StoqMA meets *distribution testing*

Yupan Liu
???

TQC 2021

Why StoqMA is important?

Dichotomy Theorem on

Constraint **S**atisfaction **P**roblem

over boolean domain

[Schaefer'78]

$$(\neg x_1 \vee x_2) \wedge (x_2 \vee \neg x_3 \vee x_4)$$

- Assume that P⊊NP

Why StoqMA is important?

Dichotomy Theorem on

Constraint **S**atisfaction **P**roblem

over boolean domain

[Schaefer'78]

$$(\neg x_1 \vee x_2) \wedge (x_2 \vee \neg x_3 \vee x_4)$$

- Assume that P⫋NP

Classification Theorem on

2-**L**ocal **H**amiltonian **P**roblem

on qubits

[Cubitt-Montanaro'13]

$$H = \Sigma_i(\sigma_i^x \otimes \sigma_{i+1}^x + \sigma_i^y \otimes \sigma_{i+1}^z)$$

Why StoqMA is important?

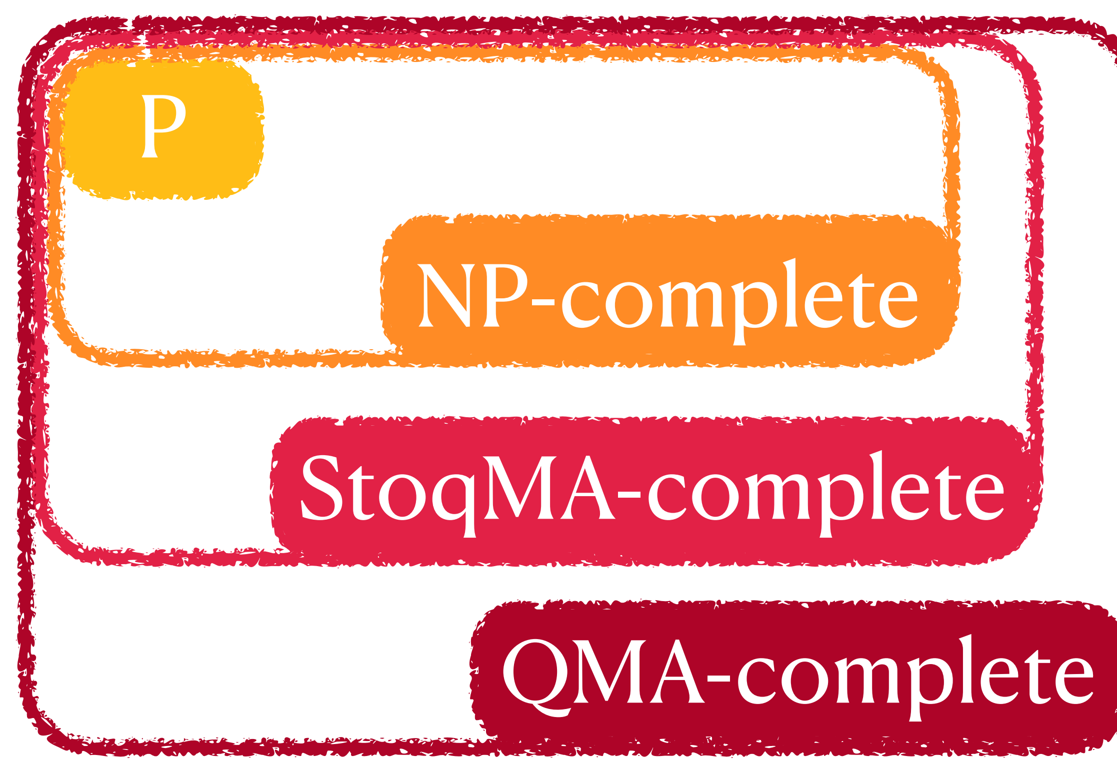
Dichotomy Theorem on
Constraint **S**atisfaction **P**roblem
over boolean domain
[Schaefer'78]

$$(\neg x_1 \vee x_2) \wedge (x_2 \vee \neg x_3 \vee x_4)$$

- Assume that $\mathrm{P} \subsetneq \mathrm{NP}$

Classification Theorem on
2-**L**ocal **H**amiltonian **P**roblem
on qubits
[Cubitt-Montanaro'13]

$$H = \Sigma_i(\sigma_i^x \otimes \sigma_{i+1}^x + \sigma_i^y \otimes \sigma_{i+1}^z)$$

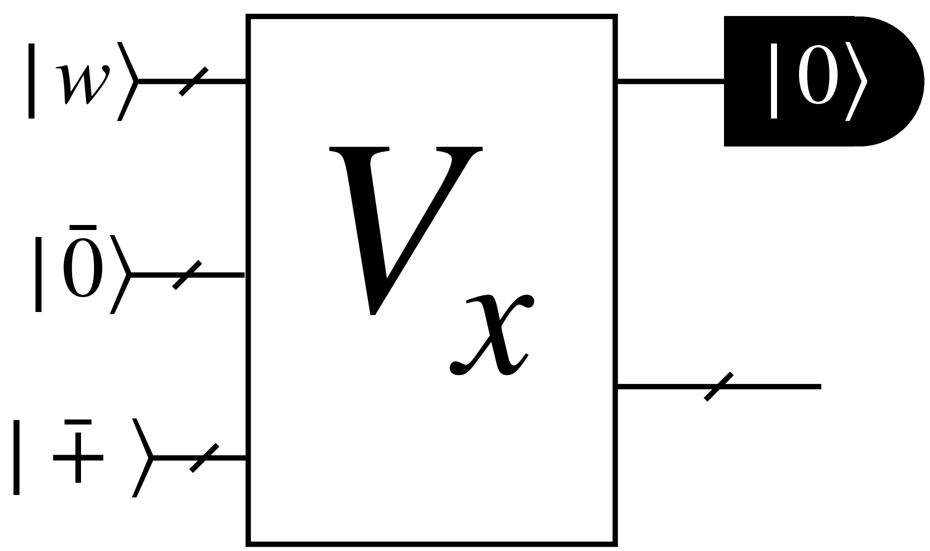


- Assume that $\mathrm{P} \subsetneq \mathrm{NP} \subsetneq \mathrm{StoqMA} \subsetneq \mathrm{QMA}$

What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

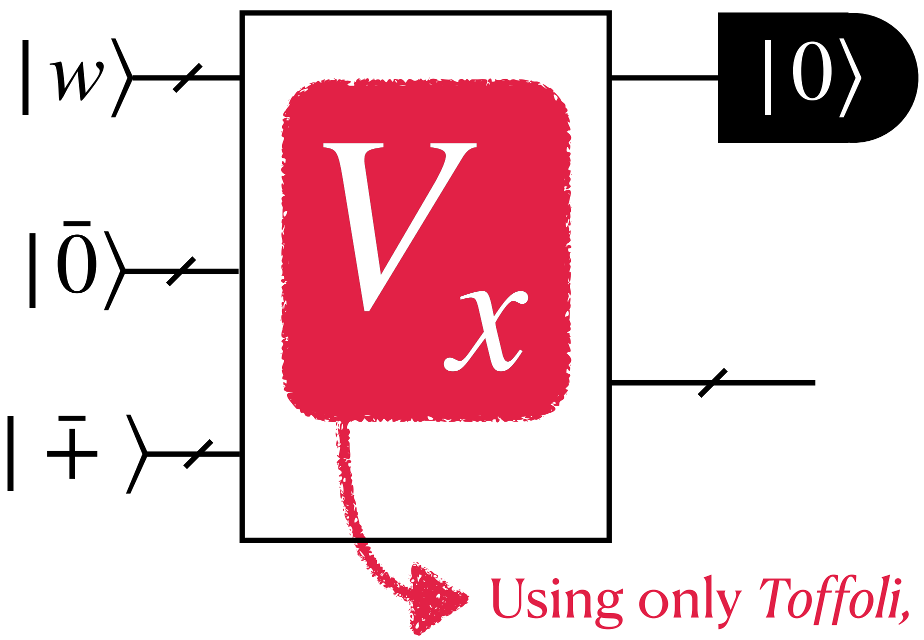
MA



What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

MA



Using only *Toffoli, CNOT, X* gates

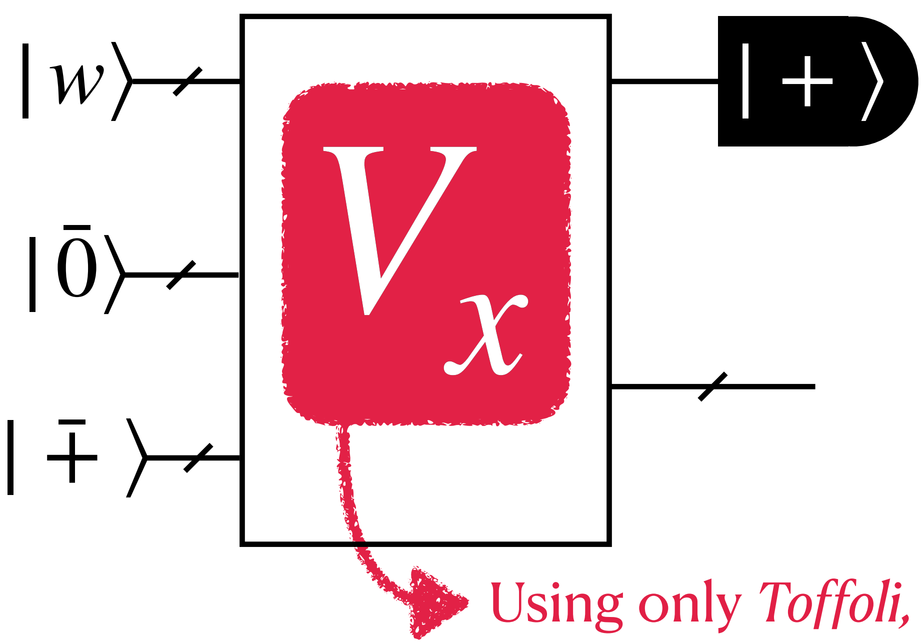
- For *yes* instances, $\Pr[V_x \text{ accepts } |w\rangle] \geq a$.
- For *no* instances, $\Pr[V_x \text{ accepts } |w\rangle] \leq b$.

where $0 \leq a, b \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$.

What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

StoqMA



Using only *Toffoli, CNOT, X* gates

- For *yes* instances, $\Pr[V_x \text{ accepts } |w\rangle] \geq a$.
- For *no* instances, $\Pr[V_x \text{ accepts } |w\rangle] \leq b$.

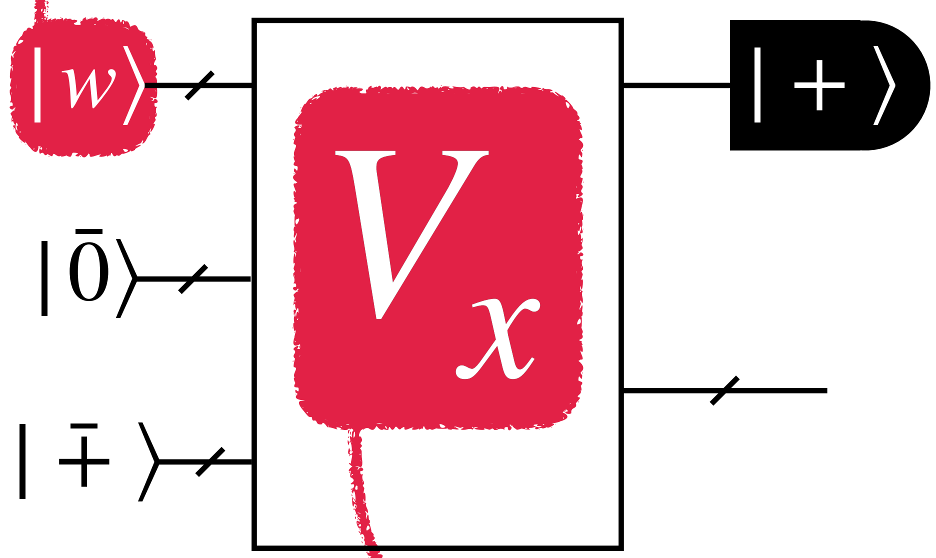
where $\frac{1}{2} \leq a, b \leq 1$ and $a - b \geq 1/\text{poly}(n)$.

What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

StoqMA

Non-negative states are sufficient (due to Perron-Frobenius theorem)



- For *yes* instances, $\Pr[V_x \text{ accepts } |w\rangle] \geq a$.
- For *no* instances, $\Pr[V_x \text{ accepts } |w\rangle] \leq b$.

where $\frac{1}{2} \leq a, b \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$.

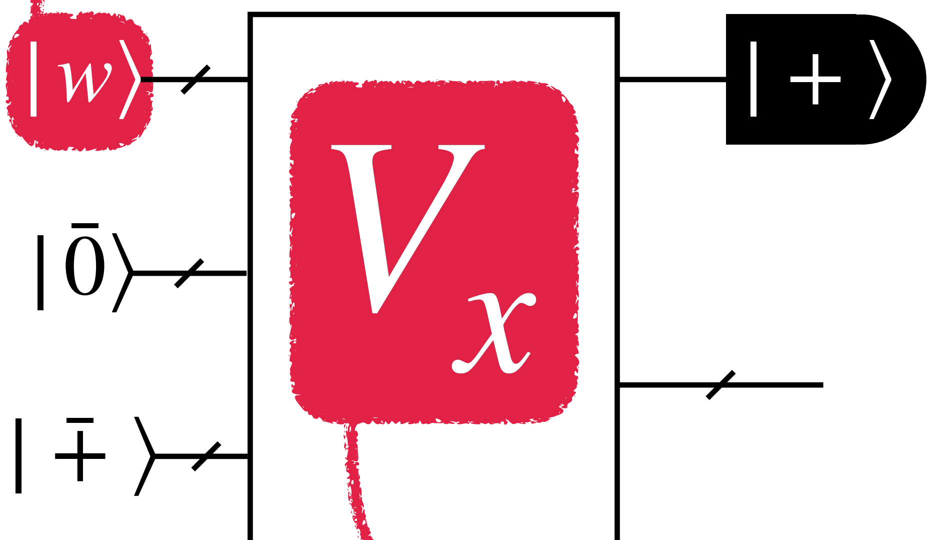
Using only *Toffoli, CNOT, X* gates

What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

StoqMA

Non-negative states are sufficient (due to Perron-Frobenius theorem)



- For *yes* instances, $\Pr[V_x \text{ accepts } |w\rangle] \geq a$.
- For *no* instances, $\Pr[V_x \text{ accepts } |w\rangle] \leq b$.

where $\frac{1}{2} \leq a, b \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$.

Using only *Toffoli, CNOT, X* gates

Off-diagonal entries are *non-positive*

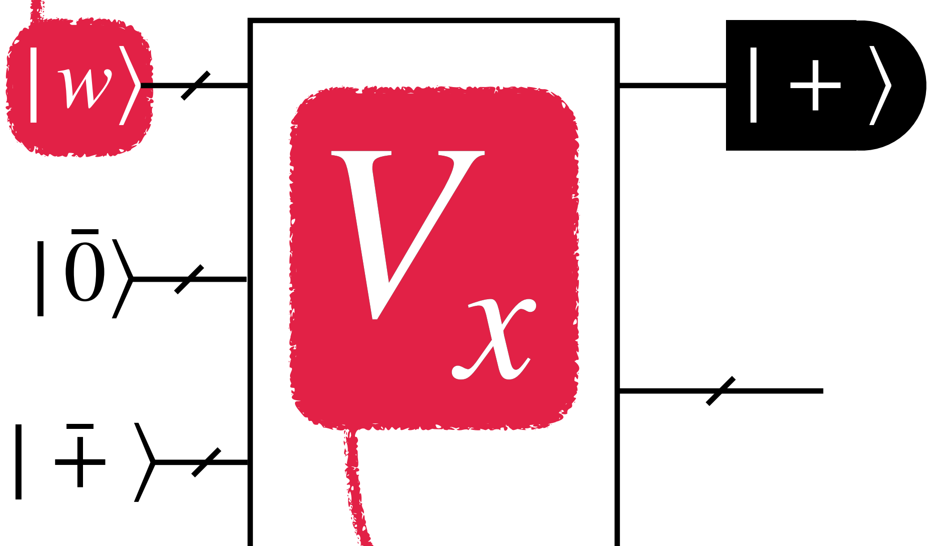
- Definition of StoqMA came from *Stoquastic Local Hamiltonian*.

What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

StoqMA

Non-negative states are sufficient (due to Perron-Frobenius theorem)



Using only *Toffoli, CNOT, X* gates

- For *yes* instances, $\Pr[V_x \text{ accepts } |w\rangle] \geq a$.
- For *no* instances, $\Pr[V_x \text{ accepts } |w\rangle] \leq b$.

where $\frac{1}{2} \leq a, b \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$.

Off-diagonal entries are *non-positive*

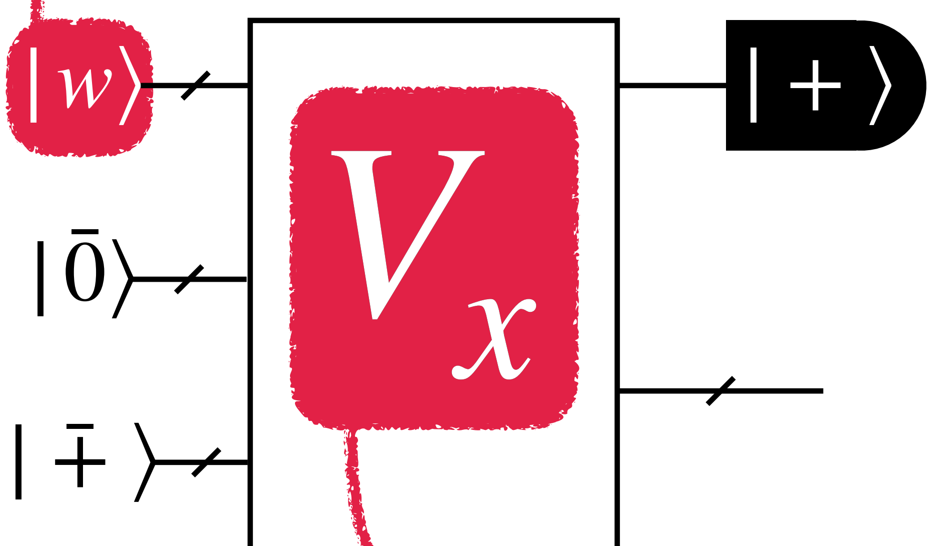
- Definition of StoqMA came from *Stoquastic Local Hamiltonian*.
- MA $\subseteq$ StoqMA $\subseteq$ AM, where AM is two-message randomized generalization of NP.

What's the complexity class StoqMA?

[Bravyi-Bessen-Terhal'06]

StoqMA

Non-negative states are sufficient (due to Perron-Frobenius theorem)



- For *yes* instances, $\Pr[V_x \text{ accepts } |w\rangle] \geq a$.
- For *no* instances, $\Pr[V_x \text{ accepts } |w\rangle] \leq b$.

where $\frac{1}{2} \leq a, b \leq 1$ and $a - b \geq 1/\mathrm{poly}(n)$.

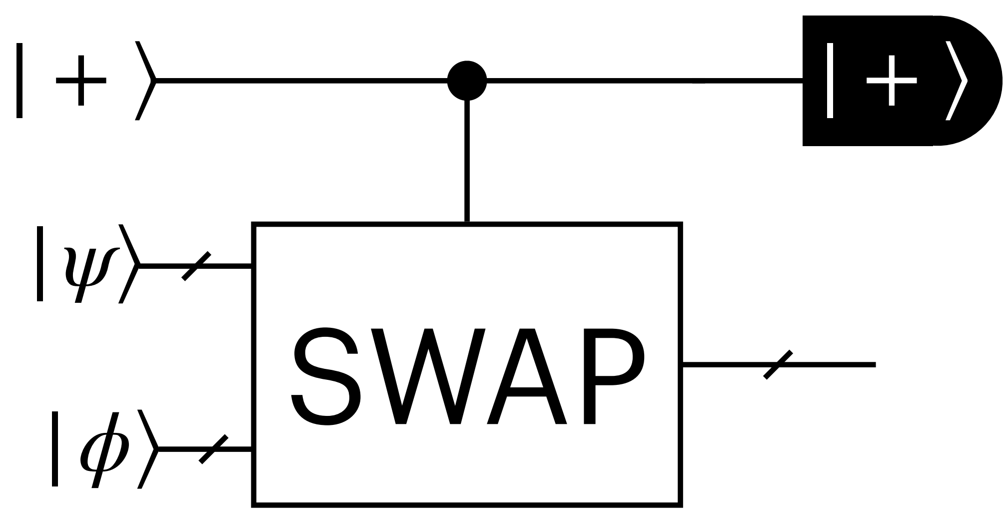
Using only *Toffoli, CNOT, X* gates

Off-diagonal entries are *non-positive*

- Definition of StoqMA came from *Stoquastic Local Hamiltonian*.
- MA $\subseteq$ StoqMA $\subseteq$ AM, where AM is two-message randomized generalization of NP.
- Error reduction (i.e., making *a,b* exponentially close to *1* and *1/2*) for StoqMA is *unknown*.

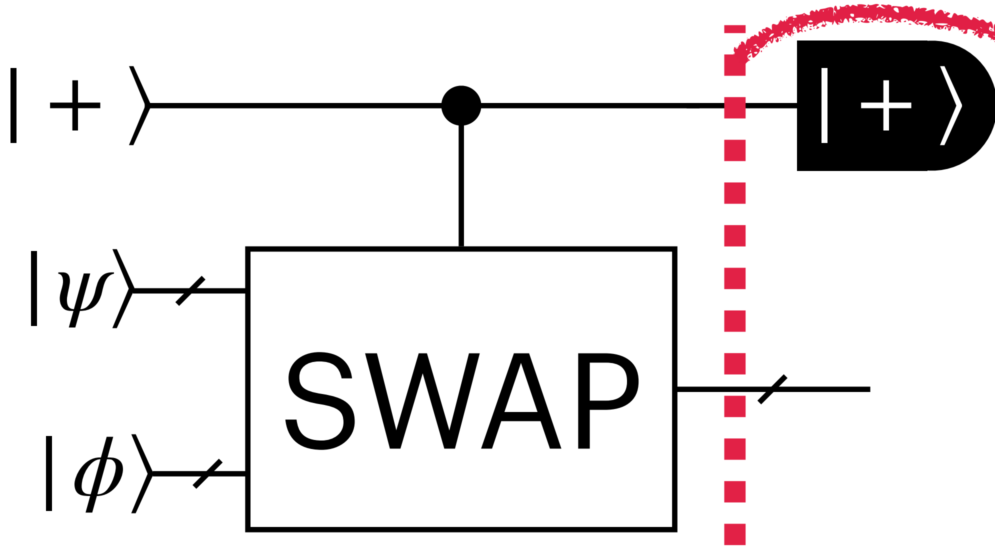
The mystery of the Hadamard-basis measurement

SWAP test



The mystery of the Hadamard-basis measurement

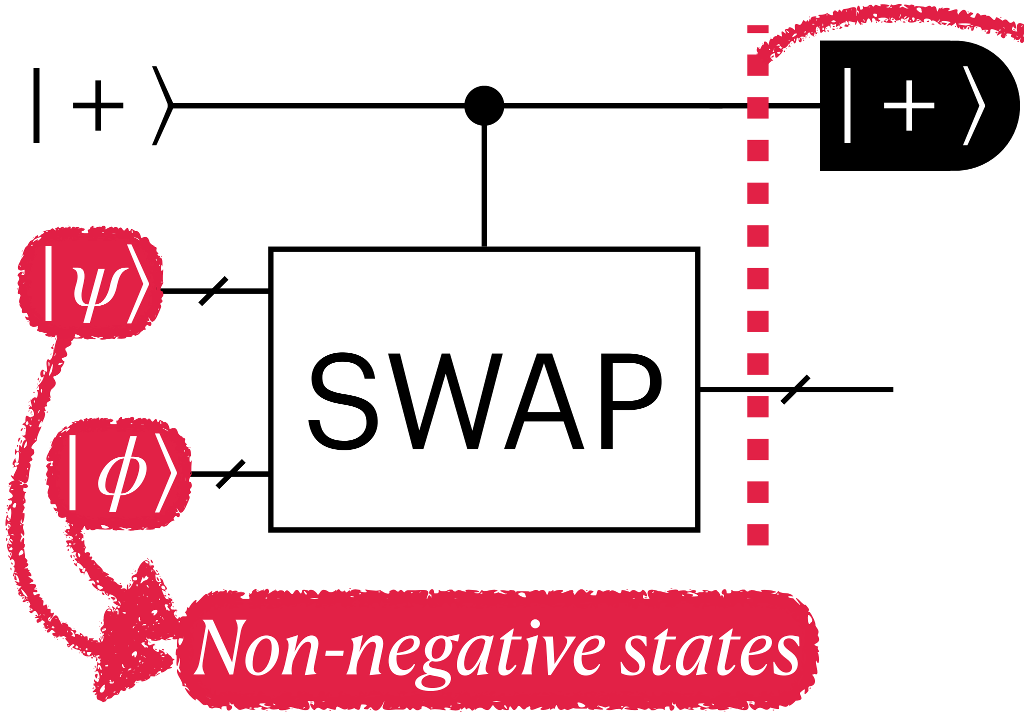
SWAP test



- Dash line: $\sim |0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle$
- Acc. Prob.: $p_{\mathrm{acc}} = |\langle\psi|\phi\rangle|^2$

The mystery of the Hadamard-basis measurement

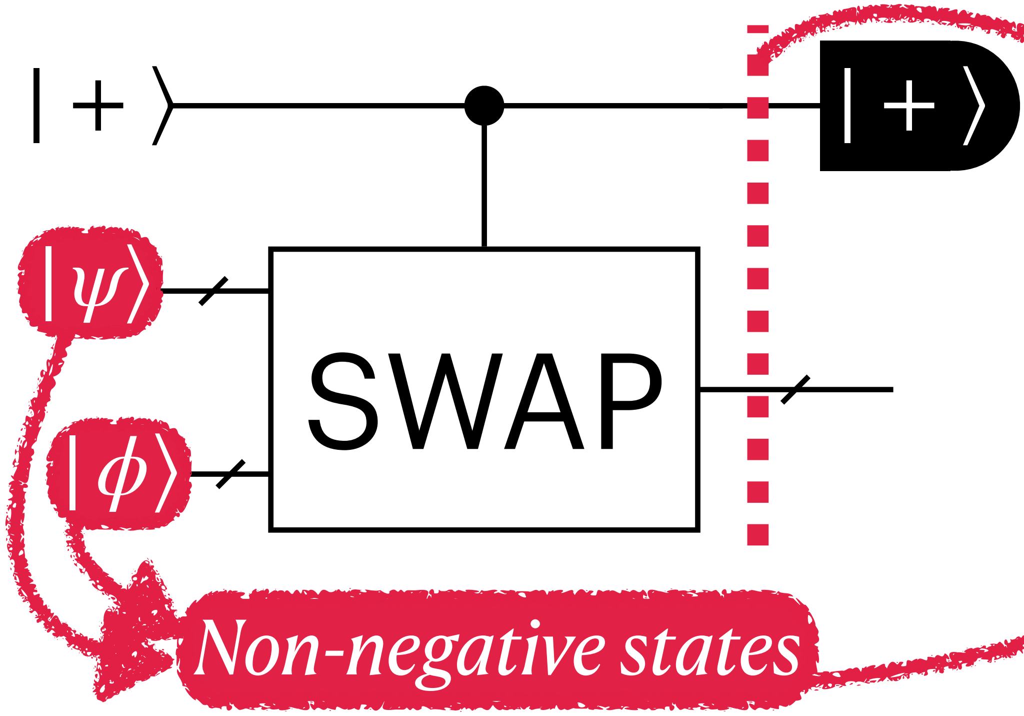
SWAP test



- Dash line: $\sim |0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle$
- Acc. Prob.: $p_{\mathrm{acc}} = |\langle\psi|\phi\rangle|^2$

The mystery of the Hadamard-basis measurement

SWAP test as a StoqMA verifier

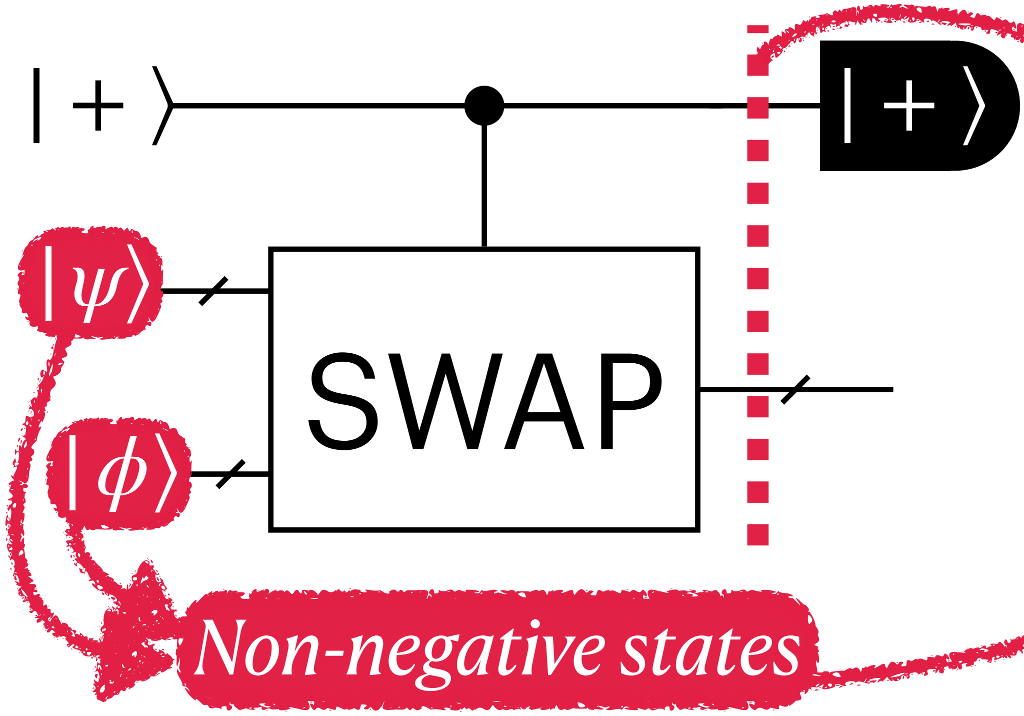


- Dash line: $\sim |0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle$
- Acc. Prob.: $p_{\text{acc}} = |\langle\psi|\phi\rangle|^2$
- Viewed as *distributions*:

$|\psi\rangle = \sum_i \sqrt{p(i)}\,|i\rangle, |\phi\rangle = \sum_i \sqrt{q(i)}\,|i\rangle$

The mystery of the Hadamard-basis measurement

SWAP test as a StoqMA verifier



- Dash line: $\sim |0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle$
- Acc. Prob.: $p_{\text{acc}} = |\langle\psi|\phi\rangle|^2$
- Viewed as *distributions*:

$|\psi\rangle = \sum_i \sqrt{p(i)}\,|i\rangle, |\phi\rangle = \sum_i \sqrt{q(i)}\,|i\rangle$

Take-home message from the SWAP test:

- Single-qubit Hadamard-basis measurement can be thought as a *distribution testing* task!

1st result: eStoqMA $\subseteq$ MA

Easy witness

Consider $|w\rangle = \sum_i \sqrt{p(i)}\,|i\rangle$ such that $\forall x, y \in \{0,1\}^n$, $\frac{p(x)}{p(y)}$ is *efficiently* computable.

- An analogous condition appears in *Guided Stoquastic Local Hamiltonian Problem* [Bravyi'15].

1st result: eStoqMA $\subseteq$ MA

Easy witness

Consider $|w\rangle = \sum_i \sqrt{p(i)}\,|i\rangle$ such that $\forall x, y \in \{0,1\}^n$, $\frac{p(x)}{p(y)}$ is *efficiently* computable.

- An analogous condition appears in *Guided Stoquastic Local Hamiltonian Problem* [Bravyi'15].

Theorem. For any $\frac{1}{2} \leq a, b \leq 1$ such that $a - b \geq 1/\mathrm{poly}(n)$, eStoqMA$(a, b) \subseteq$ MA.

1^{st} result: eStoqMA $\subseteq$ MA

Easy witness

Consider $|w\rangle = \sum_i \sqrt{p(i)}\,|i\rangle$ such that $\forall x, y \in \{0,1\}^n$, $\frac{p(x)}{p(y)}$ is *efficiently* computable.

- An analogous condition appears in *Guided Stoquastic Local Hamiltonian Problem* [Bravyi'15].

Theorem. For any $\frac{1}{2} \leq a, b \leq 1$ such that $a - b \geq 1/\mathrm{poly}(n)$, eStoqMA$(a, b) \subseteq$ MA.

Proof Sketch. Using the dual access model [Canonne-Rubinfeld'14]:

- *Sample access*: running a copy of V_x and measuring all qubits in computational basis;
- *Query access*: efficiently evaluating the quotient.

One can approximate max. acc. prob. with *polynomially many of copies* of the witness $|w\rangle$. $\square$

1st result: eStoqMA $\subseteq$ MA

Easy witness

Consider $|w\rangle = \sum_i \sqrt{p(i)}\,|i\rangle$ such that $\forall x, y \in \{0,1\}^n$, $\frac{p(x)}{p(y)}$ is *efficiently* computable.

- An analogous condition appears in *Guided Stoquastic Local Hamiltonian Problem* [Bravyi'15].

Theorem. For any $\frac{1}{2} \leq a, b \leq 1$ such that $a - b \geq 1/\mathrm{poly}(n)$, eStoqMA$(a, b) \subseteq$ MA.

Proof Sketch. Using the dual access model [Canonne-Rubinfeld'14]:

- *Sample access*: running a copy of V_x and measuring all qubits in computational basis;
- *Query access*: efficiently evaluating the quotient.

One can approximate max. acc. prob. with *polynomially many of copies* of the witness $|w\rangle$. □

- **Prop** ([Grilo20]). For any *a,b,* classical-witness-StoqMA$(a, b) \subseteq$ MA$(2a - 1, 2b - 1)$.
- The difficulty of StoqMA roots in *different kinds of optimal witness*!

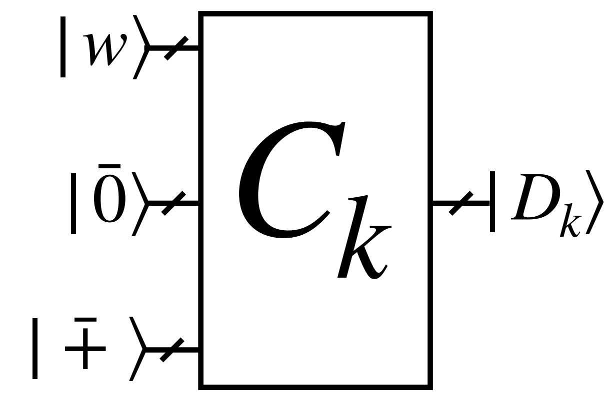
2^{nd} result: *Distinguishing reversible circuits* with non-negative states

Reversible Circuit Distinguishability is StoqMA-complete

Given *reversible circuits* C_0, C_1, define $|D_k\rangle := C_i |w\rangle |\bar{0}\rangle | \bar{+} \rangle$ for $k = 0,1$ and a *non-negative* witness $|w\rangle$:

- *Yes*: $\exists |w\rangle$ such that $\langle D_0 | D_1 \rangle \geq \alpha$;
- *No*: $\forall |w\rangle, \langle D_0 | D_1 \rangle \leq \beta$;

where $0 \leq \alpha, \beta \leq 1$ and $\alpha - \beta \geq 1/\text{poly}(n)$.



2^{nd} result: *Distinguishing reversible circuits* with non-negative states

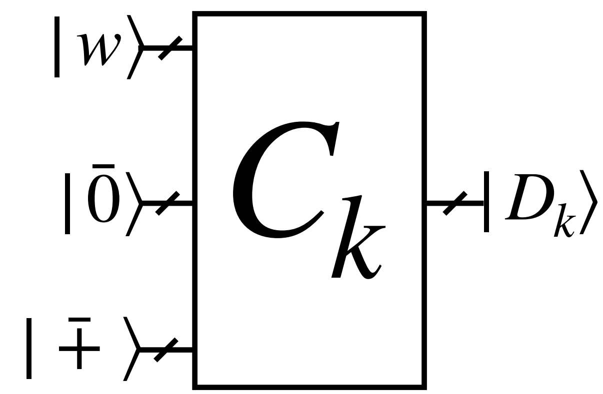
Reversible Circuit Distinguishability is **StoqMA**-complete

Given *reversible circuits C_0, C_1*, define $|D_k\rangle := C_i|w\rangle|\bar{0}\rangle|\mp\rangle$

for $k = 0,1$ and a *non-negative* witness $|w\rangle$:

- *Yes*: $\exists\, |w\rangle$ such that $\langle D_0|D_1\rangle \geq \alpha$;
- *No*: $\forall\, |w\rangle$, $\langle D_0|D_1\rangle \leq \beta$;

where $0 \leq \alpha, \beta \leq 1$ and $\alpha - \beta \geq 1/\text{poly}(n)$.



- **QMA**-complete if C_0, C_1 are *quantum circuits*
- **NP**-complete if C_0, C_1 are reversible circuits *without ancillary random bit*

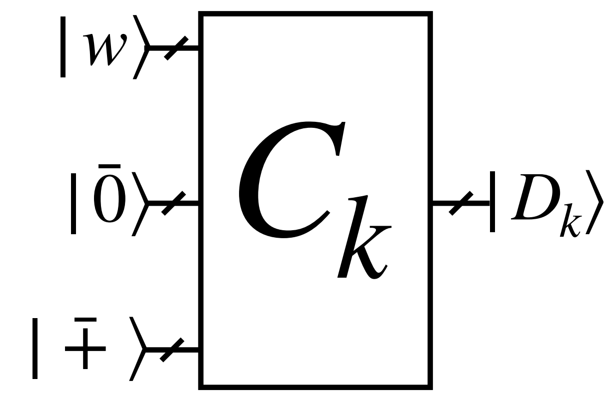
2^{nd} result: *Distinguishing reversible circuits* with non-negative states

Reversible Circuit Distinguishability is **StoqMA**-complete

Given *reversible circuits C_0, C_1* define $|D_k\rangle := C_i|w\rangle|\bar{0}\rangle|\mp\rangle$ for $k = 0,1$ and a *non-negative* witness $|w\rangle$:

- *Yes*: $\exists |w\rangle$ such that $\langle D_0|D_1\rangle \geq \alpha$;
- *No*: $\forall |w\rangle$, $\langle D_0|D_1\rangle \leq \beta$;

where $0 \leq \alpha, \beta \leq 1$ and $\alpha - \beta \geq 1/\mathrm{poly}(n)$.

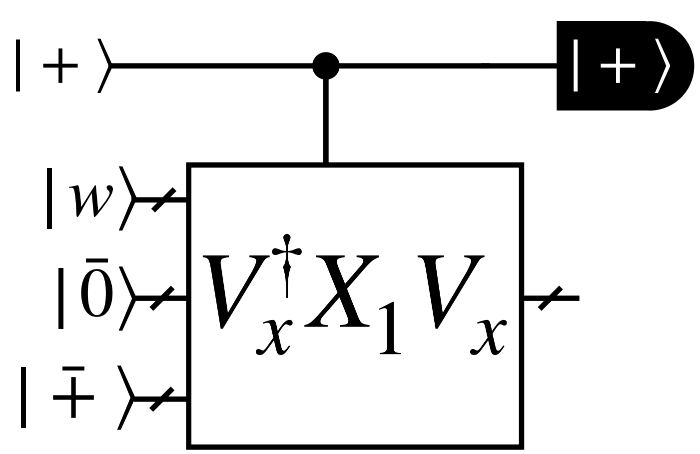


- **QMA**-complete if C_0, C_1 are *quantum circuits*
- **NP**-complete if C_0, C_1 are reversible circuits *without ancillary random bit*

Soundness error reduction

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

A message from StoqMA-hardness proof



2^{nd} result: *Distinguishing reversible circuits* with non-negative states

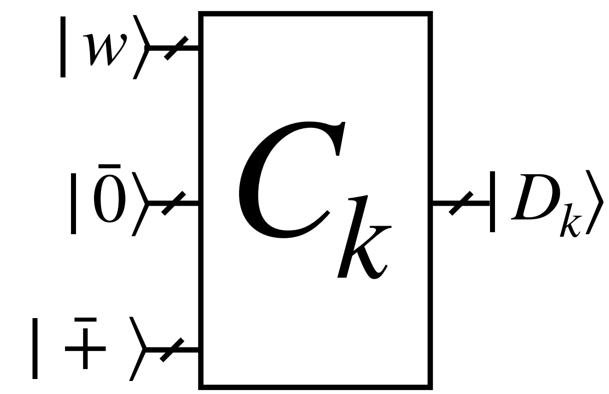
Reversible Circuit Distinguishability is **StoqMA**-complete

Given *reversible circuits* C_0, C_1, define $|D_k\rangle := C_i|w\rangle|\bar{0}\rangle|\mp\rangle$

for $k = 0,1$ and a *non-negative* witness $|w\rangle$:

- *Yes*: $\exists |w\rangle$ such that $\langle D_0|D_1\rangle \geq \alpha$;
- *No*: $\forall |w\rangle$, $\langle D_0|D_1\rangle \leq \beta$;

where $0 \leq \alpha, \beta \leq 1$ and $\alpha - \beta \geq 1/\text{poly}(n)$.

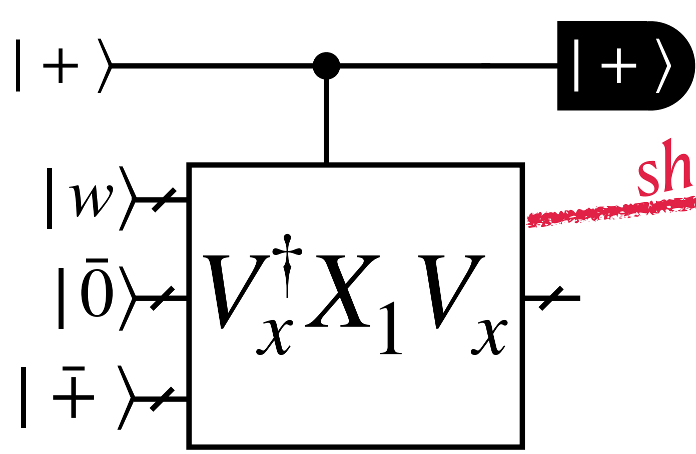


- **QMA**-complete if C_0, C_1 are *quantum circuits*
- **NP**-complete if C_0, C_1 are reversible circuits *without ancillary random bit*

Soundness error reduction

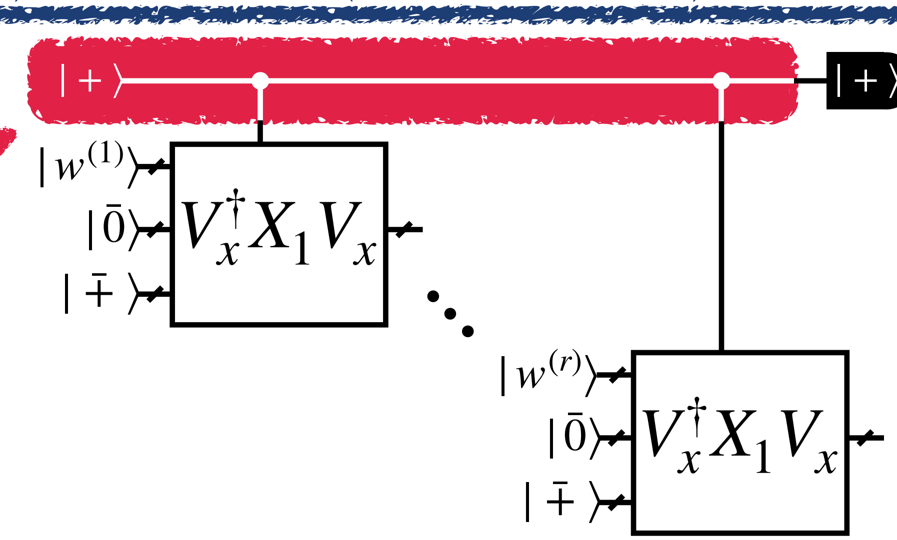
$\text{StoqMA}\left(\frac{1}{2}+\frac{a}{2}, \frac{1}{2}+\frac{b}{2}\right) \subseteq \text{StoqMA}\left(\frac{1}{2}+\frac{a^r}{2}, \frac{1}{2}+\frac{b^r}{2}\right)$

A *message* from *StoqMA-hardness proof*



shared control qubit

a special type of parallel repetation



Thanks!