Verifying commuting quantum computations via fidelity estimation of weighted graph states

Masahito Hayashi[1,2,3]

1:Graduate School of Mathematics, Nagoya University

2: Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology

3: Centre for Quantum Technologies, National University of Singapore

Collaborator: Y. Takeuchi, (T. Morimae, H. Zhu)

arXiv:1902.03369

NAGOYA UNIVERSITY

南方科技大学

SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Centre for Quantum Technologies

NUS National University of Singapore

Contents

- Why verification of weighted graph state?
- Verification of two-colorable graph state
- Verification of multiple-colorable graph state
- Verification of weighted graph state
- Application to quantum supremacy
- Conclusion

How can we demonstrate quantum supremacy?

Quantum supremacy: A task that can be realized by quantum computer but cannot be realized by classical computer.

Solving factorization via Shor's algorithm
by using quantum computer

However, there is no guarantee that *no classical algorithm realizes the same performance as Shor's algorithm*.

This type of supremacy depends on the above conjecture.

Another idea for Quantum supremacy

More convinced conjecture (Conjecture 1):

Let $f:\{0,1\}^n \to \{0,1\}$ be uniformly random degree-three polynomial over $\mathbf{F}_2$.

It is #P-hard to approximate $\left(\frac{\mathrm{gap}(f)}{2^n}\right)^2$ up to a multiplicative error of 1/4 + o(1) for a 1/24 fraction of polynomials f.

$$\mathrm{gap}(f) := |\{x : f(x)=0\}| - |\{x : f(x)=1\}|$$

Bremner, Montanaro, and Shepherd
Phys. Rev. Lett. (2016).

More people convince this conjecture.

Another idea for Quantum supremacy

The polynomial-time hierarchy (PH): a hierarychy of complexity classes,

0^{th} PH $\subset 1^{st}$ PH $\subset$ 2^{nd} PH $\subset$ 3^{rd} PH $\subset$… n^{th} PH..

Another more convinced conjecture (Conjecture 2):

The PH does not collapse to its third level.

$\cancel{0^{th} \text{ PH } \subset 1^{st} \text{ PH } \subset 2^{nd} \text{ PH } \subset 3^{rd} \text{ PH } = n^{th} \text{ PH}}$

More people convince this conjecture.

How can we demonstrate quantum supremacy?

Bremner, Montanaro, and Shepherd
Phys. Rev. Lett. (2016).

Theorem:

Assume Conjectures 1 and 2 are true.
There exists an IQP circuit whose diagonal gate D is composed of Z, C-Z, and CC-Z gates
such that its output probability distribution
cannot be classically simulated in polynomial time,
within an error 1/192 in l1 norm.

Quantum Supremacy:

Realization of the output state any IQP circuit whose diagonal gate D is composed of Z, C-Z, and CC-Z gates within an error 1/192 in l1 norm.

How to verify such output state

The output state of such an IQP circuit is given as a weighted graph state.

$$|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$$

Graph state: $$\left[\prod_{(j,k)\in E} CZ_{j,k}\right]|+\rangle^{\otimes n}$$

$$\mathrm{CZ}_{j,k} := |0\rangle\langle 0|_j \otimes I_k + |1\rangle\langle 1|_j \otimes Z_k$$

Weighted graph state: $$\left[\prod_{(j,k)\in E} \Lambda_{j,k}(\theta_{j,k})\right]|+\rangle^{\otimes n}$$

$$\Lambda_{j,k}(\theta_{j,k}) := |0\rangle\langle 0|_j \otimes I_k + |1\rangle\langle 1|_j \otimes (|0\rangle\langle 0|_k + e^{i\theta_{j,k}}|1\rangle\langle 1|_k)$$

It is sufficient to verify a weighted graph state!

How to construct graph state

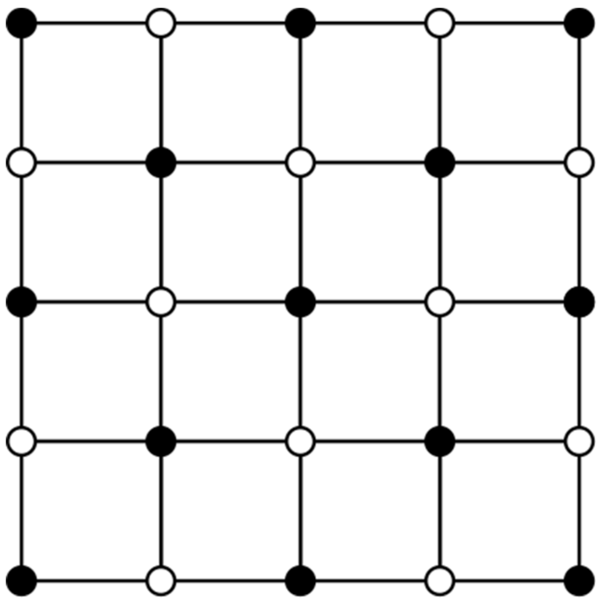
(1) For each vertex, we set the qubit system to

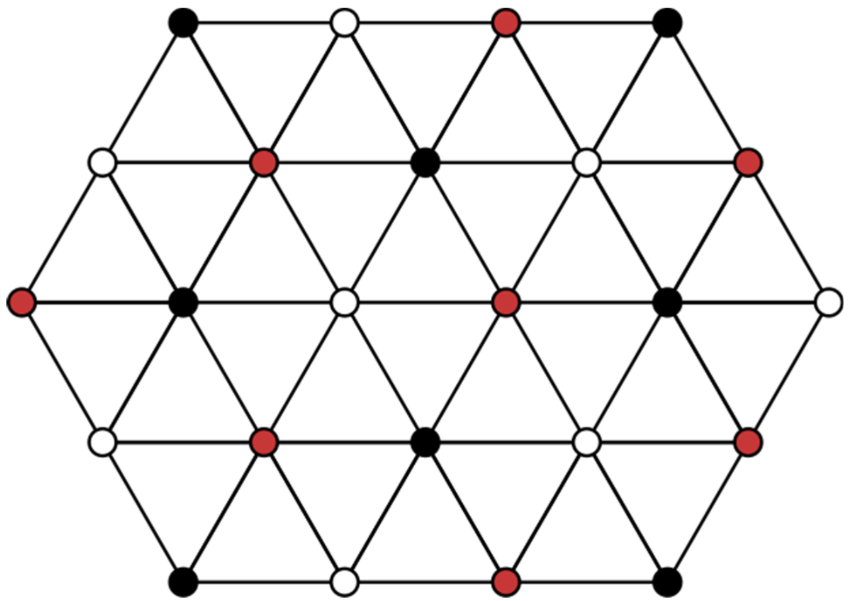
$$|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$$

(2) Apply controlled Z $\quad \mathbf{CZ} := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$

to the two-qubit systems connected by edges

$$Z := |0\rangle\langle 0| - |1\rangle\langle 1|$$





Concepts of Verification (same as QKD)

Detectability: State and measurement should be rejected when they are not properly prepared.

This condition is needed for guaranteeing the precision of computation outcome when the test is passed.

Significance level β is the maximum passing probability with incorrect state or measurements (e.g. 5%)

Fidelity between the resultant state and target state with significance level β

Acceptability: State and measurement should be accepted when they are properly prepared.

This condition is needed to accept the proper computation outcome.

Acceptance probability α is the passing probability with correct state and measurements

Verification of two-colorable graph state

Since we perfectly trust measurement, it is sufficient to verify only the two-colorable (Black and White) graph state $|G\rangle$ by local measurements.

In two-colorable state, the Z values on one color sites decide the X values on the other color sites.

MH, Morimae 2015

predicts

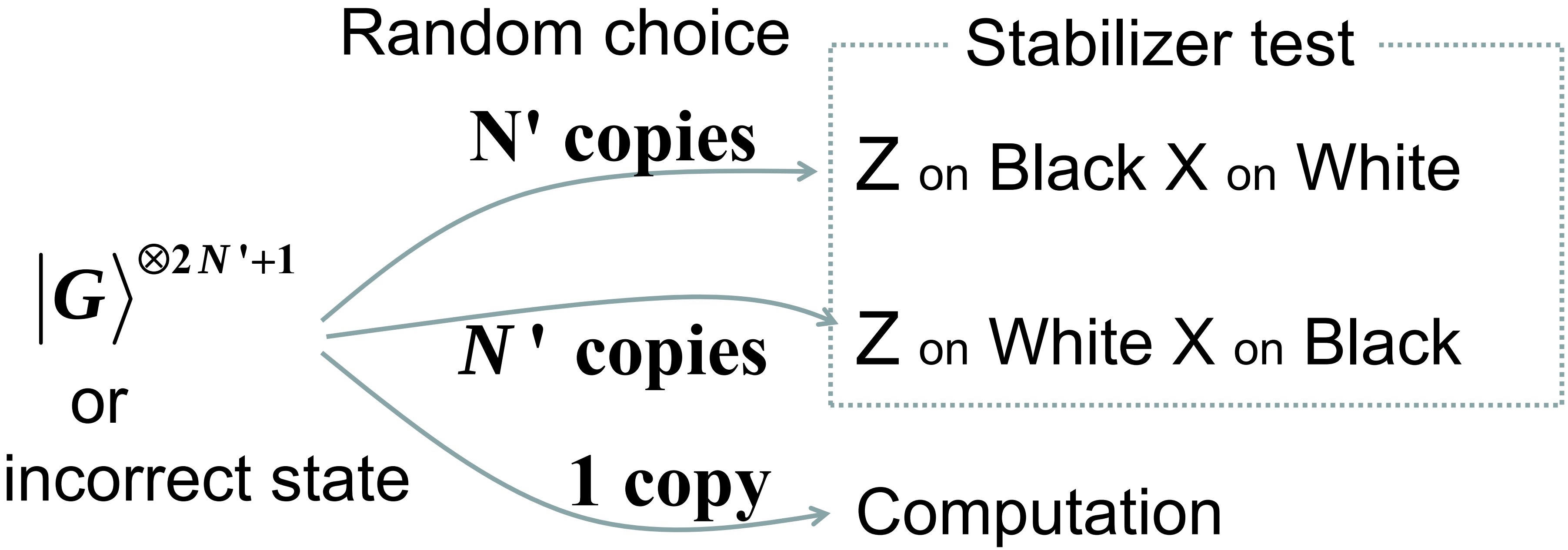
Z measurement on Black → X measurement on White

Z measurement on White → X measurement on Black

Our verification:

We check whether X outcomes equal the prediction.

Verification of two-colorable graph state



Verification of two-colorable graph state

Once *2N'* tests are passed, the state $\boldsymbol{\sigma}$ of the resultant system satisfies

$$\langle G|\sigma|G\rangle \geq 1-\frac{1}{\beta(2N'+1)}$$

with significance level *β.*

The state $|G\rangle^{\otimes 2N'+1}$ passes al least with probability 1.

With significance level *β,* the probability being incorrect computation outcome is less than $1/\sqrt{\beta(2N'+1)}$.

Verification of *m*-colorable graph state

It is natural to apply the cover protocol to *N* systems.

Cover protocol:

Zhu MH arXiv:1806.05565

(1) We randomly choose one color with equal prob 1/m.
(2) We measure node whose color is not the chosen color with Z basis.
(3) We measure node whose color is the chosen color with X basis.

To evaluate the performance of the above protocol, we need to prepare a general theory.

General theory for verification

Ω is a POVM element. $\Omega|G\rangle = |G\rangle$

Assume that we apply the measurement $\{\Omega, I-\Omega\}$ to *N* systems.

Zhu MH arXiv:1806.05565

Theorem:

Once *N* tests are passed, the state σ of the resultant system satisfies

$$\langle G|\sigma|G\rangle \geq 1 - \frac{1-\beta}{N\beta\nu(\Omega)}$$

with significance level $\beta\left(\geq \frac{1}{N\nu(\Omega)+1}\right)$

$$\nu(\Omega) := 1 - \left\| \Omega - |G\rangle\langle G| \right\|$$

Verification of m-colorable graph state

Once N tests are passed, the state $\boldsymbol{\sigma}$ of the resultant system satisfies

Zhu MH arXiv:1806.05565

$$\langle G|\sigma|G\rangle \geq 1-\frac{m(1-\beta)}{N\beta} \qquad \nu(\Omega)=\frac{1}{m}$$

with significance level β.

The state $|G\rangle^{\otimes N+1}$ passes al least with probability 1.

Adaptive verification of *m*-colorable weighted graph state with perfect match

(1) We randomly choose one color with equal prob $1/m$.

(2) We measure node whose color is not the chosen color with Z basis. Z_l : Outcome

(3) We measure node *l* whose color is the chosen color with basis $\{|\alpha_k(Z_l)\rangle, |\alpha_k(Z_l)+\pi\rangle\}$

$$|\alpha\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$

Adaptive verification of *m*-colorable weighted graph state with perfect match

Once *N* tests are passed, the state σ of the resultant system satisfies

$$\langle G|\sigma|G\rangle \geq 1-\frac{m(1-\beta)}{N\beta}$$

with significance level *β.*

The state $|G\rangle^{\otimes N+1}$ passes al least with probability 1.

Adaptive verification of *m*-colorable weighted graph state with imperfect match

(1) We randomly choose one color with equal prob $1/m$.

(2) We measure node whose color is not the chosen color with Z basis. Z_l : **Outcome**

(3) We measure node *l* whose color is the chosen color with basis $\{|\alpha_k^h(Z_l)\rangle, |\alpha_k^h(Z_l)+\pi\rangle\}$

$$|\alpha_k^h(Z_l)\rangle : \text{ One of } \left|\frac{\pi}{h}\right\rangle, \left|\frac{2\pi}{h}\right\rangle, \ldots, \left|\frac{2\pi h}{h}\right\rangle$$

$$|\alpha_k^h(Z_l) - \alpha_k(Z_l)| < \frac{\pi}{h}$$

h : **No. of meshes**

Adaptive verification of *m*-colorable weighted graph state with imperfect match

Once *N* tests are passed, the state $\boldsymbol{\sigma}$ of the resultant system satisfies

$$\langle G|\sigma|G\rangle \geq 1-\frac{m(1-\beta)}{N\beta}-n\sin\frac{\pi}{4h}$$

with significance level *β*.

The state $|G\rangle^{\otimes N+1}$ passes al least with probability

$$(1-\sin^2\frac{\pi}{4h})^{N\max_l|A_l|}$$

Non-adaptive verification of *m*-colorable weighted graph state with perfect match

(1) We choose one color with equal prob 1/*m*.

(2) We measure node whose color is not the chosen color with Z basis. Z_l **: Outcome**

(3) We measure node *l* whose color is the chosen color with basis $\{\left|\frac{\pi j}{h}\right\rangle, \left|\frac{\pi j}{h}+\pi\right\rangle\}$ J **: Outcome**

Here, *j* is chosen with equal prob 1/*h*.

$\left|\alpha^h(z_l)\right\rangle$ **is always onne of** $\left|\frac{\pi}{h}\right\rangle, \left|\frac{2\pi}{h}\right\rangle, \ldots, \left|\frac{2\pi h}{h}\right\rangle$

(4) We reject only when outcome is $\alpha_k(Z_l)+\pi$

Non-adaptive verification of *m*-colorable weighted graph state with perfect match

Once N tests are passed, the state $\boldsymbol{\sigma}$ of the resultant system satisfies

$$\langle G|\sigma|G\rangle \geq 1-\frac{m(1-\beta)h}{N\beta}$$

with significance level β.

The state $|G\rangle^{\otimes N+1}$ passes al least with probability 1.

Non-adaptive verification of *m*-colorable weighted graph state with imperfect match

(1) We randomly choose one color with equal prob $1/m$.

(2) We measure node whose color is not the chosen color with Z basis. Z_l : **Outcome**

(3) We measure node *l* whose color is the chosen color with basis $\{\left|\frac{\pi j}{h}\right\rangle, \left|\frac{\pi j}{h}+\pi\right\rangle\}$ J : **Outcome**

Here, *j* is chosen with equal prob $1/h$.

(4) We reject only when $|\alpha_k(Z_l) - \frac{\pi J}{h}| > \pi - \frac{\pi}{h}$

Non-adaptive verification of *m*-colorable weighted graph state with imperfect match

Once *N* tests are passed, the state σ of the resultant system satisfies

$$\langle G|\sigma|G\rangle \geq 1-\frac{m(1-\beta)h}{N\beta}-n\sin\frac{\pi}{4h}$$

with significance level *β.*

The state $|G\rangle^{\otimes N+1}$ passes al least with probability

$$(1-\sin^2\frac{\pi}{4h})^{N\max_l|A_l|}$$

Application to Quantum Supremacy via IQP circuit

Assume Conjectures 1 and 2 are true.

There exists an output sate $\left| G_{\mathrm{IQP}} \right\rangle$ of IQP circuit whose diagonal gate D is composed of Z, C-Z, and CC-Z gates

satisfying the following.

No distribution Q on the *n*-bit system satisfies the following;

- Q can be classically simulated in polynomial time for n.
- $\| Q - Q_G \|_1 < 1/192 \qquad Q_G(z) := | \left\langle z \middle| G_{\mathrm{IQP}} \right\rangle |^2$

Application to Quantum Supremacy via IQP circuit

We set $N = \frac{8 \cdot 192^2 \cdot n(1-\beta)}{\beta}$ ⇐ $h = 2$, $m = n$ ⇐ $\theta_{j,k} = \frac{\pi}{2}$

n : Size of IQP circuit

Once *N* tests are passed, we apply the measurement on Z to the resultant system.

Then, the output distribution Q' satisfies

$$\| Q' - Q_G \|_1 < 1/192 \qquad Q_G(z) := | \langle z | G_{\mathrm{IQP}} \rangle |^2$$

with significance level β.

Conclusion

- We have proposed a method to verify weighted graph state.
- We applied the result to quantum supremacy via IQP circuit.
- The required number of sampling is only linear for the size of circuit.

References

- MH Morimae, Phys. Rev. Lett **115**, 220502 (2015).
- Zhu, MH, arXiv:1806.05565
- MH Takeuchi, arXiv:1902.03369
- Bremner, Montanaro, and Shepherd Phys. Rev. Lett. (2016).
-