you can verify quantum proofs by measuring 1 qubit at a time

Tomoyuki Morimae

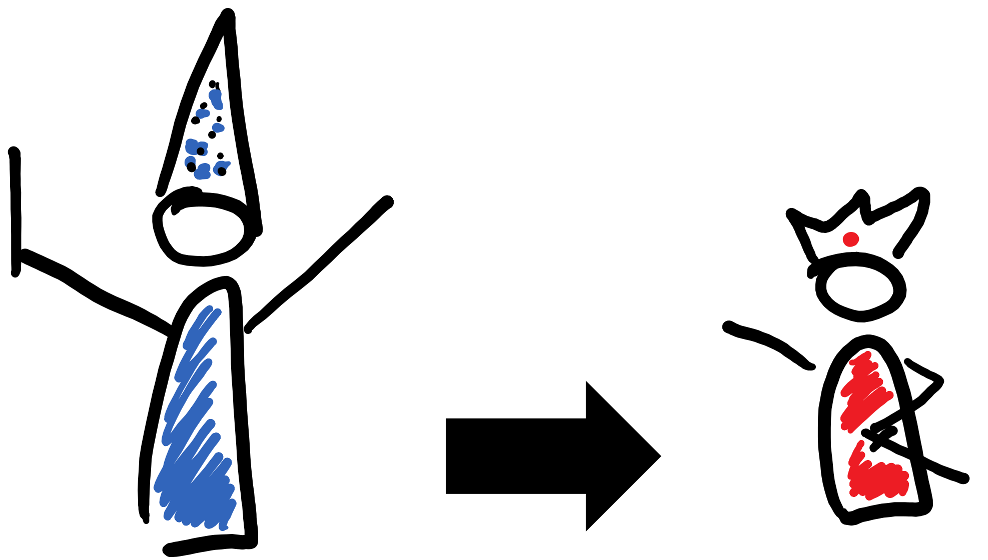
Norbert Schuch

Daniel Nagaj

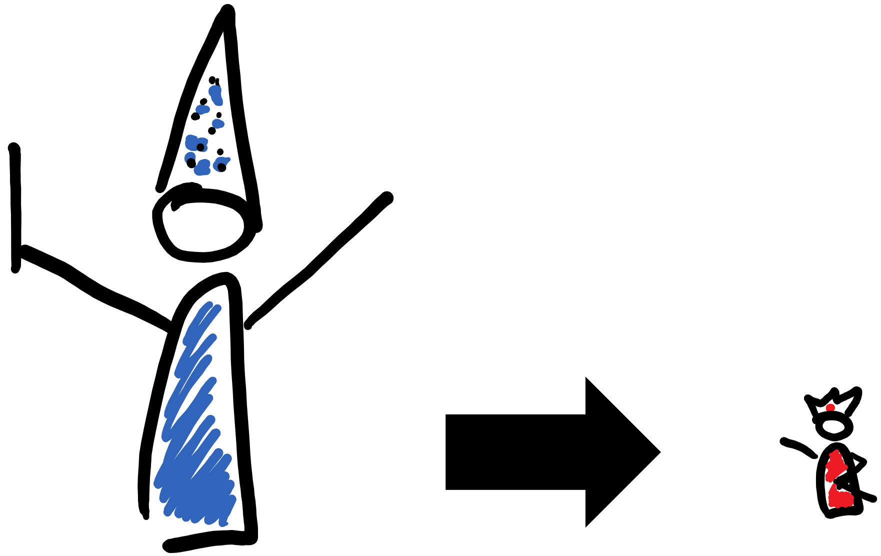
2016 | 6 | 17
CEQIP Valtice

PRA 93, 022326

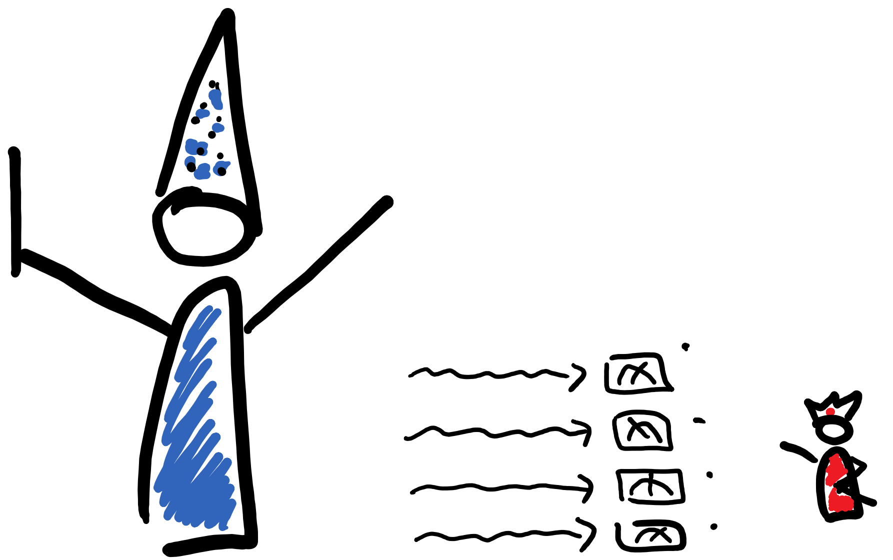
S A S P R O



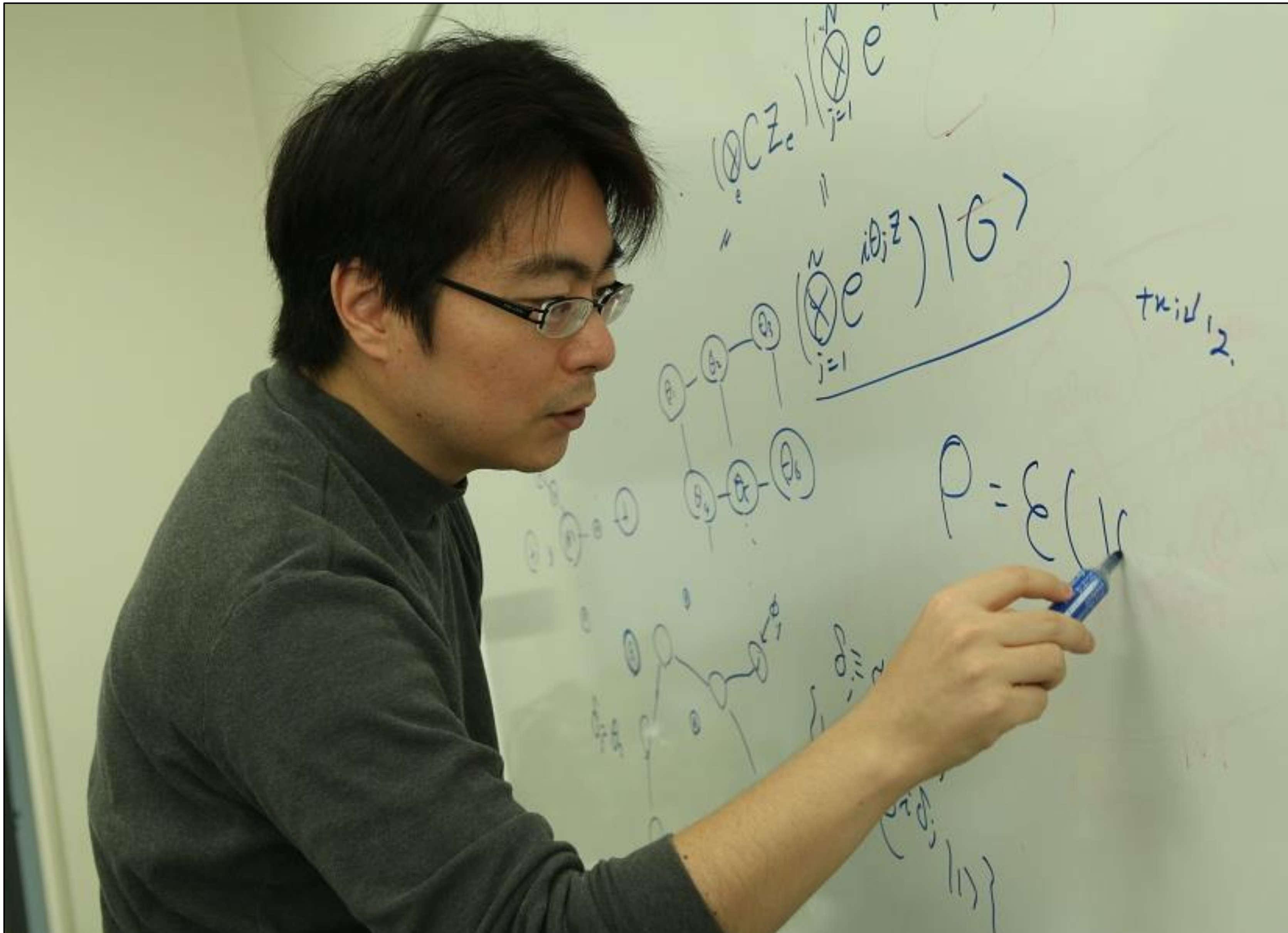
restricting the verifier's resources



restricting the verifier's resources



restricting the verifier's resources



One-way quantum verification

13

The theory of cluster-state computation is well-established by now, showing that any BQP circuit can be modified so it uses only single qubit quantum gates, possibly classically controlled, provided ample supply of a state known as the "cluster state" - which is a simple to produce stablizer state.

My question is: is a similar notion known for quantum verification - i.e. can one replace QMA circuits with classically controlled 1-qubit gates, possibly using some "special state"? At least initially, I'm unclear on why the cluster state can even work in this case.

2

quantum-computing

share cite improve this question

asked Aug 30 '12 at 20:48
Lior Eldar
531 ● 2 ● 13

cstheory.stackexchange.com/questions/12450

It is possible to restrict the QMA verifier to single-qubit measurements and classical pre- and postprocessing (with randomness) while keeping QMA-completeness.

To see why, take any class of k-local QMA-complete Hamiltonians on qubits. By adding a constant of order $\mathrm{poly}(n)$ and rescaling with a $1/\mathrm{poly}(n)$ factor, the Hamiltonian can be brought into the form

$$H = \sum_i w_i h_i \ ,$$

where $w_i > 0$, $\sum_i w_i = 1$, and $h_i = \frac{1}{2}(\mathrm{Id} \pm P_i)$, where P_i is a product of Paulis. Estimating the smallest eigenvalue of H up to accuracy $1/\mathrm{poly}(n)$ is still QMA-hard.

We can now build a circuit which only uses single-qubit measurements which, given a state $|\psi\rangle$, accepts with probability $1 - \langle\psi|H|\psi\rangle$ (which by construction is between 0 and 1). To this end, first randomly pick one of the i's according to the distribution w_i. Then, measure each of the Paulis in P_i, and take the parity π of the outcomes, which is now related to $\langle\psi|h_i|\psi\rangle$ via

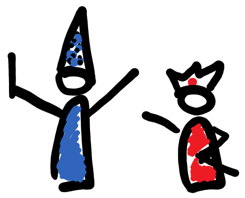
$$\langle\psi|h_i|\psi\rangle = \tfrac{1}{2}(1 \pm (-1)^\pi) \in \{0, 1\} \ .$$

The circuit now outputs $1 - \langle\psi|h_i|\psi\rangle$, and the output is therefore distributed according to $\langle\psi|H|\psi\rangle$.

This is, if we picked a yes-instance of the (QMA-complete) local Hamiltonian problem, there is a state $|\psi\rangle$ such that this verifier will accept with some probability $\geq a$, while otherwise any state will be rejected with probability $\leq b$, with $a - b > 1/\mathrm{poly}(n)$. The variant of QMA where the verifier is restricted to one-qubit measurements is therefore QMA-complete for some $1/\mathrm{poly}(n)$ gap. Finally, this version of QMA can be amplified using just the conventional amplification techniques for QMA, which finally proves it is QMA-complete independent of the gap (within the same range as QMA).

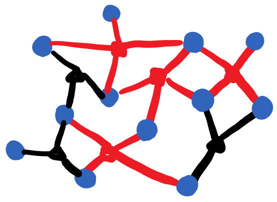
1 **QMA**

quantum proofs & verification



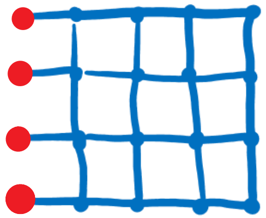
2 **Hamiltonians**

decomposing & measuring



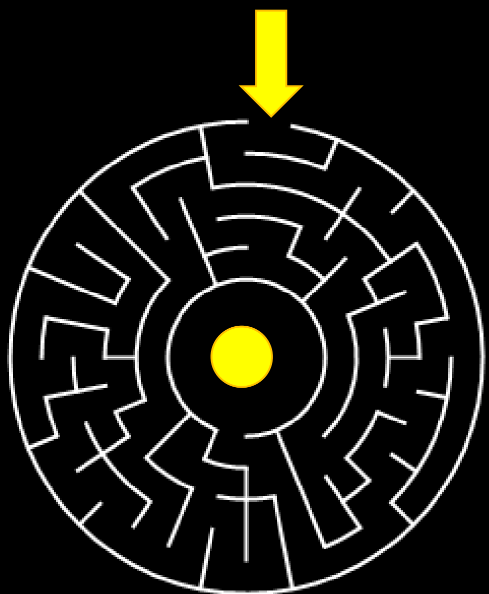
3 **MBQC**

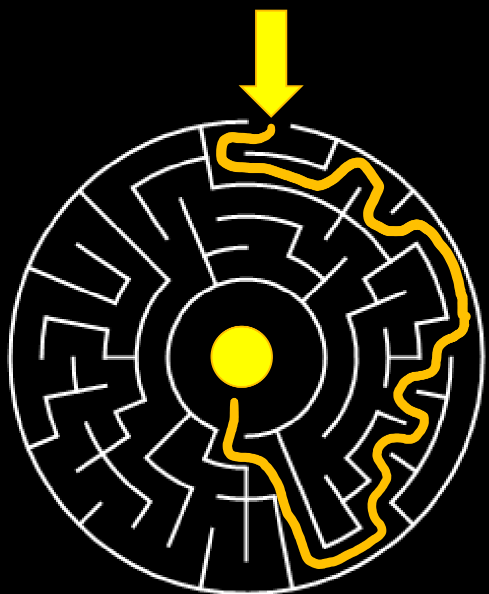
universal states, blind QC & witnesses



1 qubit at a time

proofs that
can be verified





[J. Howard Miller]

P

Verification?

Solve the problem.

+ 182 + 223 − 314 + 651

− 410 + 245 − 677 − 62

+ 3 + 916 − 120 + 874

+ 399 − 725 − 58 − 403

= 1500

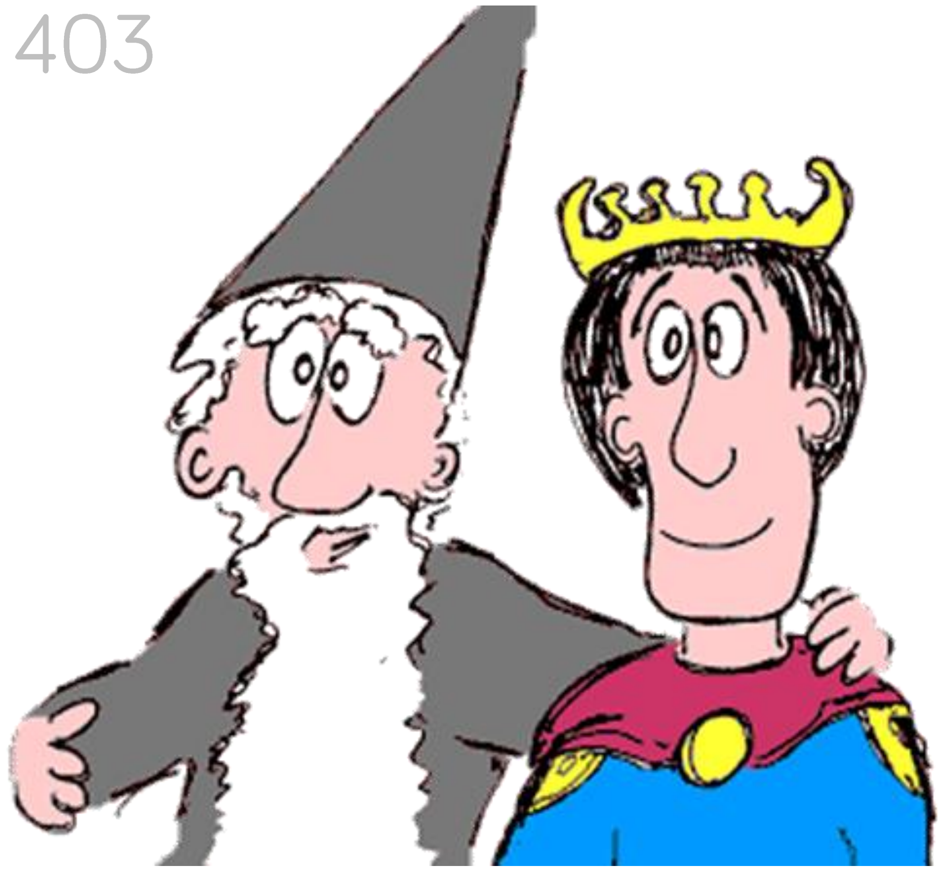
+ 182 + 223 − 314 + 651

− 410 + 245 − 677 − 62

+ 3 + 916 − 120 + 874

+ 399 − 725 − 58 − 403

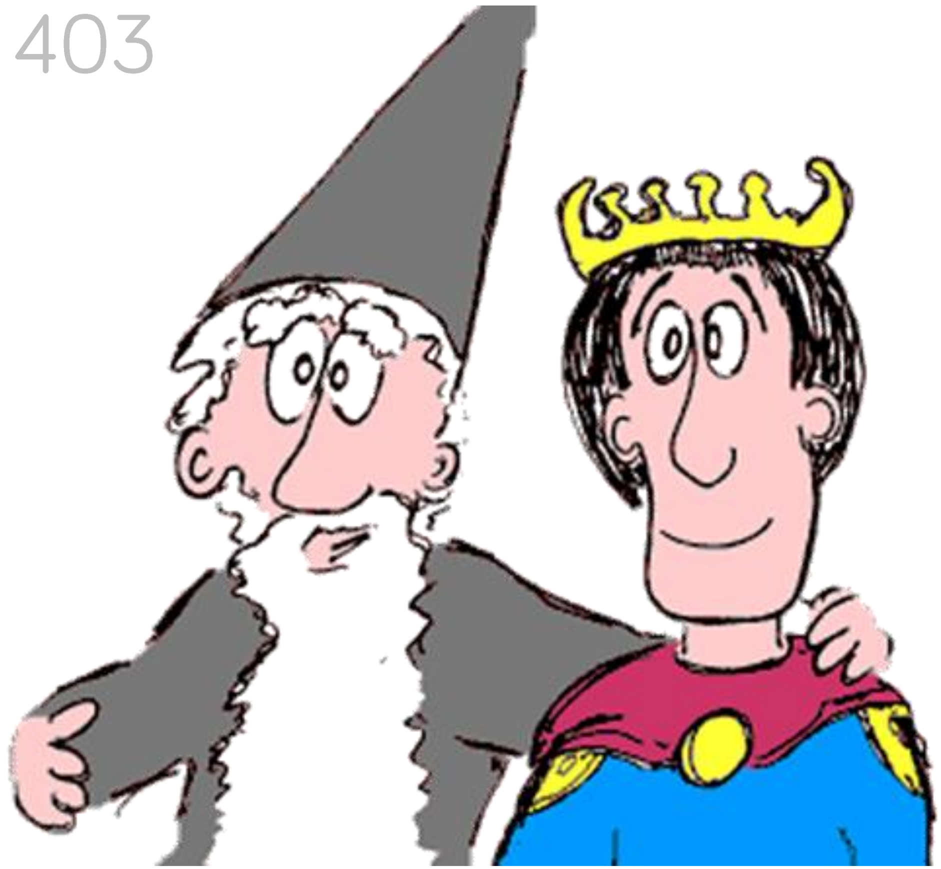
= 1500



+ 182 + 223 − 314 + 651
− 410 + 245 − 677 − 62
+ 3 + 916 − 120 + 874
+ 399 − 725 − 58 − 403

= 1500

NP

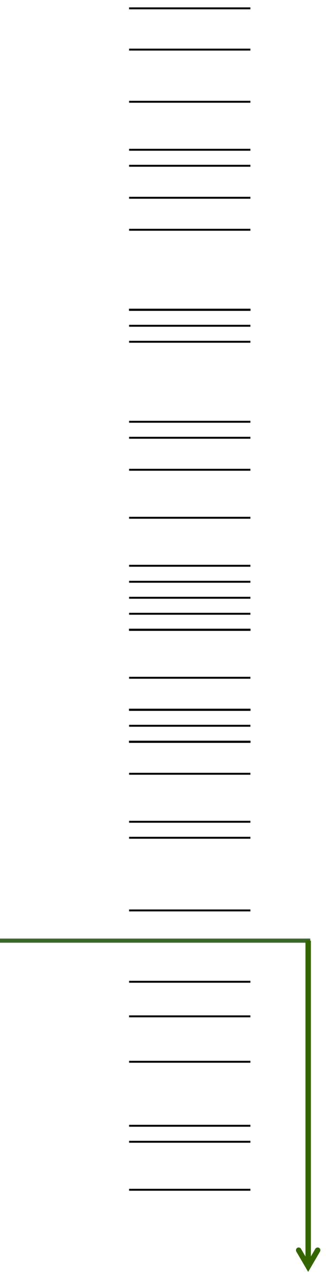


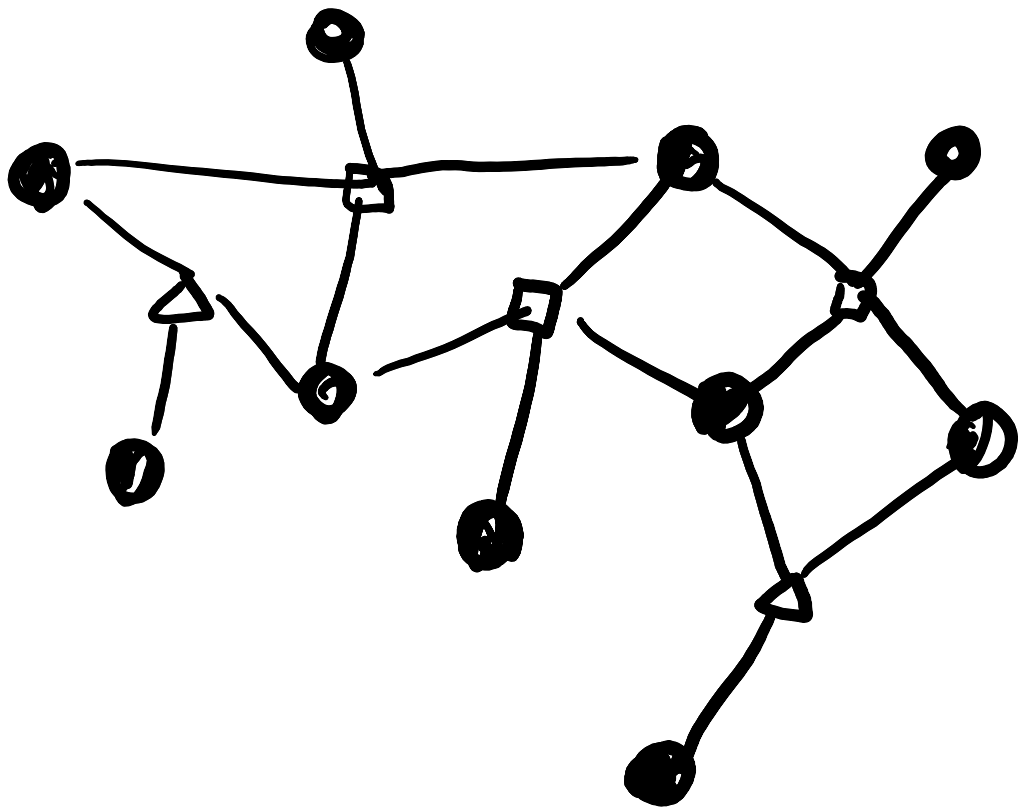
Verification?

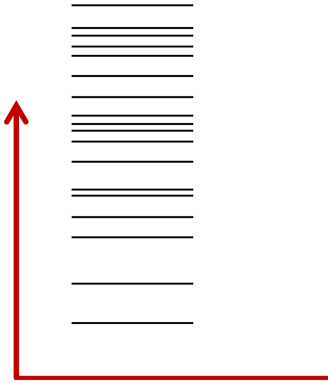
Check the solution or witness.

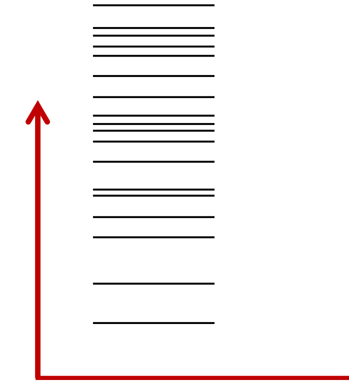
[primaryresources.co.uk]

Is the ground state energy of a Local Hamiltonian below or above a threshold?

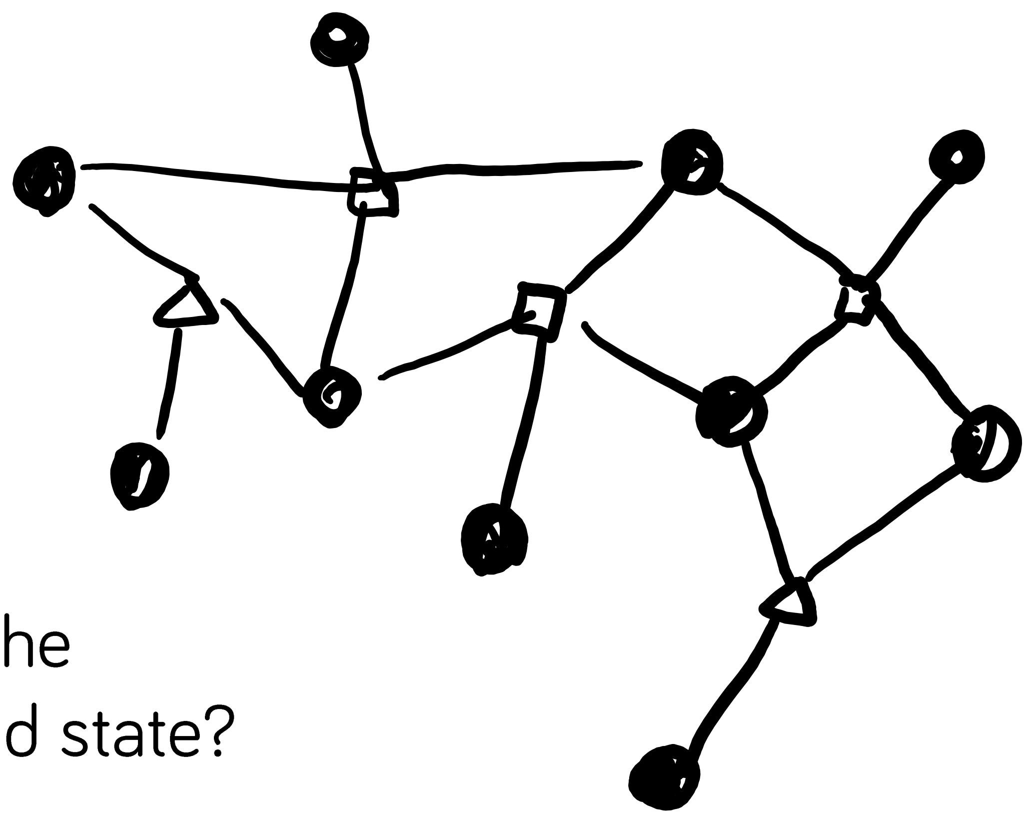


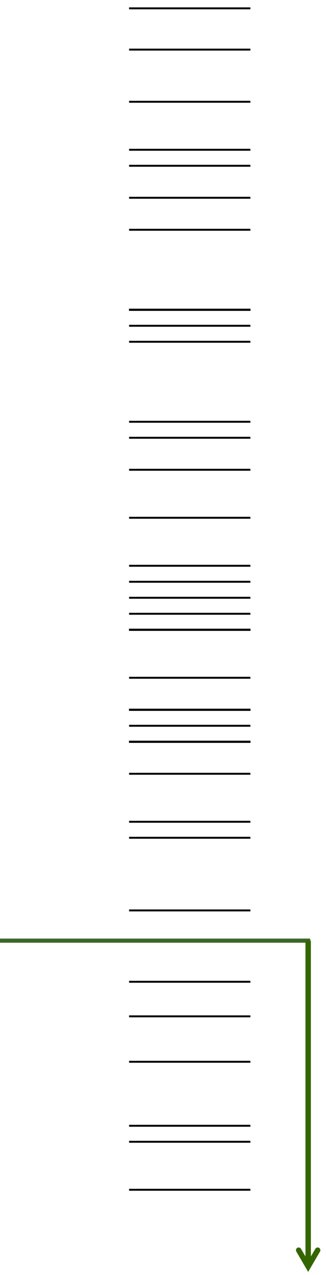






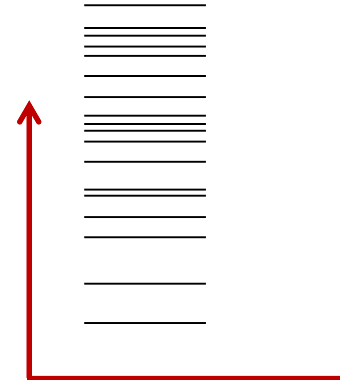
Is the ground state energy
of a Local Hamiltonian
below or above a threshold?

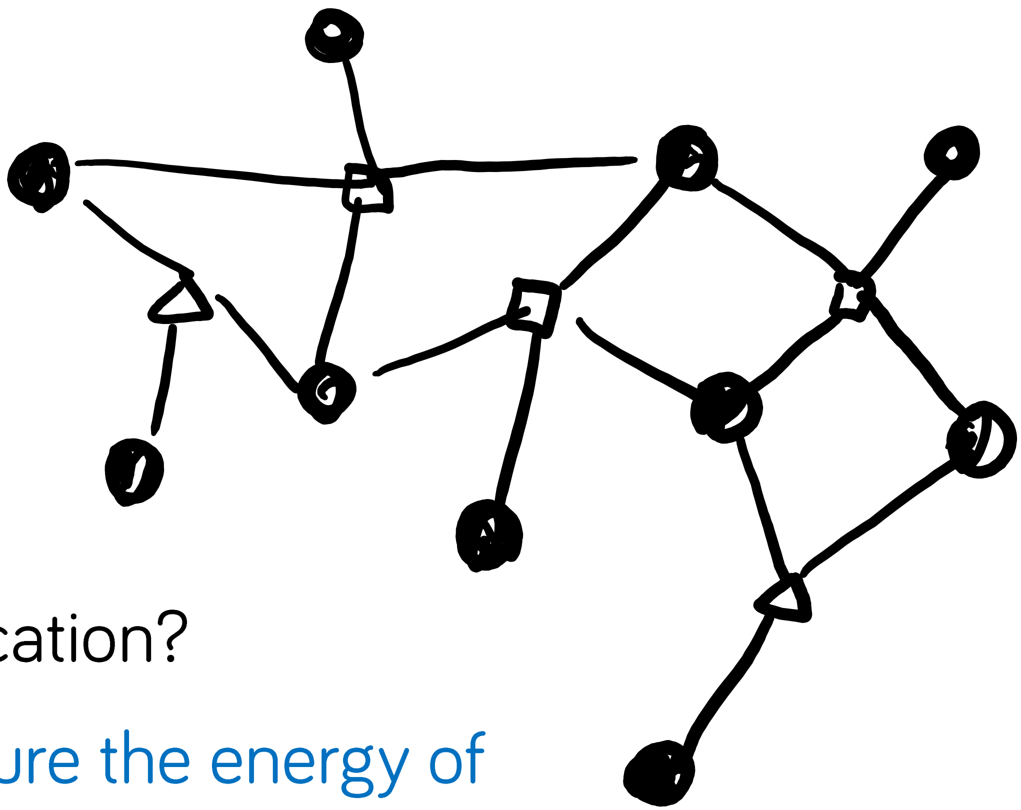


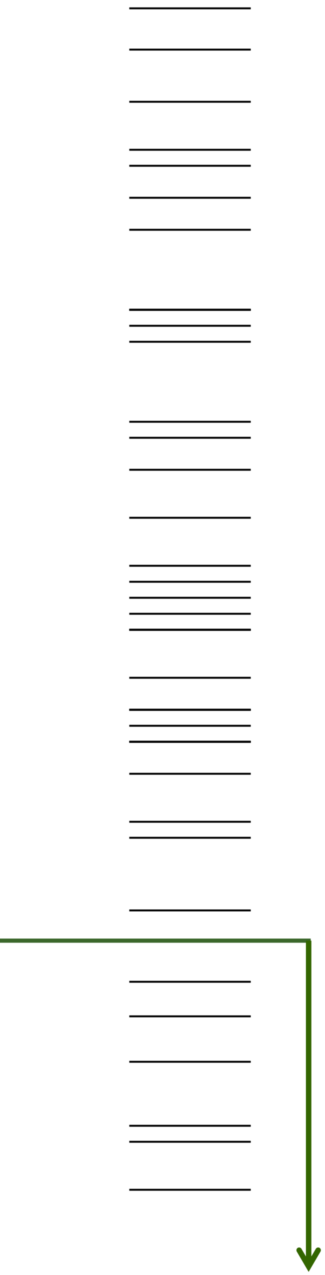


Find the
ground state?

Is the ground state energy of a Local Hamiltonian below or above a threshold?

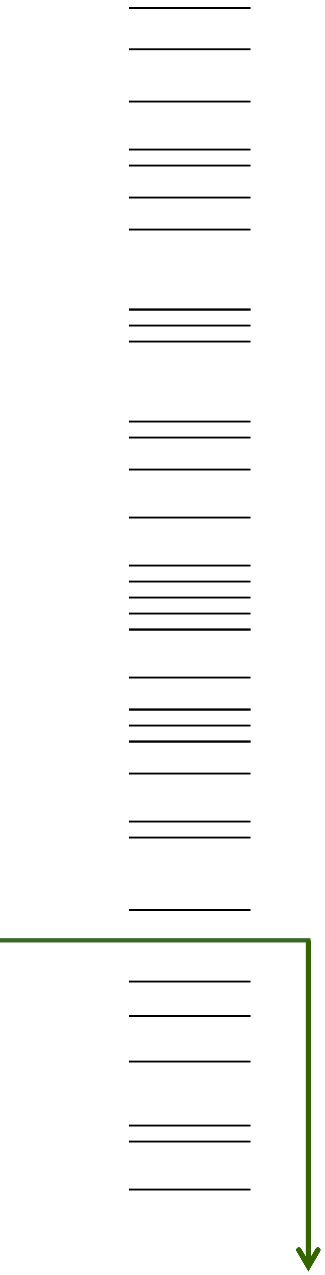




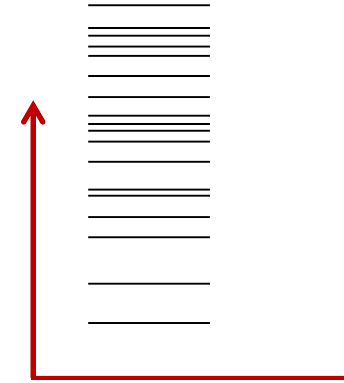


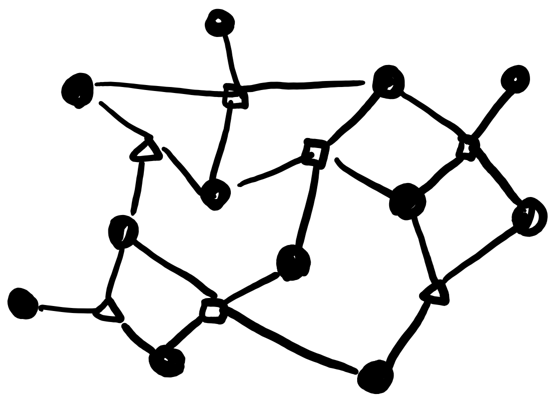
Verification?

Measure the energy of a candidate ground state.



Is the ground state energy of a Local Hamiltonian below or above a threshold?

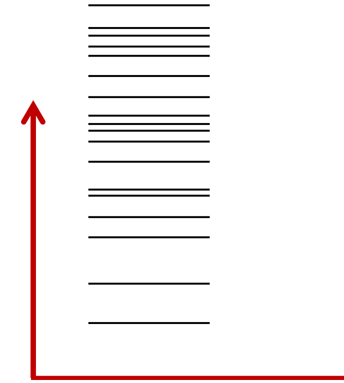




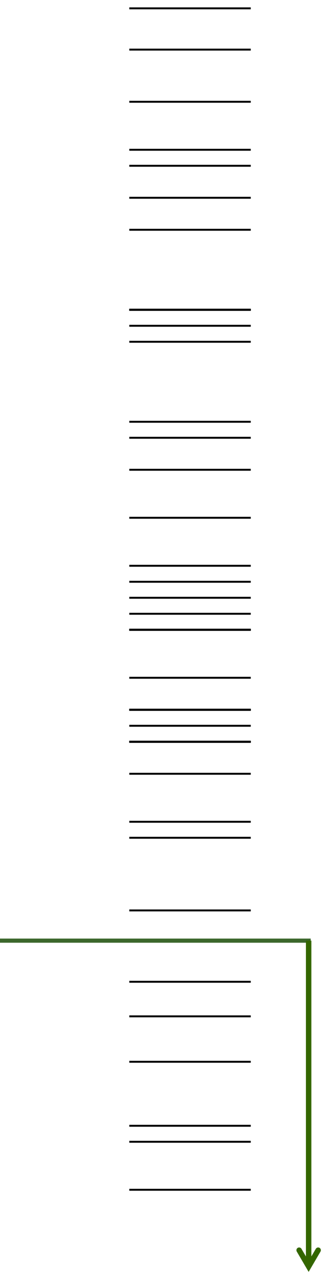
QMA

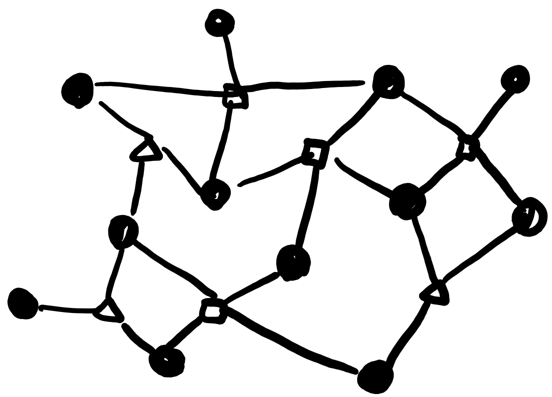
Verification?

Measure the energy of a candidate ground state.



Is the ground state energy of a Local Hamiltonian below or above a threshold?



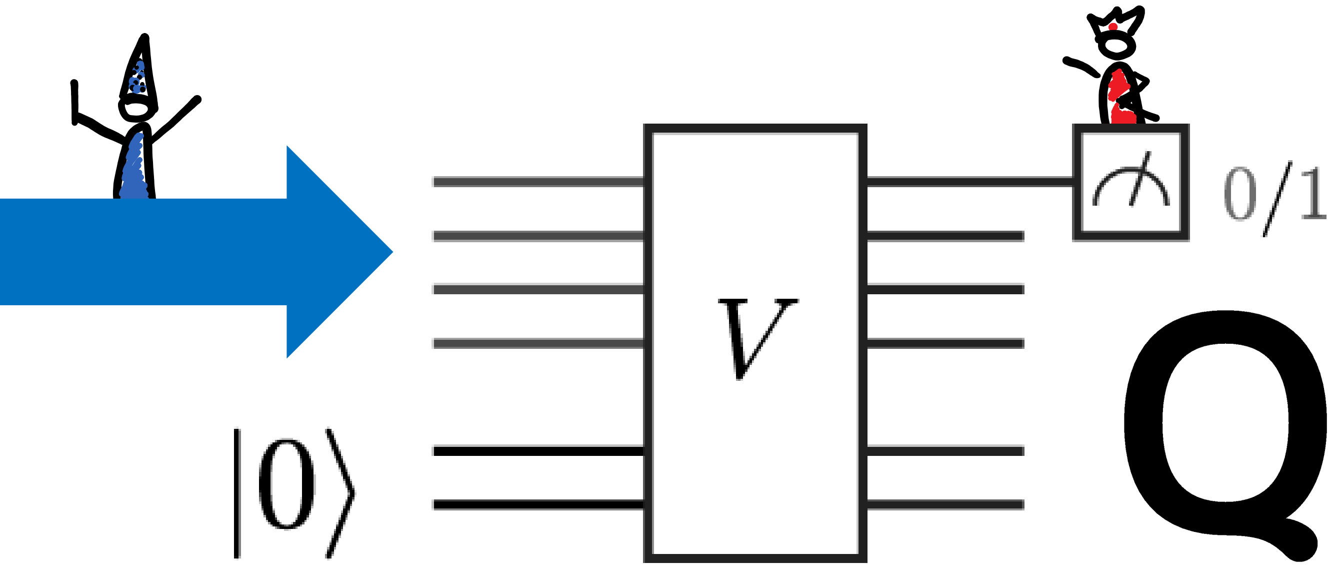


QMA

Verification?

Measure the energy of a candidate ground state.

1 How to check a quantum proof?



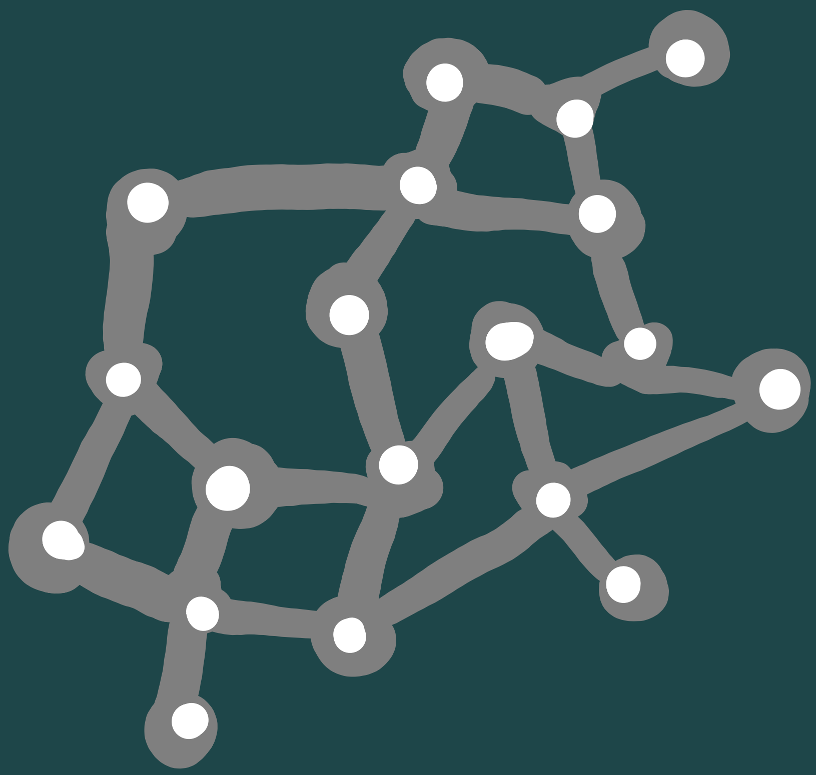
QMA

Does Arthur need a full quantum computer?

NO

1 qubit at a time

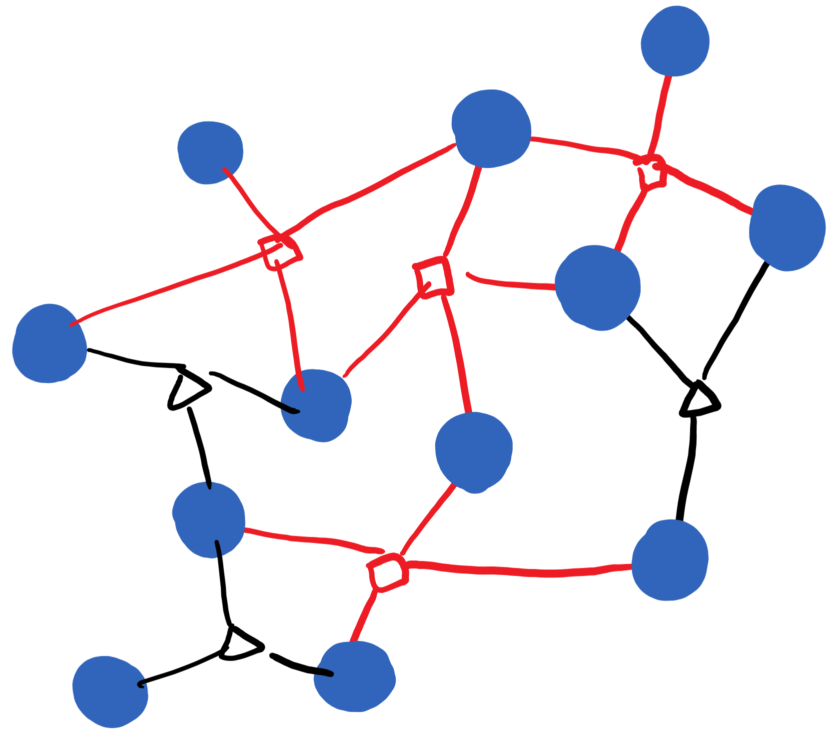
measuring the energy of a state



2 Local Hamiltonians

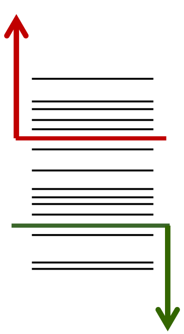
- *k*-local terms

$$H = \sum_{m=1}^{M} H_m$$



If the ground state energy is

$\geq E_b$ reject.

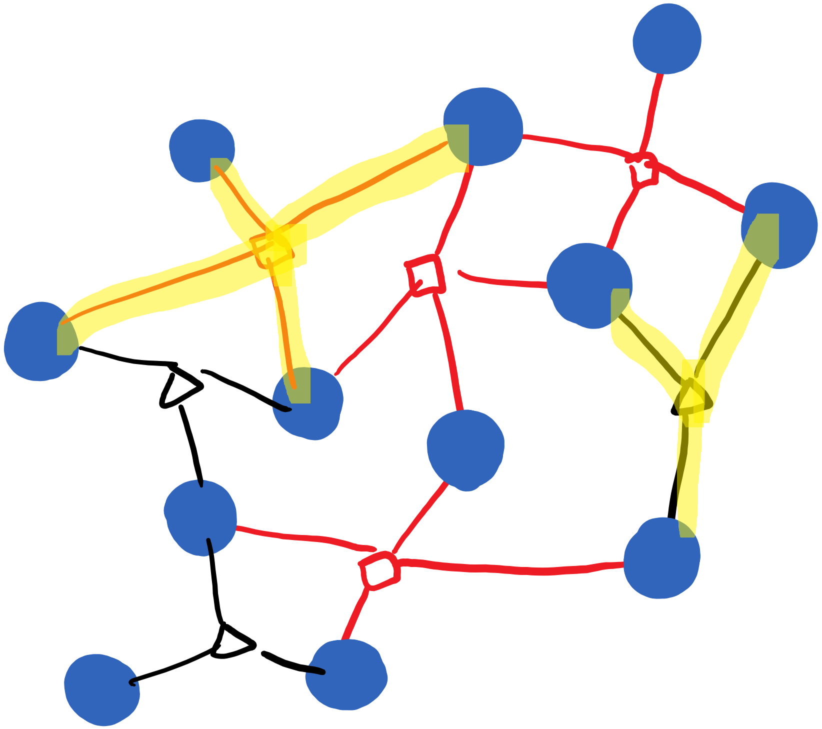


$\leq E_a$ accept.

2 Local Hamiltonians

- *k*-local terms

$$H = \sum_{m=1}^{M} H_m$$



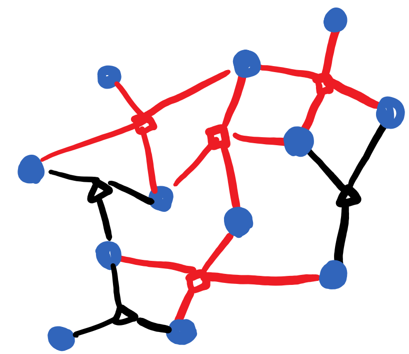
Pauli basis decomposition.

$$H_m = \sum_{S \in \mathcal{P}} c_S^m S$$

$$S = \mathbb{I} \otimes \sigma_1 \otimes \sigma_2 \otimes \mathbb{I} \otimes \sigma_3 \otimes \cdots$$

2 Local Hamiltonians

- *k*-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S\in\mathcal{P}} c_S^m S$

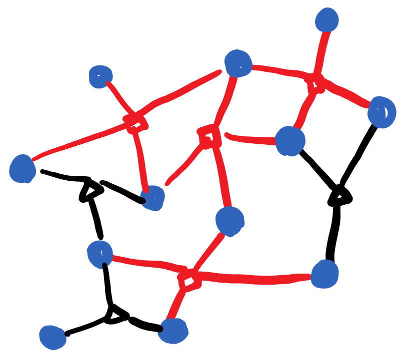


The eigenvalues are ±1.

$$S = \mathbb{I} \otimes \sigma_1 \otimes \sigma_2 \otimes \mathbb{I} \otimes \sigma_3 \otimes \cdots$$

2 Local Hamiltonians

- *k*-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S \in \mathcal{P}} c_S^m S$ $\frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$



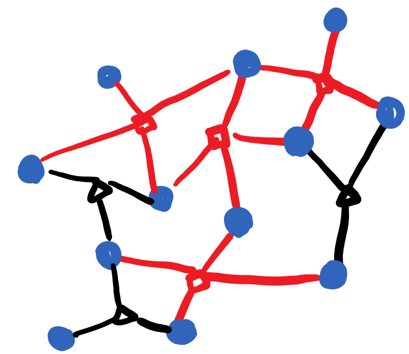
Shift by a constant to get projectors.

$$P_S$$

$$cS = 2c\,\frac{1}{2}\left(\mathbb{I} + S\right) - c\,\mathbb{I}$$

$$-dS = 2d\,\frac{1}{2}\left(\mathbb{I} - S\right) - d\,\mathbb{I}$$

2 Local Hamiltonians



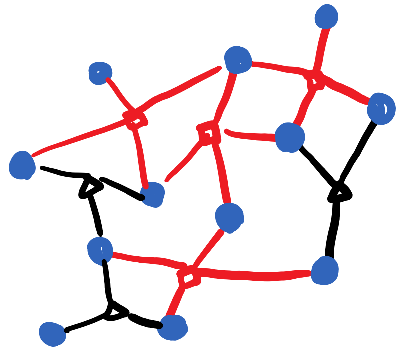
- k-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S \in \mathcal{P}} c_S^m S$ $\frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$
- projectors $\sum_{S \in \mathcal{P}} 2|d_S| P_S - \mathbb{I} \sum_{S \in \mathcal{P}} |d_S|$

Convert to a weighted sum of projectors.

$$\frac{1}{\sum_S 2|d_S|} \sum_{S \in \mathcal{P}} 2|d_S| P_S$$

2 Local Hamiltonians

- *k*-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S\in\mathcal{P}} c_S^m S$ $\frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$
- projectors $\sum_{S\in\mathcal{P}} 2|d_S| P_S - \mathbb{I} \sum_{S\in\mathcal{P}} |d_S|$

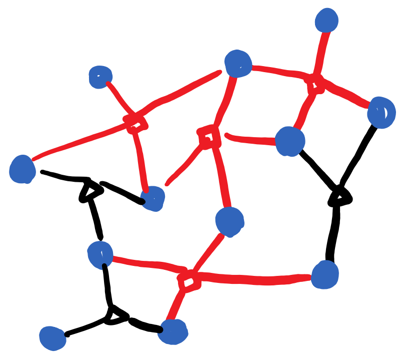


Convert to a weighted sum of projectors.

$$\frac{1}{\sum_S 2|d_S|} \sum_{S\in\mathcal{P}} 2|d_S| P_S$$

π_S

2 Local Hamiltonians

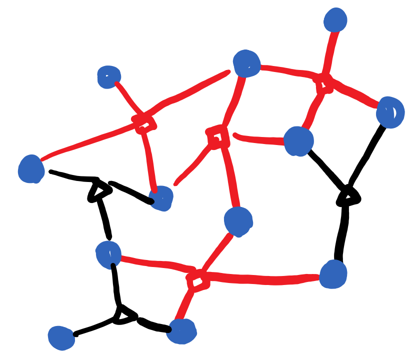


- *k*-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S \in \mathcal{P}} c_S^m S$ $\frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$
- projectors $\sum_{S \in \mathcal{P}} 2|d_S| P_S - \mathbb{I} \sum_{S \in \mathcal{P}} |d_S|$
- a sum of projectors with probabilistic weights $\sum_{S} \pi_S P_S$

Pick a random projector, measure its Paulis.

$$r = \frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$$

2 Local Hamiltonians

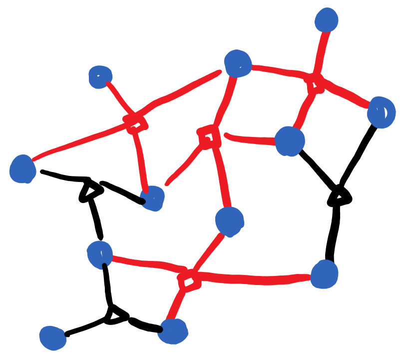


- *k*-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S \in \mathcal{P}} c_S^m S$ $\frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$
- projectors $\sum_{S \in \mathcal{P}} 2|d_S| P_S - \mathbb{I} \sum_{S \in \mathcal{P}} |d_S|$
- a sum of projectors with probabilistic weights $\sum_{S} \pi_S P_S$
- a random measurement with expectation value

$$\langle r \rangle = \frac{1}{\sum_S 2|d_S|}\left(\langle \psi | H | \psi \rangle + \sum_S |d_S| \right)$$

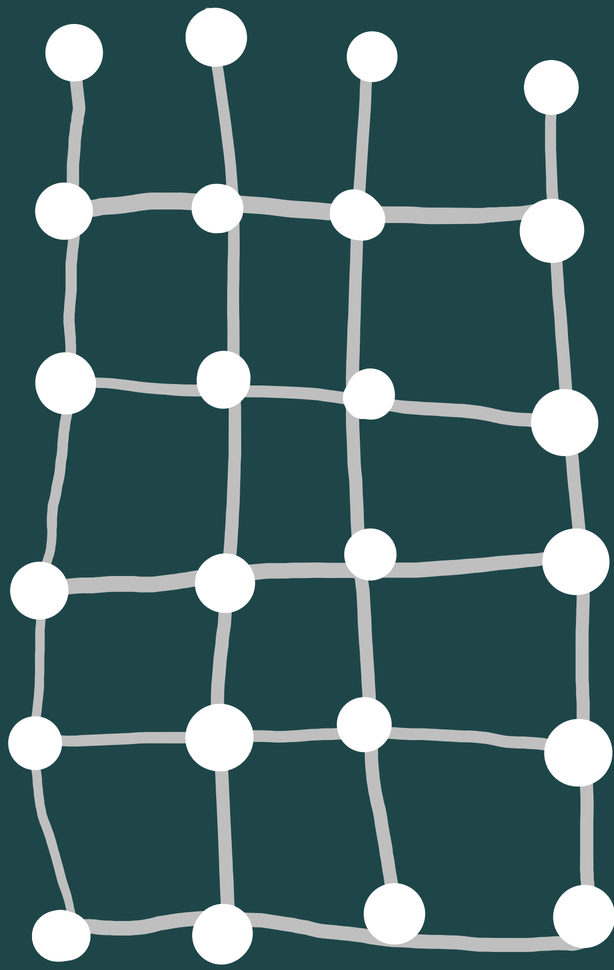
accept/reject

2 Local Hamiltonians



- *k*-local terms $\sum_{m=1}^{M} H_m$
- Pauli terms $\sum_{S\in\mathcal{P}} c_S^m S$ $\frac{1}{2}\left(\mathbb{I} \pm \sigma_1 \otimes \mathbb{I} \otimes \sigma_2 \otimes \cdots\right)$
- projectors $\sum_{S\in\mathcal{P}} 2|d_S| P_S - \mathbb{I} \sum_{S\in\mathcal{P}} |d_S|$
- a sum of projectors with probabilistic weights $\sum_{S} \pi_S P_S$
- a random measurement 1 qubit at a time: accept/reject

Repetition helps, as $p_{\text{acc}}^{\text{yes}} - p_{\text{acc}}^{\text{no}} \geqslant \dfrac{E_b - E_a}{\sum_S 2|d_S|}$.

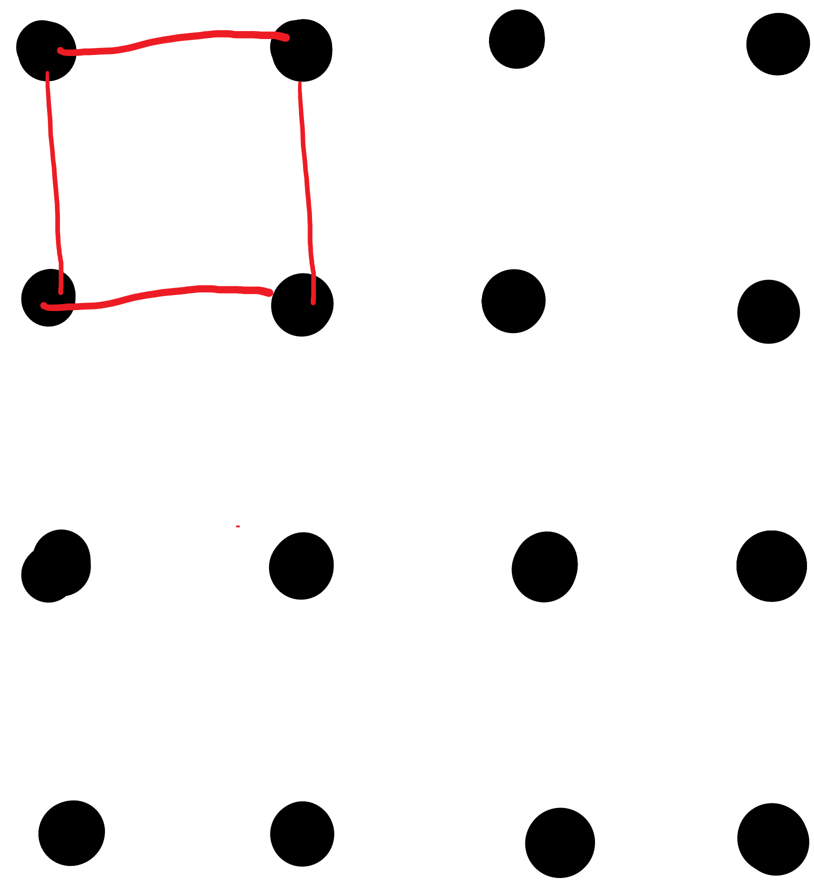


verifying proofs using a graph state

3 Measurement based quantum computing (MBQC)

- graph state creation

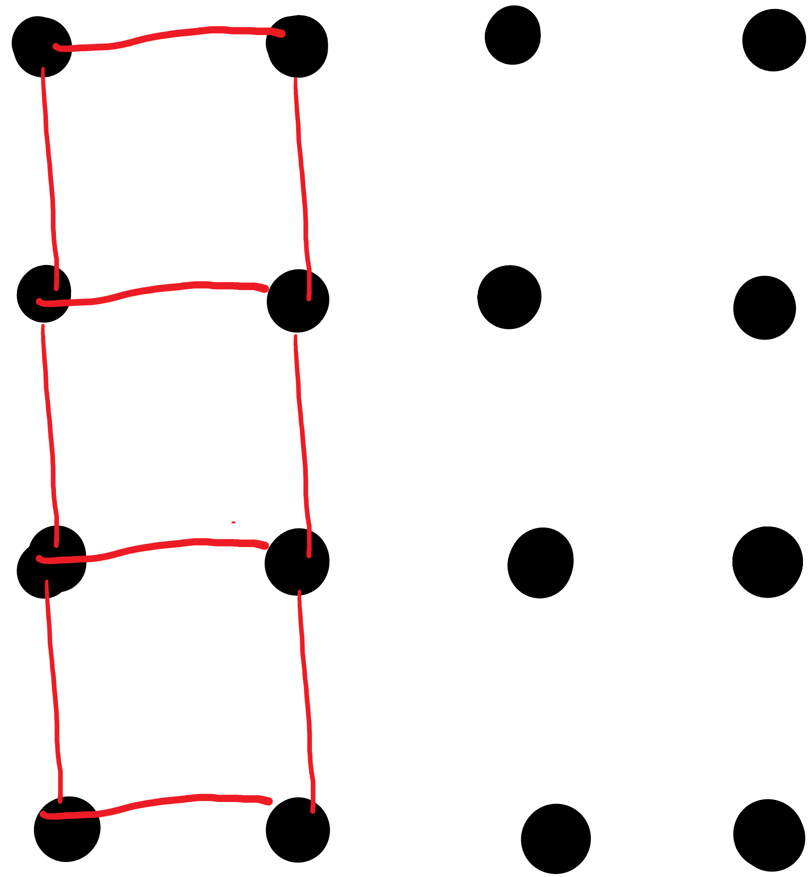
$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes |V|}$$



3 Measurement based quantum computing (MBQC)

- graph state creation

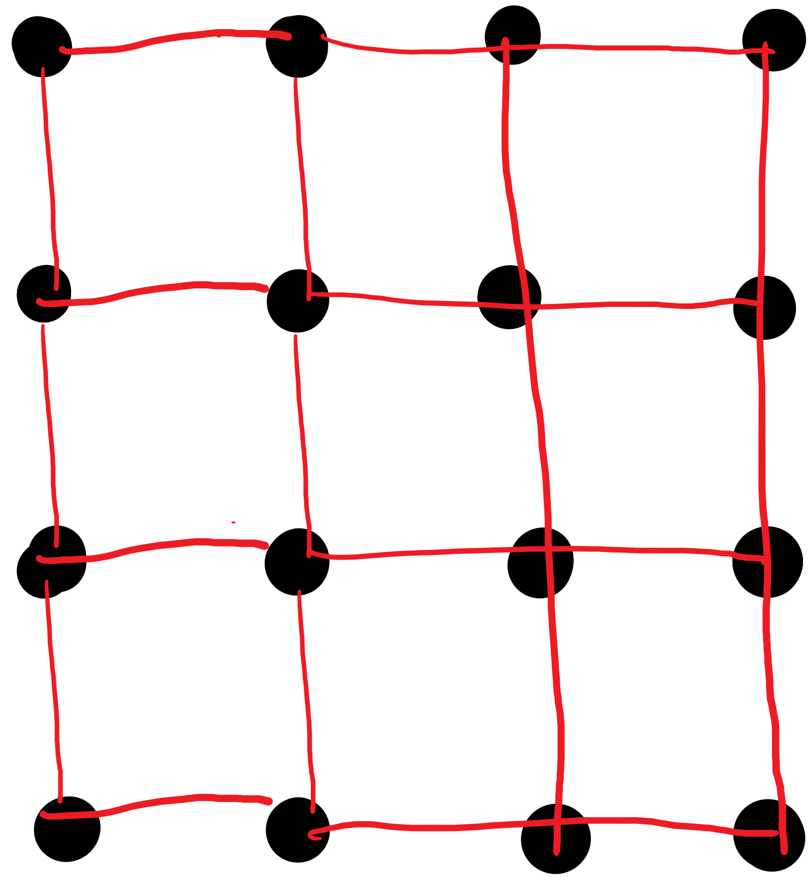
$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$



Measurement based quantum computing (MBQC)

- graph state creation

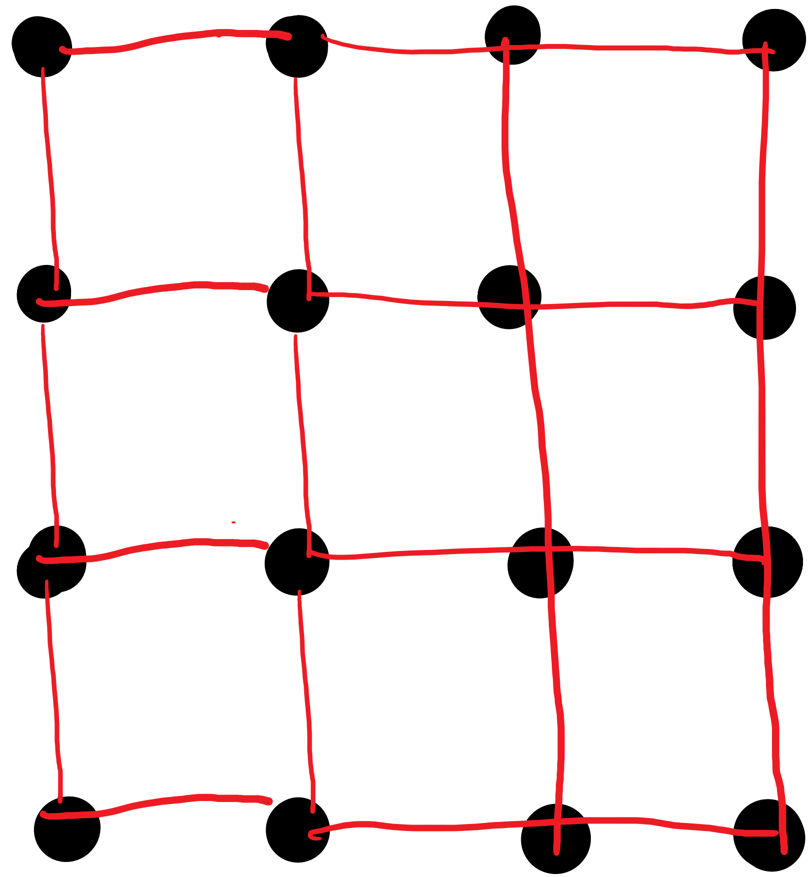
$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

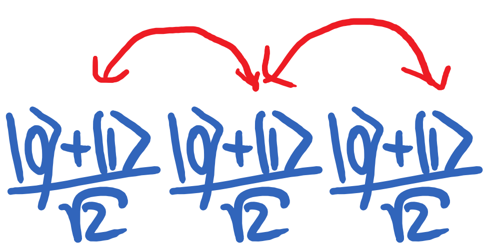


3 Measurement based quantum computing (MBQC)

- graph state creation

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$





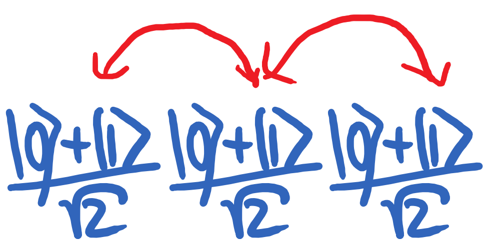
3 Measurement based quantum computing (MBQC)

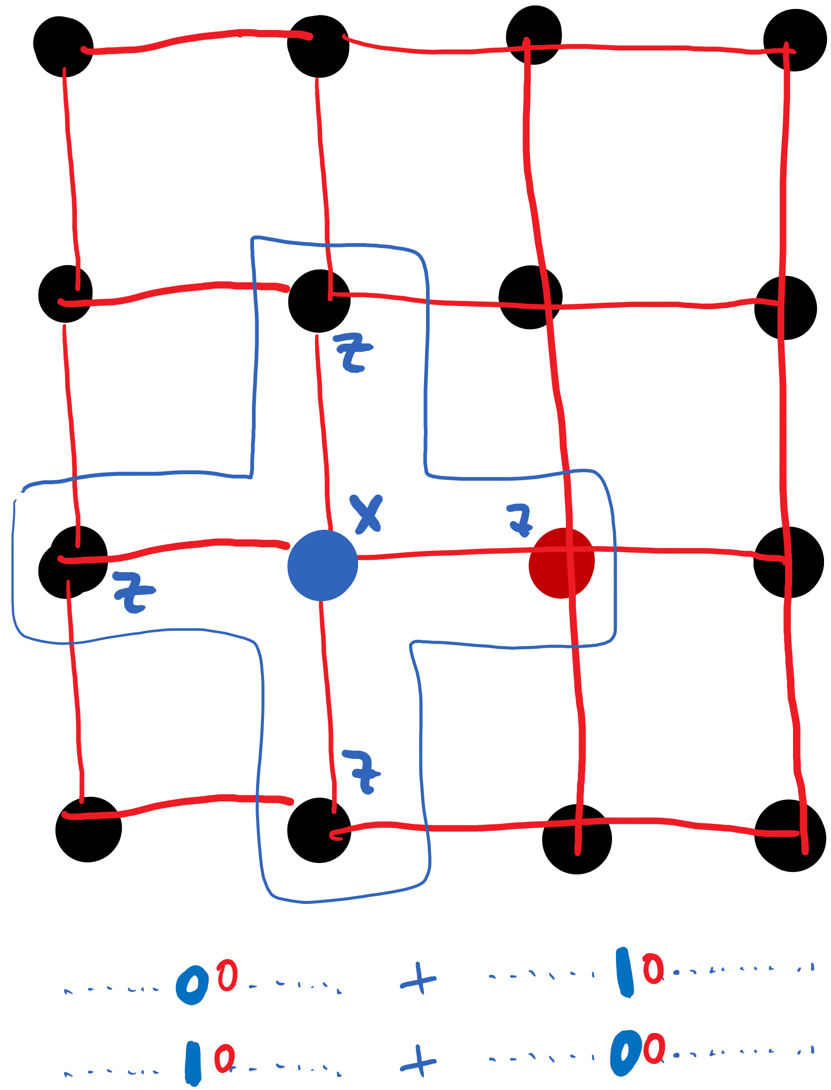
- graph state creation

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- the stabilizers

$$X_j \bigotimes_{i\in S_j} Z_i$$





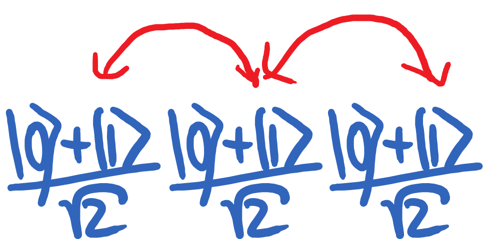
3 Measurement based quantum computing (MBQC)

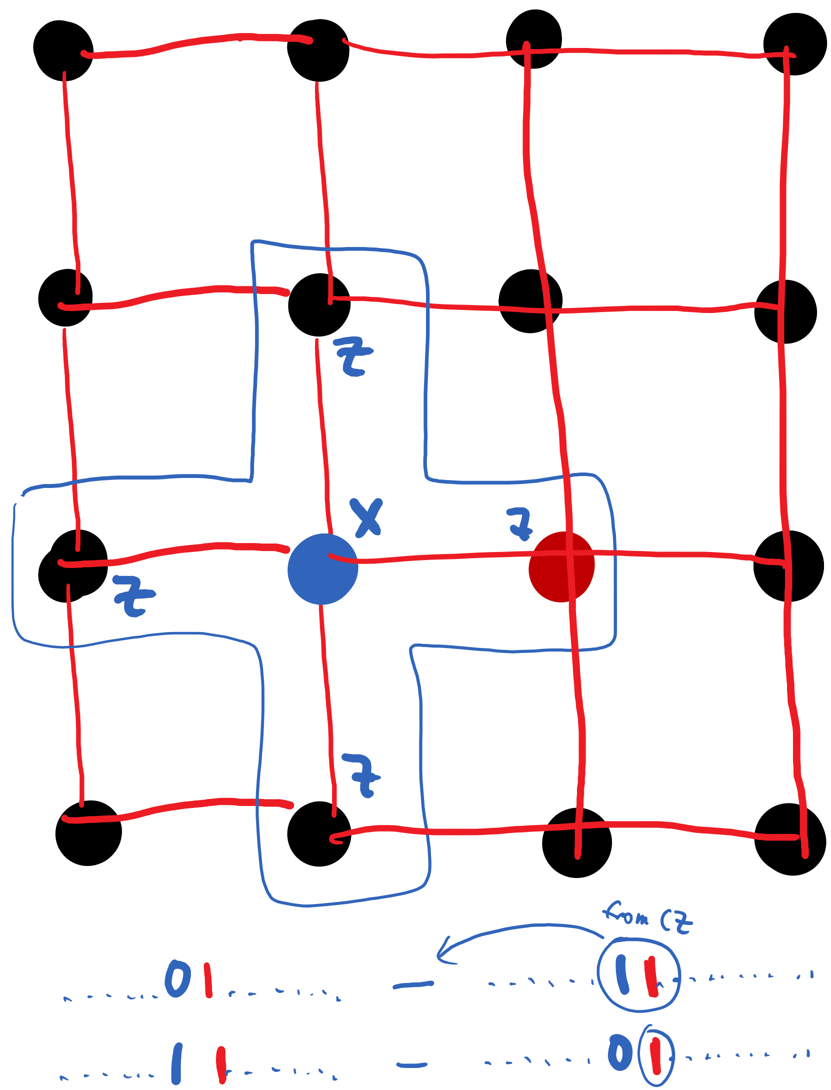
- graph state creation

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- the stabilizers

$$X_j \bigotimes_{i\in S_j} Z_i$$





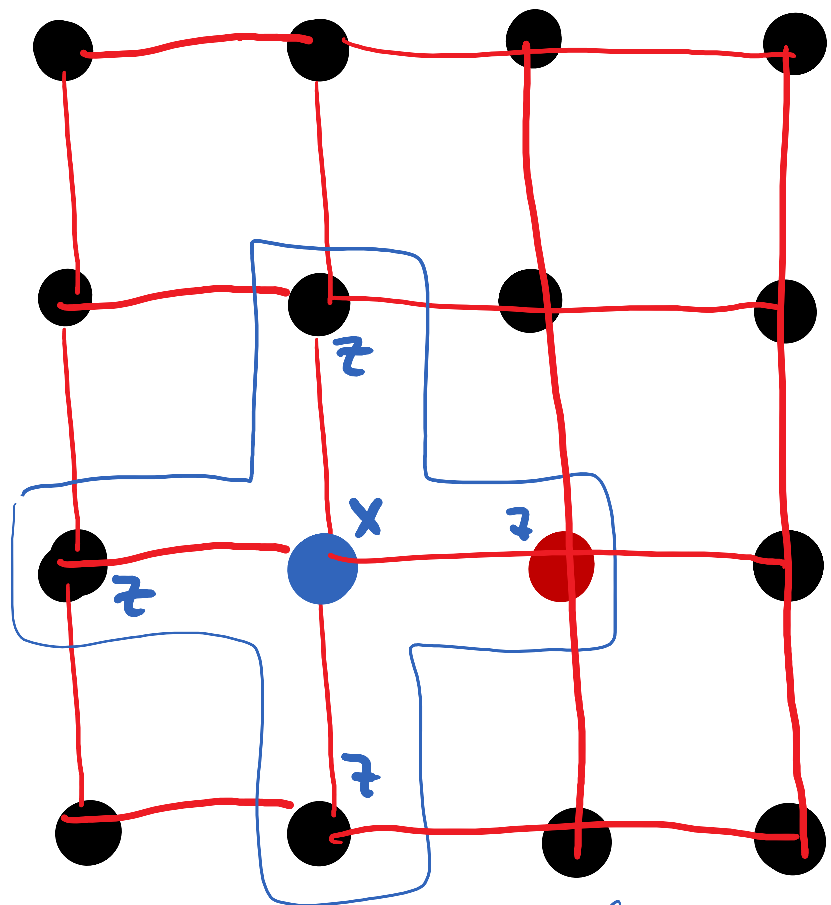
3 Measurement based quantum computing (MBQC)

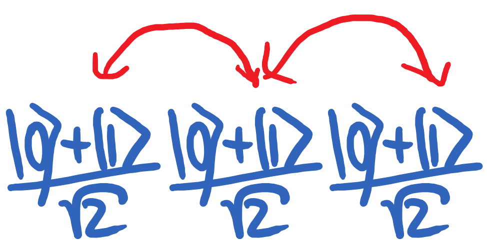
- graph state creation

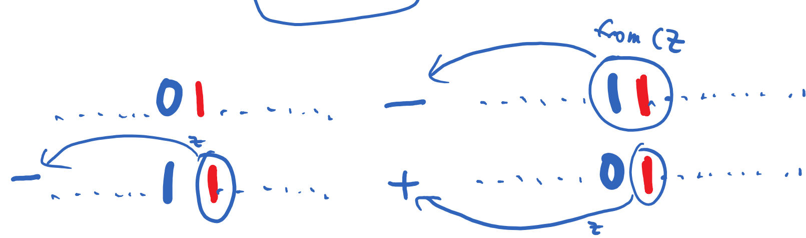
$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- the stabilizers

$$X_j \bigotimes_{i\in S_j} Z_i$$



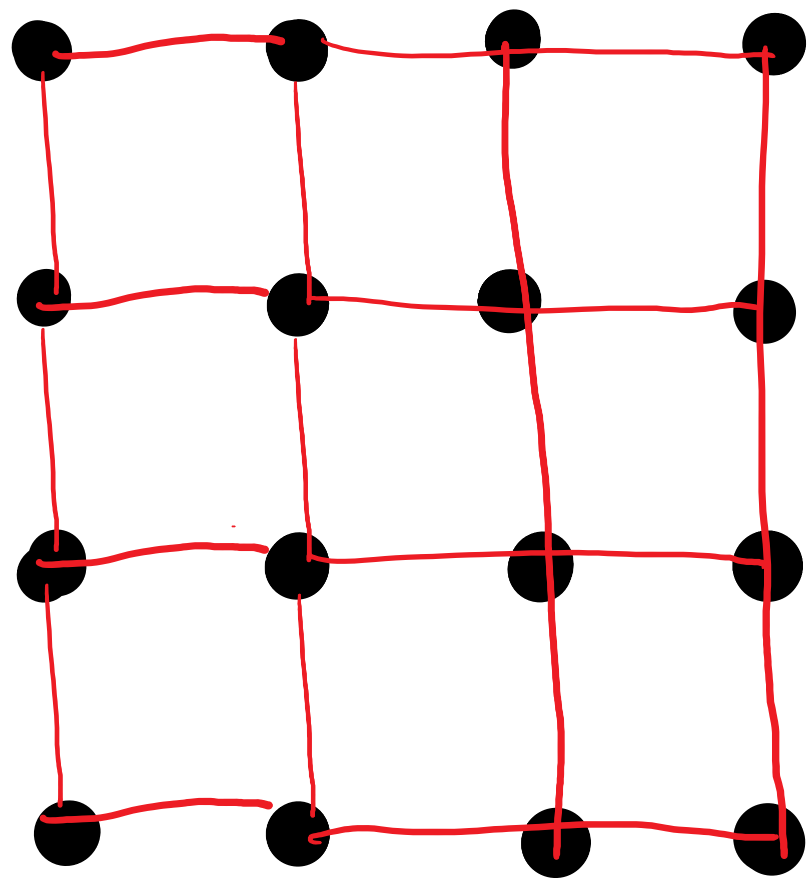




3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$



- the stabilizers

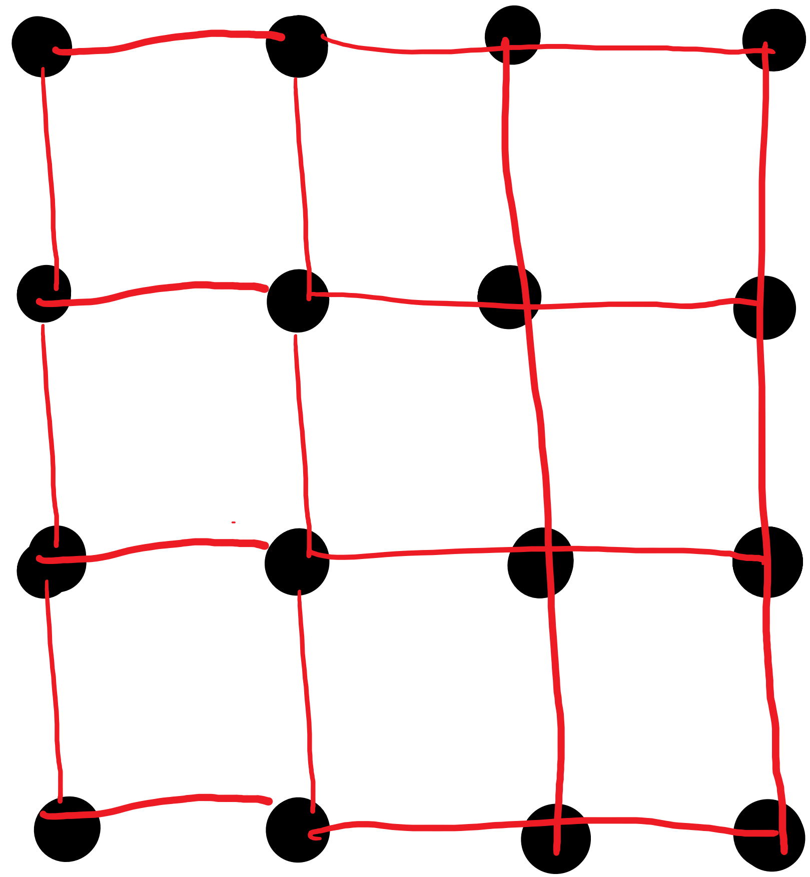
$$X_j \bigotimes_{i\in S_j} Z_i$$

- How can you verify
  that you received this state?

3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$



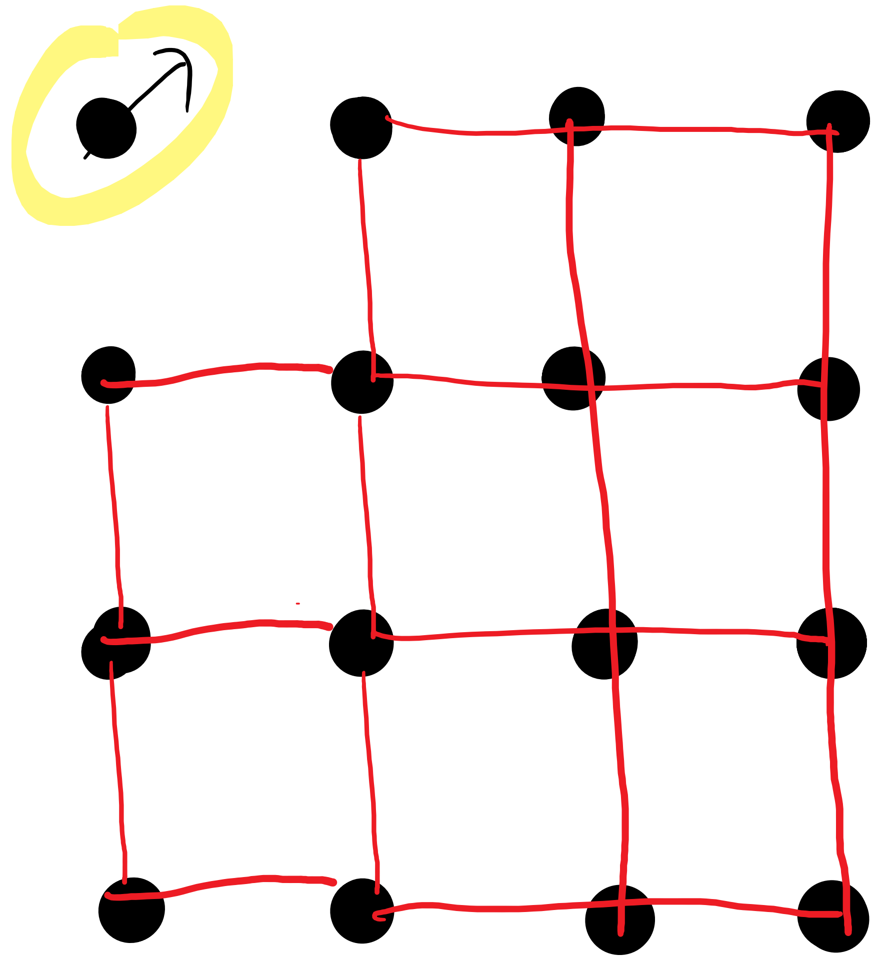
- to compute, measure 1 qubit at a time

3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- to compute, measure 1 qubit at a time

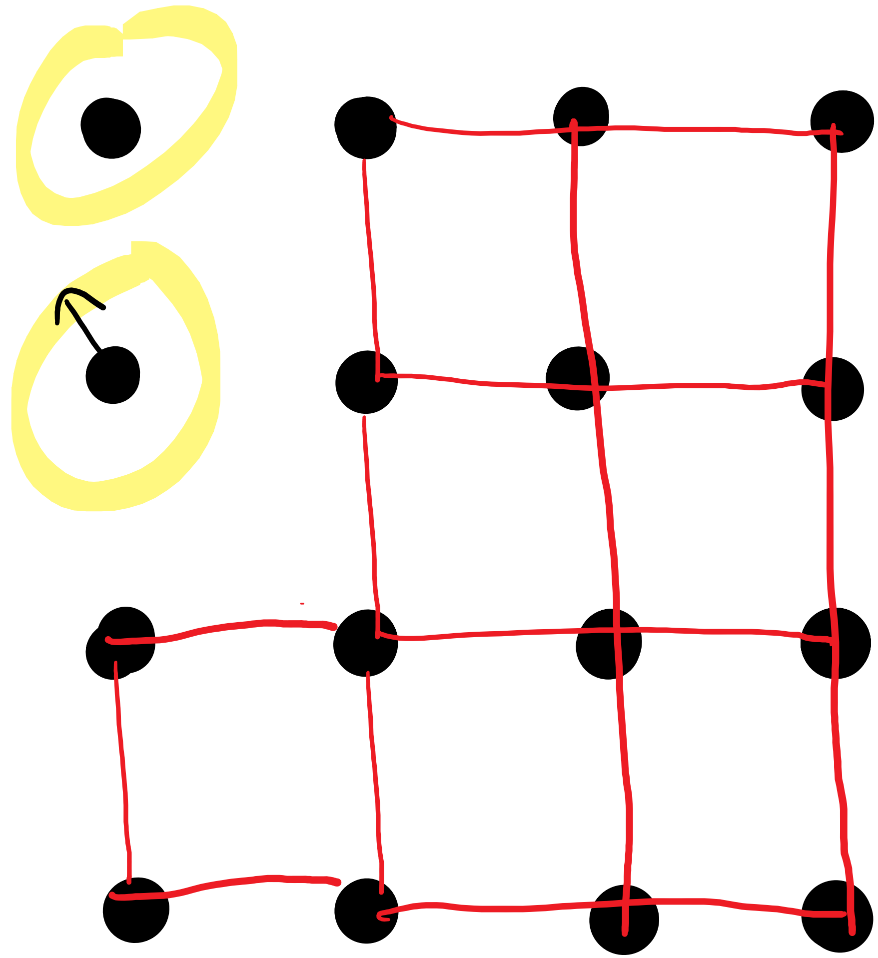


3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- to compute, measure 1 qubit at a time

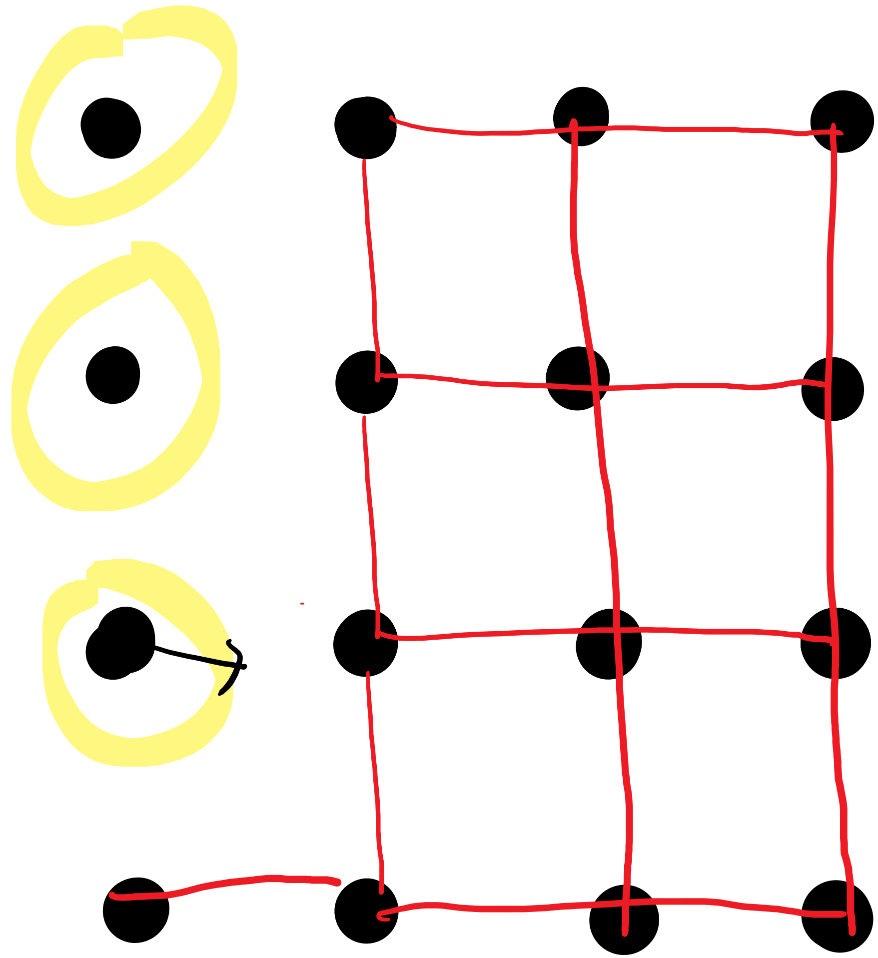


3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- to compute, measure 1 qubit at a time

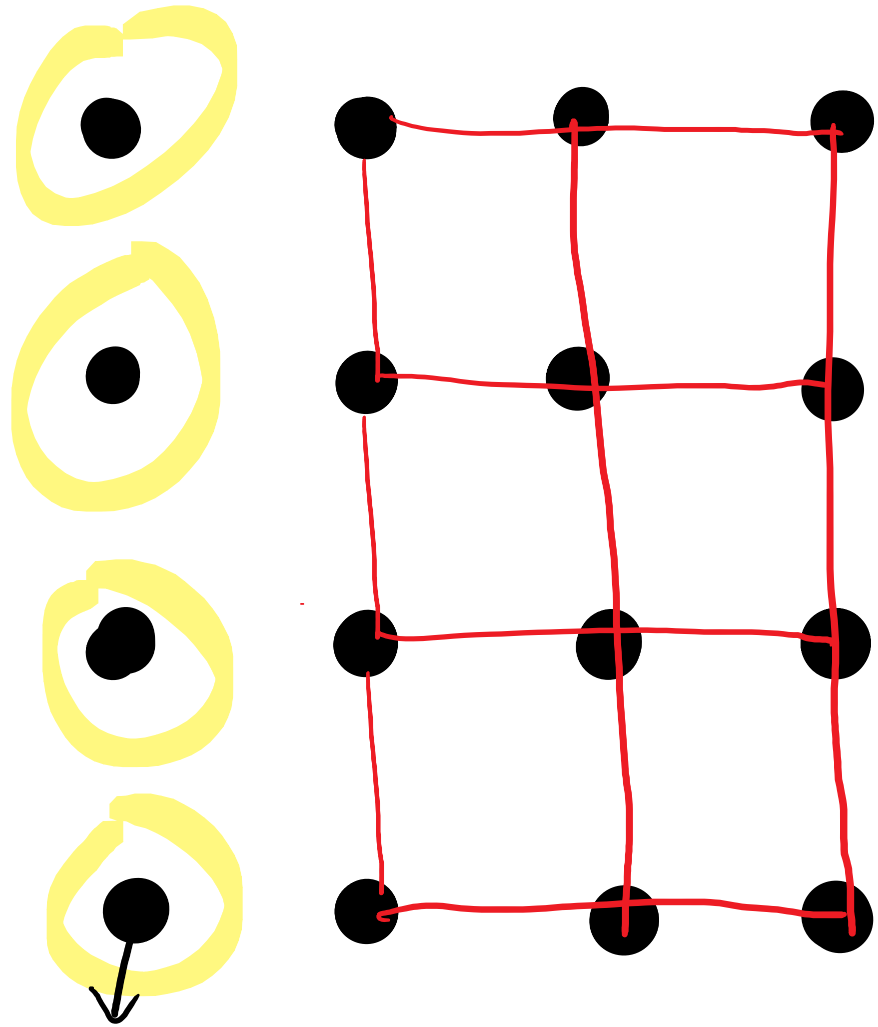


3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

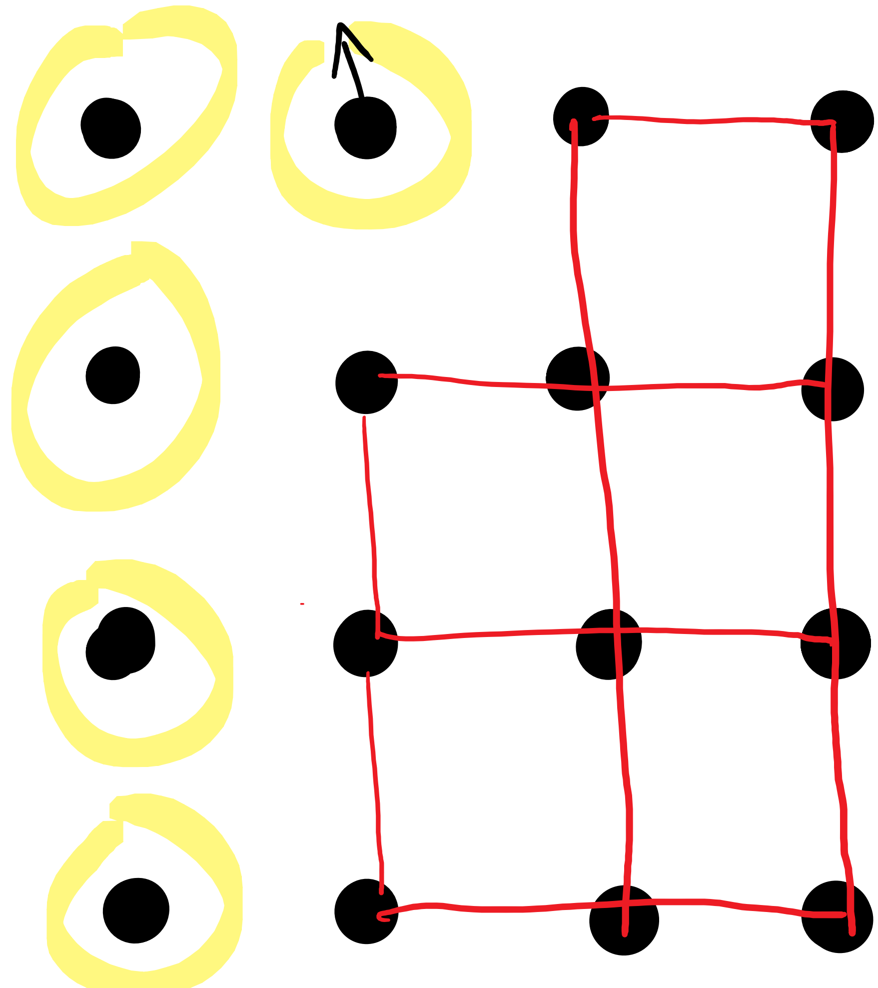
- to compute, measure 1 qubit at a time



3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$



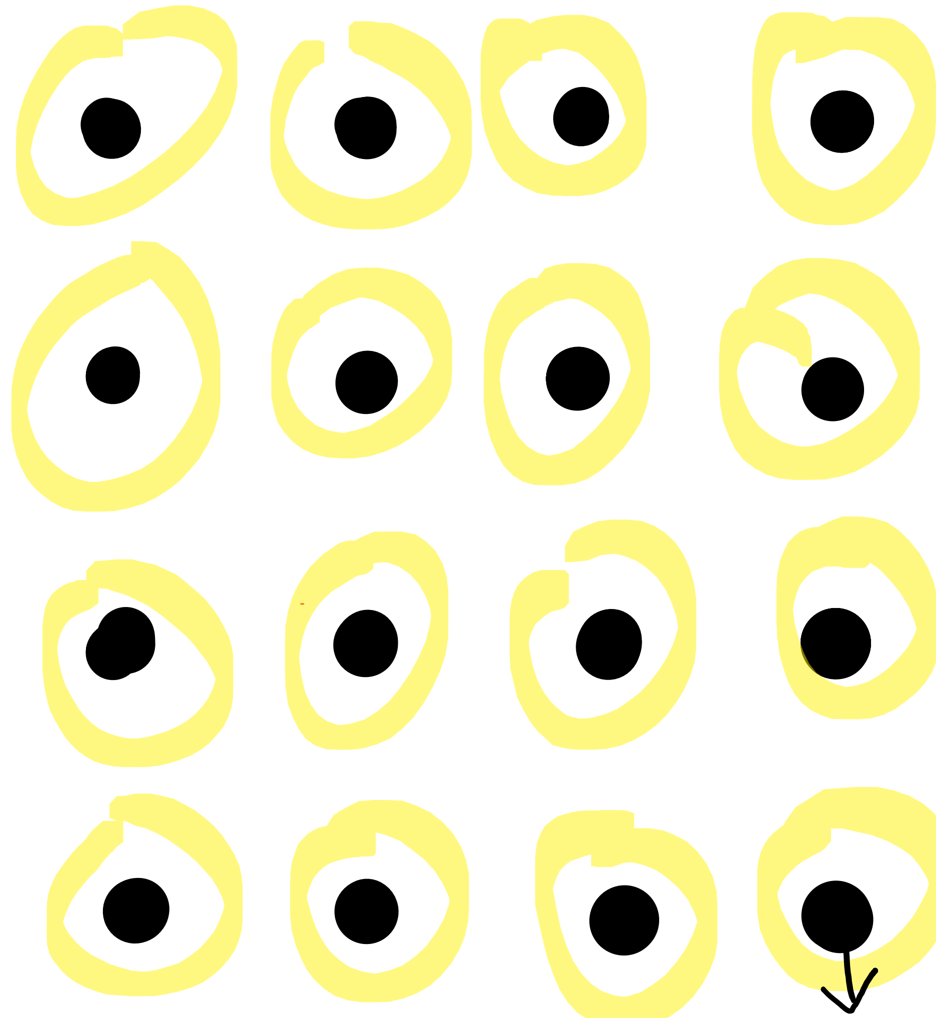
- to compute, measure 1 qubit at a time

3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

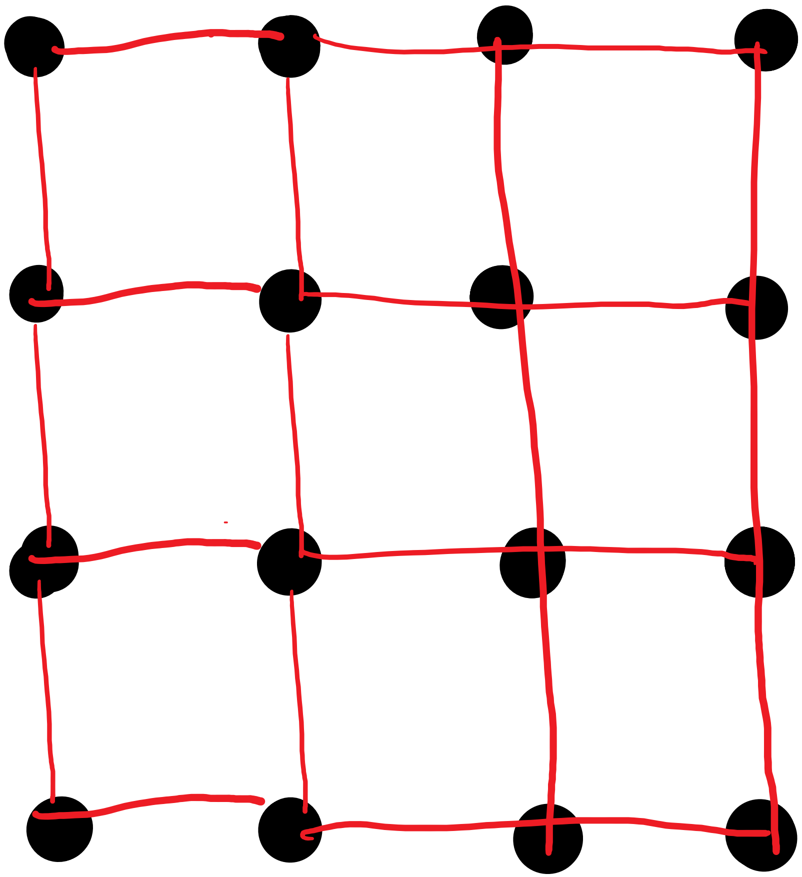
- to compute, measure 1 qubit at a time

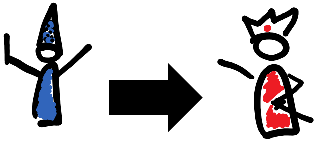


3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$



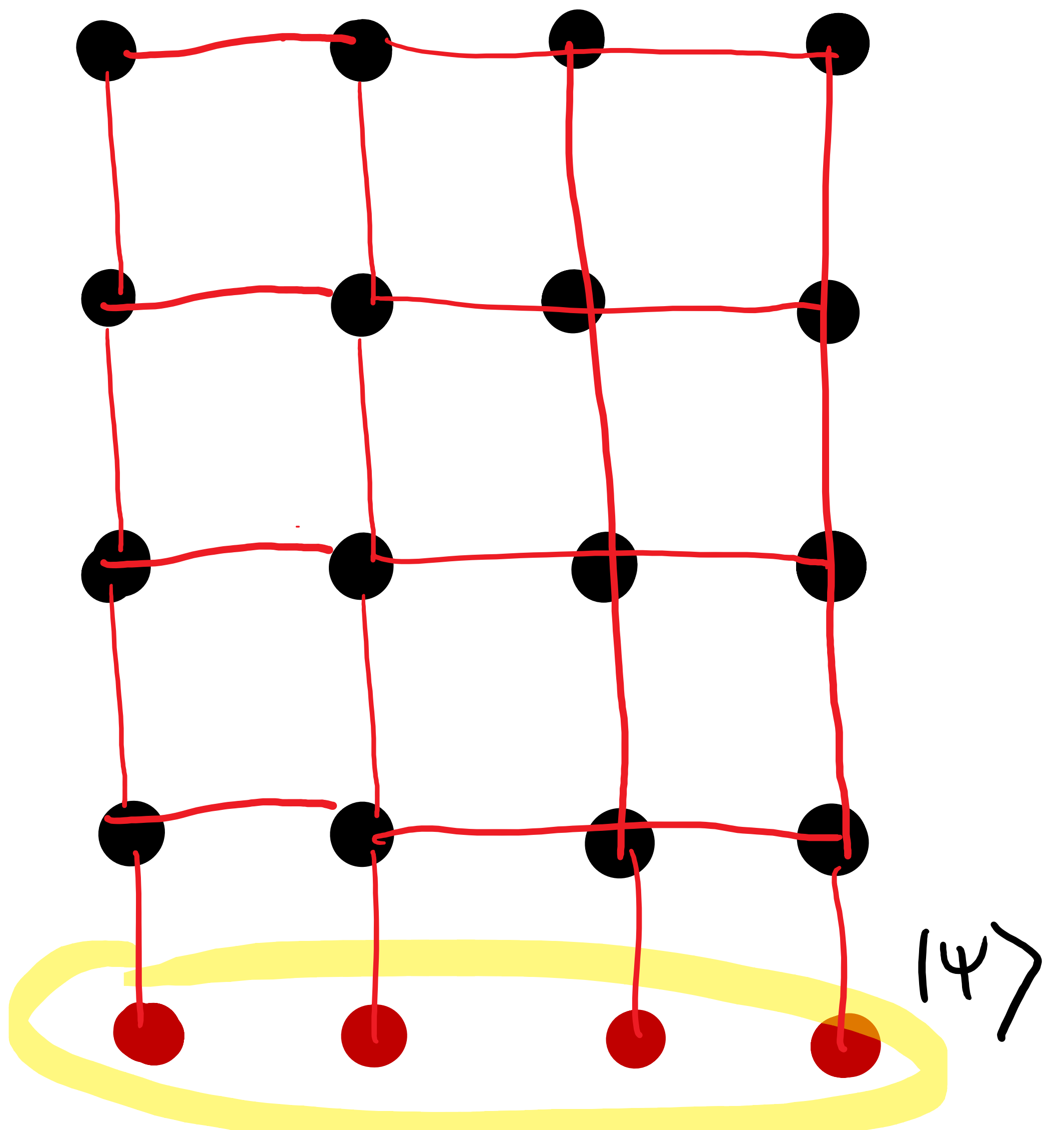


- send a witness?

3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$



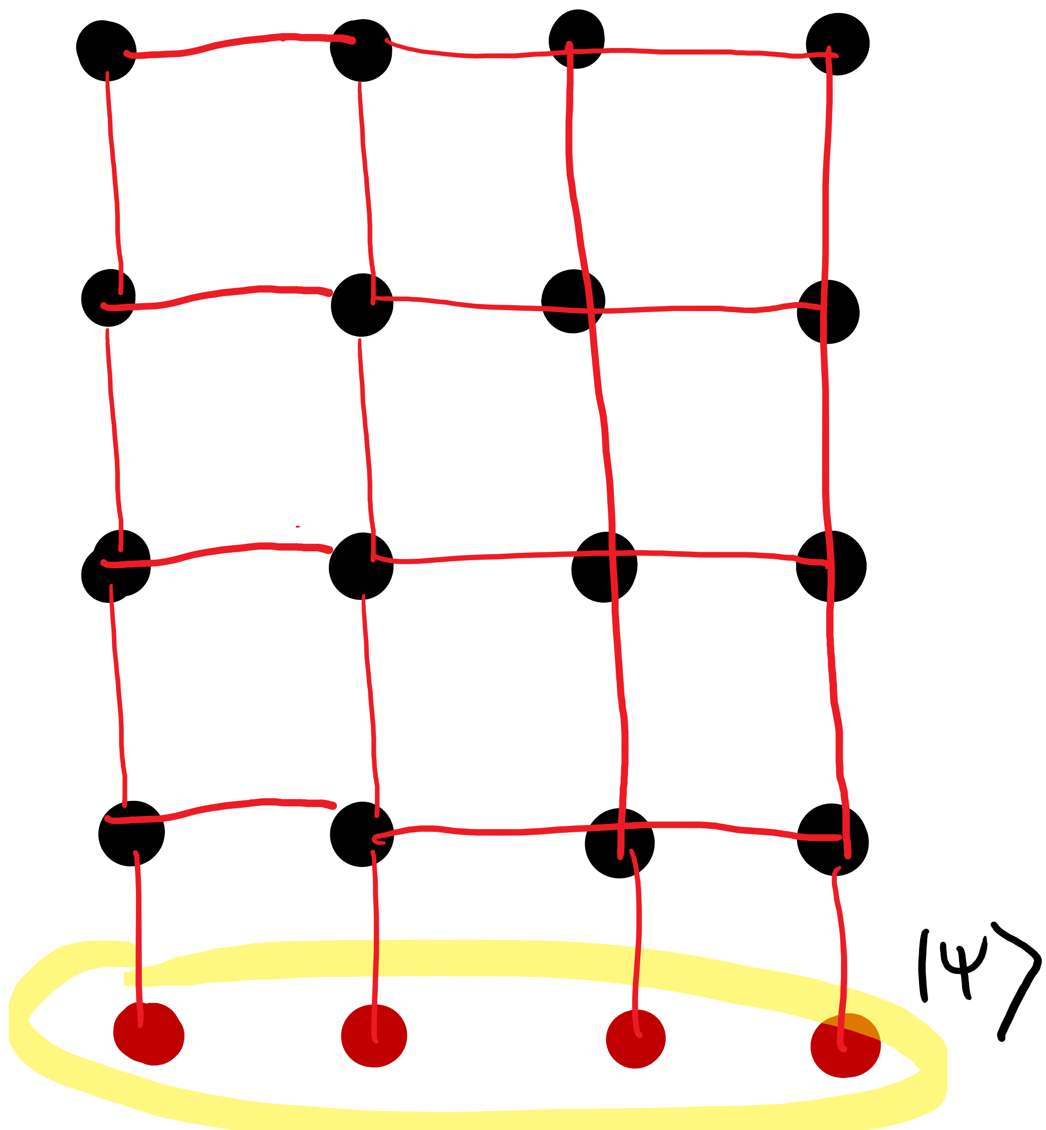
- entangle a witness

3 Measurement based quantum computing (MBQC)

- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

What are the stabilizers now?



- entangle a witness

3 Measurement based quantum computing (MBQC)

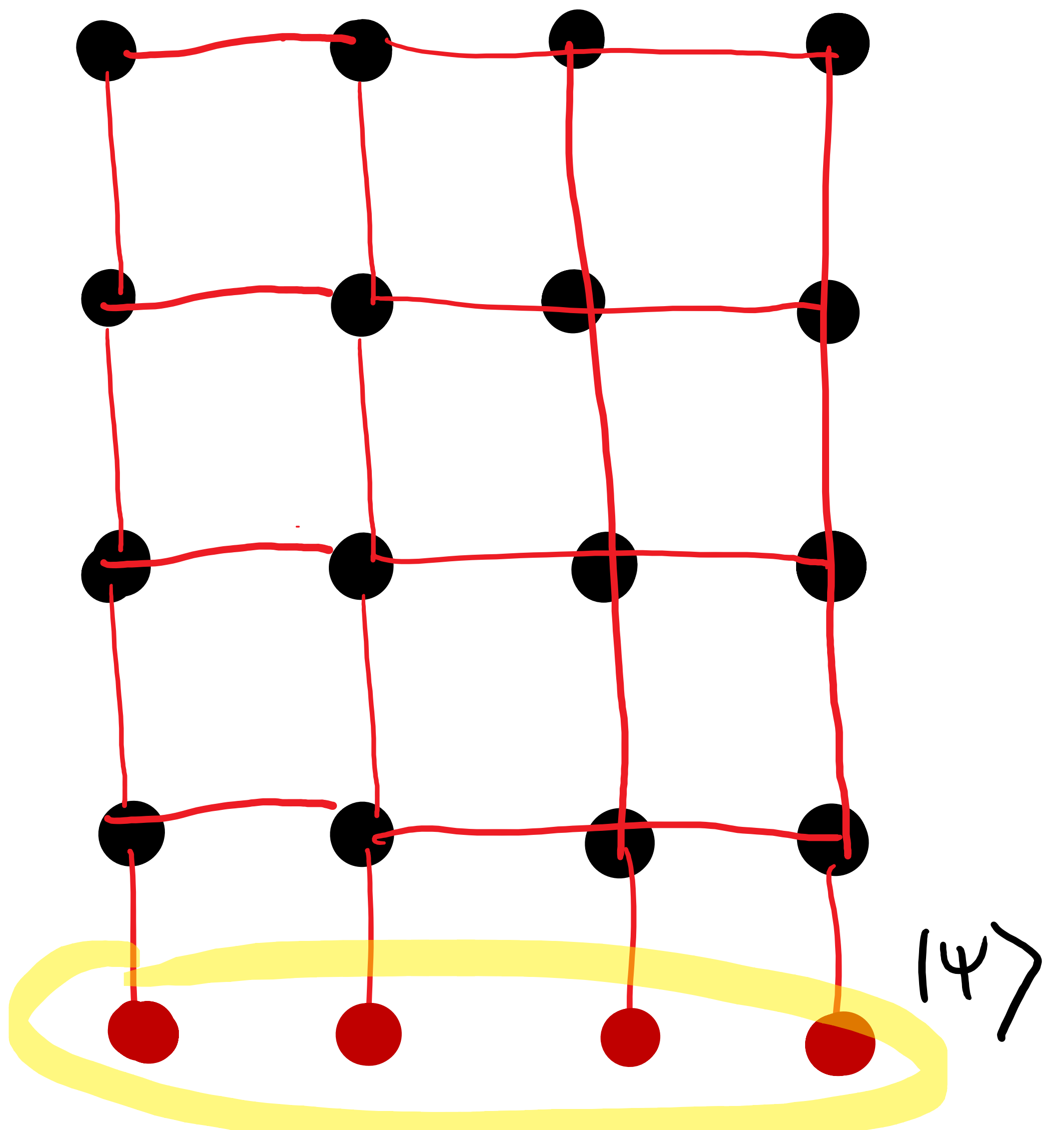
- the graph state

$$\left(\bigotimes_{e\in E} CZ_e\right)|+\rangle^{\otimes|V|}$$

- the stabilizers

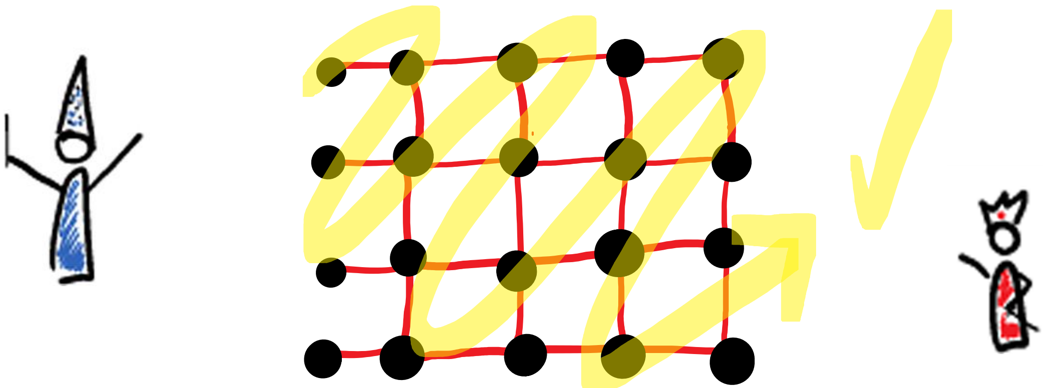
$$X_j \bigotimes_{i\in S_j} Z_i$$

- entangle a witness



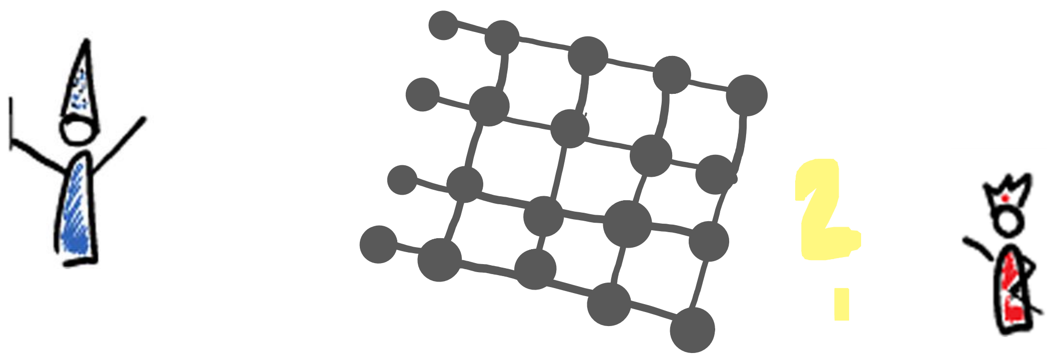
3 Completeness

- Merlin cooperates:
  sends a good state,
  Arthur computes & verifies



3 Completeness & soundness

- Merlin cooperates:
  sends a good state,
  Arthur computes & verifies

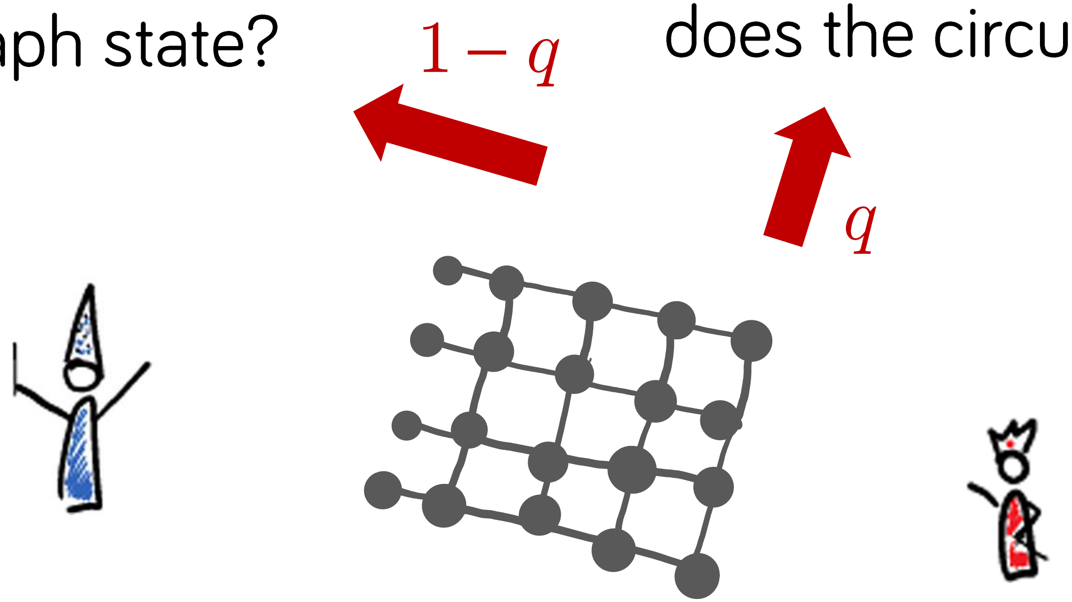


- Merlin cheats:
  sends a bad state/tries to influence the computation

3 Testing soundness

stabilizer test:
is it a graph state?

verification:
does the circuit accept?

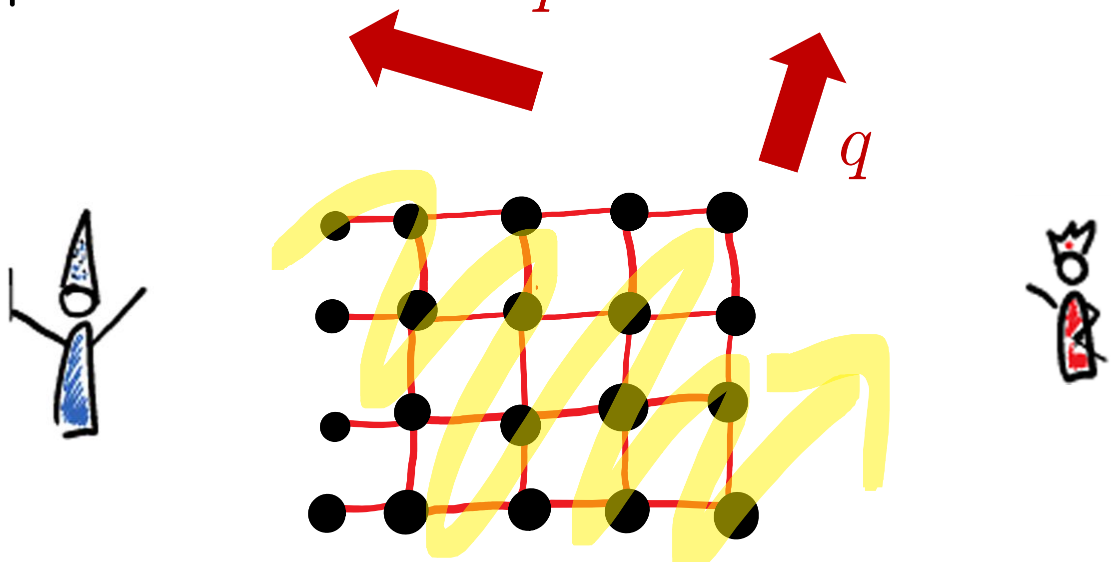


- Merlin cheats:
  sends a bad state/tries to influence the computation

3 Checking completeness

stabilizer test:
is it a graph state?

verification:
does the circuit accept?



- Merlin cooperates:
sends a good state,
Arthur computes & verifies

$$p_{\text{acc}}^{x\in L} \geqslant q a + (1-q) \equiv \alpha$$

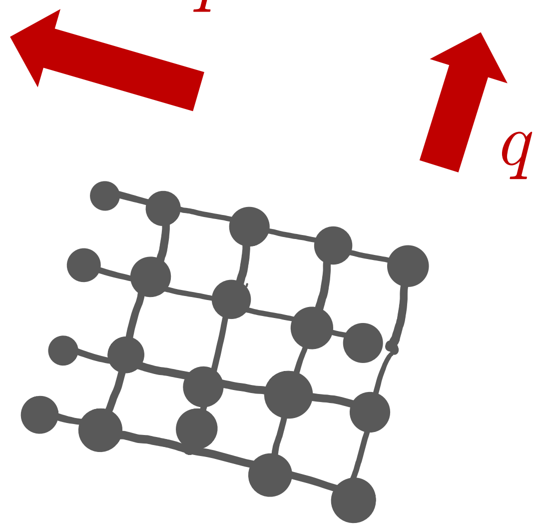
circuit soundness

3 Testing soundness

stabilizer test:
is it a graph state?

$1-q$

verification:
does the circuit accept?

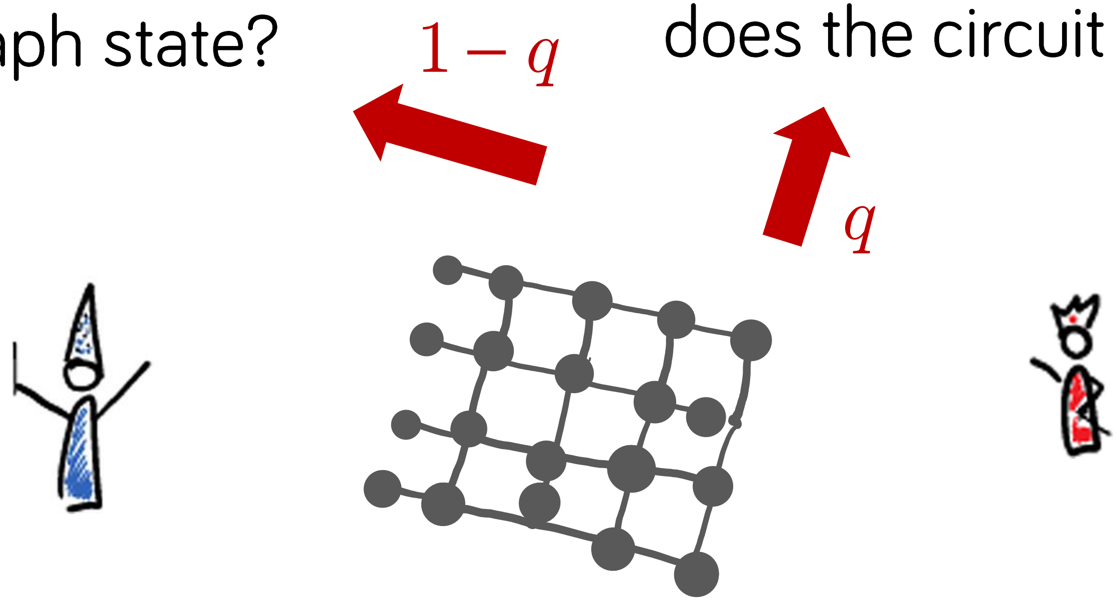


- Merlin cheats:
  sends a state with
  $p_{\text{pass}} \geq 1-\epsilon$ close to the graph state → verification

3 Testing soundness

stabilizer test:
is it a graph state?

verification:
does the circuit accept?



- Merlin cheats: sends a state with $p_{\text{pass}} \geqslant 1-\epsilon$

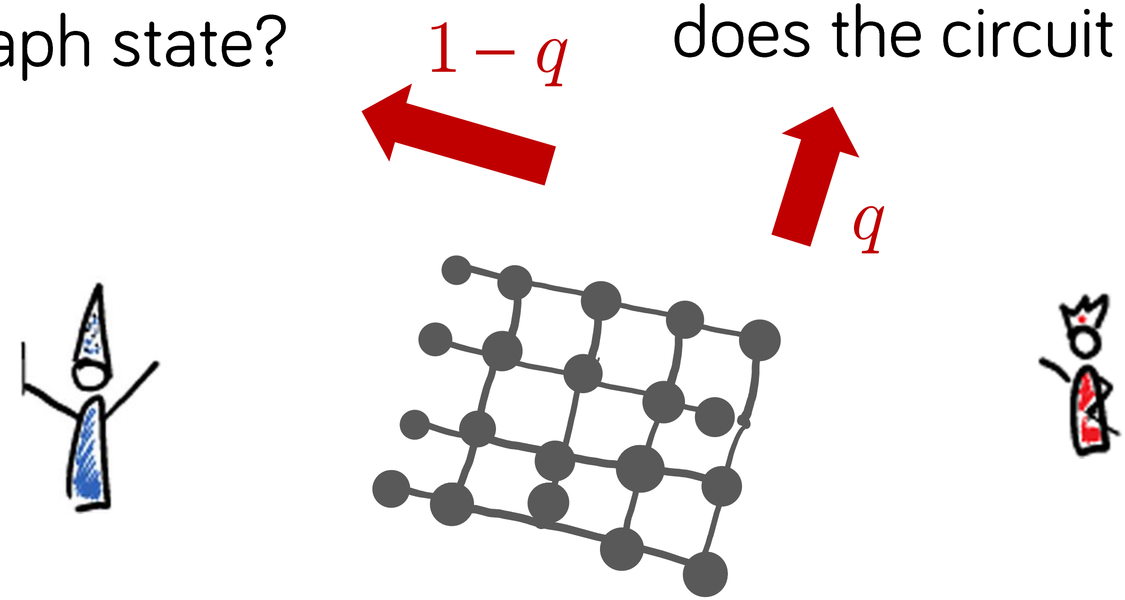
$$p_{\text{acc},1}^{x\notin L} \leqslant q(b+\sqrt{2\epsilon})+(1-q) \equiv \beta_1$$

not accepted by the circuit

3 Testing soundness

stabilizer test:
is it a graph state?

verification:
does the circuit accept?



- Merlin cheats:
  sends a pretty bad
  state with $p_{\mathrm{pass}} < 1-\epsilon$

$$p^{x\notin L}_{\mathrm{acc},2} < q + (1-q)(1-\epsilon) \equiv \beta_2$$

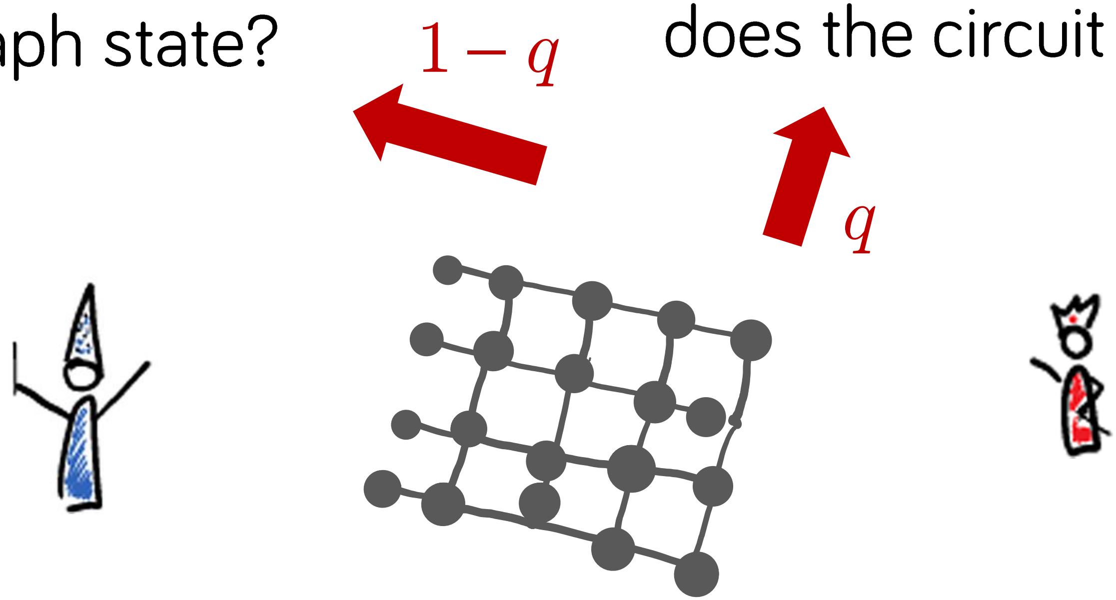
fools the circuit

caught by the s-test

3 Testing soundness

stabilizer test:
is it a graph state?

verification:
does the circuit accept?



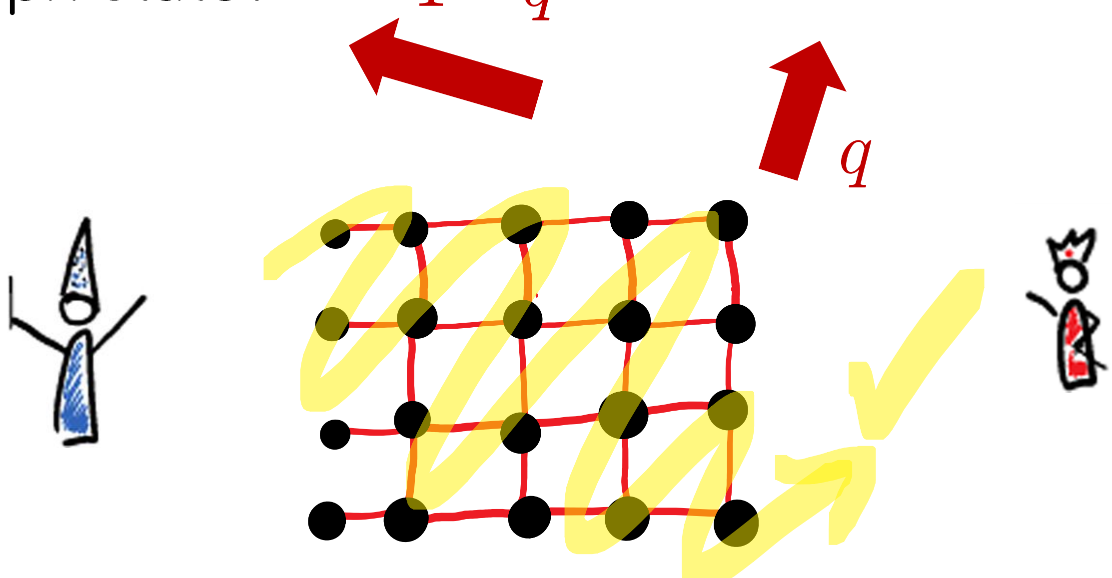
- Pick optimal ε & q to maximize the gap.

$$p_{\mathrm{acc}}^{x\in L} - p_{\mathrm{acc}}^{x\notin L} \geqslant \Delta(q^*,\epsilon) = \frac{\epsilon(a-b-\sqrt{2\epsilon})}{1+\epsilon-b-\sqrt{2\epsilon}} \geqslant \frac{1}{48|x|^2}$$

3 The MBQC-based protocol is complete & sound

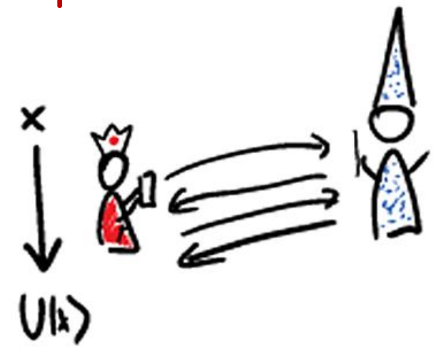
stabilizer test:
is it a graph state?

verification:
does the circuit accept?



- It also works for QMA_1 (perfect completeness).

3 More fun with graph states & interactive proofs



- Matthew McKague
  Interactive proofs for BQP via self-tested graph states
  1309.5675

- Joseph Fitzsimons, Thomas Vidick
  A multiprover interactive proof system for the local Hamiltonian problem
  1409.0260

- Zhengfeng Ji
  Classical Verification of Quantum Proofs
  1505.07432

3 The story continues tomorrow

Friday, 17.6.2016

08:00-08:45 Breakfast

09:00-12:00 MORNING SESSION (chaired by Sergey Filippov)

09:00-09:40 I **Miguel Navascues** The structure of Matrix Product States

09:40-10:05 C **Jed Kaniewski** : Self-testing of the singlet: analytic bounds fr

10:05-10:30 C **Matthias Kleinmann** : Device-independent demonstration th

10:30-11:0 [illegible]

- 11:00-11:40 **Anne Broadbent** How to verify a quantum computation

11:40-12:05 [illegible] natio

12:05-12:30 C **Thomas Bromley** : Robustness of asymmetry and coherenc

12:30-13:30 Lunch

14:00-16:10 AFTERNOON SESSION (chaired by Mario Ziman)

14:00-14:40 I **Mark Wilde** Trading communication resources in quantum Sh

14:40-15:05 C **Giacomo de Palma** : Gaussian optimizers in quantum inform

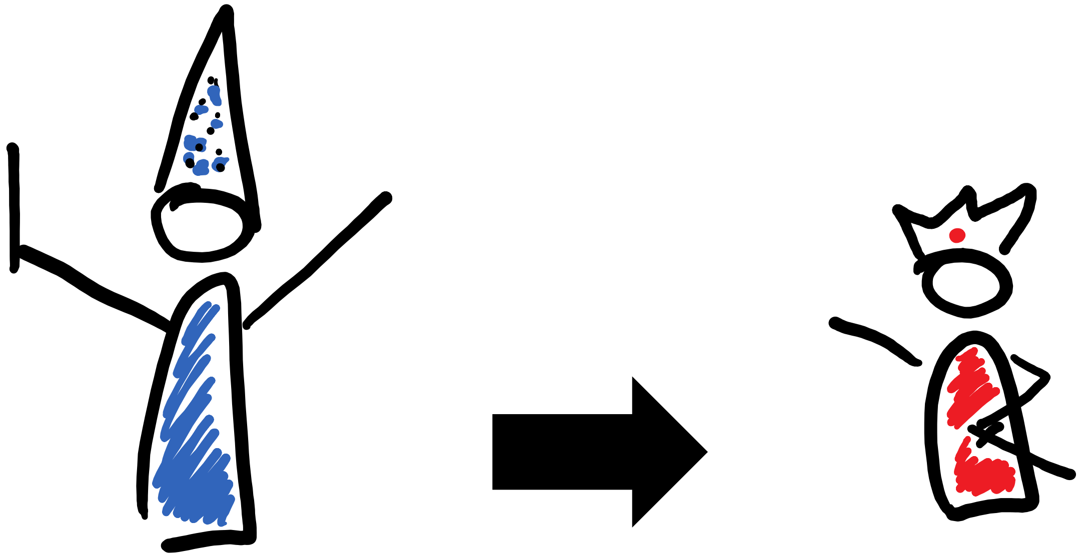
15:05-15:30 C **Julio de Vicente** : Simple conditions constraining the set of c

15:30-16:00 Coffee & Refreshment

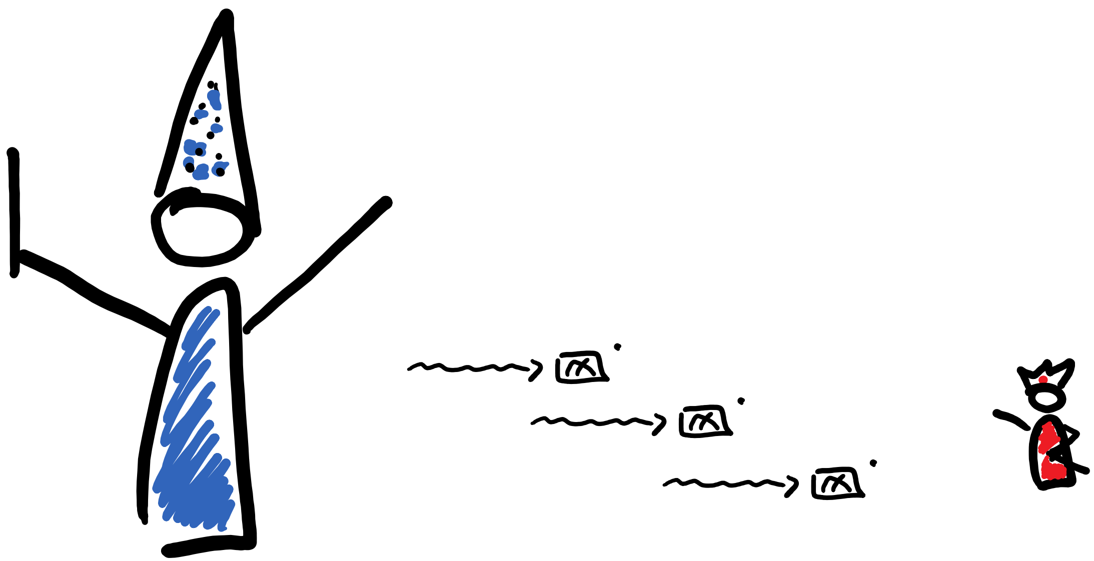
16:00-18:30 POSTER SESSION

19:00 DINNER (conference room)

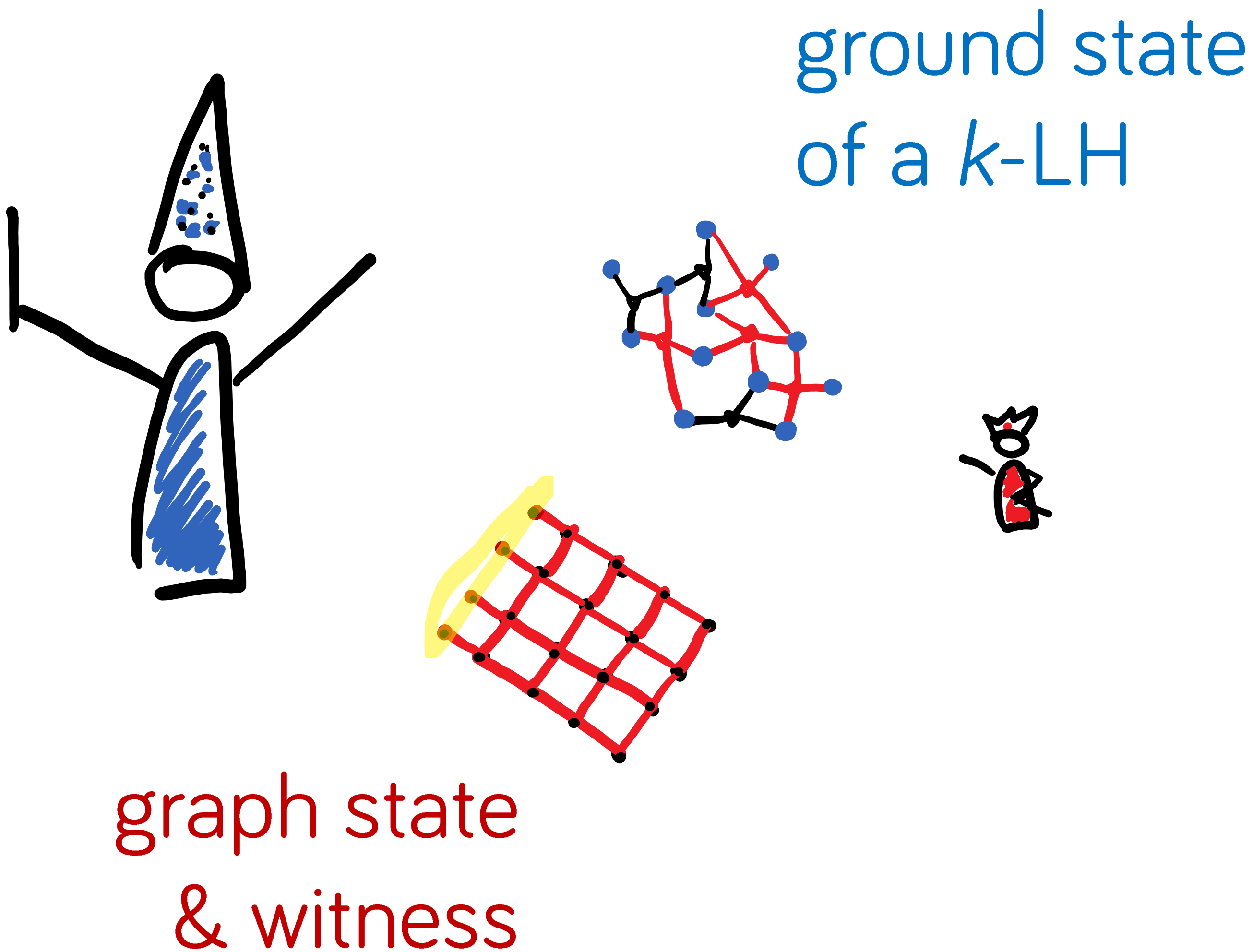
19:00-23:00 CIPHER GAME (18:30 registration)



restricting the verifier's resources



sequential 1 qubit measurements


ground state
of a k-LH
graph state
& witness

you can verify quantum proofs by measuring 1 qubit at a time

Tomoyuki Morimae

Norbert Schuch

Daniel Nagaj

2016 | 6 | 17
CEQIP Valtice

PRA 93, 022326

S A S P R O