The untold story of StoqMA

Yupan Liu

Hebrew University of Jerusalem $\rightarrow$?

Available at arXiv:2011.05733 and arXiv:2010.02835

Partially joint with Dorit Aharonov and Alex B. Grilo

YITP, Kyoto University (Virtually), Nov 2020

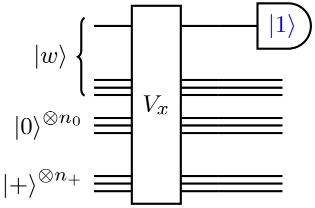
1. What is the complexity class StoqMA?
2. StoqMA: a distribution testing lens
3. Distinguishing reversible circuits
4. StoqMA vs. MA: the power of error reduction
5. Open problems

A "quantum" definition of MA

Consider a promise problem $\mathcal{L} = (\mathcal{L}_{yes}, \mathcal{L}_{no}) \in$ MA, there is a verifier such that for any input $x \in \mathcal{L}$, a uniformly generated verification circuit V_x such that

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

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



◇ Verification circuit using only classical reversible gates (i.e. Toffoli, CNOT, X).

◇ Measure the designed output qubit in the $\{|0\rangle, |1\rangle\}$ basis.

◇ Ancillary qubits $|+\rangle^{\otimes n_+}$ corresponds to randomized ancillary bits.

Acceptance probability $\Pr[V_x \text{ accepts } |w\rangle] = \| |1\rangle\langle 1|_1 V_x |w\rangle |0\rangle^{\otimes n_0} |+\rangle^{\otimes n_+} \|_2^2$

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

The weird class StoqMA

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

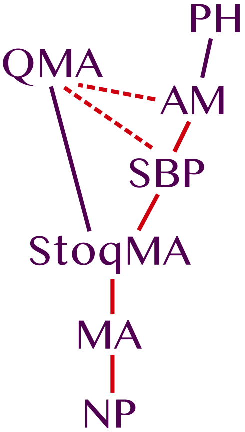
- Yes: If $x \in \mathcal{L}_{yes}$, $\exists |w\rangle$ such that $\Pr[V_x \text{ accepts } |w\rangle] \geq a$;
- No: If $x \in \mathcal{L}_{no}$, $\forall |w\rangle$, we have $\Pr[V_x \text{ accepts } |w\rangle] \leq b$; where $1 \geq a > b \geq 1/2$ and $a - b \geq 1/\text{poly}(n)$.

Acceptance probability $\Pr[V_x \text{ accepts } |w\rangle] = \| |+\rangle\langle+|_1 V_x |w\rangle |0\rangle^{\otimes n_0} |+\rangle^{\otimes n_+} \|_2^2$

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.
- StoqMA contains MA: simulating a single-qubit $\{|0\rangle, |1\rangle\}$ basis measurement by a $\{|+\rangle, |-\rangle\}$ basis measurement with ancillary qubits, viz. $\Pr\left[V_x^{(+)} \text{ accepts} |w\rangle\right] = \frac{1}{2} + \frac{1}{2}\Pr\left[V_x^{(0)} \text{ accepts} |w\rangle\right]$.
- AM (*essentially* SBP) contains StoqMA: *Set lower bound protocol* [GS86].
- $\text{StoqMA}_1 = \text{MA}$ [BBT06,BT09].
- Under derandomization assumptions [KvM02,MV05], AM *collapses* to NP: $\text{MA} = \text{StoqMA} = \text{SBP}$.

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

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 tolerant testing between D_0 and D_1 on $[N]$, namely distinguishing $d_H^2(D_0, D_1) \leq \epsilon^2/8$ from $d_H^2(D_0, D_1) \geq \epsilon^2/2$, requires $\Omega(N/\log N)$ samples, where the square Hellinger distance $d_H^2 := \frac{1}{2}\| \, |D_0\rangle - |D_1\rangle \, \|_2^2$.

Measuring non-negative states in the Hadamard basis, revisited

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

Given the state $|0\rangle|D_0\rangle + |1\rangle|D_1\rangle := V_x|w\rangle|0\rangle^{\otimes n_0}|+\rangle^{\otimes n_+}$ (before the measurement), measure the output qubit in the $\{|+\rangle, |-\rangle\}$ basis:

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

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 input, measure all qubits in the $\{|0\rangle, |1\rangle\}$ basis, then viewed the meas. outcome as a sample.
- Query access to D: Given an index i, alg. Q_D evaluates $D(i)$ efficiently.

Theorem [CR14]. Approximating the total variation distance $d_{TV}(D_0, D_1)$ with an error ϵ 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 algorithm Q_D such that the coordinate $D(i)$ can be evaluated efficiently for any index i.
  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.

Remark. Constant multiplicative error approximation of the cardinality of an efficient verifiable set is (informally) SBP-complete [Watson16,Vol20].

eStoqMA $=$ MA: proof sketch

Theorem. eStoqMA $=$ MA.

Proof Sketch. Consider state $|0\rangle|D_0\rangle + |1\rangle|D_1\rangle := V_x|w\rangle|0\rangle^{\otimes n_0}|+\rangle^{\otimes n_+}$, then

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

By Chernoff bound, an empirical estimation indicates $1/\mathrm{poly}(n)$ **additive error approximation of** $\Pr[V_x$ **accepts** $|w\rangle]$. □

Corollary. $\mathsf{StoqMA}_1 \subseteq$ 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 $\mathrm{SetCSP}_{0,1/\mathrm{poly}}$ instance (Def. is postponed). □

⋆ **Funny fact.** The proof technique of eStoqMA $\subseteq$ MA is also used in quantum inspired classical algorithm, such as [Tang19, CGLLTW20].

Remarks on StoqMA with classical witness (StoqCMA)

Proposition (Alex B. Grilo)

$\forall\ 1/2 \le b < a \le 1$, $\mathsf{StoqCMA}(a,b) \subseteq \mathsf{MA}(2a-1, 2b-1)$.

Proof Intuition. Notice $|+\rangle\langle+| = \frac{1}{2}(I+X)$, then for any $|\psi\rangle$,
$\langle\psi|V_x |+\rangle\langle+|_1 V_x^\dagger|\psi\rangle = \frac{1}{2} + \frac{1}{2}\langle\psi|V_x X_1 V_x^\dagger|\psi\rangle$. □

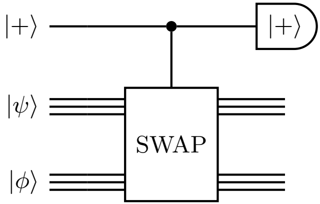
Corollary. PreciseStoqCMA = PreciseMA = $\mathsf{NP}^{\mathsf{PP}}$.
Corollary^2. $\mathsf{NP}^{\mathsf{PP}} \subseteq$ PreciseStoqMA $\subseteq$ PSPACE.

Remarks

- Classical witness is clearly easy witness, but *the opposite is not true*.
  Since preparing $|D\rangle$ from Q_D requires the postselection.
- Classical witness is not optimal for any StoqMA verifier, e.g. $V_x = I$.

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 $|0\rangle^{\otimes n_0}$ and $|+\rangle^{\otimes n_+}$. Let non-negative states that generates by C_k $(k=0,1)$ and $|w\rangle$ be $|D_k\rangle := C_k |w\rangle |0\rangle^{\otimes n_0} |+\rangle^{\otimes n_+}$, decide whether $\exists |w\rangle$ s.t. $\frac{1}{2}\| |D_0\rangle - |D_1\rangle \|_2^2 \geq a$; or $\forall |w\rangle$, $\frac{1}{2}\| |D_0\rangle - |D_1\rangle \|_2^2 \leq b$, 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 [Jor14].** Reversible Circuit Distinguishability (without randomized ancillary 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. $\mathrm{RCD}(a, 0; \mathrm{poly})$, is NP-complete.

Corollary. StoqMA with perfect soundness is contained in NP.

- **Theorem [FGMSZ89]** Arthur-Merlin games with perfect soundness $\subseteq$ NP.
- **Theorem [Tan10]** Exact Quantum Circuit Distinguishability is NQP-complete, namely QMA with perfect soundness.

Proposition 2

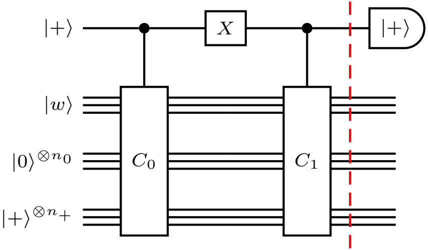
RCD without randomized ancillary bit, viz. $\mathrm{RCD}(\cdot, \cdot; 0)$, is NP-complete.

Corollary (Simplified proof of [Jor14]). $\mathrm{RCD}(\cdot, \cdot; 0)$ is NP-complete.

Reversible Circuit Distinguishability is StoqMA-complete: proof sketch

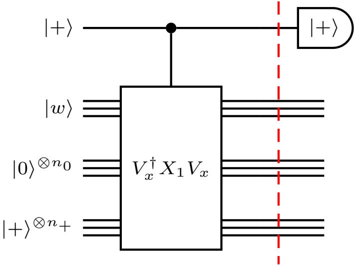
For $k = 0, 1$, let $|D_k\rangle := C_k |w\rangle |0\rangle^{\otimes n_0} |+\rangle^{\otimes n_+}$, then:

- $\mathrm{RCD}(a, b; \mathrm{poly})$ is contained in StoqMA$(1 - \frac{a}{2}, 1 - \frac{b}{2})$.
  - ◇ 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$(1 - \frac{a}{2}, 1 - \frac{b}{2})$.
  - ◇ 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].



Soundness error reduction for StoqMA

Theorem (AND-type repetition procedure of StoqMA)

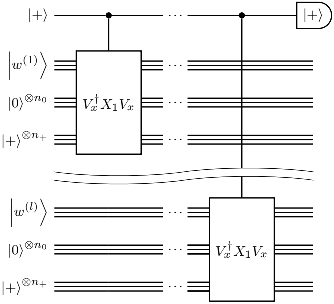
For any $l = \mathrm{poly}(n)$, StoqMA $\left(\frac{1}{2}+\frac{a}{2}, \frac{1}{2}+\frac{b}{2}\right) \subseteq$ StoqMA $\left(\frac{1}{2}+\frac{a^{l(n)}}{2}, \frac{1}{2}+\frac{b^{l(n)}}{2}\right)$.

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

Proof Sketch

Recall that $\Pr[V_x$ 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:

$\Pr\left[V_x' \text{ accepts } w^{(1)} \otimes \cdots \otimes w^{(l)}\right]$

$= \frac{1}{2}+\frac{1}{2}\lambda_{\max}(M^{\otimes l})$

$= \frac{1}{2}+\frac{1}{2}\left(\lambda_{\max}(M)\right)^l$

◇ **Yes** case: ✓

◇ **No** case: Entangled witness will not increase the maximum acceptance probability. □

1. What is the complexity class StoqMA?

2. StoqMA: a distribution testing lens

3. Distinguishing reversible circuits

4. StoqMA vs. MA: the power of error reduction
   - Why error reduction is important for StoqMA?
   - $\mathrm{SetCSP}_{\mathrm{negl},1/\mathrm{poly}}$ is $\mathsf{StoqMA}_{1-\mathrm{negl}}$-complete
   - Proof Sketch: $\mathrm{SetCSP}_{\mathrm{negl},1/\mathrm{poly}} \in \mathsf{MA}_{1-\mathrm{negl}'}$

5. Open problems

Error reduction for StoqMA implies StoqMA $=$ MA

Theorem [AGL20]

(Completeness) error reduction for StoqMA implies StoqMA $\subseteq$ MA.
Namely, StoqMA $(1-1/p_1(n), 1-1/p_2(n)) \subseteq$ MA, where p_1 is a *super-polynomial* of n and p_2 is a polynomial of n.

Proof Intuition

Notice [BBT06, BT09] essentially proves StoqMA$_1 \subseteq$ MA$_1$. It seems plausible to make it *robust*, namely StoqMA$_{1-\epsilon} \subseteq$ MA$_{1-\epsilon'}$ where ϵ and ϵ' are negligible.

MA containment Given a configuration graph $G=(V,E)$ that each node is marked either "good" or "bad", there is a R.W. that starts at node $v \in V$ such that

- Yes: $\exists v$ s.t. R.W. will not reach any "bad" node in *any* $\mathrm{poly}(n)$ steps w.h.p. .
- No: $\forall v$, R.W. will reach "bad" node in $p(n)$ steps where p is *some poly.* w.h.p. .

(See Sergey Bravyi's tutorial for more details.)

$\star$ To make this R.W. "robust", we need the probabilistic method!

- Interestingly, *the probabilistic method* and *completeness error reduction* are also used in proof of MA $\subseteq$ MA$_1$ [FGMSZ89]!

SetCSP: a combinatorial StoqMA-complete problem

Definition: k-$\mathrm{SetCSP}_{\epsilon_1,\epsilon_2}$

Given k-local set constraints $C = (C_1, \cdots, C_m)$ on $\{0,1\}^n$, where n is the number of variables and $m = \mathrm{poly}(n)$. 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 $Y_j^{(i)} \subseteq \{0,1\}^k$. Decide whether

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

where $0 \leq \epsilon_1(n) < \epsilon_2(n) \leq 1$ and $\epsilon_2(n) - \epsilon_1(n) \geq 1/\mathrm{poly}(n)$.

◇ <u>Frustration</u>: Let $B_i(S) := \{\text{bad strings}\}$ and $L_i(S) = \{\text{longing strings}\}$, then

$$\text{set-unsat}(C,S) = \frac{1}{m}\sum_{i=1}^{m} \text{set-unsat}(C_i,S) = \frac{1}{m}\sum_{i=1}^{m}\left(\frac{|B_i(S)|}{|S|} + \frac{|L_i(S)|}{|S|}\right).$$

Theorem (inspired by [BBT06, AG20])

k-$\mathrm{SetCSP}_{\mathrm{negl},1/\mathrm{poly}}$ is $\mathrm{StoqMA}_{1-\mathrm{negl}}$-complete.

SetCSP: a combinatorial StoqMA-complete problem (Cont.)

Definition: Configuration Graph

The configuration graph $G(C)=(V_C,E_C)$ is defined by:
$\forall s,t\in\{0,1\}^n$, $\exists$ edge $(s,t)\in E_C$ iff $s|_{\mathrm{supp}(C_i)},t|_{\mathrm{supp}(C_i)}\in Y_j^{(i)}$.

A node $s\in V_C$ is marked by *"bad"*, i.e. $s\in B_i(S)$, if $s|_{\mathrm{supp}(C_i)}\notin\cup_{j=1}^{l_i}Y_j^{(i)}$;
Otherwise this node is marked by *"good"*.

◇ Example: A 2-SetCSP instance $C=(C_1,C_2,C_3)$ defined on a 4-node line.

Set-constraints:

$Y(C_1)=\{\{00,11\}_{1,2}\}$,

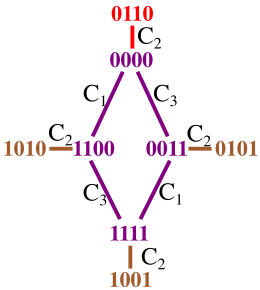
$Y(C_2)=\{\{00,11\}_{2,3},\{01,10\}_{2,3}\}$,

$Y(C_3)=\{\{00,11\}_{3,4}\}$.

Consider a subset $S=\{0000,1100,0110,0011,1111\}$,

the only bad string is $B_2(S)=\{0110\}$,

longing strings are $L_2(S)=\{1010,1001,0101\}$.

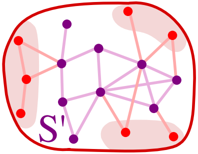


k-SetCSP$_{\mathrm{negl},1/\mathrm{poly}}$ is in MA: proof sketch (Completeness)

1. Well-approximated subset exists:

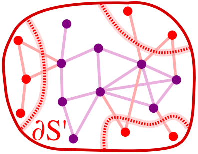
$$\text{set-unsat}(C,S) \le 1/f(n)$$
$$\Rightarrow \text{set-unsat}(C,S') \le m/f(n),$$

where S' contains only good strings.



2. Small-frustration subset implies small-size boundary:

$$\text{set-unsat}(C,S') \le 1/h(n)$$
$$\Rightarrow |\partial S'|/|S'| \le 2^k m/h(n).$$



3. Any subset with a small-size boundary has a good *starting point*:

$$\frac{|\partial S'|}{|S'|} \le \frac{1}{p_1(n)} \Rightarrow \mathop{\mathbb{E}}_{v\sim\pi_S}\left[\Pr\left[\bigwedge_{l=0}^{T} X_v^{(l)} \in S'\right]\right] \ge 1 - \frac{1}{p_2(n)} \text{ where } p_2 \propto \frac{p_1}{T}.$$

Ref. [ST08, GT12] Expectation bounds on remained probability

⋆ There is a starting point v (viz. *classical witness*) such that any $T(n)$-step lazy random walk remained in S' w.h.p. where $T(n)$ is a super-polynomial.

Conclusions and open problems

Take-home messages

1. StoqMA with easy witness (eStoqMA) is contained in MA, which simply infers $\mathsf{StoqMA}_1 \subseteq \mathsf{MA}$.
2. Reversible Circuit Distinguishability is StoqMA-complete (instead of MA-complete as expected!). The exact variant is NP-complete, which signifies that StoqMA with perfect soundness is contained in NP.
3. (Completeness) error reduction (still open!) for StoqMA implies $\mathsf{StoqMA} = \mathsf{MA}$; we know how to do soundness error reduction for StoqMA.

Open problems

1. StoqMA vs. MA and SBP vs. MA.
2. (Completeness) error reduction for StoqMA.
3. StoqMA with exponentially small gap (PreciseStoqMA).
4. The computational power of QMA with perfect soundness (i.e. NQP).
5. More StoqMA-complete problems, such as Stoquastic CLDM.

Thank you!

Slides are available on shorturl.at/cmHX1.