StoqMA meets distribution testing

Yupan Liu

TQC 2021

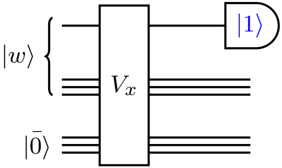
arXiv:2011.05733

A "quantum" definition of NP

Consider $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in \mathrm{NP}$, there is a verifier such that for any input $x \in \mathcal{L}$, a polynomial-time verification circuit V_x such that

- Yes: If $x \in \mathcal{L}_{yes}$, $\exists |w\rangle$ such that V_x accepts $|w\rangle$;
- No: If $x \in \mathcal{L}_{no}$, $\forall |w\rangle$, we have V_x rejects $|w\rangle$.

"Quantize" the definition: Viewed V_x as a *quantum circuit*



- ◇ Verification circuit using only classical reversible gates (i.e. Toffoli, CNOT, X).
- ◇ Measure the designated output qubit in the $\{|0\rangle, |1\rangle\}$ basis.

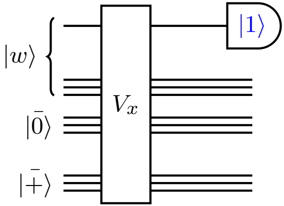
Acceptance probability $\Pr[V_x \text{ accepts } |w\rangle] = \| |1\rangle\langle 1|_1 V_x |w\rangle |\bar{0}\rangle \|_2^2$

Remark on equivalence. The optimal witness is classical witness (since the matrix $\langle \bar{0}| \left(V_x^\dagger |1\rangle\langle 1|_1 V_x \right) |\bar{0}\rangle$ is diagonal), so it is equivalent to standard def. .

A "quantum" definition of MA: adding randomness

Consider $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in$ MA, there is a verifier such that for any input $x \in \mathcal{L}$, a *randomized* polynomial-time verification circuit V_x such that

- Yes: If $x \in \mathcal{L}_{yes}$, $\exists |w\rangle$ such that $\Pr[V_x \text{ accepts } |w\rangle] \geq 2/3$;
- No: If $x \in \mathcal{L}_{no}$, $\forall |w\rangle$, we have $\Pr[V_x \text{ accepts } |w\rangle] \leq 1/3$.



◇ Ancillary qubits $|\bar{+}\rangle$ corresponds to ancillary *random* bits.

◇ **Acceptance probability**

$\Pr[V_x \text{ accepts } |w\rangle]$

$= \| |1\rangle\langle 1|_1 V_x |w\rangle |\bar{0}\rangle |\bar{+}\rangle \|_2^2.$

Remark: Error reduction for MA

Theorem. For any threshold parameters $0 \leq a, b \leq 1$ such that $a - b \geq \frac{1}{\mathrm{poly}(n)}$:

$$\mathsf{MA}(a,b) \subseteq \mathsf{MA}(1-2^{-n}, 2^{-n}) \subseteq \mathsf{MA}(2/3, 1/3).$$

Proof Sketch. Running (polynomially many) copies of the verifier in parallel, and taking the *majority vote* of the *measurement outcomes*. □

The weird class StoqMA [BBT06]

Consider $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in$ StoqMA, there is a verifier such that for any input $x \in \mathcal{L}$, a randomized polynomial-time verification circuit V_x that measures the designated output qubit in the $\{|+\rangle, |-\rangle\}$ basis such that

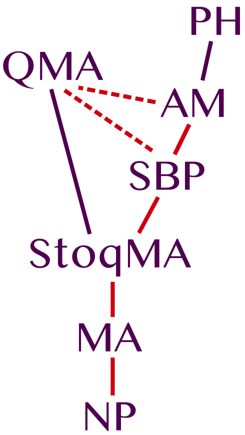
- Yes: If $x \in \mathcal{L}_{yes}$, $\exists |w\rangle$ such that $\Pr[V_x \text{ accepts } |w\rangle] \geq a$;
- No: If $x \in \mathcal{L}_{no}$, $\forall |w\rangle$, we have $\Pr[V_x \text{ accepts } |w\rangle] \leq b$; where $1 \geq a > b \geq 1/2$ and $a - b \geq 1/\mathrm{poly}(n)$.

Acceptance probability $\Pr[V_x \text{ accepts } |w\rangle] = \| |+\rangle\langle+|_1 V_x |w\rangle |\bar{0}\rangle |\bar{+}\rangle \|_2^2$

Remarks on the weirdness

- Threshold parameters a, b *cannot* be replaced by some constants since *error reduction for* StoqMA *remains unknown* since [BBT06].
- For any non-negative witness, it is evident that $\Pr[V_x \text{ accepts } w] \geq 1/2$.
- Owing to Perron-Frobenius theorem, the optimal witness is non-negative state. W.L.O.G. we can think the witness as **a probability distribution**!

The computational power of StoqMA



- Stoquastic (i.e. *sign problem* free) local Hamilton. problem is StoqMA-complete [BBT06].
- Complexity classification of 2-LHP [CM13,BH14]: P, NP-complete, StoqMA-complete, or QMA-complete.
  Schaefer's theorem CSP over $\mathbb{F}_2$ is either in P or NP-complete.
- StoqMA contains MA: simulating a single-qubit $\{|0\rangle, |1\rangle\}$ basis measurement by a $\{|+\rangle, |-\rangle\}$ basis measurement with an ancillary qubit.
- AM (*essentially* SBP) contains StoqMA: *Set lower bound protocol* [GS86], where AM is a two-message randomized generalization of NP.
- $\mathrm{StoqMA}_1 = \mathrm{MA}$ [BBT06,BT09].
- Under derandomization assumptions [KvM02,MV05], AM *collapses* to NP: $\mathrm{MA} = \mathrm{StoqMA} = \mathrm{SBP}$.

Q: Is it possible to collapse the hierarchy $\mathrm{MA} \subseteq \mathrm{StoqMA} \subseteq \mathrm{SBP}$?

1. What is the complexity class StoqMA?
2. StoqMA: a distribution testing lens
3. Distinguishing reversible circuits is StoqMA-complete
4. Towards error reduction for StoqMA
5. Open problems

1. What is the complexity class StoqMA?
2. StoqMA: a distribution testing lens
   - Proving StoqMA $\subseteq$ MA by taking samples (and failed)
   - eStoqMA $\subseteq$ MA: taking both samples and queries
3. Distinguishing reversible circuits is StoqMA-complete
4. Towards error reduction for StoqMA
5. Open problems

Distribution testing in a nutshell

Definition: Sample Access

Let D be a fixed distribution over Ω. A sampling oracle for D is an oracle S_D: when queried, S_D returns an element $x \in \Omega$ with probability $D(x)$.

Task: Tolerant Testing

Given independent (sample) oracle accesses to D_0, D_1 (both unknown), decide whether they are ϵ_1-close or ϵ_2-far from each other.

Theorem: Sample Complexity Lower Bound for Tolerant Testing in d_H^2

(A corollary of Theorem 9 in [DKW18])

There is a constant $\epsilon > 0$ such that any algorithm for distinguishing $d_H^2(D_0, D_1) \leq \epsilon^2/8$ (close) from $d_H^2(D_0, D_1) \geq \epsilon^2/2$ (far), requires $\Omega(N/\log N)$ samples, where the square Hellinger distance $d_H^2(D_0, D_1) := \frac{1}{2}\sum_{i\in[N]}\left(\sqrt{D_0(i)} - \sqrt{D_1(i)}\right)^2 = 1 - \langle D_0 | D_1 \rangle$.

Measuring a non-negative state in the Hadamard basis, revisited

First (failed) attempt: proving StoqMA $\subseteq$ MA by distribution testing

Given the state $|0\rangle|D_0\rangle + |1\rangle|D_1\rangle := V_x|w\rangle|\bar{0}\rangle|\bar{+}\rangle$ (before the measurement), measure the designated output qubit in the $\{|+\rangle, |-\rangle\}$ basis:

$\| |+\rangle\langle+|_1 (|0\rangle|D_0\rangle + |1\rangle|D_1\rangle)\|_2^2 = \frac{1}{2} + \langle D_0|D_1\rangle = 1 - d_H^2(D_0, D_1)$,

where $|D_k\rangle = \sum_i \sqrt{D_k(i)}|i\rangle$ for $k = 0,1$ and $\langle D_0|D_0\rangle + \langle D_1|D_1\rangle = 1$.

- It suffices to approximate the squared Hellinger distance $d_H^2(D_0, D_1)$ within $1/\mathrm{poly}(n)$ accuracy using only $\mathrm{poly}(n)$ sample accesses to D_0, D_1.
- Proving MA containment by distribution testing!

◇ Bad news: This "MA containment" requires *exponentially* many samples. ☹

◇ Good news: We probably could take advantage of other models! ☺

From dual access model to easy witness

Dual (query+sample) access model

- Sample access to D: Run a copy of V_x that takes $|w\rangle$ as an input, measure all qubits in the $\{|0\rangle, |1\rangle\}$ basis, then viewed the measurement outcome $i \in \{0,1\}^n$ as a sample.
- Query access to (D_0, D_1): Given an index $j \in \{0,1\}^{n-1}$, algorithm Q_D evaluates $D_0(j)/D_1(j)$ efficiently, where $D_0(\cdot) := D(0||\cdot)$ and so does D_1.

Theorem [CR14]. Approximating the total variation distance $d_{TV}(D_0, D_1)$ within ϵ accuracy requires only $\Theta(1/\epsilon^2)$ accesses to the oracle.

StoqMA with easy witness (eStoqMA)

- **Easy witness**: given a witness state $|D\rangle$, there is an algo. Q_D such that the quotient $D_0(j)/D_1(j)$ can be evaluated efficiently for any index j.
  e.g. $|S\rangle = \sum_{i \in S} \frac{1}{\sqrt{|S|}} |i\rangle$ where S's membership is *efficiently verifiable*.
- eStoqMA's definition modified from StoqMA: For *yes* instance $x \in \mathcal{L}_{yes}$ where $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in$ eStoqMA, the witness must be easy witness.

eStoqMA = MA: Proof Sketch

Theorem. eStoqMA = MA.

Proof Sketch. Consider state $|0\rangle|D_0\rangle + |1\rangle|D_1\rangle := V_x|w\rangle|\bar{0}\rangle|\bar{+}\rangle$, then

$$\frac{\Pr[V_x \text{ accepts } |w\rangle]}{\|D_1\|_1} = \frac{\frac{1}{2}\| |D_0\rangle + |D_1\rangle \|_2^2}{\|D_1\|_1} = \mathop{\mathbb{E}}_{i \sim D_1/\|D_1\|_1} \left(1 + \frac{D_0(i)}{D_1(i)}\right)^2.$$

Note $D_0(i)/D_1(i)$ is evaluated by Q_D. By Chernoff bound, an empirical estimation infers $1/\mathrm{poly}(n)$ **additive error approx. of** $\Pr[V_x$ **accepts** $|w\rangle]$. □

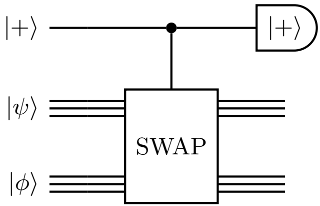
Corollary. $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$.

Proof. It is evident that $\mathsf{StoqMA}_1 \subseteq \mathsf{eStoqMA}_1$ since the easy witness is the subset state associated with the set that consists of all nodes that mark "good" on the configuration graph of a $\mathrm{SetCSP}_{0,1/\mathrm{poly}(n)}$ instance. □

Remark. *Guided Stoquastic Local Hamiltonian* [Bravyi15], which is contained in MA, can be viewed as a (generalized) Hamiltonian version of eStoqMA.

From SWAP test to Reversible Circuit Distinguishability

SWAP test [BCWdW01]



- SWAP test outputs 1 with prob. $|\langle\psi|\phi\rangle|^2$.
- Thinking $|\psi\rangle \otimes |\phi\rangle$ as a witness, then SWAP test looks like a trivial StoqMA verifier with maximum accept. prob. 1 (and the optimal witness is classical).

Reversible Circuit Distinguishability, $\mathrm{RCD}(a,b;n_+)$

Given efficient reversible circuits C_0, C_1 that utilizes ancillary states $|\bar{0}\rangle$ and $|\bar{+}\rangle$. Let non-negative states that generates by C_k $(k=0,1)$ and $|w\rangle$ be $|D_k\rangle := C_k |w\rangle |\bar{0}\rangle|\bar{+}\rangle$, decide which is the following cases:

- **Yes** (a-indistinguishable): $\exists |w\rangle$ s.t. $\langle D_0|D_1\rangle \geq a$;
- **No** (b-distinguishable): $\forall |w\rangle$, $\langle D_0|D_1\rangle \leq b$,

where $a - b \geq 1/\mathrm{poly}(n)$.

The computational complexity of distinguishing circuits

Theorem

Reversible Circuit Distinguishability, viz. $\mathrm{RCD}(\cdot,\cdot;\mathrm{poly})$, is StoqMA-complete.

- **Theorem [JWZ03].** Quantum Circuit Distinguishability is QMA-complete.
- **Theorem [Jordan14].** Reversible Circuit Distinguishability (without ancillary random bit), viz. $\mathrm{RCD}(\cdot,\cdot;0)$, is NP-complete.

$\star$ $\mathrm{RCD}(\cdot,\cdot;\mathrm{poly})$ *seems* MA-*complete but it is actually* StoqMA-*complete!*

Proposition 1

Exact Reversible Circuit Dist., viz. $\mathrm{RCD}(\cdot,0;\mathrm{poly})$, is NP-complete.

Corollary. StoqMA with perfect soundness is contained in NP.

- **Theorem [FGMSZ89]** Arthur-Merlin games with perfect soundness $\subseteq$ NP.
- **Theorem [Tanaka10]** Exact Quantum Circuit Distinguishability is NQP-complete, namely QMA with perfect soundness, which is as powerful as $\mathrm{coC_{=}P}$.

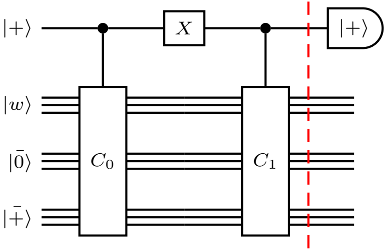
Proposition 2

RCD without ancillary random bit, viz. $\mathrm{RCD}(\cdot,\cdot;0)$, is NP-complete.

Reversible Circuit Distinguishability is StoqMA-complete: Proof Sketch

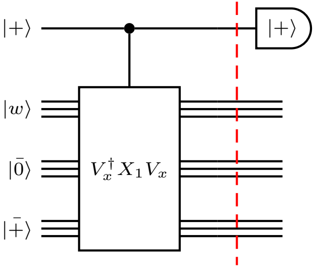
For $k = 0, 1$, let $|D_k\rangle := C_k |w\rangle |\bar{0}\rangle |\bar{+}\rangle$, then:

- $\mathrm{RCD}(a, b; \mathrm{poly})$ is contained in StoqMA$(\frac{1}{2} + \frac{a}{2}, \frac{1}{2} + \frac{b}{2})$.
  - ◇ Dash line: $\frac{1}{\sqrt{2}} |0\rangle |D_0\rangle + \frac{1}{\sqrt{2}} |1\rangle |D_1\rangle$.



- $\mathrm{RCD}(a, b; \mathrm{poly})$ is hard for StoqMA$(\frac{1}{2} + \frac{a}{2}, \frac{1}{2} + \frac{b}{2})$.
  - ◇ Set $C_0 := V_x^\dagger X_1 V_x$ and $C_1 := I$.
  - ◇ Let $M := \left\langle \bar{0} \right| \langle \bar{+} | V_x^\dagger X_1 V_x \left| \bar{0} \right\rangle |\bar{+}\rangle$, then $\Pr[V_x \text{ accepts } |w\rangle] = \frac{1}{2} + \frac{1}{2} \lambda_{\max}(M)$.

  Remark. This observation went back to (weak) error reduction for QMA [KSV02].



Why error reduction is important for StoqMA?

Conjecture: Error reduction for StoqMA

$\forall 1/2 \leq a, b \leq 1$ such that $a - b \geq 1/\mathrm{poly}(n)$, it holds that

$$\mathsf{StoqMA}(a,b) \subseteq \mathsf{StoqMA}\left(1-2^{-n}, \tfrac{1}{2}+2^{-n}\right).$$

Theorem (Soundness error reduction for StoqMA)

For any $l = \mathrm{poly}(n)$, $\mathsf{StoqMA}\left(\frac{1}{2}+\frac{a}{2}, \frac{1}{2}+\frac{b}{2}\right) \subseteq \mathsf{StoqMA}\left(\frac{1}{2}+\frac{a^{l(n)}}{2}, \frac{1}{2}+\frac{b^{l(n)}}{2}\right)$.

⋆ It suffices to reduce two-sided errors *separately* and *alternatively*, e.g., the polarization lemma of SZK [SV03] or space-efficient QMA error reduction [FKL+16].

Theorem [AGL20]: Error reduction implies StoqMA = MA

(Completeness) error reduction for StoqMA implies StoqMA $\subseteq$ MA.

Namely, $\mathsf{StoqMA}(1-1/p_1(n), 1-1/p_2(n)) \subseteq \mathsf{MA}$, where p_1 is a *super-polynomial* of n and p_2 is a polynomial of n.

Soundness error reduction for StoqMA

Theorem (restated)

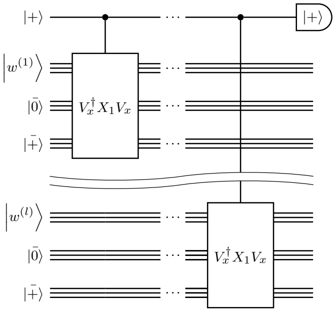
For any $l = \mathrm{poly}(n)$, StoqMA $\left(\frac{1}{2}+\frac{a}{2}, \frac{1}{2}+\frac{b}{2}\right) \subseteq$ StoqMA $\left(\frac{1}{2}+\frac{a^{l(n)}}{2}, \frac{1}{2}+\frac{b^{l(n)}}{2}\right)$.

Corollary. $\forall 1-a \geq 1/\mathrm{poly}(n)$, $l = \mathrm{poly}(n)$, StoqMA$(1, a) \subseteq$ StoqMA$(1, 2^{-l(n)})$.

Proof Sketch

Recall that $\Pr[V_x \text{ accepts } |w\rangle] = \frac{1}{2} + \frac{1}{2}\lambda_{\max}(M)$ where $M = \langle\bar{0}|\langle\bar{+}|V_x^\dagger X_1 V_x|\bar{0}\rangle|\bar{+}\rangle$.

Let us take the tensor product (i.e. "conjunction" or "AND") now:



- ◇ Maximum acceptance probability:
  $\Pr\left[V'_x \text{ accepts } w^{(1)} \otimes \cdots \otimes w^{(l)}\right]$
  $= \dfrac{1}{2} + \dfrac{1}{2}\lambda_{\max}(M^{\otimes l})$
  $= \dfrac{1}{2} + \dfrac{1}{2}\left(\lambda_{\max}(M)\right)^l$
- ◇ **Yes** case: ✓
- ◇ **No** case: Entangled witness will not increase the maximum acceptance probability. □

Conclusions and open problems

Take-home messages

1. The difficulty of StoqMA arisen from *different kinds of optimal witness*:

Witness Type	Results
Classical	$\mathsf{cStoqMA}(a,b) \subseteq \mathsf{MA}(2a-1,2b-1)$ [Grilo20]
Easy	$\forall a-b \geq 1/poly(n), \mathsf{eStoqMA}(a,b) \subseteq \mathsf{MA}(9/16,7/16)$
Non-negative	$\mathsf{StoqMA} \stackrel{?}{=} \mathsf{MA}$

2. *Soundness* error reduction for StoqMA is possible, and interestingly, the proof is inspired by showing distinguishing reversible circuits (RCD) is StoqMA-complete (*instead of* MA *as expected!*).

Open problems

1. StoqMA vs. MA and SBP vs. MA.
2. Completeness error reduction for StoqMA.
3. More (natural) StoqMA-complete problems.

Thank you!