in Σ^*, letting $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$,*

(Completeness) *if x is in A_{yes}, there exists an integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess such that the Soundness Error Reduction with Guess k associated with (V_x, p) results in acceptance with probability at least $\frac{1}{2}$, and*

(Soundness) *if x is in A_{no}, for any integer k in $\{1, \ldots, 2^{l(|x|)}\}$ as a guess, the Soundness Error Reduction with Guess k associated with (V_x, p) results in acceptance with probability at most $2^{-p(|x|)}$.*

Soundness error reduction with a random guess. Again fix arbitrarily a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be a function defined by $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$. Fix an input x. Given the pair (V_x, p), consider choosing an integer k from $\{1, \ldots, 2^{l(|x|)}\}$ uniformly at random, and performing the Soundness Error Reduction with Guess k associated with (V_x, p). The resulting procedure is called the Soundness Error Reduction with Random Guess and is summarized in Figure 6.

Lemma 4.3 below follows from the Soundness Error Reduction with Random Guess together with the properties of the Soundness Error Reduction with Guess k stated in Lemma 4.2.

▶ **Lemma 4.3.** *For any functions $p, l_{\mathsf{V}}, l_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any functions $c, s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$ and $\frac{c-s}{4\sqrt{6p}} > 2^{-p}$, there exists a function $\delta\colon \mathbb{Z}^+ \to \mathbb{N}$ that is logarithmic with*

Soundness Error Reduction with Random Guess associated with (V_x, p)

Define a function l by $l = \left\lceil \frac{1}{2} \log \frac{6p}{(c-s)^2} \right\rceil$.
Pick an integer k from $\{1, \ldots, 2^{l(|x|)}\}$ uniformly at random and perform the Soundness Error Reduction with Guess k associated with (V_x, p).

Figure 6 The Soundness Error Reduction with Random Guess.

Space-Efficient Amplification Based on Random Guess associated with (V_x, p)

Define functions q and N by $q = \left\lceil 2\left(p + \log \frac{6p}{c-s} + 1\right) \right\rceil$ and $N = \left\lceil \frac{2\sqrt{6q}}{c-s} \cdot p \right\rceil$. Consider the Soundness Error Reduction with Random Guess associated with (V_x, q). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it.
Perform the OR-Type Repetition Procedure associated with $\left(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\right)$.

Figure 7 The Space-Efficient Amplification Based on Random Guess.

respect to $\frac{p}{c-s}$ *such that*

$$\mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}}, l_{\mathsf{M}}](c, s) \subseteq \mathrm{QMA}_{\mathbf{U}}\mathrm{SPACE}[l_{\mathsf{V}} + \delta, l_{\mathsf{M}}]\left(\frac{c-s}{4\sqrt{6p}}, 2^{-p}\right).$$

Space-efficient amplification based on a random guess. Again fix a function $p\colon \mathbb{Z}^+ \to \mathbb{N}$ and functions $c, s\colon \mathbb{Z}^+ \to [0, 1]$ satisfying $c > s$ arbitrarily. Let $q, N\colon \mathbb{Z}^+ \to \mathbb{N}$ be functions defined by $q = \left\lceil 2\left(p + \log \frac{6p}{c-s} + 1\right) \right\rceil$ and $N = \left\lceil \frac{2\sqrt{6q}}{c-s} \cdot p \right\rceil$. Fix an input x. Given the pair (V_x, p), consider the Soundness Error Reduction with Random Guess associated with (V_x, q). Let V'_x be the unitary transformation induced by it, let Π'_{init} be the projection onto the subspace spanned by the legal initial states of it, and let Π'_{acc} be the projection onto the subspace spanned by the accepting states of it. From the triplet $\left(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}\right)$ and a positive integer $N(|x|)$, one constructs the OR-Type Repetition Procedure associated with $\left(V'_x, \Pi'_{\text{init}}, \Pi'_{\text{acc}}, N(|x|)\right)$, and performs it. The resulting procedure is called the Space-Efficient Amplification Based on Random Guess and is summarized in Figure 7.

Now Theorem 1.1, the main theorem of this paper, is proved by using the Space-Efficient Amplification Based on Random Guess combined with the properties of the Soundness Error Reduction with Random Guess and the OR-Type Repetition Procedure stated in Lemma 4.3 and Proposition 3.4, respectively.

Acknowledgements. BF and CYL are supported by the Department of Defense. HK and HN are supported by the Grant-in-Aid for Scientific Research (A) Nos. 24240001 and 16H01705 of the Japan Society for the Promotion of Science. TM is supported by the Program to Disseminate Tenure Tracking System of the Ministry of Education, Culture, Sports, Science and Technology in Japan, the Grant-in-Aid for Scientific Research on Innovative Areas No. 15H00850 of the Ministry of Education, Culture, Sports, Science and Technology in Japan, and the Grant-in-Aid for Young Scientists (B) No. 26730003 of the Japan Society for the Promotion of Science. HN is also supported by the Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the Ministry of Education, Culture, Sports, Science and Technology in Japan, which HK is also grateful to. HN further acknowledges support from the Grant-in-Aid for Scientific Research (C) No. 25330012 of the Japan Society for the Promotion of Science.

References

1 Andris Ambainis and Rūsiņš Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *39th Annual Symposium on Foundations of Computer Science*, pages 332–341, 1998. doi:10.1109/SFCS.1998.743469.

2 Charles H. Bennett. Time/space trade-offs for reversible computation. *SIAM Journal on Computing*, 18(4):766–776, 1989. doi:10.1137/0218053.

3 Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, and Harumichi Nishimura. Space-efficient error reduction for unitary quantum computations. arXiv.org e-Print archive, arXiv:1604.08192 [quant-ph], 2016. arXiv:1604.08192.

4 Bill Fefferman and Cedric Lin. Quantum Merlin Arthur with exponentially small gap. arXiv.org e-Print archive, arXiv:1601.01975 [quant-ph], 2016. arXiv:1601.01975.

5 Bill Fefferman and Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. arXiv.org e-Print archive, arXiv:1604.01384 [quant-ph], 2016. arXiv:1604.01384.

6 Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, 1996. doi:10.1145/237814.237866.

7 Tsuyoshi Ito, Hirotada Kobayashi, and John Watrous. Quantum interactive proofs with weak error bounds. In *ITCS'12, Proceedings of the 2012 ACM Conference on Innovations in Theoretical Computer Science*, pages 266–275, 2012. doi:10.1145/2090236.2090259.

8 Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):0461–0471, 2012.

9 Richard Jozsa, Barbara Kraus, Akimasa Miyake, and John Watrous. Matchgate and space-bounded quantum computations are equivalent. *Proceedings of the Royal Society A*, 466(2115):809–830, 2010. doi:10.1098/rspa.2009.0433.

10 Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000. doi:10.1145/335305.335387.

11 Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002. doi:10.1090/gsm/047.

12 Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. *SIAM Journal on Computing*, 44(2):243–289, 2015. doi:10.1137/140971944.

13 Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. doi:10.1007/s00037-005-0194-x.

14 Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory of Computing*, 8:1–51 (Article 1), 2012. doi:10.4086/toc.2012.v008a001.

15 Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information and Computation*, 9(11–12):1053–1068, 2009.

16 Anand Natarajan and Xiaodi Wu. Private communication, January 2016.

17 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

18 Amnon Ta-Shma. Inverting well conditioned matrices in quantum logspace. In *STOC'13, Proceedings of the 2013 ACM Symposium on Theory of Computing*, pages 881–890, 2013. doi:10.1145/2488608.2488720.

19 Barbara M. Terhal and David P. DiVincenzo. Classical simulation of noninteracting-fermion quantum circuits. *Physical Review A*, 65:article 032325, 2002. doi:10.1103/PhysRevA.65.032325.

20 Leslie G. Valiant. Quantum circuits that can be simulated classically in polynomial time. *SIAM Journal on Computing*, 31(4):1229–1254, 2002. doi:10.1137/S0097539700377025.

21 John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999. doi:10.1006/jcss.1999.1655.

22 John Watrous. Quantum simulations of classical random walks and undirected graph connectivity. *Journal of Computer and System Sciences*, 62(2):376–391, 2001. doi:10.1006/jcss.2000.1732.

23 John Watrous. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12(1–2):48–84, 2003. doi:10.1007/s00037-003-0177-8.

24 John Watrous. Quantum computational complexity. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer New York, 2009. doi:10.1007/978-0-387-30440-3_428.

25 John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. doi:10.1137/060670997.

26 Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. doi:10.1017/CBO9781139525343.