StoqMA Meets Distribution Testing

Yupan Liu
Shenzhen, China

Abstract

StoqMA captures the computational hardness of approximating the ground energy of local Hamiltonians that do not suffer the so-called sign problem. We provide a novel connection between StoqMA and distribution testing via reversible circuits. First, we prove that easy-witness StoqMA (viz. eStoqMA, a sub-class of StoqMA) is contained in MA. Easy witness is a generalization of a subset state such that the associated set's membership can be efficiently verifiable, and all non-zero coordinates are not necessarily uniform. This sub-class eStoqMA contains StoqMA with perfect completeness (StoqMA_1), which further signifies a simplified proof for $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$ [9, 12]. Second, by showing distinguishing reversible circuits with ancillary random bits is StoqMA-complete (as a comparison, distinguishing quantum circuits is QMA-complete [26]), we construct soundness error reduction of StoqMA. Additionally, we show that both variants of StoqMA that without any ancillary random bit and with perfect soundness are contained in NP. Our results make a step towards collapsing the hierarchy $\mathsf{MA} \subseteq \mathsf{StoqMA} \subseteq \mathsf{SBP}$ [9], in which all classes are contained in AM and collapse to NP under derandomization assumptions.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases StoqMA, distribution testing, error reduction, reversible circuits

Digital Object Identifier 10.4230/LIPIcs.TQC.2021.4

Related Version *Full Version*: https://arxiv.org/abs/2011.05733

Funding The author was supported by ISF Grant No. 1721/17 when he was affiliated with the Hebrew University of Jerusalem.

Acknowledgements The author thanks Alex B. Grilo for his contribution during the early stage of Section 4.1, and the proof of Proposition 19. The author also thanks anonymous reviewers for pointing out an error in the proof of Proposition 16 and valuable suggestions. Additionally, the author thanks Tomoyuki Morimae and Dorit Aharonov for helpful discussion. Circuit diagrams were drawn by the Quantikz package [28].

1 Introduction

This tale originates from Arthur-Merlin protocols, such as complexity classes MA and AM, introduced by Babai [5]. MA is a randomized generalization of the complexity class NP, namely the verifier could take advantage of the randomness. AM is additionally allowing two-message interaction. Surprisingly, two-message Arthur-Merlin protocols are as powerful as such protocols with a constant-message interaction, whereas it is a long-standing open problem whether MA = AM. It is evident that $\mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{AM}$. Moreover, under well-believed derandomization assumptions [31, 32], these classes collapse all the way to NP. Despite limited progresses on proving MA = AM, is there any intermediate class between MA and AM?

StoqMA is a natural class between MA and AM, initially introduced by Bravyi, Bessen, Terhal [9]. StoqMA captures the computational hardness of the stoquastic local Hamiltonian problems. The local Hamiltonian problem, defined by Kitaev [29], is substantially approximating the minimum eigenvalue (a.k.a. ground energy) of a sparse exponential-size matrix (a.k.a. local Hamiltonian) within inverse-polynomial accuracy. Stoquastic Hamiltonians [10] are a family of Hamiltonians that do not suffer the sign problem, namely all off-diagonal

16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021).
Editor: Min-Hsiu Hsieh; Article No. 4; pp. 4:1–4:22
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

entries in the Hamiltonian are non-positive. StoqMA also plays a crucial role in the Hamiltonian complexity – StoqMA-complete is a level in the complexity classification of 2-local Hamiltonian problems on qubits [17, 11], along with P, NP-complete, and QMA-complete.

Inspiring by the Monte-Carlo simulation in physics, Bravyi and Terhal [9, 12] propose a MA protocol for the stoquastic frustration-free local Hamiltonian problem, which further signifies StoqMA with perfect completeness (StoqMA_1) is contained in MA. A uniformly restricted variant[1] of this problem, which is also referred to as SetCSP [3][2], essentially captures the MA-hardness.

To characterize StoqMA through the distribution testing lens, we begin with an informal definition of StoqMA and leave the details in Section 2.2. For a language $\mathcal{L}$ in StoqMA, there exists a verifier V_x that takes $x \in \mathcal{L}$ as an input, where the verifier's computation is given by a classical reversible circuit, viewed as a quantum circuit. Besides a non-negative state[3] in the verifier's input as a witness, to utilize the randomness, ancillary qubits in the verifier's input consist of not only state $|0\rangle$ but also $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$. After applying the circuit, the designated output qubit is measured in the Hadamard basis[4]. A problem is in $\mathsf{StoqMA}(a, b)$ for some $a > b \geq 1/2$, if for *yes* instances, there is a witness making the verifier accept with probability at least a; whereas for *no* instances, all witness make the verifier accepts with probability at most b. The gap between a and b is at least an inverse polynomial since error reduction for StoqMA is unknown.

The optimality of *non-negative* witnesses suggests a novel connection to *distribution testing*. Let $|0\rangle |D_0\rangle + |1\rangle |D_1\rangle$ be the state before the final measurement, where $|D_k\rangle = \sum_{i \in \{0,1\}^{n-1}} \sqrt{D_k(i)}\, |i\rangle$ for $k = 0, 1$ and n is the number of qubits utilized by the verifier. A straightforward calculation indicates that the acceptance probability of a StoqMA verifier is linearly dependent on the *squared Hellinger distance* $d_H^2(D_0, D_1)$ between D_0 and D_1, which indeed connects to distribution testing! Consequently, to prove $\mathsf{StoqMA} \subseteq \mathsf{MA}$, it suffices to approximate $d_H^2(D_0, D_1)$ within an inverse-polynomial accuracy using merely polynomially many samples[5].

1.1 Main results

StoqMA with easy witness (eStoqMA). With this connection to distribution testing, it is essential to take advantage of the *efficient query access* of a non-negative witness where a witness satisfied with this condition is the so-called *easy witness*. For this sub-class of StoqMA (viz. eStoqMA) such that there exists an easy witness for any *yes* instances, we are then able to show an MA containment by utilizing both query and sample accesses to the witness. Informally, easy witness is a generalization of a subset state such that the associated state's membership is efficiently verifiable, and all non-zero coordinates are unnecessarily uniform. It is evident that a classical witness is also an easy witness, but the opposite is not necessarily true (See Remark 17). Now let us state our first main theorem:

---

[1] It is the projection uniform stoquastic local Hamiltonian problem, namely each local term in Hamiltonian is exactly a projection. See Definition 2.10 in [4].

[2] Namely, a modified constraint satisfaction problem such that both constraints and satisfying assignments are a subset.

[3] A witness here could be any quantum state, but the optimal witness is a non-negative state, see Remark 10.

[4] It is worthwhile to mention that we can define MA [10] (see Definition 7) in the same fashion, namely replacing the measurement on the output qubit by the computational basis.

[5] Each sample is actually the measurement outcome after running an independent copy of the verifier, see Remark 12.

▶ **Theorem 1** (Informal of Theorem 15). eStoqMA = MA*.*

It is worthwhile to mention that easy witness also relates to SBP (Small Bounded-error Probability) [7]. In particular, Goldwasser and Sipser [22] propose the celebrated Set Lower Bound protocol – it is an AM protocol for the problem of approximately counting the cardinality of such an efficient verifiable set. Recently, Watson [42] and Volkovich [40] separately point out that such a problem is essentially SBP-complete.

Although eStoqMA seems only a sub-class of StoqMA, we could provide an arguably simplified proof for $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$ [9]. Namely, employed the local verifiability of SetCSP [3], it is evident to show eStoqMA contains StoqMA with perfect completeness, which infers $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$. However, it remains open whether all StoqMA verifier has easy witness, whereas an analogous statement is false for classical witnesses (see Proposition 27).

Reversible Circuit Distinguishability is StoqMA-complete. It is well-known that distinguishing quantum circuits (a.k.a. the Non-Identity Check problem), namely given two efficient quantum circuits and decide whether there exists a pure state that distinguishes one from the other, is QMA-complete [26]. Moreover, if we restrict these circuits to be reversible (with the same number of ancillary bits), this variant is NP-complete [27]. What happens if we also allow *ancillary random bits*, viewed as quantum circuits with ancillary qubits which is initially state $|+\rangle$? It seems reasonable to believe this variant is MA-complete; however, it is actually StoqMA-complete, as stated in Theorem 2:

▶ **Theorem 2** (Informal of Theorem 22). *Distinguishing reversible circuits with ancillary random bits within an inverse-polynomial accuracy is* StoqMA*-complete.*

In fact, Theorem 2 is a consequence of the distribution testing explanation of a StoqMA verifier's maximum acceptance probability. We can view Theorem 2 as new strong evidence of StoqMA = MA. It further straightforwardly inspires a simplified proof of [27]:

▶ **Proposition 3** (Informal of Proposition 28). *Distinguishing reversible circuits without ancillary random bits is* NP*-complete.*

Apart from the role of randomness, Proposition 4 is analogous for StoqMA regarding the well-known derandomization property [21] of Arthur-Merlin systems with *perfect soundness*:

▶ **Proposition 4** (Informal of Proposition 23). StoqMA *with perfect soundness is in* NP*.*

Notably, the NP-containment in Proposition 4 holds even for $\mathsf{StoqMA}(a, b)$ verifiers with arbitrarily small gap $a - b$. It is arguably surprising since $\mathsf{StoqMA}(a, b)$ with an exponentially small gap (i.e., the precise variant) at least contains $\mathsf{NP}^{\mathsf{PP}}$ [33], but such a phenomenon does not appear in this scenario.

Soundness error reduction of StoqMA. Error reduction is a rudimentary property of many complexity classes, such as P, BPP, MA, QMA, etc. . It is peculiar that such property of StoqMA is open, even though this class has been proposed since 2006 [9]. An obstacle follows from the limitation of performing a single-qubit Hadamard basis final measurement, so we cannot directly take *the majority vote* of outcomes from the verifier's parallel repetition. Utilized the gadget in the proof of Theorem 2, we have derived soundness error reduction of StoqMA, which means we could take *the conjunction* of verifier's parallel repetition's outcomes:

▶ **Theorem 5** (Soundness error reduction of StoqMA). *For any polynomial* $r = \mathrm{poly}(n)$*,*

$$\mathsf{StoqMA}\left(\frac{1}{2}+\frac{a}{2}, \frac{1}{2}+\frac{b}{2}\right) \subseteq \mathsf{StoqMA}\left(\frac{1}{2}+\frac{a^r}{2}, \frac{1}{2}+\frac{b^r}{2}\right).$$

1.2 Discussion and open problems

Towards SBP = MA. As stated before, it is known MA ⊆ StoqMA ⊆ SBP ⊆ AM [7, 9]. Note a subset state associated with an efficient membership-verifiable set is an easy witness. Could we utilize this connection and deduce proof of SBP ⊆ eStoqMA?

Owing to the wide uses of the Set Lower Bound protocol [22], such a solution would be a remarkable result with many complexity-theoretic applications. Unfortunately, even a QMA containment for this kind of approximate counting problem is unknown. Despite such smart usage of the Grover algorithm implies an $O(\sqrt{2^n/|S|})$-query algorithm [2, 8, 39], we are not aware of utilizing a quantum witness. Furthermore, an oracle separation between SBP and QMA [1] suggests that such a proof of SBP ⊆ QMA is supposed to be in a non-black-box approach, which signifies a better understanding beyond a query oracle is required.

Besides SBP vs. MA, it remains open whether StoqMA = MA. It is natural to ask whether each StoqMA verifier has easy witness. However, we even do not know how to prove StoqMA$(1-a, 1-1/\mathrm{poly}(n))$ has easy witness, where a is negligible (i.e., an inverse super-polynomial). In [4], they prove StoqMA$(1-a, 1-1/\mathrm{poly}(n))$ ⊆ MA by applying the probabilistic method on a random walk, whereas the existence of easy witness seems to require a stronger structure[6].

Towards error reduction of StoqMA. Error reduction of StoqMA is an open problem since Bravyi, Bessen, and Terhal define this class in 2006 [9]. We first state this conjecture:

▶ **Conjecture 6** (Error reduction of StoqMA)**.** *For any a, b such that $1/2 \leq b < a \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$, the following holds for any polynomial $l(n)$:* StoqMA(a, b) ⊆ StoqMA$\left(1-2^{-l(n)}, 1/2+2^{-l(n)}\right)$.

As [4] shows that StoqMA with a negligible completeness error is contained in MA, (completeness) error reduction of StoqMA plays a crucial role in proving StoqMA = MA. Instead of performing the majority vote among parallelly running verifiers, another commonplace approach is first reducing errors of completeness and soundness separately, then utilizing these two procedures alternatively with well-chosen parameters. For instance, the renowned polarization lemma of SZK [36, 6], and the space-efficient error reduction of QMA [19]. Since Theorem 5 already states soundness error reduction of StoqMA, is it possible to also construct a completeness error reduction? Namely, a mechanism that builds a new StoqMA$(1/2+a'/2, 1/2+b'/2)$ verifier from the given StoqMA$(1/2+a/2, 1/2+b/2)$ verifier such that a' is super-polynomially close to 1. It seems to require new ideas since a direct analog of the XOR lemma in the polarization lemma of SZK, such as Lemma 4.11 in [6], does not work here.

StoqMA with exponentially small gap. Fefferman and Lin prove [20] that PreciseQMA is as powerful as PSPACE, where PreciseQMA is a variant of QMA(a, b) with exponentially small gap $a - b$. Moreover, we know that both PreciseQCMA and PreciseMA are equal to $\mathsf{NP}^{\mathsf{PP}}$ [33], where PreciseQCMA is a precise variant of QMA with a classical witness of the verifier. It is evident that PreciseStoqMA is between $\mathsf{NP}^{\mathsf{PP}}$ and PSPACE, also the classical-witness variant of this class is precisely $\mathsf{NP}^{\mathsf{PP}}$ (see Section 3.3). Does PreciseStoqMA an intermediate class between $\mathsf{NP}^{\mathsf{PP}}$ and PSPACE, or even strong enough to capture the full PSPACE power?

[6] The candidate here is the set S of all good strings (see Appendix B) of the given SetCSP instance, which is unnecessary an optimal witness. It is thus unclear whether the frustration of S remains negligible.

Paper organization

Section 2 introduces useful terminologies and notations. Section 3 proves that easy-witness StoqMA is contained in MA, which indicates an arguably simplified proof of $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$, together with remarks on classical-witness StoqMA. Section 4 presents a new StoqMA-complete problem named reversible circuit distinguishability, and the complexity of this problem's exact variant, which infers StoqMA with perfect soundness is in NP. Section 5 provides error reduction of StoqMA regarding soundness error.

2 Preliminaries

2.1 Non-negative states

We assume familiarity with quantum computing on the levels of [34]. Beyond this, we then introduce some notations which are more particular for this paper: the *support* of $|\psi\rangle$, $supp(|\psi\rangle) := \{i \in \{0,1\}^n : \langle\psi|i\rangle \neq 0\}$, is the set strings with non-zero amplitude. A quantum state $|\psi\rangle$ is *non-negative* of $\langle i|\psi\rangle \geq 0$ for all $i \in \{0,1\}^n$. For any $S \subseteq \{0,1\}^n$, we refer to the state $|S\rangle := \frac{1}{\sqrt{|S|}}\sum_{i\in S}|i\rangle$ as the subset state corresponding to the set S [41].

2.2 Complexity class: MA and StoqMA

A (promise) problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ consists of two non-overlapping subsets $\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}} \subseteq \{0,1\}^*$. These classes MA and StoqMA considered in this paper using the language of reversible circuits, as Definition 7 and Definition 9.

▶ **Definition 7** (MA, adapted from [9]). *A promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in \mathsf{MA}$ if there exists an* MA *verifier such that for any input $x \in \mathcal{L}$, an associated uniformly generated verification circuit V_x using only classical reversible gates (i.e. Toffoli, CNOT, X) on $n := n_w + n_0 + n_+$ qubits and a computational-basis measurement on the output qubit, where n_w is the number of qubits for a witness, and n_0 (or n_+) is the number of $|0\rangle$ (or $|+\rangle$) ancillary qubits, such that*

Completeness. *If $x \in \mathcal{L}_{\text{yes}}$, then there exists an n-qubit non-negative witness $|w\rangle$ such that $\Pr[V_x \text{ accepts } |w\rangle] \geq 2/3$.*

Soundness. *If $x \in \mathcal{L}_{\text{no}}$, we have $\Pr[V_x \text{ accepts } |w\rangle] \leq 1/3$ for any n-qubit witness $|w\rangle$.*

For simplicity, we denote $|\bar{0}\rangle := |0\rangle^{\otimes n_0}$ and $|\bar{+}\rangle := |+\rangle^{\otimes n_+}$ for the rest of this paper. We refer the equivalence between Definition 7 and the standard definition of MA to as Remark 8, which is first observed by [10].

▶ Remark 8 (Equivalent definitions of MA). The standard definition of MA only allows classical witnesses, viz. binary strings. To show it is equivalent to Definition 7, it suffices to prove the optimal witness for *yes* instances is classical. Notice that $\Pr[V_x \text{ accepts } |w\rangle] = \langle\psi_{\text{in}}| V_x^\dagger \Pi_{\text{out}} V_x |\psi_{\text{in}}\rangle$ where $|\psi_{\text{in}}\rangle := |w\rangle \otimes |\bar{0}\rangle \otimes |\bar{+}\rangle$ and $\Pi_{\text{out}} = |0\rangle\langle 0|_1 \otimes I_{\text{else}}$. Since $V_x^\dagger \Pi_{\text{out}} V_x$ is a diagonal matrix, the optimal witness of V_x is classical.

Analogously, we could define NP using classical reversible gates by setting $n_+ = 0$ in Definition 7. Now we proceed with the definition of StoqMA.

▶ **Definition 9** (StoqMA, adapted from [9]). *A promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in \mathsf{StoqMA}$ if there is a* StoqMA *verifier such that for any input $x \in \mathcal{L}$, a uniformly generated verification circuit V_x using Toffoli, CNOT, X gates on $n := n_w + n_0 + n_+$ qubits and a Hadamard-basis measurement on the output qubit, where n_w is the number of qubits for a witness, and n_0*

(or n_+) is the number of $|0\rangle$ (or $|+\rangle$) ancillary qubits, such that for efficiently computable functions $a(n)$ and $b(n)$:

Completeness. *If $x \in \mathcal{L}_{\text{yes}}$, then there exists an n-qubit non-negative witness $|w\rangle$ such that $\Pr[V_x \text{ accepts } |w\rangle] \geq a(n)$.*

Soundness. *If $x \in \mathcal{L}_{\text{no}}$, we have $\Pr[V_x \text{ accepts } |w\rangle] \leq b(n)$ for any n-qubit witness $|w\rangle$.*

Moreover, $a(n)$ and $b(n)$ satisfy $1/2 \leq b(n) < a(n) \leq 1$ and $a(n) - b(n) \geq 1/\text{poly}(n)$.

Error reduction of StoqMA remains open since this class was defined in 2006 [9] because this class does not permit amplification of gap between thresholds a, b based on majority voting. Hence, this gap is at least an inverse polynomial. We leave the remarks regarding the non-negativity of witnesses and parameters to Remark 10.

▶ Remark 10 (Optimal witnesses of a StoqMA verifier is non-negative). Analogous to QMA, the maximum acceptance probability of a StoqMA verifier V_x is precisely the maximum eigenvalue of $M_x := \langle\bar{0}|\langle\bar{+}| V_x^\dagger |+\rangle\langle+|_1 V_x |\bar{0}\rangle|\bar{+}\rangle$ due to $\Pr[V_x \text{ accepts } |\psi\rangle] = \langle\psi| M_x |\psi\rangle$. Notice the matrix M_x is entry-wise non-negative. Owing to the Perron-Frobenius theorem (see Theorem 8.4.4 in [24]), a straightforward corollary is that the eigenvector ψ (i.e., the optimal witness) maximizing the acceptance probability has non-negative amplitudes in the computational basis, namely it suffices to consider only non-negative witness for *yes* instances. Additionally, it is clear-cut that the acceptance probability for any non-negative witness $|\psi\rangle$, regardless of the optimality, is at least $1/2$ by a direct calculation.

2.3 Distribution testing

Distribution testing is generally about telling whether one probability distribution is close to the other. We further recommend a comprehensive survey [15] for a detailed introduction. We begin with the squared Hellinger distance $d_H^2(D_0, D_1)$ between two (sub-)distributions D_0, D_1, where $d_H^2(D_0, D_1) := \frac{1}{2}\| |D_0\rangle - |D_1\rangle \|_2^2$ and $|D_k\rangle = \sum_i \sqrt{D_k(i)}\,|i\rangle$ for any $k = 0, 1$. This distance is comparable with the total variation distance (see Proposition 1 in [18]). We then introduce a specific model used for this paper, namely the *dual access model*:

▶ **Definition 11** (Dual access model, adapted from [14]). *Let D be a fixed distribution over $[2^n]$. A dual oracle for D is a pair of oracles $(\mathsf{S}_D, \mathsf{Q}_D)$:*

- *Sample access: S_D returns an element $i \in \{0,1\}^n$ with probability $D(i)$. And it is independent of all previous calls to any oracle.*
- *Query access: Q_D takes an input a query element $j \in \{0,1\}^{n-1}$, and returns the quotient $D(0||j)/D(1||j)$ where $D(a||j)$ is the probability weight that D puts on $a||j$ for $a \in \{0,1\}$.*

We then explain how to implement these oracles here in Remark 12:

▶ Remark 12 (Implementation of dual access model). The sample access oracle in Definition 11 could be implemented by running an independent copy of the circuit that generates the state $|0\rangle|D_0\rangle + |1\rangle|D_1\rangle$, and measuring all qubits on the computational basis. Meanwhile, the query access oracle is substantially an efficient evaluation algorithm corresponding to the quotient $D_0(i)/D_1(i)$ for given index i.

In [14], Canonne and Rubinfeld show that approximating the total variation distance between two distributions within an additive error ϵ requires only $\Theta(1/\epsilon^2)$ oracle accesses (see Theorems 6 and 7 in [14]). However, suppose we allow to utilize only sample accesses. In that case, such a task requires $\Omega(N/\log N)$ samples even within constant accuracy (see Theorem 9 in [18]), where N is the dimension of distributions.

3 StoqMA with easy witnesses

This section will prove that StoqMA with easy witnesses, viz. eStoqMA, is contained in MA. *Easy witness* is named in the flavor of the seminal *easy witness lemma* [25], which means that an n-qubit non-negative state witness of a StoqMA verifier has a *succinct* representation. In particular, there exists an efficient algorithm to output the quotient $D_0(i)/D_1(i)$ for given index i. It is a straightforward generalization of subset states where the membership of the corresponding subset is efficiently verifiable. We here define eStoqMA formally:

▶ **Definition 13** (eStoqMA). *A promise problem* $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in$ eStoqMA *if there is a* StoqMA *verifier such that for any input* $x \in \mathcal{L}$*, a uniformly generated verification circuit* V_x *using only Toffoli, CNOT, X gates on* $n := n_w + n_0 + n_+$ *qubits and a Hadamard-basis measurement on the output qubit, where* n_w *is the number of qubits for a witness, and* n_0 *(or* n_+*) is the number of* $|0\rangle$ *(or* $|+\rangle$*) ancillary qubits, such that for efficiently computable functions* $a(n)$ *and* $b(n)$*:*

Completeness. *There exists an* n*-qubit non-negative witness* $|w\rangle := \sum_{i\in\{0,1\}^n} \sqrt{D_w(i)}\,|i\rangle$ *such that* $\Pr[V_x \text{ accepts } |w\rangle] \geq a(n)$*, and there is an efficient algorithm* Q_w *that outputs* $D_w(0||i)/D_w(1||i)$ *(or* $D_w(1||i)/D_w(0||i)$*) of index* $1||i$ *(or* $0||i$*) sampled from the distribution* D_w *where* $i \in \{0,1\}^{n-1}$*.*

Soundness. *For any* n*-qubit witness* $|w\rangle$*,* $\Pr[V_x \text{ accepts } |w\rangle] \leq b(n)$*.*

Moreover, $a(n)$ *and* $b(n)$ *satisfy* $1/2 \leq b(n) < \alpha(n) \leq 1$ *and* $a(n) - b(n) \geq 1/\text{poly}(n)$*.*

▶ Remark 14 (Subset-state witnesses require only membership). To show a subset-state witness $|w\rangle$ is an easy witness, it suffices to decide the membership of $\text{supp}(|w\rangle)$ for the associated algorithm Q_w. Notice any coordinate $D_w(j)$ in D_w is $1/|\text{supp}(|w\rangle)|$ if $j \in \text{supp}(|w\rangle)$; otherwise $D_w(j) = 0$. Moreover, if $D_w(1||i) = 0$ for some i, the corresponding point will never be sampled. Hence, the quotient $D_w(0||i)/D_w(1||i)$ is 1 if both $0||i$ and $1||i$ belong to $\text{supp}(|w\rangle)$ (i.e., $D_w(0||i) = D_w(1||i) \neq 0$); otherwise the quotient is 0.

Distribution testing techniques inspire an MA containment of eStoqMA, as Theorem 15. Precisely, employed with the dual access model (see Definition 11) adapted from Canonne and Rubinfeld [14], we obtain an empirical estimation within inverse-polynomial accuracy of an eStoqMA verifier's acceptance probability, where both sample complexity and time complexity are efficient.

▶ **Theorem 15** (eStoqMA ⊆ MA). *For any* $1/2 \leq b < a \leq 1$ *and* $a - b \geq 1/\text{poly}(n)$*,*

$$\mathsf{eStoqMA}(a,b) \subseteq \mathsf{MA}\left(\tfrac{9}{16}, \tfrac{7}{16}\right).$$

In [9, 12], Bravyi, Bessen, and Terhal proved $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$, utilizing a relatively complicated random walk based argument. By taking advantage of eStoqMA, we here provide an arguably simplified proof by plugging Proposition 16 into Theorem 15:

▶ **Proposition 16.** $\mathsf{StoqMA}_1 \subseteq \mathsf{eStoqMA}$.

The proof of Proposition 16 straightforwardly follows from the definition of SetCSP (see Definition 30), namely any $\text{SetCSP}_{0,1/\text{poly}}$ instance certainly has easy witness, and it is indeed optimal. We further leave the technical details regarding SetCSP in Appendix B.

How strong is the eStoqMA? Remark 17 suggests eStoqMA seems more powerful than classical-witness StoqMA (i.e., cStoqMA):

▶ Remark 17 (eStoqMA is not trivially contained in cStoqMA). Classical witness is clearly also easy witness, but the opposite is unnecessarily true. Even though Merlin could send the algorithm Q_{D_w} as classical witness to Arthur, Arthur only can prepare $|w\rangle$ by a post-selection, which means cStoqMA does not trivially contain eStoqMA.

Furthermore, the proof of $\mathsf{StoqMA}(a,b)$ with classical witnesses is in MA [23] could preserve completeness and soundness parameters. By inspection, it is clear-cut that this proof even holds when the gap $a-b$ is *arbitrarily small*, whereas the proof of Theorem 15 works only for inverse-polynomial accuracy. Further remarks of classical witness' limitations can be found in Section 3.3.

3.1 eStoqMA $\subseteq$ MA: the power of distribution testing

To derive an MA containment of eStoqMA, it suffices to distinguish two non-negative states (viz., approximating the maximum acceptance probability) within an inverse-polynomial accuracy regarding the inner product (i.e., squared Hellinger distance). It seems plausible to prove StoqMA $\subseteq$ MA by taking *samples* and post-processing. However, the known sample complexity lower bound (See Section 2.3) indicates that (almost) exponentially many samples are unavoidable. Fortunately, we could circumvent this barrier for showing eStoqMA $\subseteq$ MA, since easy witness guarantees *efficient query access* to $D_0(i)/D_1(i)$ for given index i. In particular, employing both sample and query oracle accesses to D_0, D_1, such approximation within an additive error ϵ requires merely $\Theta(1/\epsilon^2)$ samples and queries! This advantage first noticed by Rubinfeld and Servedio [35], and then almost fully characterized by Canonne and Rubinfeld [14]. Recently, this technique also has algorithmic applications used in quantum-inspired classical algorithms for machine learning [16, 38].

▶ **Lemma 18** (Approximating a single-qubit Hadamard-basis measurement). *In the dual access model, there is a randomized algorithm $\mathcal{T}$ which takes an input x, $1/2 \leq b(|x|) < a(|x|) \leq 1$, as well as access to $(\mathsf{S}_D, \mathsf{Q}_D)$, where the non-negative state before the measurement is $|\psi\rangle = \sum_{i\in[2^n]} \sqrt{D(i)}\,|i\rangle$. After making $O\left(1/(a-b)^2\right)$ calls to the oracles, $\mathcal{T}$ outputs either* ACCEPT *or* REJECT *such that:*

- *If $\frac{1}{2}\| \,|D_0\rangle + |D_1\rangle \,\|_2^2 \geq a$, $\mathcal{T}$ outputs* ACCEPT *with probability at least $9/16$;*
- *If $\frac{1}{2}\| \,|D_0\rangle + |D_1\rangle \,\|_2^2 \leq b$, $\mathcal{T}$ outputs* ACCEPT *with probability at most $7/16$,*

where D_k $(k \in \{0,1\})$ is a sub-distribution such that $\forall i \in \{0,1\}^{n-1}, D_k(i) := D(k||i)$.

Proof Intuition. To construct this algorithm $\mathcal{T}$, the main idea is writing the acceptance probability p_{acc} of a StoqMA verifier's easy witness as an expectation over D_1 (or D_0) of some random variable regarding coordinates quotients $D_0(i)/D_1(i)$. Note that the quotient $\sqrt{D_0(i)}/\sqrt{D_1(i)}$ could be computed by running the evaluation algorithm Q_w (i.e., query oracle access). Hence, $\mathcal{T}$ only require to calculate an empirical estimation of $\mathbb{E}[X]$ (see the RHS of Equation (1)) within $1/\mathrm{poly}(|x|)$ accuracy. Such an approximation could be achieved by averaging $\mathrm{poly}(|x|)$ sample with a standard concentration bound, which is analogous to Theorem 6 in [14].

Now we proceed with the explicit construction (i.e., Algorithm 1) and analysis.

Proof of Lemma 18. We begin with estimating the quantity $\| |D_0\rangle + |D_1\rangle \|_2^2 / 2\,\|D_1\|_1$ up to some additive error $\epsilon := (a-b)/8$. We first observe that

$$\frac{\| |D_0\rangle + |D_1\rangle \|_2^2}{2\|D_1\|_1} = \frac{1}{2} \sum_{i\in\{0,1\}^{n-1}} \left(1 + \frac{\sqrt{D_0(i)}}{\sqrt{D_1(i)}}\right)^2 \frac{D_1(i)}{\|D_1\|_1} = \mathop{\mathbb{E}}_{i\sim D_1/\|D_1\|_1} \left[\frac{1}{2}\left(1+\frac{\sqrt{D_0(i)}}{\sqrt{D_1(i)}}\right)^2\right]. \quad (1)$$

Since the inner product is symmetric, it also implies $\frac{\| |D_0\rangle + |D_1\rangle \|_2^2}{2\|D_0\|_1} = \mathbb{E}_{i\sim \frac{D_0}{\|D_0\|_1}} \left[\frac{1}{2}\left(1+\frac{\sqrt{D_1(i)}}{\sqrt{D_0(i)}}\right)\right]$.

Algorithm 1 $O(1/(a-b)^2)$-additive approximation tester $\mathcal{T}$ of $\frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2$.

Require: S_D and Q_D oracle accesses; parameters $\frac{1}{2} \le b < a \le 1$.
Set $m, m' := \Theta(1/\epsilon^2)$, where $\epsilon := (a-b)/8$;
Draw samples $o_1, \cdots, o_{m'}$ from
 D_{out} := marginal distribution of the designated output qubit;
Compute $\hat{Z} := \frac{1}{m'}\sum_{i=1}^{m'} Z_i$, where $Z_i := o_i$;
Draw samples $s_1, \cdots, s_m$ from D;
For $i = 1, \cdots, m$ **Do**
  If $\hat{Z} \ge \frac{1}{2}$ **Then** with Q_D, get $X_i := \frac{1}{2}\left(1 + \frac{\sqrt{D_0(s_i)}}{\sqrt{D_1(s_i)}}\right)^2$;
  Else with Q_D, get $X_i := \frac{1}{2}\left(1 + \frac{\sqrt{D_1(s_i)}}{\sqrt{D_0(s_i)}}\right)^2$;
End
Compute $\hat{X} := \frac{1}{m}\sum_{i=1}^{m} X_i$;
If $\hat{Z} \ge \frac{1}{2}$ *and* $\hat{X}\hat{Z} \ge \frac{1}{2}(a+b)$ **Then** output ACCEPT;
Else If $\hat{Z} < \frac{1}{2}$ *and* $\hat{X}(1-\hat{Z}) \ge \frac{1}{2}(a+b)$ **Then** output ACCEPT;
Else output REJECT;

Notice $\mathcal{T}$ only require to achieve an empirical estimate of this expected value, which suffices to utilize $m = O\left(1/(a-b)^2\right)$ samples s_i from D_1, querying $\frac{D_0(s_i)}{D_1(s_i)}$, and computing $X_i = \frac{1}{2}\left(1 + \frac{\sqrt{D_0(s_i)}}{\sqrt{D_1(s_i)}}\right)^2 \|D_1\|_1$. We here provide the explicit construction of $\mathcal{T}$, as Algorithm 1.

Analysis. Define random variables Z_i as in Algorithm 1. We obviously have $\mathbb{E}[Z_i] = \|D_1\|_1 \in [0,1]$. Since all Z_is' are independent, a Chernoff bound ensures

$$\Pr\left[\left|\hat{Z} - \|D_1\|_1\right| \le \epsilon\right] \ge 1 - 2e^{-2m'/\epsilon^2}, \tag{2}$$

which is at least $3/4$ by an appropriate choice of m'.

Note drawing samples from p_0 implicitly by post-selecting the output qubit to be 0. However, due to the inner product's symmetry and $\|D_0\|_1 + \|D_1\|_1 = 1$, there must exist $i \in \{0,1\}$ such that $\|D_i\|_1 \ge 1/2$. Hence, the required sample complexity will be enlarged merely by a factor of 2.

Let us also define random variables X_i as in Algorithm 1. W.L.O.G. assume that $\|D_1\|_1 \ge 1/2 \ge \|D_0\|_1$. By Equation (1), we obtain $\mathbb{E}_{i\sim D_1/\|D_1\|_1}[X_i] = \left\||D_0\rangle + |D_1\rangle\right\|_2^2 / 2\|D_1\|_1$. Because the X_i's are independent and takes value in $[1/2, 1]$, by Chernoff bound,

$$\Pr\left[\left|\hat{X} - \frac{\left\||D_0\rangle + |D_1\rangle\right\|_2^2}{2\|D_1\|_1}\right| \le \epsilon\right] \ge 1 - 2e^{-2m/\epsilon^2}. \tag{3}$$

Therefore, by our choice of m, $\hat{X}$ is an ϵ-additive approximation of $\left\||D_0\rangle + |D_1\rangle\right\|_2^2 / 2\|D_1\|_1$ with probability at least $3/4$. Note that X_i, Z_i are independent, we obtain $\mathbb{E}\left[\hat{X}\hat{Z}\right] = \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2$. Hence, notice $1/2 \le \|D_1\|_1 \le 1$ and $1/2 \le \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 \le 1$, by combining Equations (2) and (3), we obtain with probability $9/16$:

$$\hat{X}\hat{Z} \le \left(\frac{\||D_0\rangle+|D_1\rangle\|_2^2}{2\|D_1\|_1} + \epsilon\right)(\|D_1\|_1 + \epsilon) \le \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 + \epsilon^2 + \epsilon + 2\epsilon \le \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 + 4\epsilon;$$

$$\hat{X}\hat{Z} \ge \left(\frac{\||D_0\rangle+|D_1\rangle\|_2^2}{2\|D_1\|_1} - \epsilon\right)(\|D_1\|_1 - \epsilon) \ge \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 + \epsilon^2 - \epsilon - 2\epsilon \ge \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 - 4\epsilon.$$

It implies that $\Pr\left[\left|\hat{X}\hat{Z} - \frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2\right| \leq 4\epsilon\right] \geq 9/16$. We thereby conclude that

- If $\frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 \geq a$, then $\hat{X}\hat{Z} \geq a - 4\epsilon$ and $\mathcal{T}$ outputs ACCEPT w.p. at least 9/16.
- If $\frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2 \leq b$, then $\hat{X}\hat{Z} \leq b + 4\epsilon$ and $\mathcal{T}$ outputs ACCEPT w.p. at most 7/16.

Furthermore, the algorithm $\mathcal{T}$ makes $m' + 2m$ calls for S_D and m calls for Q_D . ◀

It is worthwhile to mention that this construction in the proof of Theorem 15 is optimal regarding the sample complexity, as Theorem 7 stated in [14].

Finally, we complete the proof of Theorem 15 by Lemma 18.

Proof of Theorem 15. Given an $\mathsf{eStoqMA}(a, b)$ verifier V_x, we here construct a MA verifier V_x' that follows from Algorithm 1 in the proof of Lemma 18:

(1) For each call to the sample oracle S_{D_w}, we run the $\mathsf{eStoqMA}$ verifier V_x (without measuring the output qubit) with the witness w, and draw samples by performing measurements:
   - For samples s_i $(1 \leq i \leq m)$ from distribution D, measure all qubits utilized by the verification circuit in the computational basis;
   - For samples o_j $(1 \leq j \leq m')$ from distribution D_{out}, measure the designated output qubit in the computational basis.

(2) For each call to the query oracle Q_{D_w} with index i, find the corresponding index i' at the beginning by performing the permutation associated with $V_x^\dagger$ on i, and then evaluate the value $D_w(i'')/D_w(i')$ by utilizing the given algorithm associated with this easy witness, where i'' is given by flipping the first bit of i'.

(3) Compute an empirical estimation of $\frac{1}{2}\left\||D_0\rangle + |D_1\rangle\right\|_2^2$ as Algorithm 1, and then decide whether V_x accepts w.

The circuit size of V_x' is a polynomial of $|x|$ since both sample and query complexity are efficient. We thus conclude that the new MA verifier V_x' is efficient, and only requires $O\left(1/(a-b)^2\right)$ copies of the witness w, which finishes the completeness case.

For the soundness case, the acceptance probability p_{acc} of the $\mathsf{eStoqMA}$ verifier V_x for all witnesses is obviously upper-bounded by b, regardless of whether such a witness is easy or not. Furthermore, entangled witnesses are useless since we draw samples by performing measurements separately. Hence, the maximum acceptance probability of the new MA verifier V_x' is also at most b. ◀

3.2 StoqMA with perfect completeness is in eStoqMA

We here complete proof of Proposition 16. By Theorem 15, it infers $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$.

Proof of Proposition 16. By Theorem 31, we know that $\text{SetCSP}_{0,1/\text{poly}}$ is StoqMA_1-complete, so it suffices to show that $\text{SetCSP}_{0,1/\text{poly}}$ is contained in $\mathsf{eStoqMA}_1$.

By Lemma 35, given a $\text{SetCSP}_{0,b}$ instance C, we can construct a $\mathsf{StoqMA}\left(1, 1 - b/2\right)$ verifier. The corresponding subset $S \subseteq \{0,1\}^n$, where S satisfies all set-constraints of C, is an optimal witness. It is left to show that this subset states is an easy witness.

We achieve the proof by inspection. Let S be the set of all good strings of C, then set-unsat$(C, S) = 0$. Note $x \in S$ is a good string of C iff x is a good string of all set-constraints $C_i(1 \leq i \leq m)$, the membership of S thus can be decided efficiently, which infers the subset state $|S\rangle$ is easy witness by Remark 14. ◀

3.3 Limitations of classical-witness StoqMA

As we have shown StoqMA with easy witness is contained in MA. What about classical witness, namely cStoqMA? In fact, we could show such a containment that preserves both completeness and soundness parameters.

▶ **Proposition 19** ([23]). *For any* $1/2 \leq b < a \leq 1$ *and* $a - b \geq 1/\mathrm{poly}(n)$, $\mathsf{cStoqMA}(a, b) \subseteq \mathsf{MA}(2a - 1, 2b - 1)$.

Proof Sketch. We only illustrate the intuition: for any $s \in \{0,1\}^n$ and any reversible circuit U, we have $\langle s| U^\dagger |+\rangle \langle +|_1 U |s\rangle = \frac{1}{2} + \frac{1}{2} \langle s| U^\dagger X_1 U |s\rangle$ since $|+\rangle \langle +| = \frac{1}{2}(X + I)$. The detailed proof is left in Appendix A.1. ◀

The proof of Proposition 19 immediately infers the *precise variant* of StoqMA with classical witnesses, where the completeness-soundness gap is exponentially small, is equal to PreciseMA. However, the proof of Theorem 15 no longer works for precise scenarios, indicating that StoqMA with classical witness seems not interesting.

Furthermore, it is not hard to see that classical witness is optimal for StoqMA_1 verifier[7]. However, it does not mean that a classical witness is optimal for *any* StoqMA_1 verifier. In fact Appendix A.2 provides a simple counterexample by considering an identity as a verifier. However, this impossibility result is unknown for easy witness yet.

4 Complexity of reversible circuit distinguishability

This section will concentrate on the complexity classification of distinguishing reversible circuits, namely given two efficient reversible circuits, and decide whether there is a non-negative state that *cannot* tell one from the other. With ancillary random bits, this problem is StoqMA-complete, as Theorem 22. However, this problem's exact variant, namely assuming two reversible circuits are indistinguishable with respect to any non-negative witness for *no* instances (viz., StoqMA with perfect soundness), is NP-complete (see Proposition 23). Moreover, Theorem 22 also implies that distinguishing reversible circuits without any ancillary random bit is NP-complete, which signifies a simplified proof of [27].

4.1 Reversible circuit distinguishability is StoqMA-complete

We begin with the formal definition of the *Reversible Circuit Distinguishability* problem.

▶ **Definition 20** (Reversible Circuit Distinguishability). *Given a classical description of two reversible circuits* C_0, C_1 *(using Toffoli, CNOT, X gates) on* $n := n_w + n_0 + n_+$ *qubits, where* n_w *is the number of qubits of a non-negative state witness* $|w\rangle$, n_0 *is the number of* $|0\rangle$ *ancillary qubits, and* n_+ *is the number of* $|+\rangle$ *ancillary qubits. Let the resulting state before measuring the output qubit be* $|R_i\rangle := C_i |w\rangle |\bar{0}\rangle |\bar{+}\rangle$, $i \in \{0,1\}$*. Promise that* C_0 *and* C_1 *with respect to witness state(s) are either* α*-indistinguishable or* β*-distinguishable, decide whether*

- **Yes** *(*α*-indistinguishable): there exists a non-negative witness* $|w\rangle$ *such that* $\langle R_0|R_1\rangle \geq \alpha$*;*
- **No** *(*β*-distinguishable): for any non-negative witness* $|w\rangle$*, then* $\langle R_0|R_1\rangle \leq \beta$*;*

where $\alpha - \beta \geq 1/\mathrm{poly}(n)$[8].

---

[7] By combining $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}_1$ and the gadget in the proof of Proposition 36, we could construct a StoqMA_1 verifier such that a classical witness is optimal.

[8] Note $\langle R_0|R_0\rangle = \langle R_1|R_1\rangle = 1$ which differs from $\langle D_0|D_0\rangle + \langle D_1|D_1\rangle = 1$ previously used in Section 3, we obtain that the acceptance probability $p_{\rm acc} = \frac{1}{2} + \frac{1}{2}\langle R_0|R_1\rangle = 1 - \frac{1}{2} \cdot \frac{1}{2} \| |R_0\rangle - |R_1\rangle \|_2^2$.

Since Definition 20 seems slightly inconsistent with known results regarding distinguishing circuits [26, 27, 37], it is worthwhile to mention a slightly different version (see Remark 21) of Definition 20, which is co-StoqMA-complete.

▶ Remark 21 (Equivalence Check of Reversible Circuits is co-StoqMA-complete). Consider the same scenario in Definition 20, and the task is checking whether C_0 and C_1 are approximately equivalent (with respect to witness states). More concretely, decide whether $\langle R_0|R_1\rangle \geq \alpha$ for any $|w\rangle$; or there exists $|w\rangle$ such that $\langle R_0|R_1\rangle \leq \beta$. The co-StoqMA-completeness straightforwardly follows from the constructions in the proof of Theorem 22.

Now we state the main theorem in Section 4.

▶ **Theorem 22** (Reversible Circuit Distinguishability is StoqMA-complete). *For any $\alpha - \beta \geq 1/\mathrm{poly}(n)$, (α, β)-Reversible Circuit Distinguishability is* StoqMA$\,(1/2 + \alpha/2, 1/2 + \beta/2)$*-complete.*

We will then proceed with an intuitive explanation regarding proof of Theorem 22.

Proof Intuition. The StoqMA-containment proof is inspired by the SWAP test for distinguishing two quantum states [13], since it could be thought of as a StoqMA verification circuit with the maximum acceptance probability 1. We below provide a procedure (see Figure 1) to distinguish two reversible circuits C_0, C_1 using a non-negative witness, and such a procedure is apparently a StoqMA verifier. The StoqMA-hardness proof is straightforward: replacing C_0 and C_1 by identity and $V_x^\dagger X_1 V_x$ (see Figure 2), respectively, where V_x is the given StoqMA verification circuit.

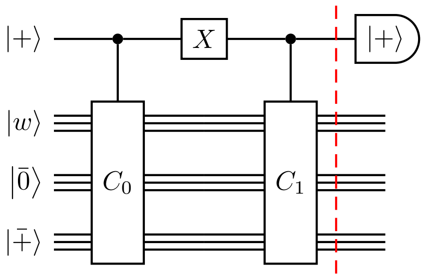

Figure 1 RCD is in StoqMA.

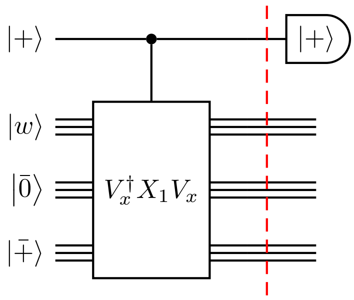

Figure 2 RCD is StoqMA-hard.

Now we proceed with the technical details.

Proof of Theorem 22. We first show (α, β)-RCD is StoqMA$\,(1/2 + \alpha/2, 1/2 + \beta/2)$-hard. Consider a StoqMA verifier V_x as Figure 2, let $C_0 := V_x^\dagger X_1 V_x$ where the X gate in the middle acts on the output qubit, and let C_1 be identity. Then for any witness $|w\rangle$, we obtain:

$$\begin{aligned}\Pr\left[V_x \text{ accepts } |w\rangle\right] &= \langle w| \langle\bar{0}| \langle\bar{+}| \left(V_x^\dagger |+\rangle\langle+|_1 V_x\right) |w\rangle |\bar{0}\rangle |\bar{+}\rangle\,; \\ \langle R_0|R_1\rangle &= \langle w| \langle\bar{0}| \langle\bar{+}| \left(V_x^\dagger X_1 V_x\right) |w\rangle |\bar{0}\rangle |\bar{+}\rangle\,.\end{aligned} \tag{4}$$

Note that $|+\rangle\langle+| = (X + I)/2$, we thereby complete the StoqMA-hardness proof by Equation (4): $\Pr\left[V_x \text{ accepts } |w\rangle\right] = 1/2 + \langle R_0|R_1\rangle/2$.

Now it is left to show the StoqMA$\,(1/2 + \alpha/2, 1/2 + \beta/2)$ containment of (α, β)-RCD. Given reversible circuits C_0, C_1, we construct a StoqMA verifier as Figure 1. Hence, we obtain the state before measuring the output qubit (viz. the red dash line):

$$\mathrm{Ctrl}{-}C_1 \cdot X_1 \cdot \mathrm{Ctrl}{-}C_0 \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |w\rangle \, |\bar{0}\rangle \, |\bar{+}\rangle \right) = \frac{1}{\sqrt{2}} |0\rangle \, |R_0\rangle + \frac{1}{\sqrt{2}} |1\rangle \, |R_1\rangle := |\mathrm{RHS}\rangle \, .$$

We thus complete the StoqMA-containment proof:
$\Pr\left[V_x \text{ accepts } |w\rangle\right] = \left\| |+\rangle \langle +|_1 \, |\mathrm{RHS}\rangle \right\|_2^2 = 1/2 + \langle R_0 | R_1 \rangle / 2.$ ◀

4.2 Exact Reversible Circuit Distinguishability is NP-complete

We will prove that the exact variant of the Reversible Circuit Distinguishability is NP-complete. Moreover, it will signify that StoqMA with perfect soundness (even the gap between thresholds $\alpha, 1/2$ is arbitrarily small) is in NP.

▶ **Proposition 23** (Exact RCD is NP-complete). *Exact Reversible Circuit Distinguishability (RCD), namely $(\alpha, 0)$-Reversible Circuit Distinguishability for any $0 \leq \alpha < 1$, is NP-complete.*

Proof Sketch. It suffices to show an NP containment. By an analogous idea in [21], we could find two matched pairs (s, r) and (s', r') as classical witness, where s, s' are indices of non-zero coordinates in the given witness, and r, r' are random bit strings. Specifically, for *yes* instances, there exist two such pairs such that the resulting strings $C_0(s, r)$ [9] and $C_1(s', r')$ are identical; whereas it is evident that no matched pairs exist for *no* instances. The details are left in Appendix A.3. ◀

As a corollary, Proposition 23 will imply StoqMA with perfect soundness is in NP:

▶ **Corollary 24** (StoqMA with perfect soundness is in NP). $\bigcup_{a>1/2} \mathsf{StoqMA}\left(a, \frac{1}{2}\right) = \mathsf{NP}$.

StoqMA without any ancillary random bit is in NP. In fact, distinguishing reversible circuits without any ancillary random bit is NP-complete. By analogous reasoning, we also provide an alternating proof of *Strong Equivalence of Reversible Circuits* is co-NP-complete [27]. We leave the detailed proof in Appendix A.4.

5 Soundness error reduction of StoqMA

In this section, we will partially solve Conjecture 6 by providing a procedure that reduces the soundness error of any StoqMA verifier.

▶ **Theorem 25** (restated of Theorem 5). *For any $r = \mathrm{poly}(n)$,*

$$\mathsf{StoqMA}\left(\frac{1}{2} + \frac{a}{2}, \frac{1}{2} + \frac{b}{2}\right) \subseteq \mathsf{StoqMA}\left(\frac{1}{2} + \frac{a^r}{2}, \frac{1}{2} + \frac{b^r}{2}\right).$$

Consequently, Theorem 25 infers a direct error reduction for StoqMA_1 by choosing appropriate parameters a, b, r.

▶ **Corollary 26** (Error reduction of StoqMA_1). *For any s such that $1/2 \leq s \leq 1$ and $1 - s \geq 1/\mathrm{poly}(n)$, $\mathsf{StoqMA}(1, s) \subseteq \mathsf{StoqMA}\left(1, 1/2 + 2^{-n}\right)$.*

Proof. Choosing a, b such that $1 = 1/2 + a/2$ and $s = 1/2 + b/2$, we have $a = 1$ and $b = 2s - 1$. By Theorem 25, we obtain $\mathsf{StoqMA}\left(\frac{1}{2} + \frac{1}{2} \cdot 1, \frac{1}{2} + \frac{1}{2}(2s-1)\right) \subseteq \mathsf{StoqMA}\left(1, \frac{1}{2} + \frac{1}{2}(2s-1)^r\right)$. To finish the proof, it remains to choose a parameter r such that $r \geq (n+1)/\log_2\left(1/(2s-1)\right)$, since $(2s-1)^r/2 \leq 2^{-n}$ implies that $2^{-r\log_2(1/(2s-1))-1} \leq 2^{-n}$. ◀

[9] A reversible circuit takes (s, r) as an input, and permutes it to the other binary string as the output.

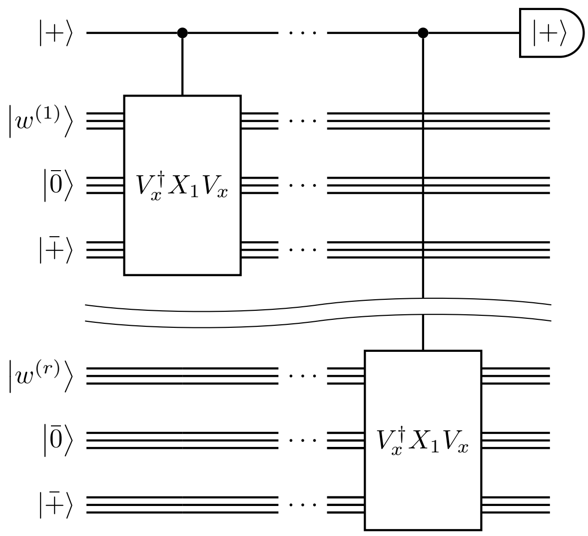

Figure 3 AND-type repetition procedure of a StoqMA verifier.

5.1 AND-type repetition procedure of a StoqMA verifier

Proof Intuition. The main idea is doing a parallel repetition of a StoqMA verifier V_x, and taking the conjunction (viz., AND) of the outcomes cleverly. More concretely, given a StoqMA verification circuit V_x where x is in $\mathcal{L} \in$ StoqMA, we result in a new StoqMA verifier by separately substituting an identity and $V_x^\dagger X_1 V_x$ for C_0, C_1 (as Figure 2). Notice the acceptance probability of a StoqMA verifier's non-negative witness $|w\rangle$, $\Pr[V_x \text{ accepts } |w\rangle] = \frac{1}{2} + \frac{1}{2}\langle D_0|D_1\rangle$, is linearly dependent to an inner product between states associated with two distributions D_0, D_1 where $|D_0\rangle := |w\rangle \left|\bar{0}\right\rangle |\bar{+}\rangle$ and $|D_1\rangle := V_x |w\rangle \left|\bar{0}\right\rangle |\bar{+}\rangle$. We could then take advantage of this new StoqMA verifier by running $r = \text{poly}(|x|)$ copies of these reversible circuits parallelly with the same target qubit, which is denoted as V_x' (see Figure 3).

For *yes* instances, it follows that an inner product of two tensor products of distributions is equal to the product of inner products of states associated with these distributions, namely, $\Pr[V_x' \text{ accepts } |w\rangle] = \frac{1}{2} + \frac{1}{2}\langle D_0|D_1\rangle^r$. However, it seems problematic for *no* instances, since a dishonest prover probably wants to cheat with an entangled witness instead of a tensor product among repetitive verifiers. We resolve this issue by an observation used in the QMA error reduction [30]: the maximum acceptance probability of a verifier V_x is the same as the maximum eigenvalue of a projection $\Pi_0 V_x^\dagger \Pi_1 V_x \Pi_0$ where Π_1 is the final measurement on the designated output qubit and $\Pi_0 := \left|\bar{0}\right\rangle \left\langle\bar{0}\right| \otimes |\bar{+}\rangle \langle\bar{+}|$. Eventually, an entangled witness will not help a dishonest prover. This is because the maximum eigenvalue of the tensor product of the projection $\Pi_0 V_x^\dagger \Pi_1 V_x \Pi_0$ is also the product of the maximum eigenvalue of this projection.

Finally, we proceed with the proof of Theorem 25.

Proof of Theorem 25. Given a promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in \text{StoqMA}(1/2+a/2, 1/2+b/2)$. For any input $x \in \mathcal{L}$, we have a StoqMA verifier V_x which is equivalent to a new StoqMA verifier $\tilde{V}_x$ as Figure 2, by the StoqMA-hardness proof of reversible circuit distinguishability as Theorem 22. Namely, $\tilde{V}_x$ is starting on a $|+\rangle$ ancillary qubit, applying a controlled-unitary $V_x^\dagger X_1 V_x$ on $n_w + n_0 + n_+$ qubits, and measuring the designated output qubit.

Let $|R_w\rangle := |w\rangle \left|\bar{0}\right\rangle |\bar{+}\rangle$ where $|w\rangle$ is a witness, we obtain

$$\left\| |+\rangle \langle+|_1 \left(\frac{1}{\sqrt{2}} |0\rangle \otimes |R_w\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes \left(V_x^\dagger X_1 V_x \right) |R_w\rangle \right) \right\|_2^2 = \| \, |+\rangle \langle+|_1 V_x |R_w\rangle \, \|_2^2. \quad (5)$$

By an observation used in the QMA error reduction, namely Lemma 14.1 in [30], we notice that the maximum acceptance probability of a StoqMA verifier V_x is proportion to the maximum eigenvalue of a matrix $M_x := \langle\bar{0}| \langle\bar{+}| V_x^\dagger X_1 V_x \left|\bar{0}\right\rangle |\bar{+}\rangle$ associated with V_x:

$$\Pr\left[V_x \text{ accepts } |w\rangle\right] = \frac{1}{2} + \frac{1}{2} \max_{|w\rangle} \mathrm{Tr}(M_x |w\rangle \langle w|) = \frac{1}{2} + \frac{1}{2} \lambda_{\max}(M_x). \quad (6)$$

AND-type repetition procedure of a StoqMA verifier. We now construct a new StoqMA verifier V_x' using r copies of the witness $|w\rangle$ on $r(n_w + n_0 + n_+) + 1$ qubits. As Figure 3, V_x' is starting from a $|+\rangle$ ancillary qubit as a control qubit, then applying controlled-unitary $V_x^\dagger X_1 V_x$ on qubits associated with different copies of the witness $\left|w^{(i)}\right\rangle$ for any $1 \leq i \leq r$.

By an analogous calculation of Equation (5), we have derived the acceptance probability of a witness $w^{(1)} \otimes \cdots \otimes w^{(k)}$ of the new StoqMA verifier V_x':

$$\Pr\left[V_x' \text{ accepts } \left(w^{(1)} \otimes \cdots \otimes w^{(r)}\right)\right] = \frac{1}{2} + \frac{1}{2} \mathrm{Tr}\left(\left|w^{(i)}\right\rangle \left\langle w^{(i)}\right| M_x^{\otimes r} \right),$$

where M_x is defined in Equation (6). Hence, the maximum acceptance probability of V_x':

$$\max_{|w'\rangle} \Pr\left[V_x' \text{ accepts } |w'\rangle\right] = \frac{1}{2} + \frac{1}{2} \lambda_{\max}\left(M_x^{\otimes r}\right) = \frac{1}{2} + \frac{1}{2} \left(\lambda_{\max}(M_x)\right)^r, \quad (7)$$

where the second equality thanks to the property of the tensor product of matrices. Equation (7) indicates that entangled-state witnesses are harmless since any entangled-state witness' acceptance probability is not larger than a tensor-product state witness'.

Finally, we complete the proof by analyzing the maximum acceptance probability of the new StoqMA verifier V_x' regarding the promises: For *yes* instances, we obtain $\lambda_{\max}(M_x) \geq a$ since there exists $|w\rangle$ such that $\Pr\left[V_x \text{ accepts } |w\rangle\right] \geq 1/2 + a/2$. By Equation (7), we have derived $\Pr\left[V_x' \text{ accepts } |w\rangle^{\otimes r}\right] = \frac{1}{2} + \frac{1}{2}\left(\lambda_{\max}(M_x)\right)^r \geq \frac{1}{2} + \frac{a^r}{2}$. For *no* instances, we have $\lambda_{\max}(M_x) \leq b$ since $\Pr\left[V_x \text{ accepts } |w\rangle\right] \leq 1/2 + b/2$ for all witness $|w\rangle$. By Equation (7), we further deduce $\forall w', \Pr\left[V_x' \text{ accepts } |w'\rangle\right] = \frac{1}{2} + \frac{1}{2}\left(\lambda_{\max}(M_x)\right)^r \leq \frac{1}{2} + \frac{b^r}{2}$. ◀

References

1 Scott Aaronson, Robin Kothari, William Kretschmer, and Justin Thaler. Quantum lower bounds for approximate counting via laurent polynomials. In *Proceedings of the 35th Computational Complexity Conference*, pages 1–47, 2020.

2 Scott Aaronson and Patrick Rall. Quantum approximate counting, simplified. In *Symposium on Simplicity in Algorithms*, pages 24–32. SIAM, 2020.

3 Dorit Aharonov and Alex B Grilo. Two combinatorial ma-complete problems. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

4 Dorit Aharonov, Alex B Grilo, and Yupan Liu. StoqMA vs. MA: the power of error reduction. *arXiv preprint arXiv:2010.02835*, 2020.

5 László Babai. Trading group theory for randomness. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 421–429, 1985.

6 Itay Berman, Akshay Degwekar, Ron D Rothblum, and Prashant Nalini Vasudevan. Statistical difference beyond the polarizing regime. In *Theory of Cryptography Conference*, pages 311–332. Springer, 2019.

7 Elmar Böhler, Christian Glaßer, and Daniel Meister. Error-bounded probabilistic computations between MA and AM. *Journal of Computer and System Sciences*, 72(6):1043–1076, 2006.

8 Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002.

9 Sergey Bravyi, Arvid J Bessen, and Barbara M Terhal. Merlin-arthur games and stoquastic complexity. *arXiv preprint quant-ph/0611021*, 2006.

10 Sergey Bravyi, David P Divincenzo, Roberto Oliveira, and Barbara M Terhal. The complexity of stoquastic local hamiltonian problems. *Quantum Information & Computation*, 8(5):361–385, 2008.

11 Sergey Bravyi and Matthew Hastings. On complexity of the quantum ising model. *Communications in Mathematical Physics*, 349(1):1–45, 2017.

12 Sergey Bravyi and Barbara Terhal. Complexity of stoquastic frustration-free hamiltonians. *SIAM Journal on Computing*, 39(4):1462–1485, 2010.

13 Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

14 Clément Canonne and Ronitt Rubinfeld. Testing probability distributions underlying aggregated data. In *International Colloquium on Automata, Languages, and Programming*, pages 283–295. Springer, 2014.

15 Clément L Canonne. A survey on distribution testing: Your data is big. but is it blue? *Theory of Computing*, pages 1–100, 2020.

16 Nai-Hui Chia, András Gilyén, Tongyang Li, Han-Hsuan Lin, Ewin Tang, and Chunhao Wang. Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing quantum machine learning. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 387–400, 2020.

17 Toby Cubitt and Ashley Montanaro. Complexity classification of local hamiltonian problems. *SIAM Journal on Computing*, 45(2):268–316, 2016.

18 Constantinos Daskalakis, Gautam Kamath, and John Wright. Which distribution distances are sublinearly testable? In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2747–2764. SIAM, 2018.

19 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.

20 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.

21 Martin Furer, Oded Goldreich, Yishay Mansour, Michael Sipser, and Stathis Zachos. On completeness and soundness in interactive proof systems. *Advainces in Computing Research: A Research Annual,*, 5:429–442, 1989.

22 Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 59–68, 1986.

23 Alex B. Grilo. Private communication, 2020.

24 Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

25 Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. In search of an easy witness: Exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002.

26 Dominik Janzing, Pawel Wocjan, and Thomas Beth. "non-identity-check" is QMA-complete. *International Journal of Quantum Information*, 3(03):463–473, 2005.

27 Stephen P Jordan. Strong equivalence of reversible circuits is coNP-complete. *Quantum Information & Computation*, 14(15-16):1302–1307, 2014.

28 Alastair Kay. Tutorial on the quantikz package. *arXiv preprint arXiv:1809.03842*, 2018.

29 Alexei Kitaev. Quantum NP. *Talk at AQIP*, 99, 1999.

30 Alexei Y. Kitaev, Alexander Shen, and Mikhail N. Vyalyi. *Classical and quantum computation*. American Mathematical Soc., 2002.

31 Adam R Klivans and Dieter van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5):1501–1526, 2002.

32 Peter Bro Miltersen and N Variyam Vinodchandran. Derandomizing arthur–merlin games using hitting sets. *Computational Complexity*, 14(3):256–279, 2005.

33 Tomoyuki Morimae and Harumichi Nishimura. Merlinization of complexity classes above bqp. *Quantum Information & Computation*, 17(11-12):959–972, 2017.

34 Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

35 Ronitt Rubinfeld and Rocco A Servedio. Testing monotone high-dimensional distributions. *Random Structures & Algorithms*, 34(1):24–44, 2009.

36 Amit Sahai and Salil Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM (JACM)*, 50(2):196–249, 2003.

37 Yu Tanaka. Exact non-identity check is NQP-complete. *International Journal of Quantum Information*, 8(05):807–819, 2010.

38 Ewin Tang. A quantum-inspired classical algorithm for recommendation systems. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 217–228, 2019.

39 Ramgopal Venkateswaran and Ryan O'Donnell. Quantum approximate counting with nonadaptive grover iterations. In Markus Bläser and Benjamin Monmege, editors, *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, March 16-19, 2021, Saarbrücken, Germany (Virtual Conference)*, volume 187 of *LIPIcs*, pages 59:1–59:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

40 Ilya Volkovich. The untold story of SBP. In *International Computer Science Symposium in Russia*, pages 393–405. Springer, 2020.

41 John Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 537–546. IEEE, 2000.

42 Thomas Watson. The complexity of estimating min-entropy. *Computational Complexity*, 25(1):153–175, 2016.

A Missing proofs

A.1 Proof of Proposition 19: cStoqMA $\subseteq$ MA

Proof of Proposition 19. Given a cStoqMA verifier V_x on $n = n' + n_0 + n_w$ qubits where n' is the number of qubits of a witness, we construct a new MA verifier $\tilde{V}_x$ on $n = n' + n_0 + n_w$ qubits: first run the verification circuit V_x (without measuring the output qubit), then apply an X gate on the output qubit, after that run the verification circuit's inverse $V_x^\dagger$, finally measure the first $n' + n_0$ qubits in the computational basis; $\tilde{V}_x$ accepts iff the first n' bits of the measurement outcome is exactly $s_1 \cdots s_{n'}$ and the remained bits are all zero.

We then calculate the acceptance probability of a classical witness $|s\rangle$ of a cStoqMA verifier V_x, where $w = w_1 \cdots w_{n'} \in \{0,1\}^{n'}$. Notice $|+\rangle\langle+| = \frac{1}{2}(I + X)$, we obtain

$$\begin{aligned}\Pr\left[V_x \text{ accepts } s\right] &= \| \,|+\rangle\langle+|_1 \, V_x |s\rangle \left|\bar{0}\right\rangle \left|\bar{+}\right\rangle \|_2^2 \\ &= \frac{1}{2} + \frac{1}{2} \langle s| \left\langle\bar{0}\right| \left\langle\bar{+}\right| V_x^\dagger \left(X \otimes I_{n-1}\right) V_x |s\rangle \left|\bar{0}\right\rangle \left|\bar{+}\right\rangle .\end{aligned} \tag{8}$$

By a direct calculation, the acceptance probability of a classical witness $|s\rangle$ of $\tilde{V}_x$:

$$\Pr\left[\tilde{V}_x \text{ accepts } s\right] = \langle R|R\rangle \text{ where } |R\rangle := \left(\langle s| \left\langle\bar{0}\right| \otimes I_{n_+}\right) V_x^\dagger \left(X \otimes I_{n-1}\right) V_x |s\rangle \left|\bar{0}\right\rangle \left|\bar{+}\right\rangle . \tag{9}$$

It is evident that $|R\rangle$ is a subset state and $\text{supp}(|R\rangle) \subseteq \{0,1\}^{n_+}$. Together with Equations (8) and (9), we have completed the proof by noticing $\Pr[V_x \text{ accepts } s] = \frac{1}{2} + \frac{1}{2}\langle\bar{+}|R\rangle = \frac{1}{2} + \frac{1}{2}\langle R|R\rangle = \frac{1}{2} + \frac{1}{2}\Pr\left[\tilde{V}_x \text{ accepts } s\right]$. ◀

Could we extend Proposition 19 from a classical witness to a probabilistic witness $\sum_{s_i}\sqrt{D(i)}\,|s_i\rangle$ with a polynomial-size support[10]? Notice that the crucial equality $\langle\bar{+}|\,|R\rangle = \langle R|R\rangle$ utilized in Proposition 19 does not hold anymore, we need *an efficient evaluation algorithm* calculating $D(i)$ given an index i. Moreover, we have to calculate each coordinate's contribution on the acceptance probability *separately*, so the accumulated additive error is still supposed to be inverse-polynomial, which indicates the support size of this probabilistic witness is *negligible* for some polynomial.

A.2 Classical witness is not optimal for any StoqMA_1 verifier

▶ **Proposition 27.** *Classical witness is not optimal for any* StoqMA_1 *verifier.*

Proof. Consider a StoqMA_1 verifier V_x that uses only identity gates, then

(1) For all classical witness $s_i \in \{0,1\}^{n_w}$, $\Pr[V_x \text{ accepts } s_i] = \frac{1}{2}$ since $\langle R_0|R_1\rangle = 0$ where the resulting state before the measurement is $|0\rangle \otimes |R_0\rangle + |1\rangle \otimes |R_1\rangle$.

(2) For any classical witness $s_i, s_j \in \{0,1\}^{n_w}$ such that s_i and s_j are identical except for the first bit, one can construct a witness $|s\rangle = \frac{1}{\sqrt{2}}|s_i\rangle + \frac{1}{\sqrt{2}}|s_j\rangle$, $\Pr[V_x \text{ accepts } s] = 1$ since $\langle R_0|R_1\rangle = 1$.

We thus conclude that classical witness is not optimal for this StoqMA_1 verifier. ◀

A.3 Proof of Proposition 23: Exact RCD is NP-complete

Proof of Proposition 23. Exact RCD is NP-hard, namely $\mathsf{NP} \subseteq \mathsf{StoqMA}(1, 1/2)$, straightforwardly follows from the proof of Proposition 36. It suffices to prove that the exact RCD is in NP. By Theorem 22, $(2\alpha-1, 0)$-RCD is $\mathsf{StoqMA}(\alpha, 1/2)$-complete. Let $|w\rangle$ be an n_w-qubit non-negative witness such that $|w\rangle := \sum_{s_i \in \text{supp}(w)} \sqrt{D_w(s_i)}\,|s_i\rangle$, then $\Pr[V_x \text{ accepts } |w\rangle] = \frac{1}{2} + \frac{1}{2}\langle R_0|R_1\rangle = \frac{1}{2} + \frac{1}{2}\langle w|\langle\bar{0}|\langle\bar{+}|C_0^\dagger C_1|w\rangle|\bar{0}\rangle|\bar{+}\rangle$.

For *yes* instances, note that $\langle R_0|R_1\rangle = 2\alpha - 1$ and $\alpha > 1/2$, we have derived

$$\langle R_0|R_1\rangle = \sum_{s_i,s_j \in \text{supp}(w)} \sum_{r,r' \in \{0,1\}^{n_+}} \frac{\sqrt{D_w(s_i)D_w(s_j)}}{2^{n_+}} \langle s_i|\langle\bar{0}|\langle r|C_0^\dagger C_1|s_j\rangle|\bar{0}\rangle|r'\rangle > 0. \tag{10}$$

Since $\forall s_i, s_j$, $D_w(s_i)D_w(s_j) \geq 0$, there exists $s_i, s_j \in \text{supp}(w)$ and $r, r' \in \{0,1\}^{n_+}$ such that

$$\langle s_i|\langle\bar{0}|\langle r|C_0^\dagger C_1|s_j\rangle|\bar{0}\rangle|r'\rangle = 1. \tag{11}$$

For *no* instances, combining $\langle R_0|R_1\rangle = 0$ and Equation (10), it infers

$$\forall s_i, s_j \in \text{supp}(w), \forall r, r' \in \{0,1\}^{n_+}, \langle s_i|\langle\bar{0}|\langle r|C_0^\dagger C_1|s_j\rangle|\bar{0}\rangle|r'\rangle = 0. \tag{12}$$

We eventually construct an NP verifier as follows. The input is the classical description of two reversible circuits C_0 and C_1, and the witness is two pairs of binary strings (s_0, r_0) and (s_1, r_1). The verifier accepts iff $C_0(s_0, 0^{n_0}, r_0)$ and $C_1(s_1, 0^{n_0}, r_1)$ are identical where $C_i (i = 0, 1)$ takes $(s_i, 0^{n_0}, r_i)$ as an input and permutes it as the output. Notice these strings s_0, r_0, s_1, r_1 exists for *yes* instances owing to Equation (11), whereas they do not exist for *no* instances due to Equation (12), which achieves the proof. ◀

[10] Such witnesses are clearly easy witnesses, but not all easy witnesses have polynomial-bounded size support. See the explicit construction in Section 3.2 as an example.

A.4 StoqMA without any ancillary random bit is in NP

▶ **Proposition 28.** StoqMA *without any ancillary random bit is* NP*-complete.*

Proof. It suffices to show that StoqMA without any ancillary random bit (viz. ancillary qubits which is initially $|+\rangle$) is in NP. As a straightforward corollary of Theorem 22, distinguishing reversible circuits without $|+\rangle$ ancillary qubit is complete for StoqMA without $|+\rangle$ ancillary qubit, which is essentially NP according to Section 2.2.

Consider reversible circuits C_0 and C_1 act on $n_w + n_0$ qubits where n_0 is the number of $|0\rangle$ ancillary qubits, we observe that if C_0 and C_1 are not distinguishable with respect to any classical witness, then $\exists s \in \{0,1\}^{n_w}, \langle s| \langle\bar{0}| C_0^\dagger C_1 |s\rangle |\bar{0}\rangle = 1$ since reversible circuits C_0 and C_1 are bijections. Otherwise, it is evident that $\forall w, \langle w| \langle\bar{0}| C_0^\dagger C_1 |w\rangle |\bar{0}\rangle = 0$ provided C_0 and C_1 are distinguishable with respect to any witness. It is thus sufficient to only consider classical witnesses for distinguishing C_0 and C_1, namely, classical witness is optimal.

Now we provide an NP verifier. The input is the classical description of two reversible circuits C_0 and C_1, and the witness is a n_w-bit string s. The verifier accepts iff $C_0(s, 0^{n_0})$ is identical to $C_1(s, 0^{n_0})$. Note by inspection, the analysis is completed by above showing classical witness is optimal, which finishes the proof. ◀

By analogous reasoning, we provide an alternating proof of [27] with respect to the variant of RCD defined in Remark 21.

▶ **Proposition 29.** *Equivalence check of reversible circuits without any ancillary random bit is* co-NP*-complete.*

Proof. Consider reversible circuits C_0, C_1 act on $n_w + n_0$ qubits, we observe that if C_0 and C_1 are not exactly equivalent, then $\exists s \in \{0,1\}^{n_w}, \langle s| \langle\bar{0}| C_0^\dagger C_1 |s\rangle |\bar{0}\rangle = 0$ since reversible circuits C_0 and C_1 are essentially bijections. Otherwise, it is evident that $\forall w, \langle w| \langle\bar{0}| C_0^\dagger C_1 |w\rangle |\bar{0}\rangle = 1$ provided C_0 and C_1 are exactly equivalent. Therefore, classical witness is optimal, and the remained proof follows from the proof of Proposition 28. ◀

B $\mathrm{SetCSP}_{0,1/\mathrm{poly}}$ is StoqMA_1-complete

We start from the definition of SetCSP with frustration:

▶ **Definition 30** (k-$\mathrm{SetCSP}_{\epsilon_1,\epsilon_2}$, adapted from Section 4.1 in [3]). *Given a sequence of k-local set-constraints $C = (C_1, \cdots, C_m)$ on $\{0,1\}^n$, where k is a constant, n is the number of variables, and m is a polynomial of n. A set-constraint C_i acts on k distinct elements of $[n]$, and it consists of a collection $Y(C_i) = \{Y_1^{(i)}, \cdots, Y_{l_i}^{(i)}\}$ of disjoint subsets $Y_j^{(i)} \subseteq \{0,1\}^k$. Promise that one of the following holds, decide whether*

- **Yes***: There exists a subset $S \subseteq \{0,1\}^n$ s.t.* $\text{set-unsat}(C,S) \leq \epsilon_1(n)$*;*
- **No***: For any subset $S \subseteq \{0,1\}^n$,* $\text{set-unsat}(C,S) \geq \epsilon_2(n)$*,*

where ϵ_1 and ϵ_2 are efficiently computable function and $\epsilon_2 - \epsilon_1 \geq 1/\mathrm{poly}(n)$.

Now we briefly define a SetCSP instance C's frustration. We leave the formal definition in Proposition 34. The frustration of a set-constraint C regarding a subset S is $\text{set-unsat}(C,S) = \frac{1}{m}\sum_{i=1}^m \text{set-unsat}(C_i,S) = \frac{1}{m}\sum_{i=1}^m \left(\frac{|B_i(S)|}{|S|} + \frac{|L_i(S)|}{|S|}\right)$, where $B_i(S)$ is the set of bad strings of C_i, namely $\forall s \in B_i(S)$, $s|_{\mathrm{supp}(C_i)} \notin \cup_{j=1}^{l_i} Y_j^{(i)}$; And $L_i(S)$ is the set of longing strings of the subset S regarding C_i.

We will prove Theorem 31 in the remainder of this section.

▶ **Theorem 31.** $\mathrm{SetCSP}_{\mathrm{negl},1/\mathrm{poly}}$ *is* $\mathsf{StoqMA}_{1-\mathrm{negl}}$*-complete.*

B.1 $\text{SetCSP}_{\text{negl},1/\text{poly}}$ is StoqMA$(1 - \text{negl}, 1/\text{poly})$-hard

To prove Theorem 31, we will first show that $\text{SetCSP}_{0,1/\text{poly}}$ is StoqMA_1-hard.

▶ **Proposition 32** (SetCSP is hard for StoqMA$(1-\text{negl}, 1/\text{poly})$)**.** *For any super-polynomial $q(n)$ and polynomial $q_1(n)$, there exists a polynomial $q_2(n)$ such that* $\text{SetCSP}_{1/q(n),1/p_2(n)}$ *is hard for* $\mathsf{StoqMA}\left(1-1/q(n), 1/p_1(n)\right)$*.*

Proof. The $\mathsf{StoqMA}\left(1-1/q(n), 1/p_1(n)\right)$-hardness proof is straightforwardly analogous to the circuit-to-Hamiltonian construction used in MA-hardness proof of SetCSP in [3]. The only difference is replacing $Y(C^{\text{out}}) = \{\{00\},\{01\},\{11\}\}$ by $Y(C^{\text{out}}) = \{\{00\},\{01\},\{10,11\}\}$ in Section 4.4.2, since the final measurement on the $(T+1)$-qubit is on the Hadamard basis instead of the computational basis. The rest of the proof follows from an inspection of Section 4.4 in [3]. ◀

Then Corollary 33 is an immediate corollary of Proposition 32 by substituting 0 for $1/q(n)$:

▶ **Corollary 33.** $\text{SetCSP}_{0,1/\text{poly}}$ *is* StoqMA_1*-hard.*

B.2 $\text{SetCSP}_{a,b}$ is in StoqMA$(1 - a/2, 1 - b/2)$

It now remains to show a StoqMA_1 containment of $\text{SetCSP}_{0,1/\text{poly}}$. We will complete the proof by mimicking the StoqMA containment of the stoquastic local Hamiltonian problem in Section 4 in [9]. The starting point is an alternating characterization of the frustration of a set-constraint C_i in a SetCSP instance C. The proof of Proposition 34 is deferred in the end of this section.

▶ **Proposition 34** (Local matrix associated with set-constraint)**.** *For any k-local set-constraint $C_i (1 \leq i \leq m)$, given a subset $S \subseteq \{0,1\}^n$, the frustration*

$$\text{set-unsat}(C_i, S) = 1 - \sum_{j=1}^{|Y(C_i)|} \sum_{x,y \in Y_j^{(i)}} \tfrac{1}{|Y_j^{(i)}|} \langle S| \left(|x\rangle \langle y| \otimes I_{n-k}\right) |S\rangle.$$

Now we state the StoqMA containment of SetCSP, as Lemma 35.

▶ **Lemma 35.** *For any* $0 \leq a < b \leq 1$, $\text{SetCSP}_{a,b} \in \mathsf{StoqMA}\left(1-a/2, 1-b/2\right)$*. Moreover, for a subset $S \subseteq \{0,1\}^n$ such that $S = \text{argmin}_{S'}\, \text{set-unsat}(C, S')$, the subset state $|S\rangle$ is an optimal witness of the resulting* StoqMA *verifier.*

The proof of Lemma 35 tightly follows from Section 4 in [9]. We here provide a somewhat simplified proof using the SetCSP language by avoiding unnecessary normalization.

Proof of Lemma 35. Given a $\text{SetCSP}_{a,b}$ instance $C = (C_1, \cdots, C_m)$. For each set-constraint $C_i (1 \leq i \leq m)$, we first construct a local Hermitian matrix M_i preserves the frustration, then construct a family of StoqMA verifiers for such a M_i. For any set-constraint C_i, we obtain a k-local matrix M_i by Proposition 34 such that for any subset $S \subseteq \{0,1\}^n$:

$$\text{set-unsat}(C_i, S) = 1 - \langle S| M_i \otimes I_{n-k} |S\rangle \text{ where } M_i = \sum_{j=1}^{|Y(C_i)|} \sum_{x,y \in Y_j^{(i)}} \frac{1}{|Y_j^{(i)}|} |x\rangle \langle y|. \quad (13)$$

Moreover, for a set $Y_j^{(i)}$ of strings associated with the set-constraint C_i, we further have

$$\begin{aligned}\sum_{x,y\in Y_j^{(i)}} |x\rangle\langle y| &= \sum_{x\in Y_j^{(i)}} |x\rangle\langle x| + \frac{1}{2}\sum_{x\neq y\in Y_j^{(i)}} \left(|x\rangle\langle y| + |y\rangle\langle x|\right)\\ &= \sum_{x\in Y_j^{(i)}} V_x |0\rangle\langle 0|^{\otimes k} V_x^\dagger + \frac{1}{2}\sum_{x\neq y\in Y_j^{(i)}} V_{x,y}\left(X\otimes|0\rangle\langle 0|^{\otimes k-1}\right)V_{x,y}^\dagger,\end{aligned} \tag{14}$$

where V_x is a depth-1 reversible circuit with X such that $\forall x, |x\rangle = U_x\left|0^k\right\rangle$, and $V_{x,y}$ is a $O(k)$-depth reversible circuit with CNOT and X such that $\forall x, y, U_{x,y}\left|0^k\right\rangle\left|10^{k-1}\right\rangle U_{x,y}^\dagger$.

Notice that the resulting local observables in Equation (14) are either $|0\rangle\langle 0|^{\otimes k}$ (i.e. a single-qubit computational-basis measurement) or $X\otimes|0\rangle\langle 0|^{\otimes k-1}$ (i.e. a single-qubit Hadamard-basis measurement). To construct a StoqMA verifier, we only allow local observables in form $X\otimes I^{\otimes O(k)}$. Namely, we are supposed to simulate a computational-basis measurement by ancillary qubits and a Hadamard-basis measurement, which is achieved by Proposition 36.

▶ **Proposition 36** (Adapted from Lemma 3 in [9]).

(1) *For any integer k, there exists an $O(k)$-depth reversible circuit W using k $|0\rangle$ ancillary qubits and a $|+\rangle$ ancillary qubits s.t.*

$$\forall|\psi\rangle, \langle\psi|\,|0\rangle\langle 0|^{\otimes k}|\psi\rangle = \langle\psi|\langle 0|^{\otimes k}\langle +|W^\dagger\left(X\otimes I^{\otimes 2k}\right)W|\psi\rangle|0\rangle^{\otimes k}|+\rangle.$$

(2) *For any integer k, there exists an $O(k)$-depth circuit V using $k-1$ $|0\rangle$ ancillary qubits s.t.*

$$\forall|\psi\rangle, \langle\psi|X\otimes|0\rangle\langle 0|^{\otimes k-1}|\psi\rangle = \langle\psi|\langle 0|^{\otimes k-1}W^\dagger\left(X\otimes I^{\otimes 2k-2}\right)W|\psi\rangle|0\rangle^{\otimes k-1}.$$

It is worthwhile to mention that the gadgets used in the proof (see Section A.4 in [9]) further provide proof of MA ⊆ StoqMA that preserves both completeness and soundness parameters.

Let $\mathrm{Idx}(C_i)$ be the set of indices, and let $\alpha_{(j,x,y)}$ be the weight of an index (j,x,y),

$$\begin{aligned}\mathrm{Idx}(C_i) &:= \left\{(j,x,y): 1\leq j\leq |Y_i(C)|, (x,y)\in\binom{Y_j^{(i)}}{2}\sqcup\left\{(x,x): x\in Y_j^{(i)}\right\}\right\};\\ \alpha_{(j,x,y)} &:= \frac{1}{(1+\mathbb{I}(x\neq y))m|Y_j^{(i)}|}, \text{ where the indicator } \mathbb{I}(x\neq y)) = 1 \Leftrightarrow x\neq y.\end{aligned}$$

Plugging Proposition 36 and Equation (14) into Equation (13), we have derived

$$1-\text{set-unsat}(C_i,S) = \sum_{l\in\mathrm{Idx}(C_i)} \alpha_l\langle S|\left(\langle 0|^{\otimes k}\langle +|U_k^\dagger\left(X\otimes I^{\otimes 2k}\right)U_k|0\rangle^{\otimes k}|+\rangle\right)\otimes I_{n-k}|S\rangle. \tag{15}$$

For a SetCSP instance $C=(C_1,\cdots,C_m)$, by Equation (15), by substituting $|+\rangle\langle +| = \frac{1}{2}(X+I)$ into Equation (15), we thus arrive at a conclusion that

$$\Pr\left[V_x \text{ accepts } |S\rangle\right] = \frac{1}{m}\sum_{i=1}^m\left(1-\frac{1}{2}\cdot\text{set-unsat}(C_i,S)\right) = 1-\frac{1}{2}\cdot\text{set-unsat}(C,S). \tag{16}$$

Note that the set of StoqMA verifiers V_x with the same number of input qubits and witness qubits is linear, namely a convex combination of l StoqMA verifiers $(V_1,p_1),\cdots,(V_l,p_l)$ can be implemented by additional $|+\rangle$ ancillary qubits and controlled $V_i(1\leq i\leq l)$. Therefore, by Equation (16), we conclude that $\forall a,b$, $\text{SetCSP}_{a,b}$ is in StoqMA $(1-a/2, 1-b/2)$. ◀

Finally, we achieve proof of Proposition 34:

Proof of Proposition 34. Given a k-local set-constraint C_i, the set of good strings $G_i = \sqcup_{1\leq j\leq |Y(C_i)|} Y_j^{(i)}$, and the set of bad strings $B_i = \{0,1\}^{|J(C_i)|} \setminus G_i$. Also, for any subset $S\{0,1\}^n$, the set of bad strings in S is $B_i(S)$. By direction calculation, notice that

$$\frac{|B_i(S)|}{|S|} = \langle S| \left(\sum_{x\in B_i} |x\rangle \langle x| \otimes I_{n-k} \right) |S\rangle$$
$$\sum_{j=1}^{|Y(C_i)|} \frac{|L_j^{(i)}(S)|}{|S|} = \langle S| \left(\sum_{x\in G_i} |x\rangle \langle x| \otimes I_{n-k} \right) |S\rangle - \sum_{j=1}^{|Y(C_i)|} \sum_{x,y\in Y_j^{(i)}} \frac{1}{|Y_j^{(i)}|} \langle S| \left(|x\rangle \langle y| \otimes I_{n-k}\right) |S\rangle. \tag{17}$$

Plugging Equation (17) and $\{0,1\}^{|J(C_i)|} = B_i \sqcup G_i$ into set-unsat$(C_i, S) = \frac{|B_i(S)|}{|S|} + \sum_{j=1}^{|Y(C_i)|} \frac{|L_j^{(i)}(S)|}{|S|}$, we then finish the proof. ◀