Verifiable measurement-based quantum computation on hypergraph states

References:

- Phys. Rev. X **8**, 021060 (2018)
- npj Quantum Inf. **5**, 27 (2019)
- Sci. Rep. **9**, 13585 (2019)
- arXiv:2006.05416 (2020)
- Phys. Rev. A **106**, 012405 (2022)
- arXiv:2312.16433 (2023)

Yuki Takeuchi

NTT Communication Science Labs.

NTT Research Center for Theoretical Quantum Information

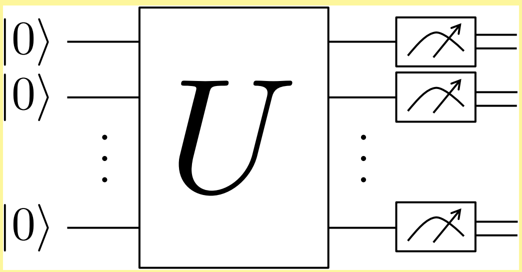
11:30 – 12:00, 22 Feb. 2024

Quantum TUT workshop

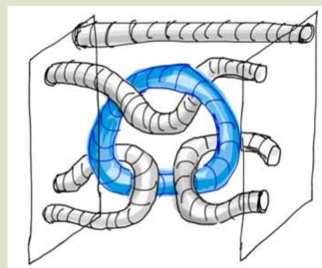
[1] K. Fujii, *Quantum Computation with Topological Codes: From Qubit to Topological Fault-Tolerance* (2015).
[2] J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne, and E. Andersson, Phys. Rev. A **82**, 020301(R) (2010).

Universal quantum computation models

Quantum circuit model

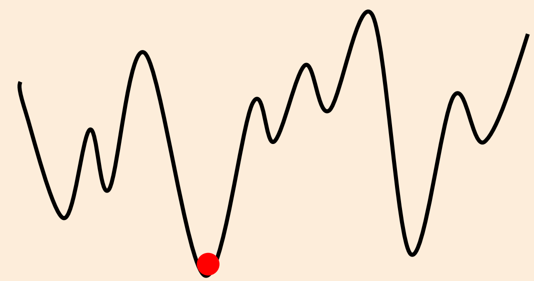


Topological quantum computation

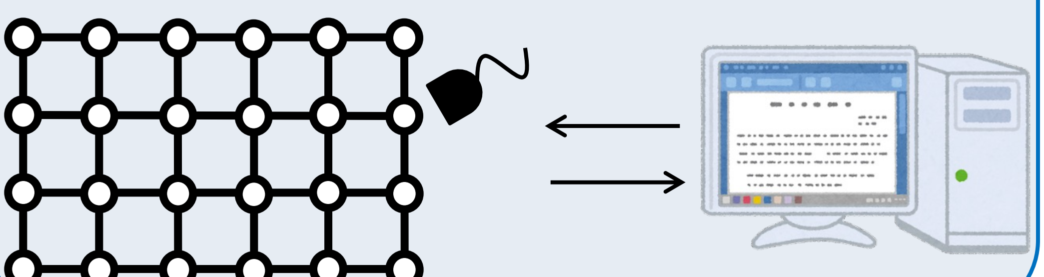


[1]

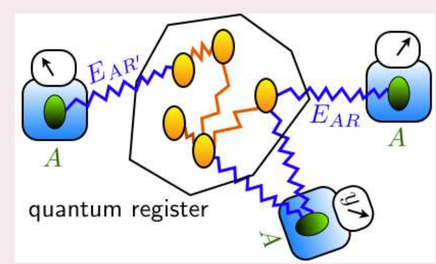
Adiabatic quantum computation (AQC)



Measurement-based quantum computation (MBQC)



Ancilla-driven quantum computation (ADQC)



[2]

They have their own advantage and disadvantage.

Measurement-based quantum computation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

MBQC: a computation model specific to quantum computation

- Its computational power is equivalent to that of the quantum circuit model.
- It utilizes entangled states.

Measurement-based quantum computation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

MBQC: a computation model specific to quantum computation

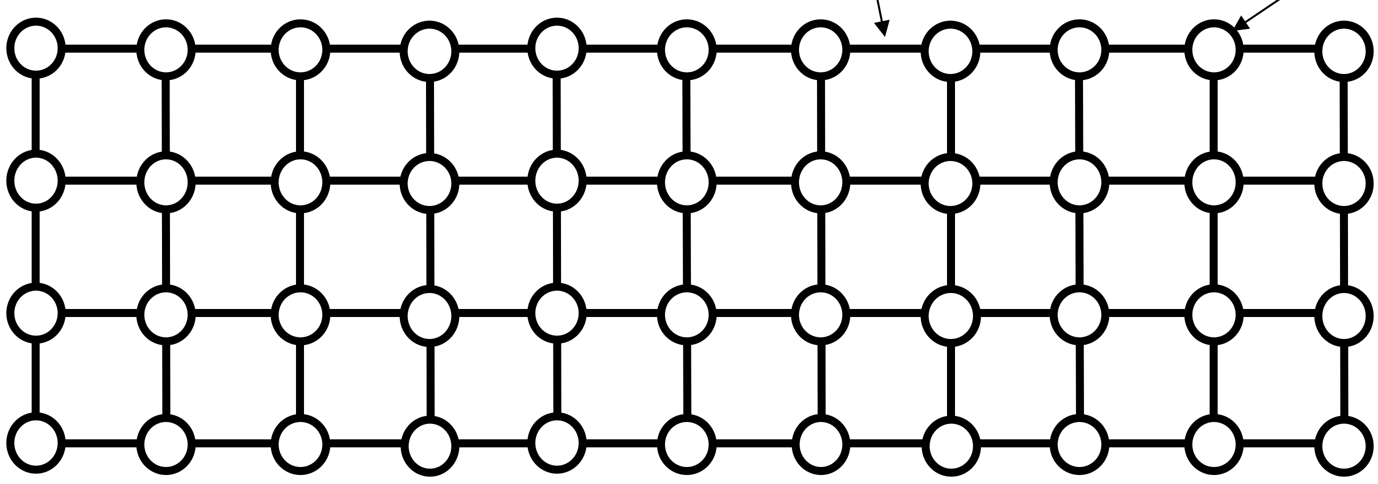
- Its computational power is equivalent to that of the quantum circuit model.
- It utilizes entangled states.

$$CZ \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

1. Prepare the cluster state.

[H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).]

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



Measurement-based quantum computation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

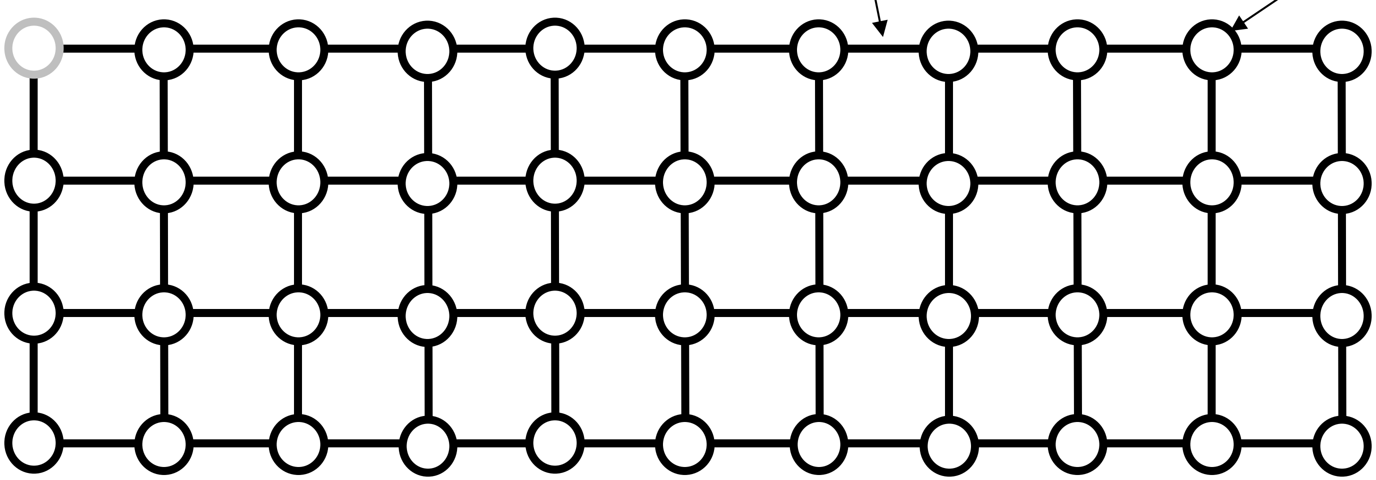
MBQC: a computation model specific to quantum computation

- Its computational power is equivalent to that of the quantum circuit model.
- It utilizes entangled states.

$$CZ \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

2. Measure qubits one by one.

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



Measurement-based quantum computation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

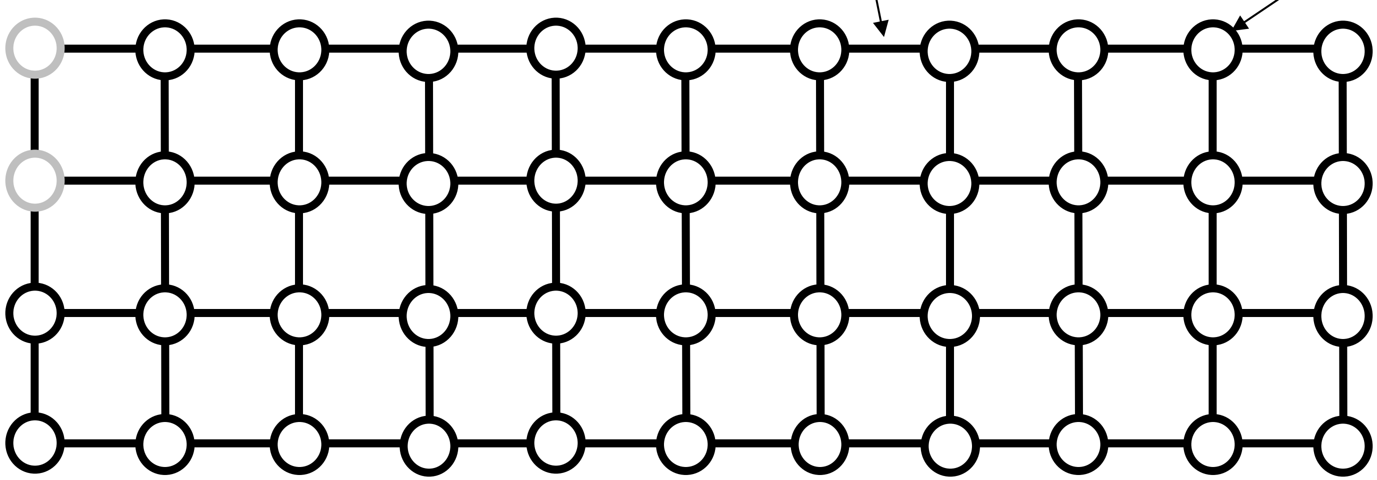
MBQC: a computation model specific to quantum computation

- Its computational power is equivalent to that of the quantum circuit model.
- It utilizes entangled states.

$$CZ \equiv |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

2. Measure qubits one by one.

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



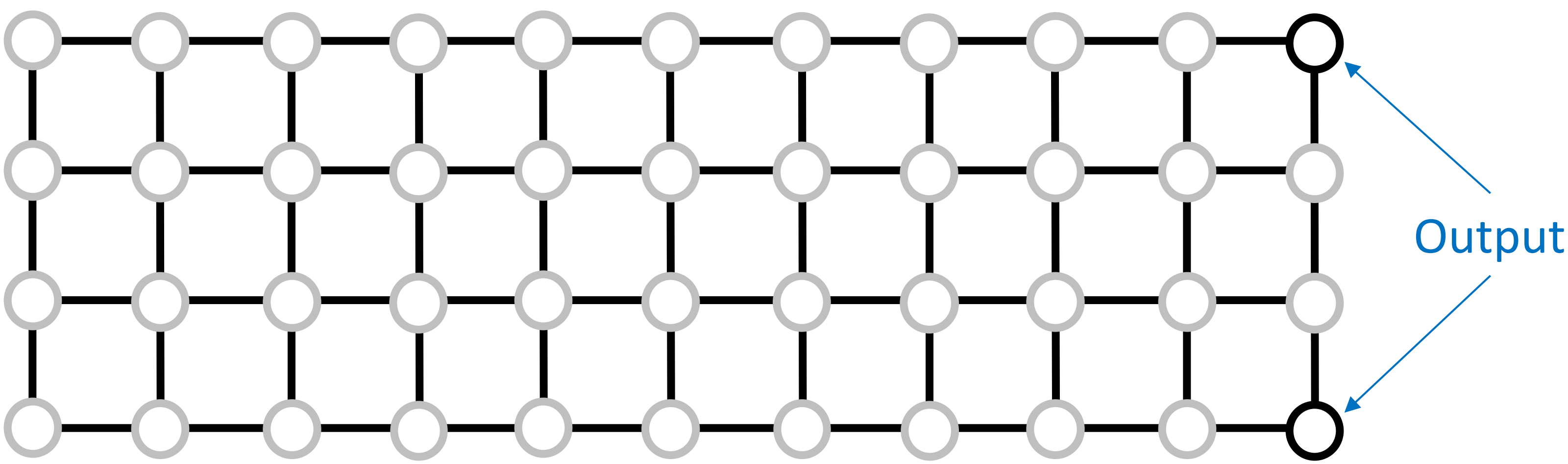
Measurement-based quantum computation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

MBQC: a computation model specific to quantum computation

- Its computational power is equivalent to that of the quantum circuit model.
- It utilizes entangled states.

2. Measure qubits one by one.



Measurement-based quantum computation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

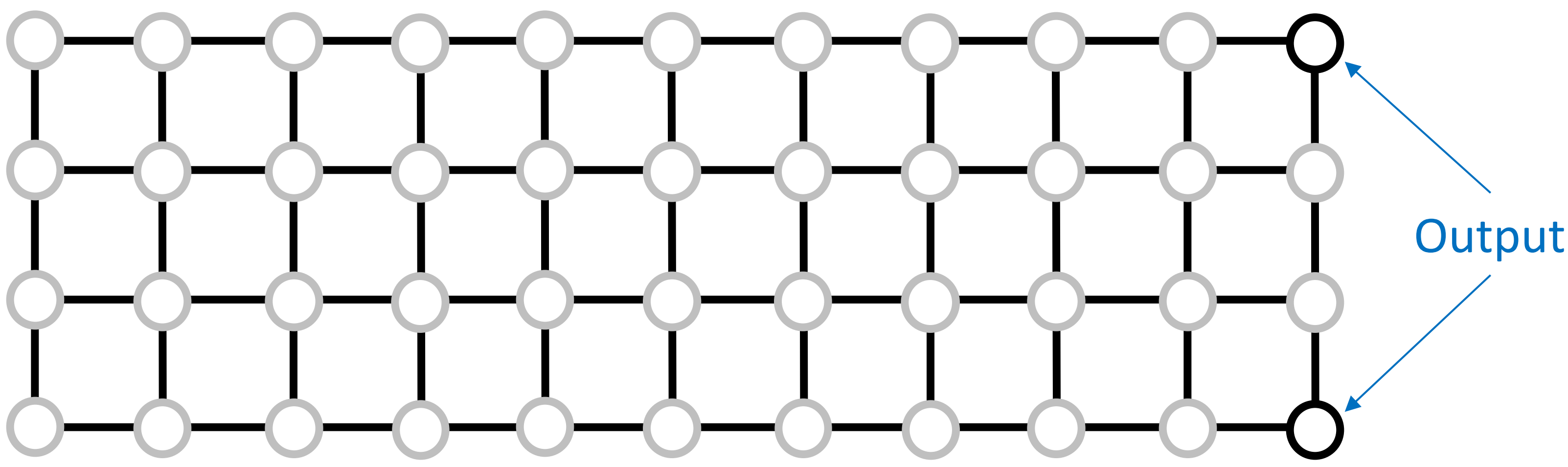
MBQC: a computation model specific to quantum computation

- Its computational power is equivalent to that of the quantum circuit model.
- It utilizes entangled states.

2. Measure qubits one by one.

Disadvantage of MBQC

A single quantum gate requires a single qubit.

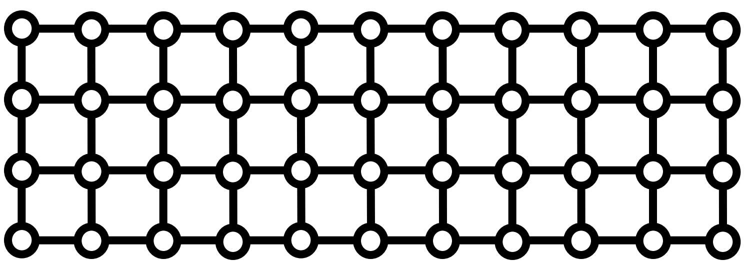


Measurement-based quantum computation

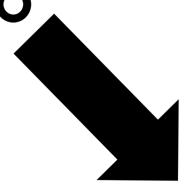
[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

Advantage of MBQC

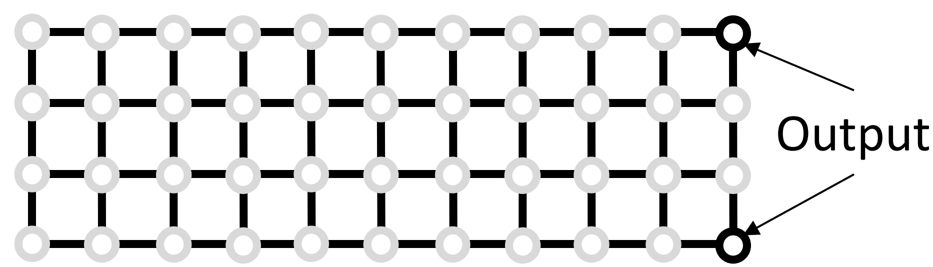
1. Preparation of cluster state



- Two-qubit operations are necessary.
- This step is independent of quantum algorithms.



2. Single-qubit measurements



- Only single-qubit operations are necessary.
- This step depends on quantum algorithms.

Measurement-based quantum computation

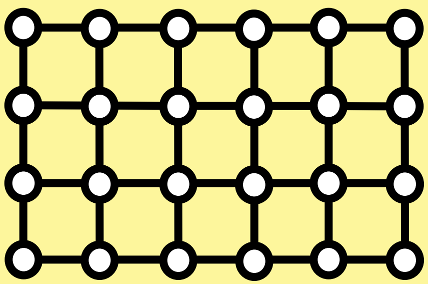
[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

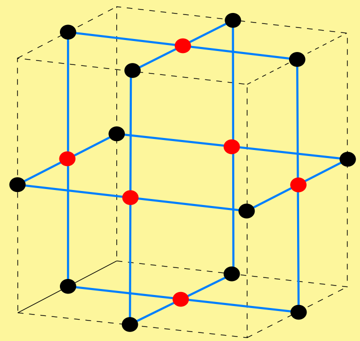
Applications of MBQC

- Linear optical quantum computing
  [M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **115**, 020502 (2015).]
- Quantum cryptography (blind quantum computation)
  [J. F. Fitzsimons, npj Quantum Inf. **3**, 23 (2017).]
- Condensed matter physics (e.g., **BQP**-completeness of partition functions)
  [A. Matsuo, K. Fujii, and N. Imoto, Phys. Rev. A **90**, 022304 (2014).]
- Quantum computational supremacy (non-adaptive MBQC)
  [M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A **467**, 459 (2011).]
- Resource theory (e.g., GHZ states + XOR = universal classical computation)
  [J. Anders and D. E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).]
- Quantum error correction (3D cluster states)
  [R. Raussendorf, J. Harrington, and K. Goyal, Annals of Physics **321**, 2242 (2006).]
- Quantum computational theory (e.g., **QMA**)
  [T. Morimae, D. Nagaj, and N. Schuch, Phys. Rev. A **93**, 022326 (2016).]
- Verification of quantum computation
  [A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory Comput. Syst. **63**, 715 (2019).]

Universal resource states for MBQC

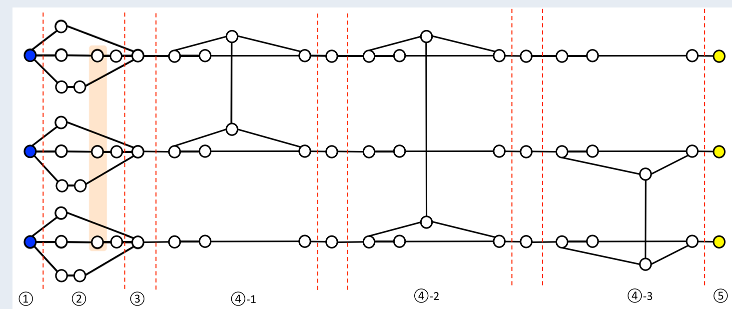
Graph states





[R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).]

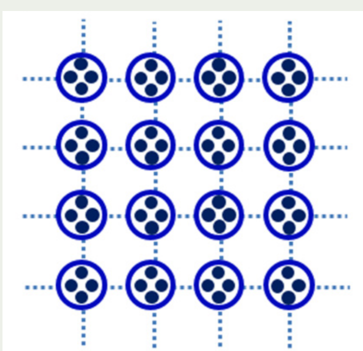
Hypergraph states



[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Tnesor-network states (e.g., AKLT states)

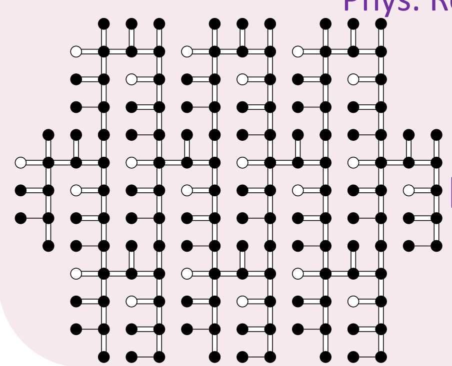
[D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).]



[T.-C. Wei and R. Raussendorf, Phys. Rev. A **92**, 012310 (2015).]

Weighted graph states

[D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Phys. Rev. A **76**, 052315 (2007).]

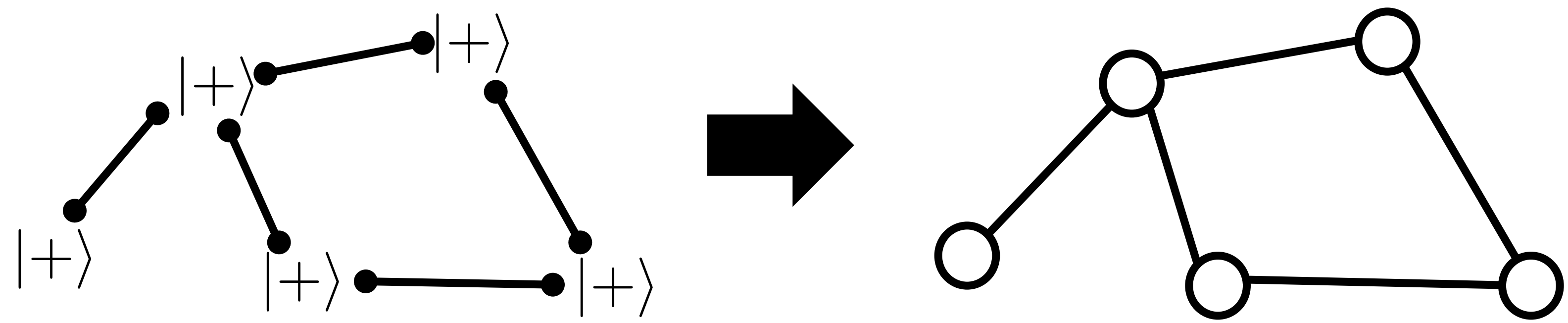


[A. Kissinger and J. van de Wetering, Quantum **3**, 134 (2019).]

Hypergraph states

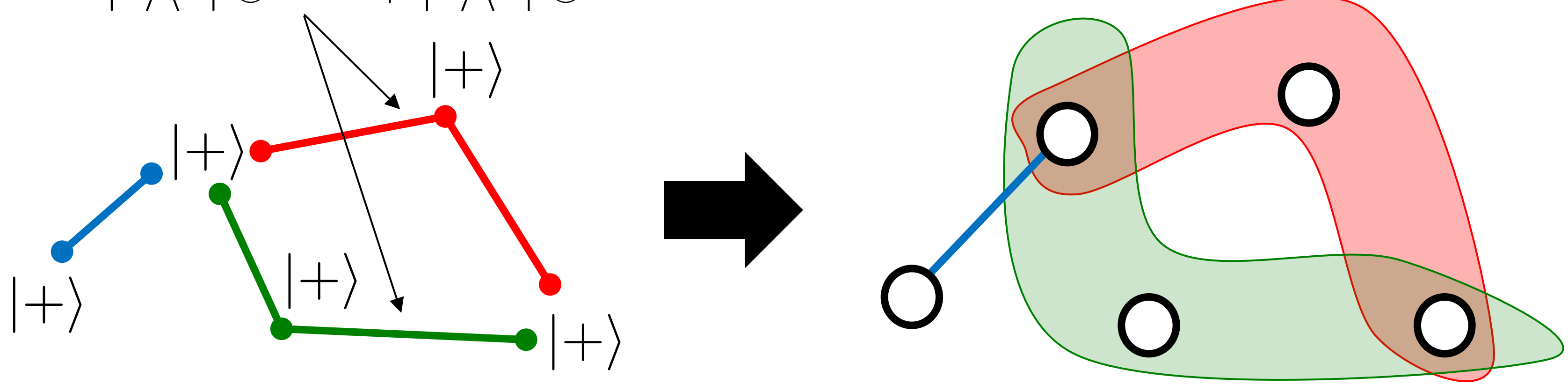
[M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, New J. Phys. **15**, 113022 (2013).]

- Graph states (e.g., cluster states)



- Hypergraph states: a **generalization** of graph states

$$CCZ \equiv |0\rangle\langle 0| \otimes I^{\otimes 2} + |1\rangle\langle 1| \otimes CZ$$



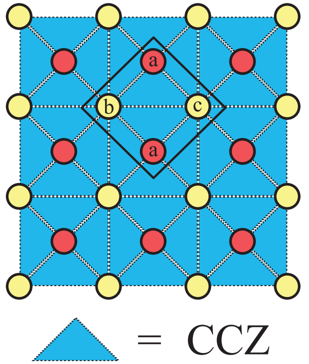
Usefulness of hypergraph states

[J. Miller and A. Miyake, npj Quantum Inf. **2**, 16036 (2016).]

1. Universality for Pauli MBQC

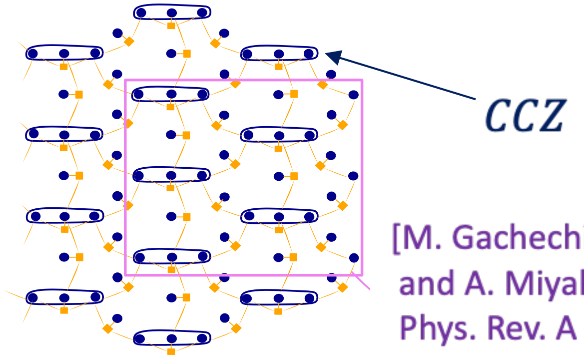
The Union Jack state enables us to perform universal MBQC with **Pauli-X, Y, and Z measurements.**

Due to the Gottesman-Knill theorem, it is impossible for graph states.



2. Parallelization of ***CCZ*** **gates**

The MBQC on graph states can apply Clifford gates in parallel.



[M. Gachechiladze, O. Gühne, and A. Miyake, Phys. Rev. A **99**, 052304 (2019).]

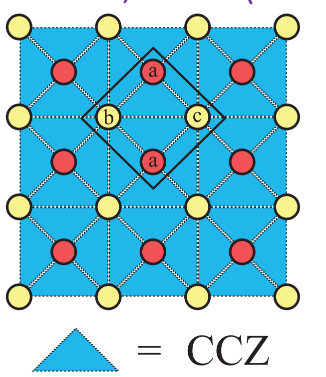
3. Exponential violation of Bell inequalities

[M. Gachechiladze, C. Budroni, and O. Gühne, Phys. Rev. Lett. **116**, 070401 (2016).]

Usefulness of hypergraph states

[J. Miller and A. Miyake, npj Quantum Inf. **2**, 16036 (2016).]

1. Universality for Pauli MBQC

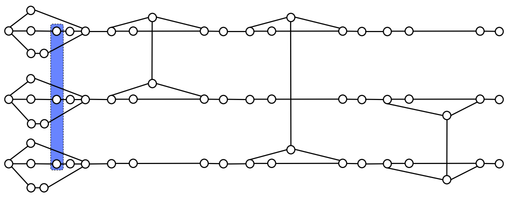


The Union Jack state enables us to perform universal MBQC with **Pauli-X, Y, and Z measurements**.

Due to the Gottesman-Knill theorem, it is impossible for graph states.

Our result

Pauli-X and Z measurements are sufficient for universal MBQC on hypergraph states.



[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

Fact 1 [Y. Shi, arXiv:qunt-ph/0205115 (2002).]

Any quantum computation (with **classical output**) can be realized by combining

$$H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$$

$$CCZ \equiv |0\rangle\langle 0| \otimes I^{\otimes 2} + |1\rangle\langle 1| \otimes CZ$$

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| .$$

Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

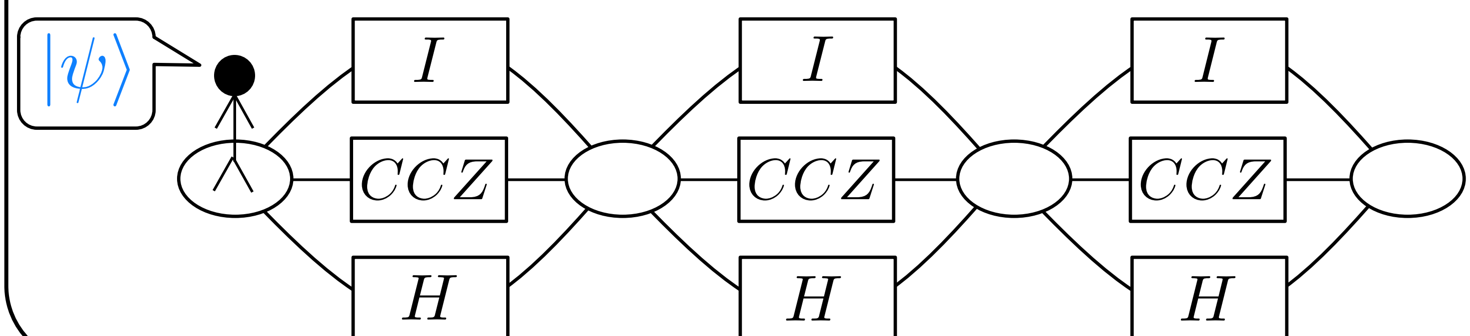
$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

<u>Fact 1</u> [Y. Shi, arXiv:qunt-ph/0205115 (2002).]

Any quantum computation (with **classical output**) can be realized by combining

$$H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$$
$$CCZ \equiv |0\rangle\langle 0| \otimes I^{\otimes 2} + |1\rangle\langle 1| \otimes CZ$$
$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| .$$

<u>Our idea</u>: we embed these three quantum gates into a hypergraph state.



Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

Fact 1 [Y. Shi, arXiv:qunt-ph/0205115 (2002).]

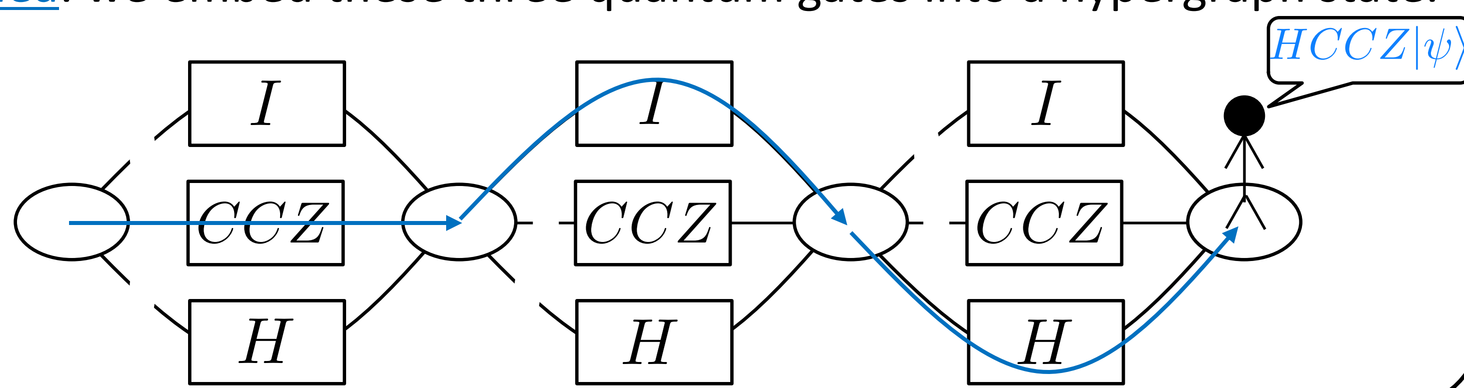
Any quantum computation (with **classical output**) can be realized by combining

$$H \equiv |+\rangle\langle 0| + |-\rangle\langle 1|$$

$$CCZ \equiv |0\rangle\langle 0| \otimes I^{\otimes 2} + |1\rangle\langle 1| \otimes CZ$$

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| .$$

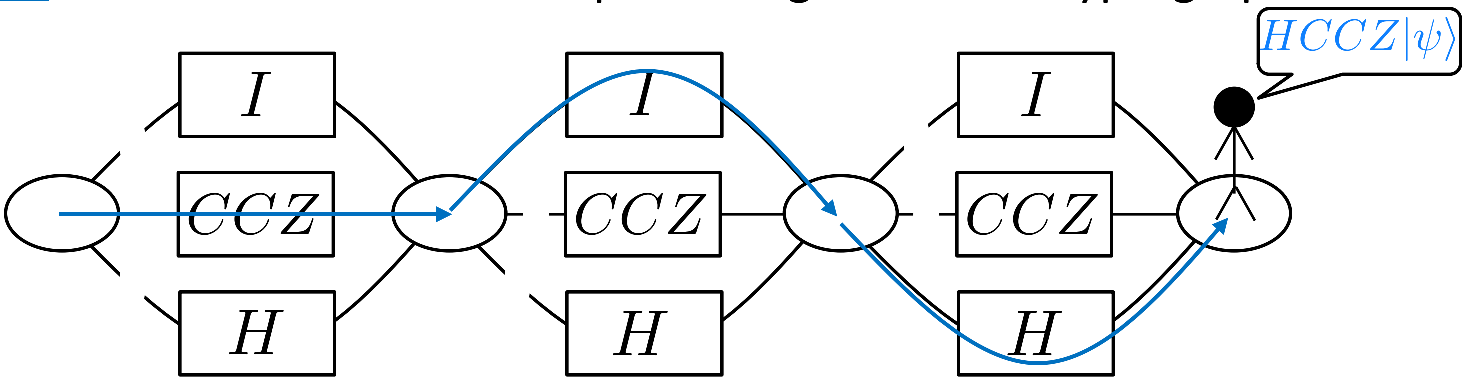
Our idea: we embed these three quantum gates into a hypergraph state.



Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Our idea: we embed these three quantum gates into a hypergraph state.



We realize

- "Moving" operation
- "Cutting" operation

by using MBQC on hypergraph states.

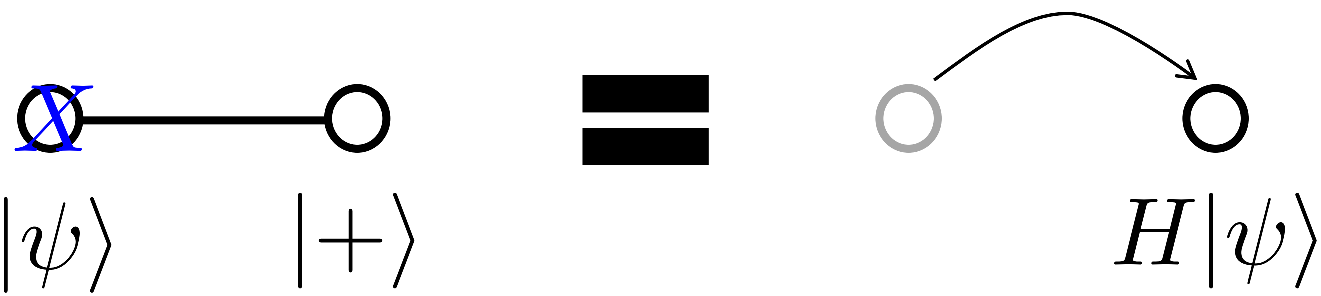
Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

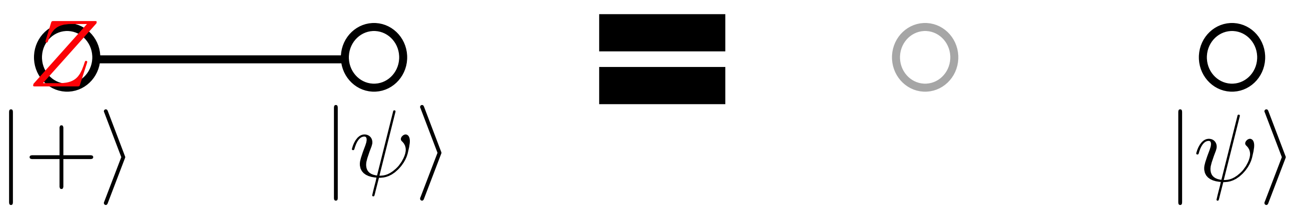
Fact 2: Gate teleportation & break operation

[R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).]

- Gate teleportation (**“moving”** operation)



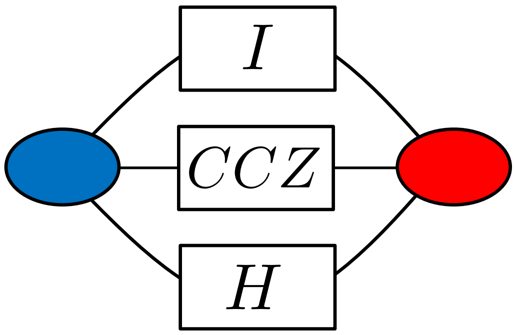
- Break operation (**“cutting”** operation)

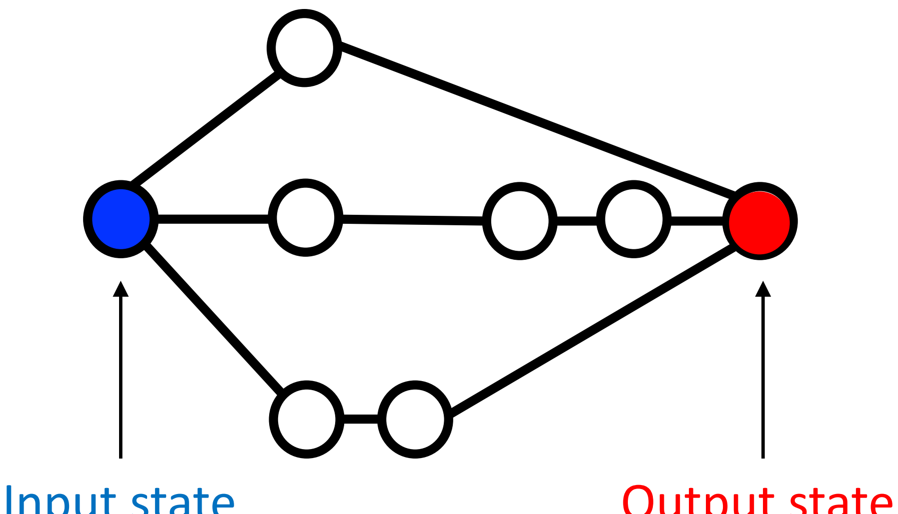


Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Identity gate I

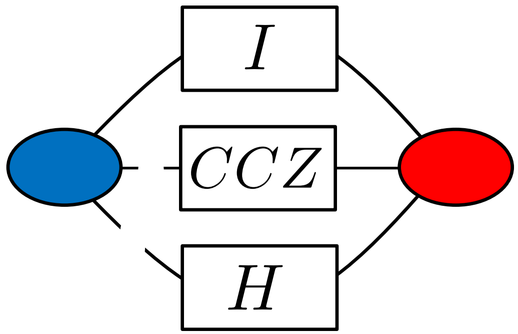


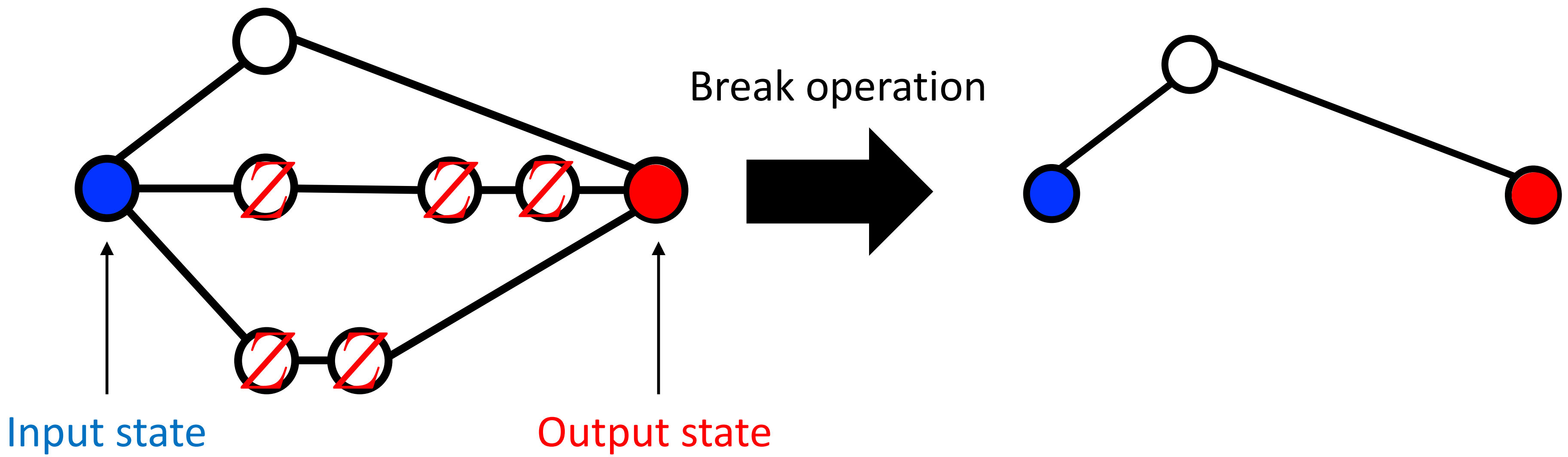


Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Identity gate I

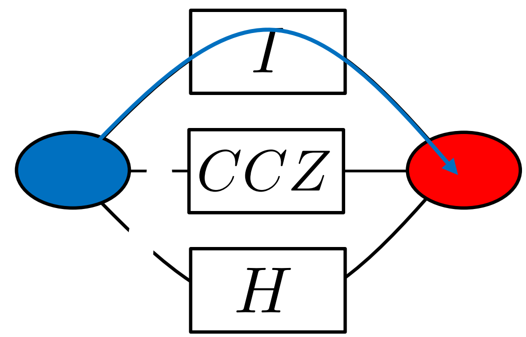


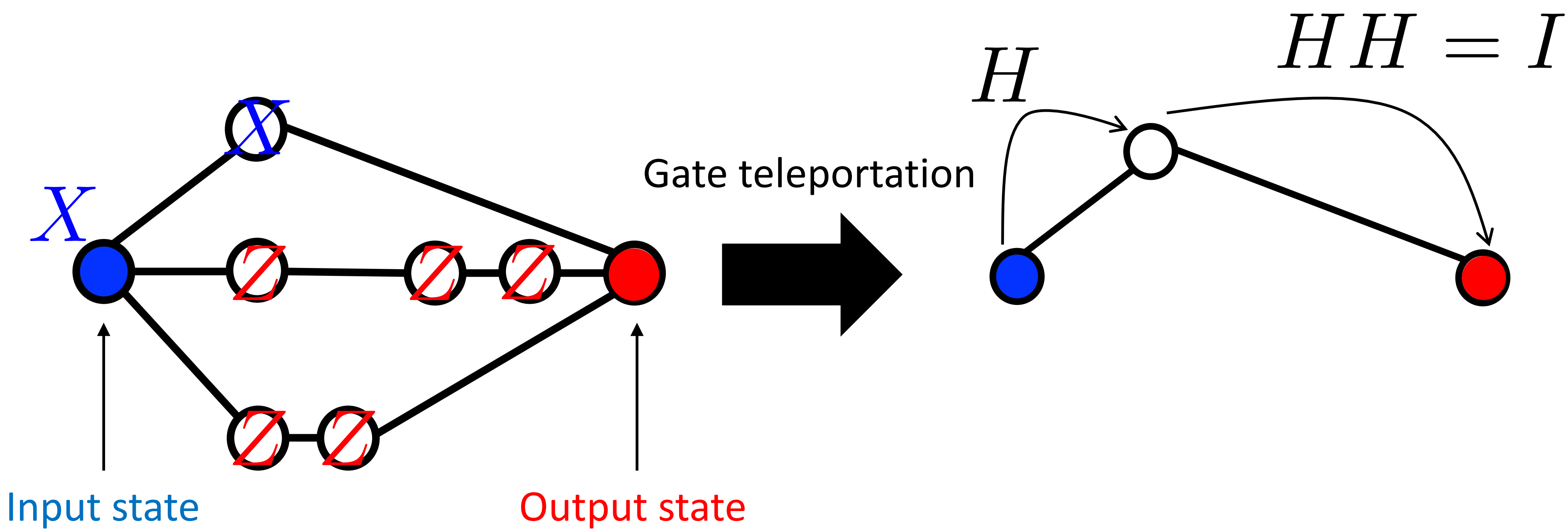


Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Identity gate I

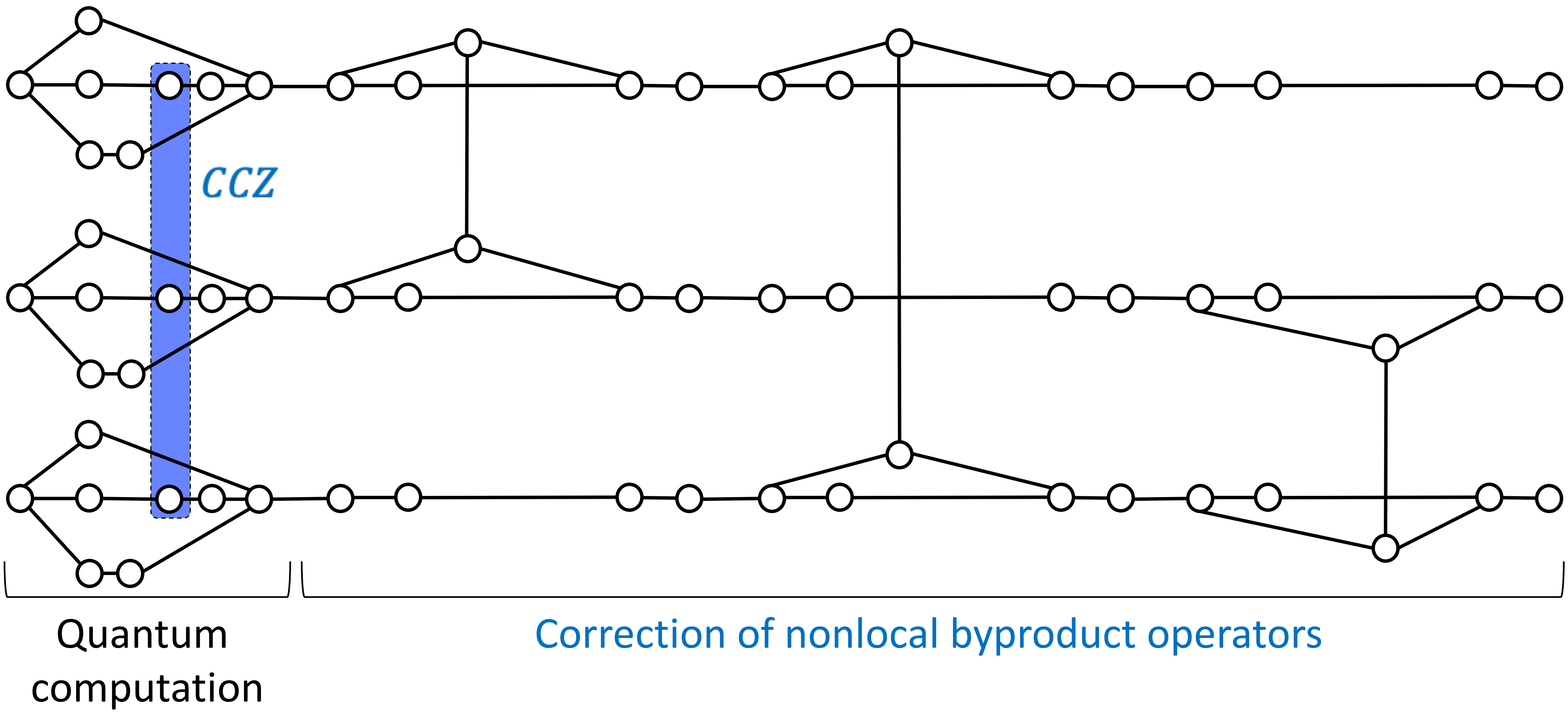




Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

Universal hypergraph state



Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

$\boldsymbol{d}$-depth quantum computation with $\boldsymbol{n}$ input qubits

- The size (i.e., the number of qubits) of our hypergraph states is

$$O(dn^4).$$

- Our hypergraph state is computationally universal.

Our result: Pauli-X, Z universal hypergraph state

[YT, T. Morimae, and M. Hayashi, Sci. Rep. **9**, 13585 (2019).]

***d*-depth quantum computation with *n* input qubits**

- The size (i.e., the number of qubits) of our hypergraph states is

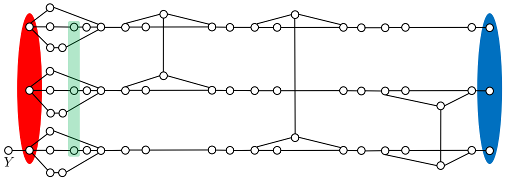
$$O(dn^4).$$

- Our hypergraph state is computationally universal.

+ Catalytic transformation

+ Sorting network

Strict universality with three Pauli measurements



[YT, arXiv:2312.16433 (2023).]

Optimal size (up to log factor)

$$O(dn\log n)$$

[H. Yamasaki, K. Fukui, YT, S. Tani, and M. Koashi, arXiv:2006.05416 (2020).]

Comparison with graph states

	Computational universality	Strict universality	Class
Graph states	$X, Y, TXT^\dagger$	$X, Y, TXT^\dagger$	Stabilizer states
Hypergraph states	X, Z	X, Y, Z	Non-stabilizer states

Advantage of hypergraph states

Comparison with graph states

	Computational universality	Strict universality	Class
Graph states	$X, Y, TXT^\dagger$	$X, Y, TXT^\dagger$	Stabilizer states
Hypergraph states	X, Z	X, Y, Z	Non-stabilizer states

Advantage of hypergraph states

Q. How hard to estimate the fidelity between ideal and actually-prepared hypergraph states?

Comparison with graph states

	Computational universality	Strict universality	Class
Graph states	$X, Y, TXT^\dagger$	$X, Y, TXT^\dagger$	Stabilizer states
Hypergraph states	X, Z	X, Y, Z	Non-stabilizer states

Advantage of hypergraph states

Q. How hard to estimate the fidelity between ideal and actually-prepared hypergraph states?

A. **Pauli-X and Z measurements** are sufficient, which is the same as graph states. [YT and T. Morimae, Phys. Rev. X **8**, 021060 (2018).]

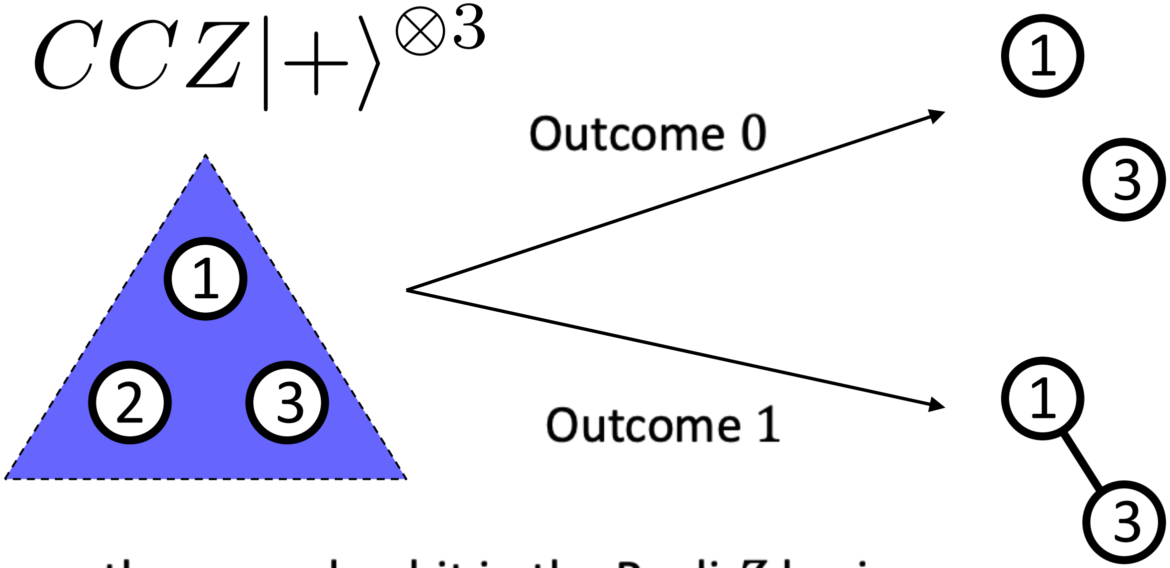
Verification of hypergraph states

[YT and T. Morimae, Phys. Rev. X **8**, 021060 (2018).]

By measuring appropriate qubits in the **Pauli-Z basis,**
any (polynomial-time-generated) **hypergraph state reduces to graph states.**

Ex.)

$$CCZ|+\rangle^{\otimes 3}$$



Measure the second qubit in the Pauli-Z basis.

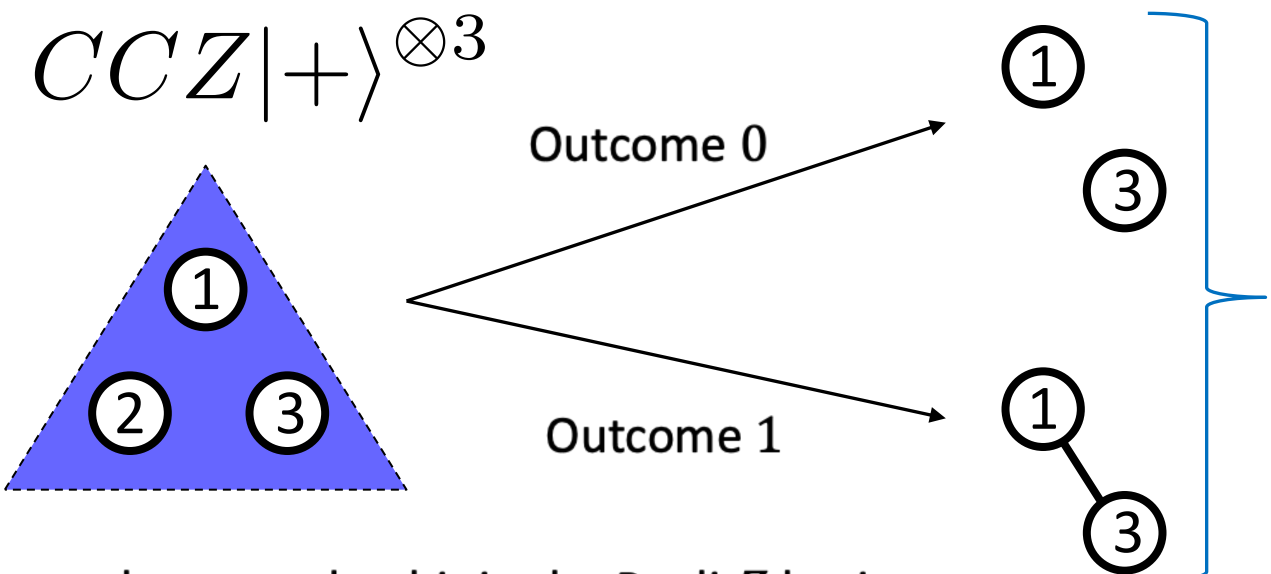
Verification of hypergraph states

[YT and T. Morimae, Phys. Rev. X **8**, 021060 (2018).]

By measuring appropriate qubits in the **Pauli-Z basis**,
any (polynomial-time-generated) **hypergraph state reduces to graph states.**

Ex.)

$$CCZ|+\rangle^{\otimes 3}$$



They are testable
as with graph states.

Pauli-X and Z meas.
are sufficient!

Measure the second qubit in the Pauli-Z basis.

Verification of hypergraph states

[YT and T. Morimae, Phys. Rev. X **8**, 021060 (2018).]

Theorem

If the received state ρ passes our verification protocol, then

$$\langle HG|\rho|HG\rangle \geq 1 - O(1/n)$$

is guaranteed with significance level $O(1/n)$.

$|HG\rangle$: Hypergraph state

Remark

1. Pauli-X and Z measurements are sufficient.
2. The sample complexity is $O(n^{21})$.
3. Due to the quantum de Finetti theorem [K. Li and G. Smith, Phys. Rev. Lett. **114**, 160503 (2015).], the i.i.d. property of quantum states is unnecessary.

It increases only a polynomial number of samples.

Verification of hypergraph states

[YT and T. Morimae, Phys. Rev. X **8**, 021060 (2018).]

<u>Recent progress</u>

1. In our protocol, Pauli-X and Z measurements are sufficient.

→ When the noise is the thermal or phase-flip noise,
a single measurement setting is sufficient for some hypergraph states.

[K. Akimoto, S. Tsuchiya, R. Yoshii, and YT, Phys. Rev. A **106**, 012405 (2022).]

2. Our sample complexity is $O(n^{21})$.

→ It was improved to $O(n \log n)$, which should be optimal.

[H. Zhu and M. Hayashi, Phys. Rev. Applied **12**, 054047 (2019).]

3. Our protocol is applicable to **qubit** hypergraph states.

→ It was extended to

- Qudit hypergraph states [H. Zhu and M. Hayashi, Phys. Rev. Applied **12**, 054047 (2019).], and
- Continuous-variable hypergraph states.

[YT, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, npj Quantum Inf. **5**, 27 (2019).]