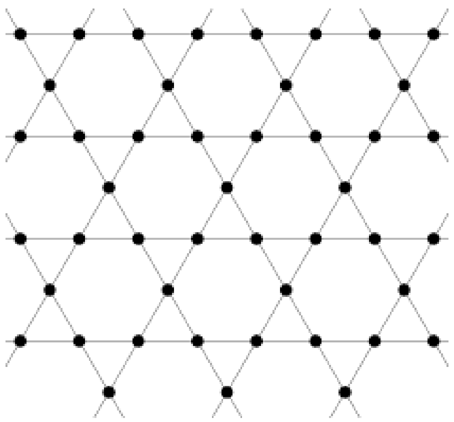
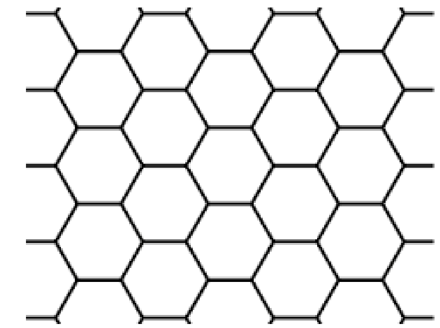
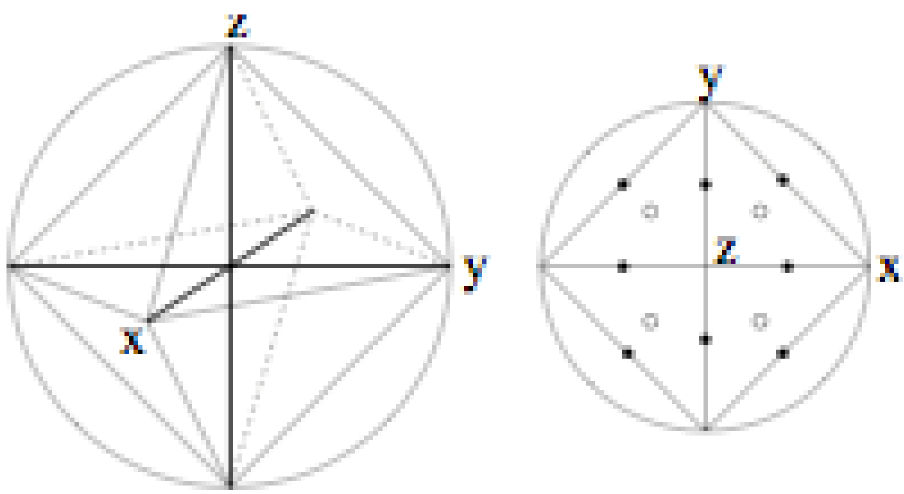
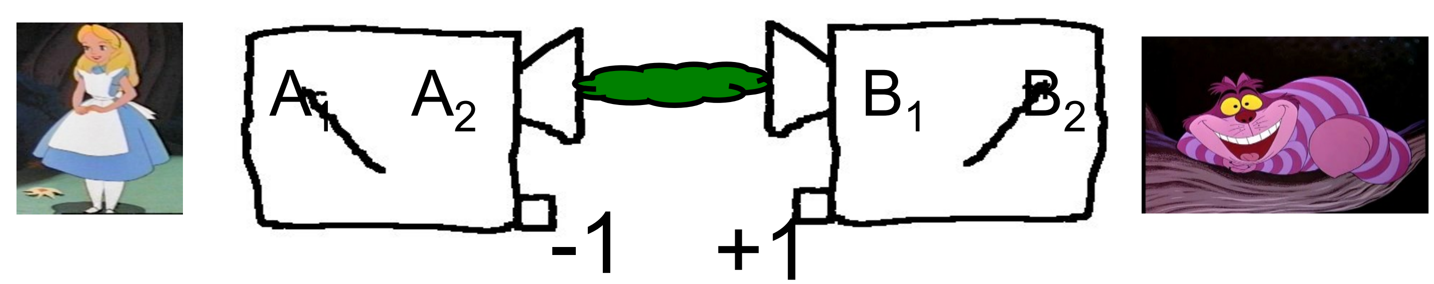


Introduction to measurement-based quantum computation



Ernesto F. Galvão (INL, UFF)





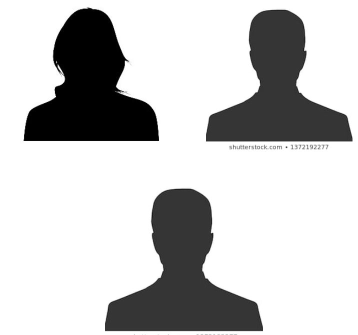
Invited lecture, Master's in Physics Engineering, UMinho, 5/1/2022

Quantum and Linear-Optical Computation group

- Established at INL in July, 2019. Research lines:

- Principles enabling photonic quantum computation
- Information processing with integrated photonic chips
- Resources in different models of quantum computation

Secured funding for 3 postdocs



+5 recently admitted PhD students

Anita Camillini

Raman Chaudhary

Angelos Bampounis

Rafael Wagner

Antonio Molero

Ernesto Galvão

(Group leader)

Rui Soares Barbosa

(Staff Researcher)

[on-going hiring process]

(Staff Researcher)

Carlos Fernandes

(PhD student)

Michael Oliveira

(PhD student)

Filipa Peres

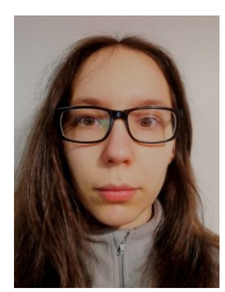
(PhD student)

Alexandra da Costa Alves

(Master's)

Ana Filipa Carvalho

(Master's)



Mafalda da Costa Alves

(Master's)

José Guimarães

(Master's)

António Pereira

(Master's)

Introduction to measurement-based quantum computation

Outline:

- Clifford circuits
  - Pauli and Clifford groups
  - Simulability of Clifford circuits
  - Upgrading Clifford circuits to universal QC

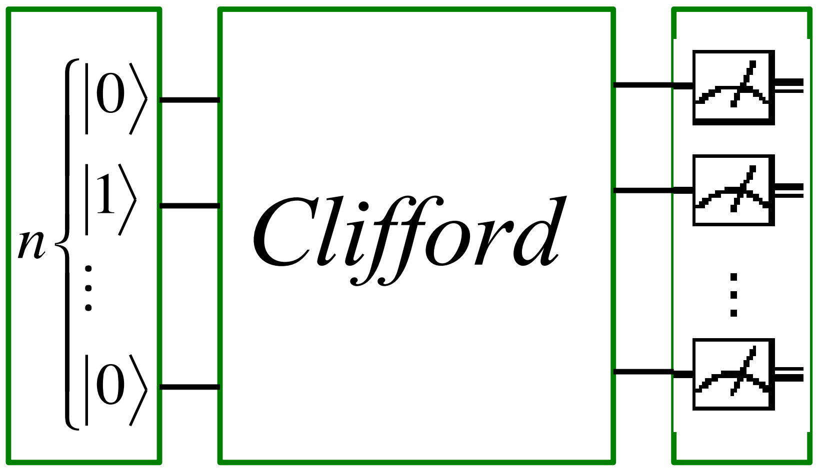
- How MBQC works
  - One-bit teleportation circuit
  - Gate teleportation
  - Concatenating MBQC gates

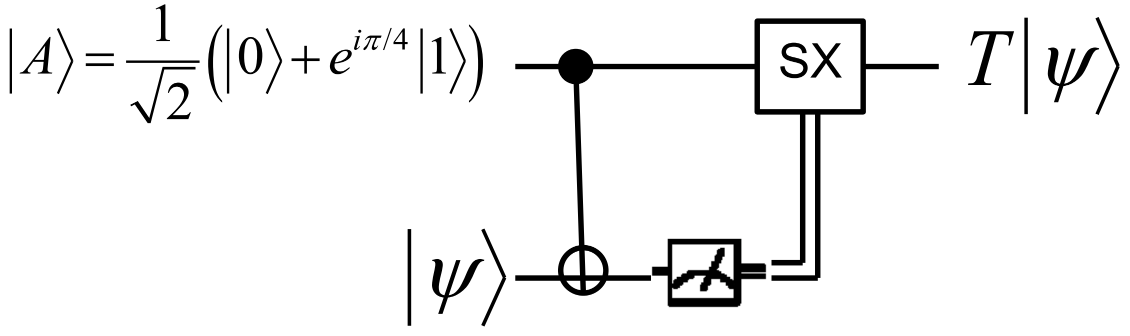
- Resources for MBQC: graph and cluster states

- Experimental implementations

- Resources for MBQC: contextuality and non-locality

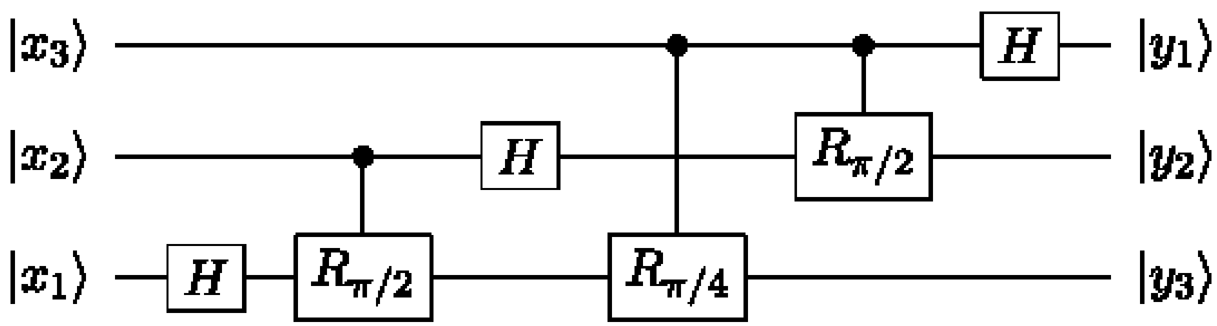
Clifford circuits



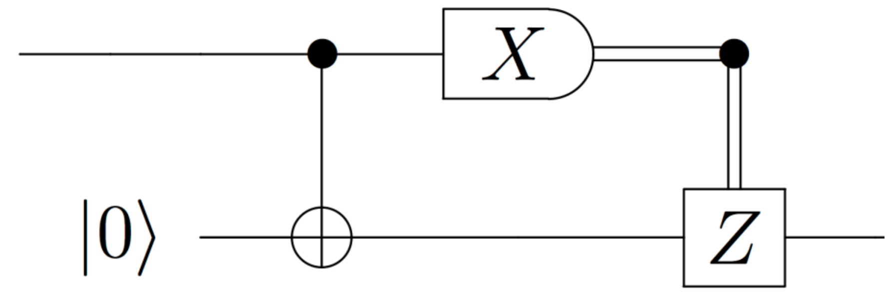


Basics of the circuit model

- The most well-known model for quantum computation is the circuit model, obtained in analogy with classical circuits

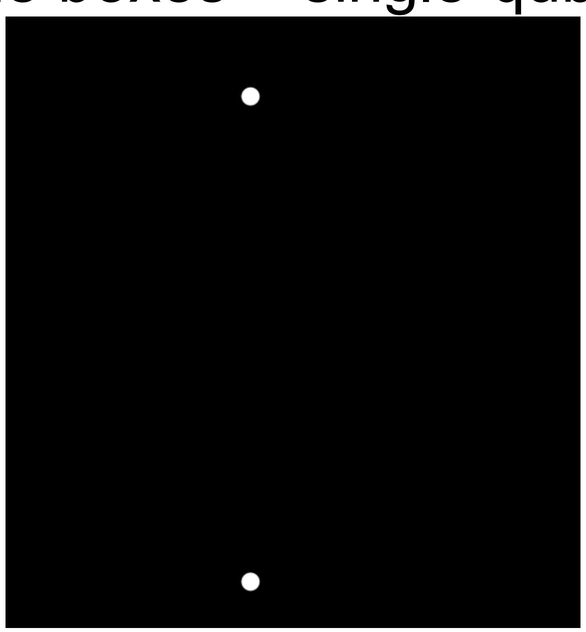


3-qubit QFT

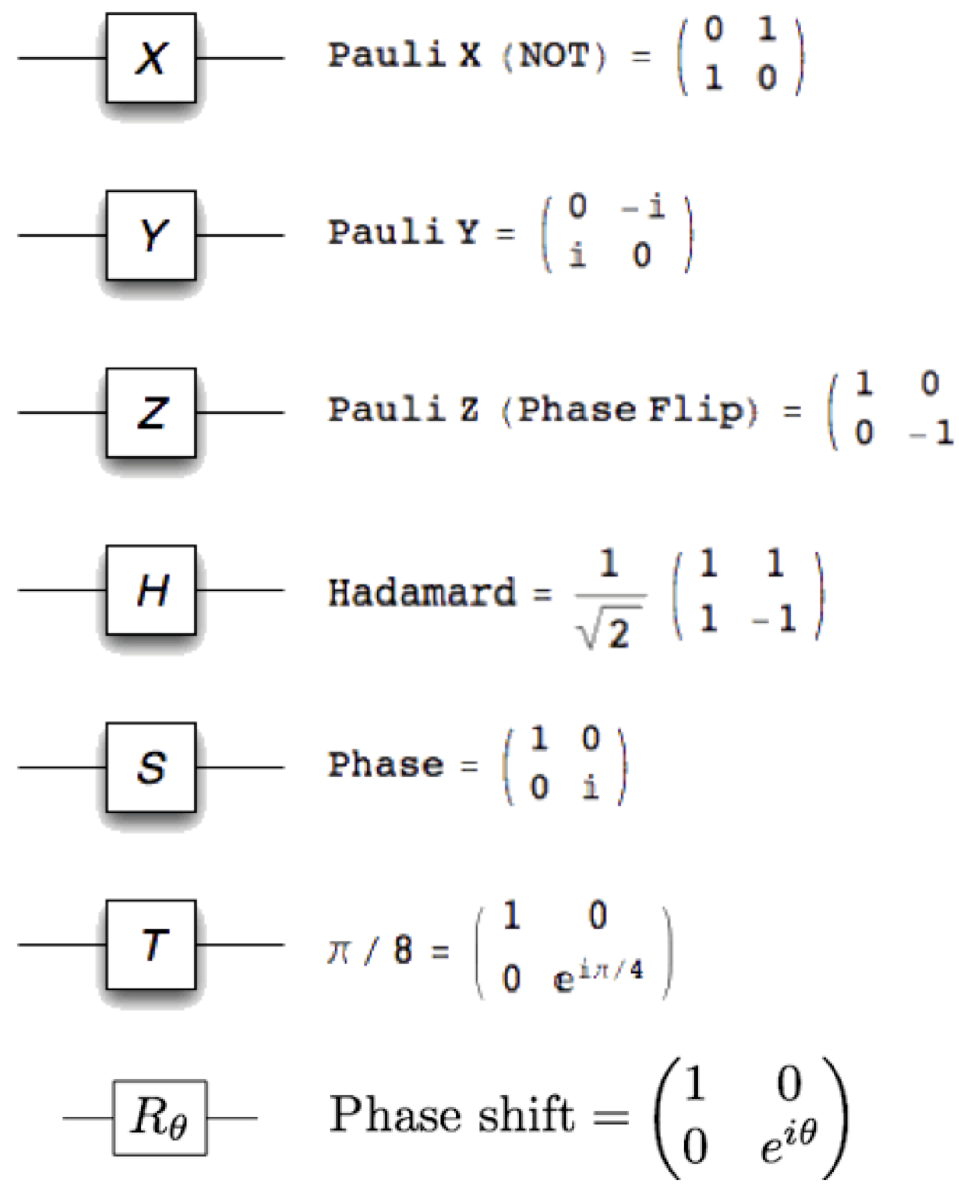


1-bit Z teleportation

- wires = qubits (i.e. 2-level systems)
- little boxes = single-qubit gates



$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$



Clifford circuits

- **Pauli group**: tensor products of $\pm I, \pm iI, X, Z$

- example: $-iZ_1 \otimes X_2 \otimes I_3$

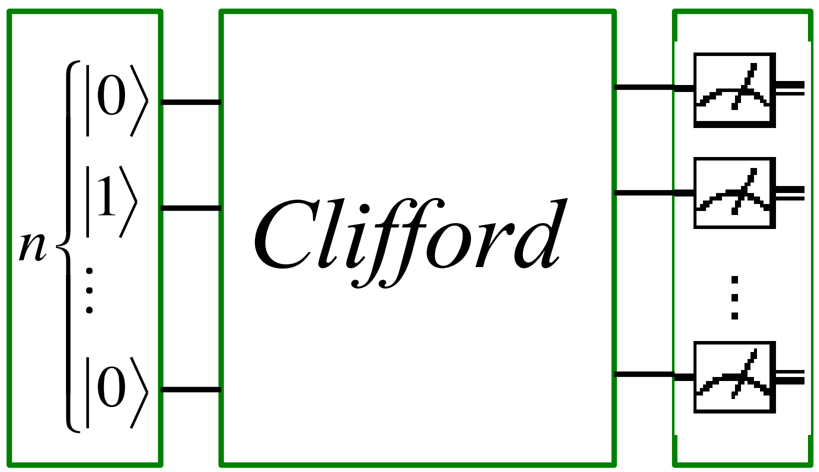
Clifford circuits

- **Pauli group**: tensor products of $\pm I, \pm iI, X, Z$

\- example: $-iZ_1 \otimes X_2 \otimes I_3$

- **Clifford group**: unitaries C that map Paulis into Paulis:

$$CP_iC^+ = P_j \Leftrightarrow CP_i = P_jC$$

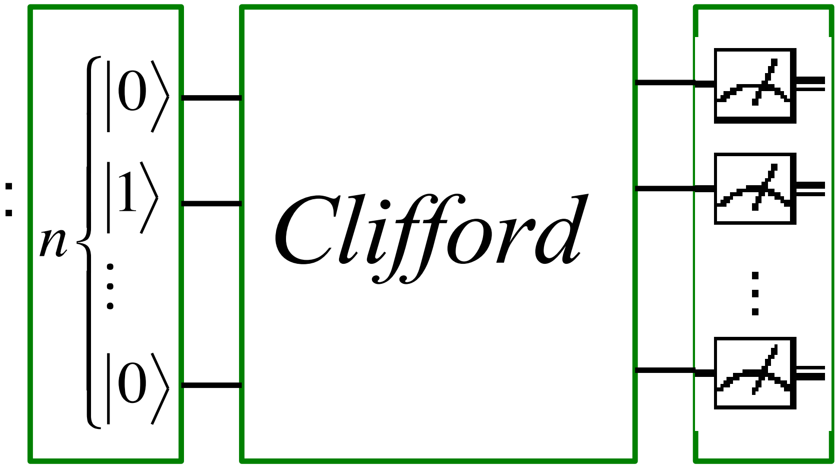


- Clifford group is generated by $\{H, P, CNOT\}$

- Clifford circuits create large amounts of entanglement, are useful for teleportation, error correction…

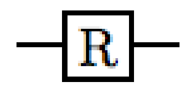
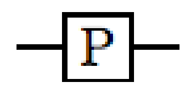
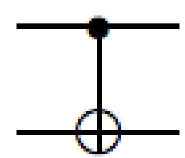
…but are **efficiently simulable**.

Clifford circuits



- **Pauli group**: tensor products of $\pm I, \pm iI, X, Z$
- **Clifford group**: unitaries C that map Paulis into Paulis:

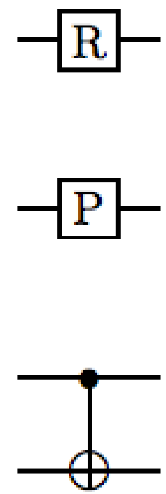
$$CP_iC^{+} = P_j \Leftrightarrow CP_i = P_jC$$

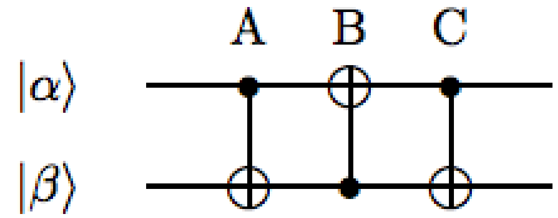
R	$X \rightarrow Z$ $Z \rightarrow X$	
P	$X \rightarrow Y$ $Z \rightarrow Z$	
CNOT	$X \otimes I \rightarrow X \otimes X$ $I \otimes X \rightarrow I \otimes X$ $Z \otimes I \rightarrow Z \otimes I$ $I \otimes Z \rightarrow Z \otimes Z$	

- The key simulation idea is to use Heisenberg picture:
  - initial state is eigenstate of Pauli operator
  - each Clifford gate maps it into a new Pauli (efficient computation)
  - keep track of the Pauli transformation until end, when measurement outcomes can be efficiently computed.
- Clifford circuits are not believed even to be able to do universal classical computation…

Example: Heisenberg simulation of Clifford circuit

R	$X \to Z$ $Z \to X$	
P	$X \to Y$ $Z \to Z$	
CNOT	$X \otimes I \to X \otimes X$ $I \otimes X \to I \otimes X$ $Z \otimes I \to Z \otimes I$ $I \otimes Z \to Z \otimes Z$	





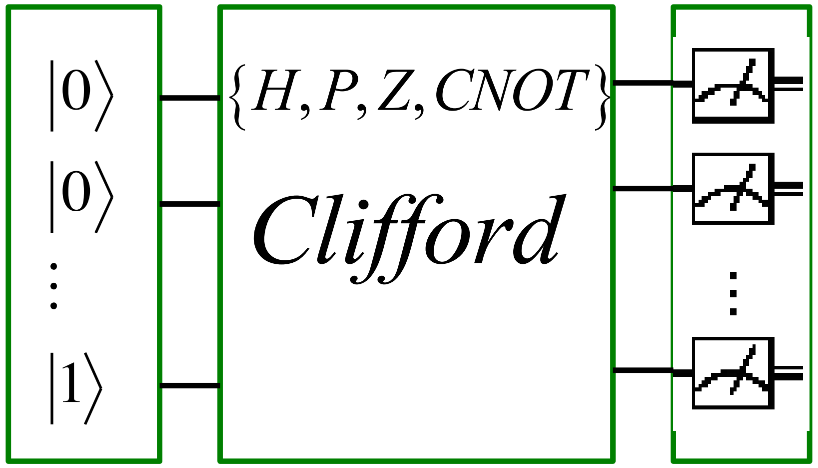
b)

A: CNOT$(1 \to 2)$	$\overline{X}_1$	$X \otimes X$
	$\overline{X}_2$	$I \otimes X$
	$\overline{Z}_1$	$Z \otimes I$
	$\overline{Z}_2$	$Z \otimes Z$
B: CNOT$(2 \to 1)$	$\overline{X}_1$	$I \otimes X$
	$\overline{X}_2$	$X \otimes X$
	$\overline{Z}_1$	$Z \otimes Z$
	$\overline{Z}_2$	$Z \otimes I$
C: CNOT$(1 \to 2)$	$\overline{X}_1$	$I \otimes X$
	$\overline{X}_2$	$X \otimes I$
	$\overline{Z}_1$	$I \otimes Z$
	$\overline{Z}_2$	$Z \otimes I$

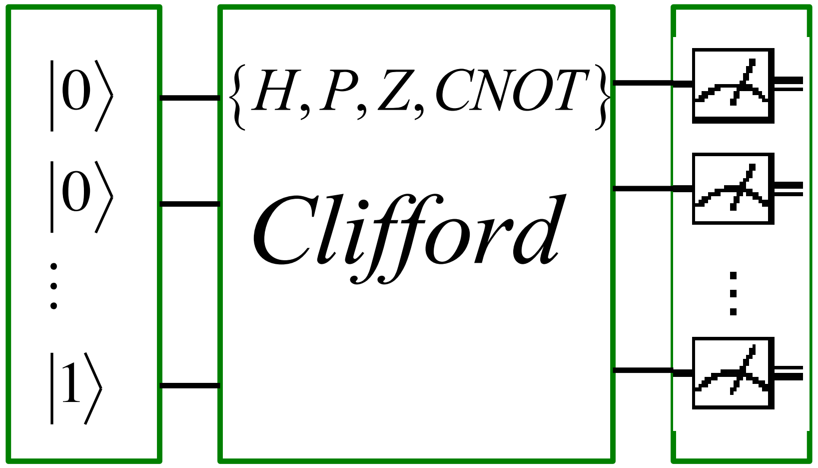
- The key simulation idea is to use Heisenberg picture:
  - initial state is eigenstate of Pauli operator
  - each Clifford gate maps it into a new Pauli (efficient computation)
  - keep track of the Pauli transformation until end, when measurement outcomes can be efficiently computed.

"Upgrading" a Clifford computer

- Clifford: $\{H, P, Z, CNOT\}$, all that's missing is *T* gate



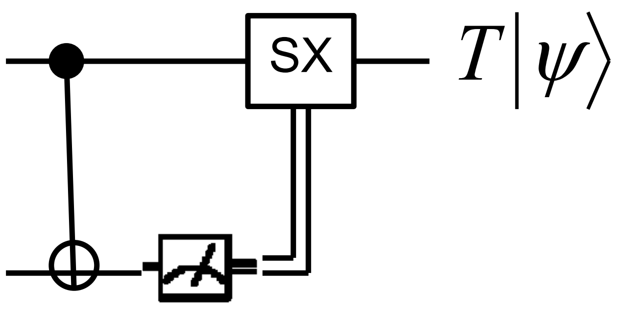
“Upgrading” a Clifford computer



- Clifford: $\{H,P,Z,CNOT\}$, all that’s missing is *T* gate
- There’s a work-around using:
    - **magic input states** and
    - **adaptativity**

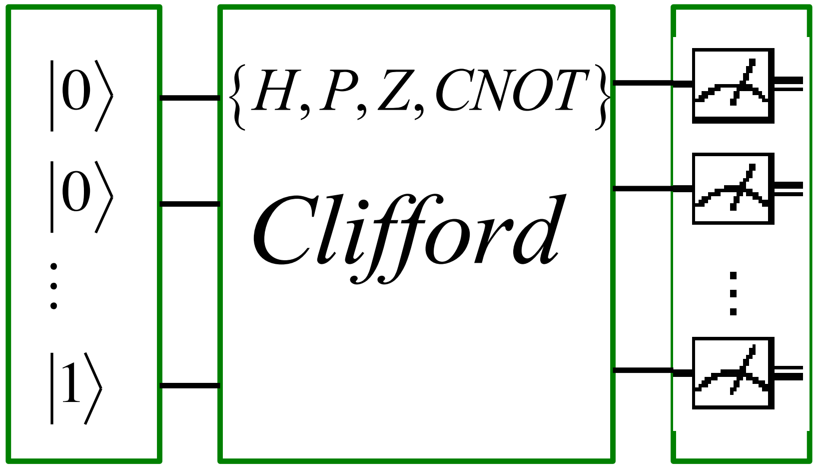
  [Bravyi, Kitaev PRA 71, 022136 (2005)]

$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$



“Upgrading” a Clifford computer

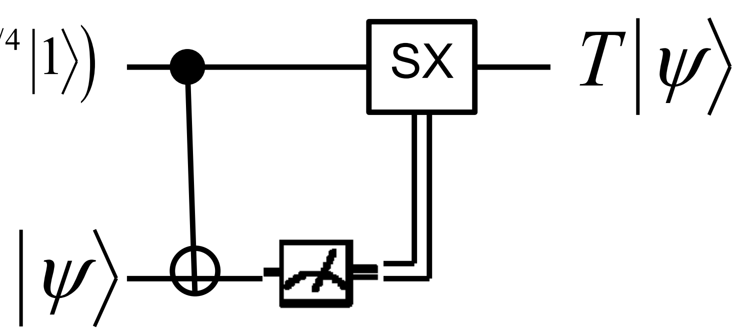
- Clifford: $\{H, P, Z, CNOT\}$, all that’s missing is *T* gate

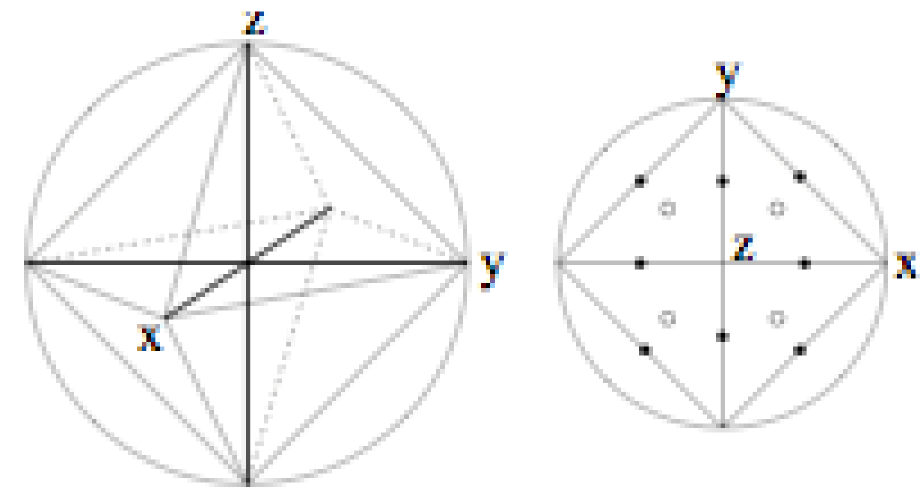


- There’s a work-around using:
  - **magic input states** and
  - **adaptativity**

  [Bravyi, Kitaev PRA 71, 022136 (2005)]

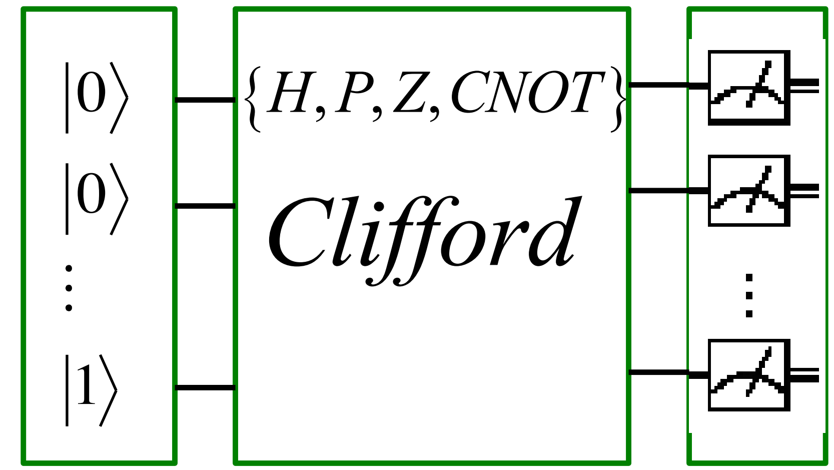
$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$





"Upgrading" a Clifford computer

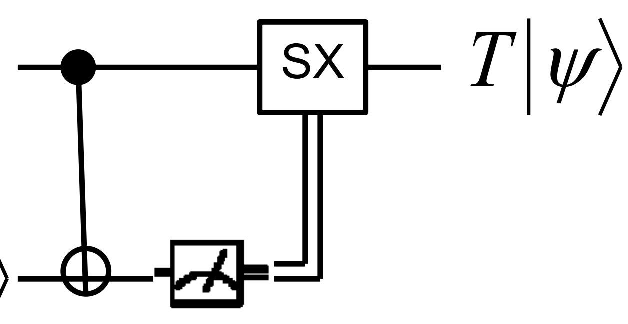
- Clifford: $\{H, P, Z, CNOT\}$, all that's missing is *T* gate

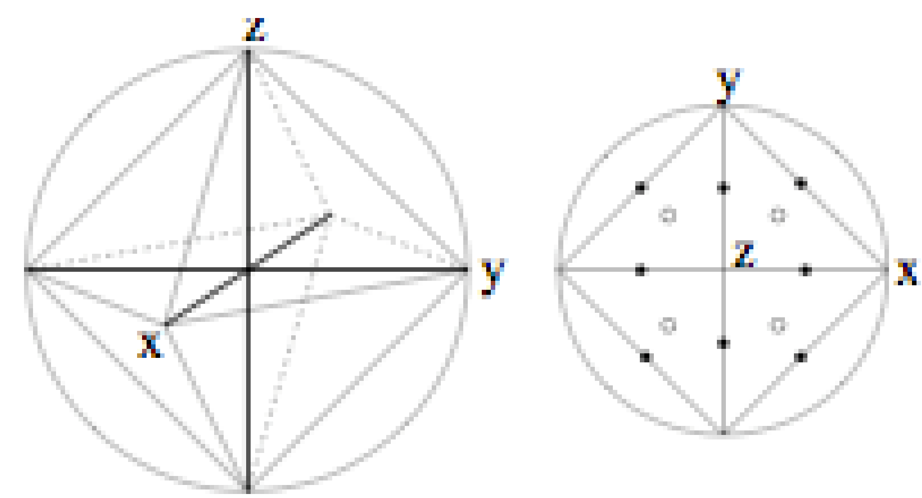


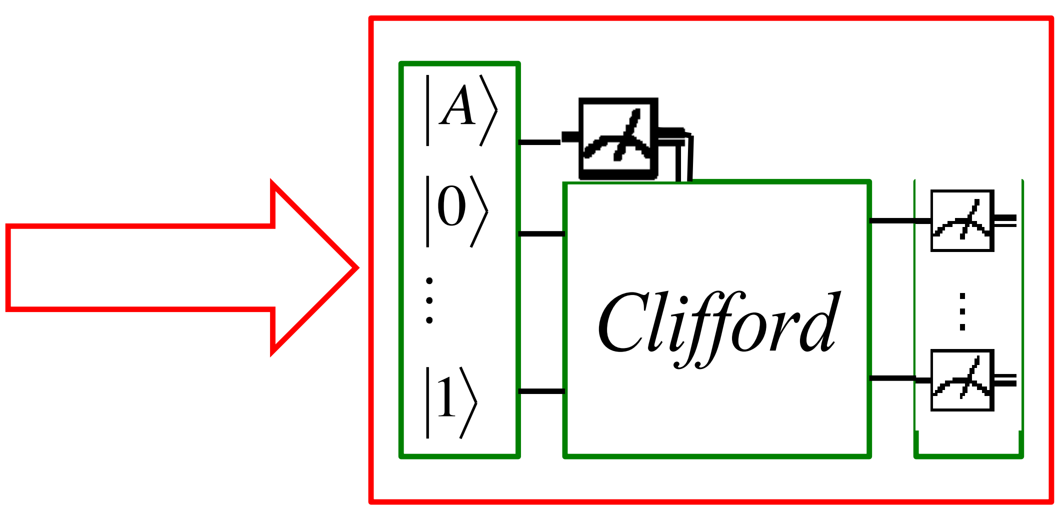
- There's a work-around using:
  - **magic input states** and
  - **adaptativity**

  [Bravyi, Kitaev PRA 71, 022136 (2005)]

$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$



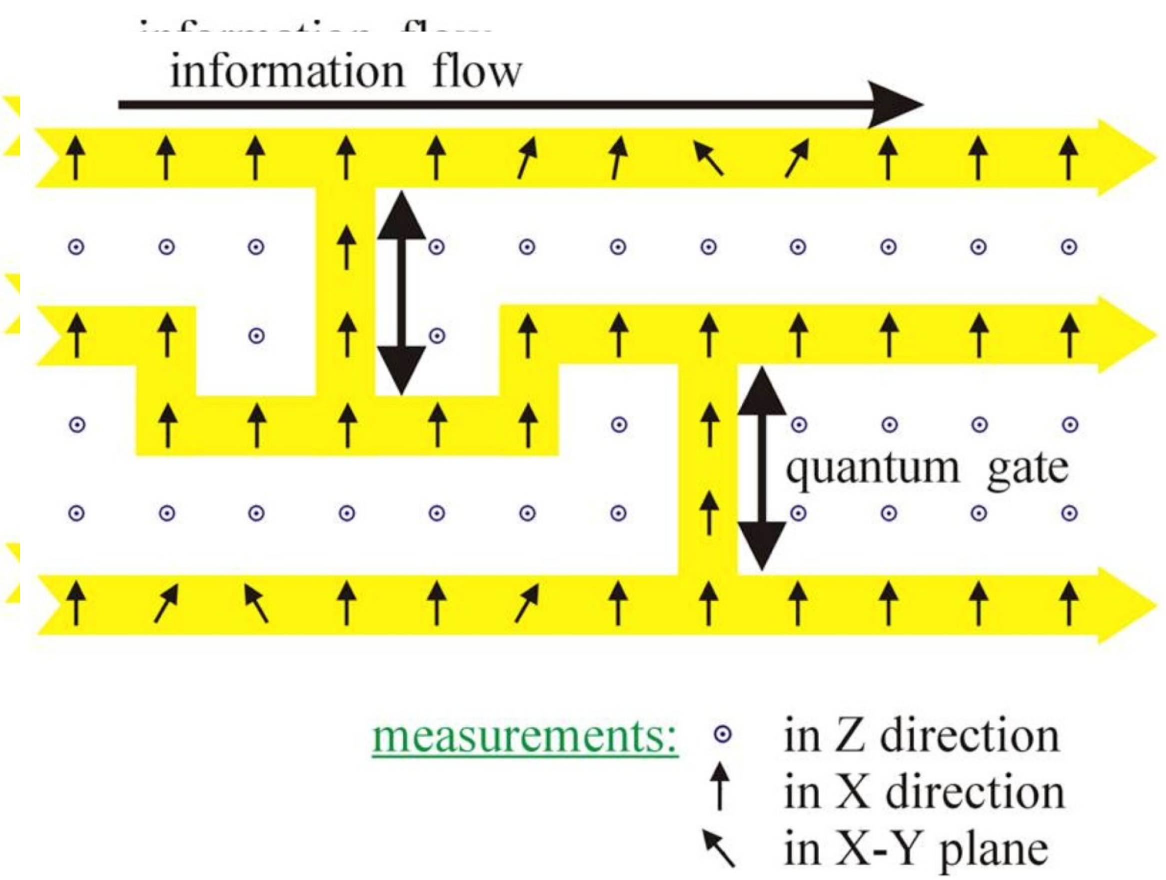


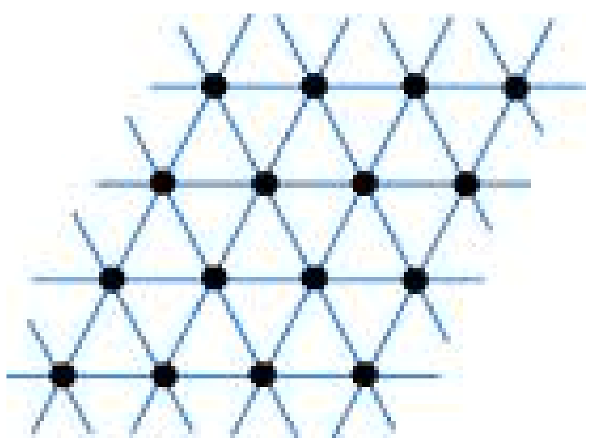


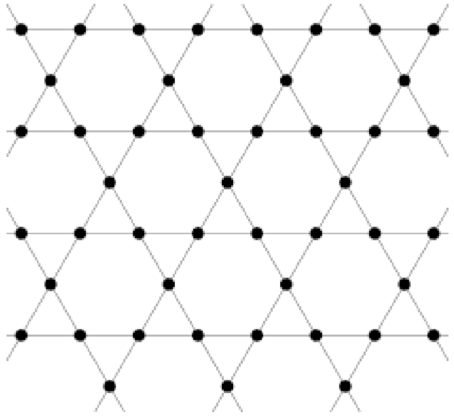
is universal for QC

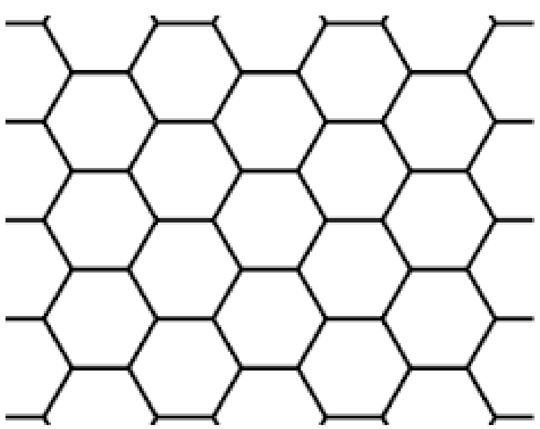
- Relevant for topological quantum computation with anyons, as for example Ising model implements Clifford operations in a topologically protected way

Measurement-based quantum computation (MBQC)



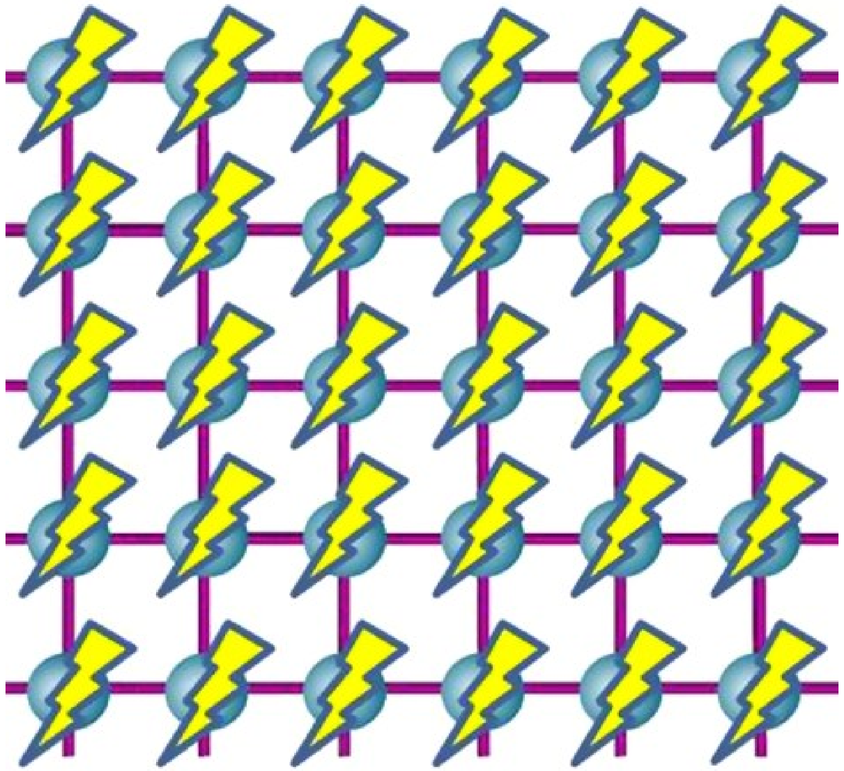






MBQC: basic ingredients

- Class of QC models where the computation is driven by measurements on previously entangled states



1- Initialization by CZ gates on $|+\rangle$ states;

2- Sequence of single-qubit, adaptive measurements.

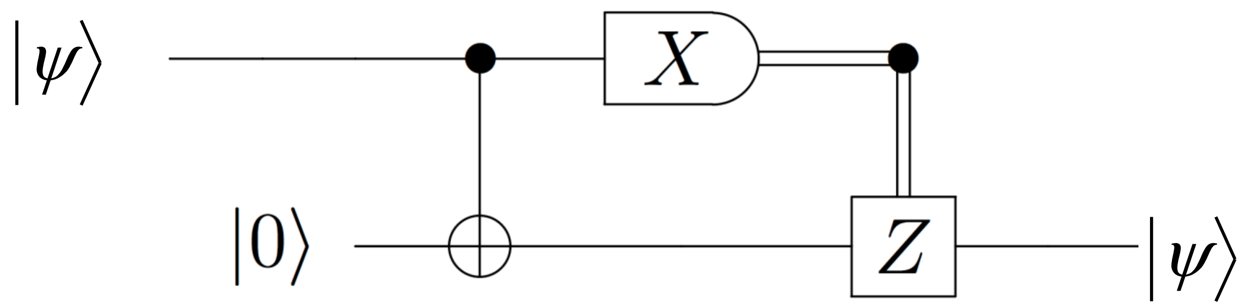
- Origin: gate teleportation idea [Gottesman, Chuang, Nature 402, 390 (1999)]

- Most well-know variant is the one-way model (1WQC)[Raussendorf, Briegel PRL 86, 5188 (2001)]

- Brief introduction to MBQC based on McKague's paper "Interactive proofs for BQP via self-tested graph states" arxiv:1309.5675 (2013)

MBQC: step-by-step

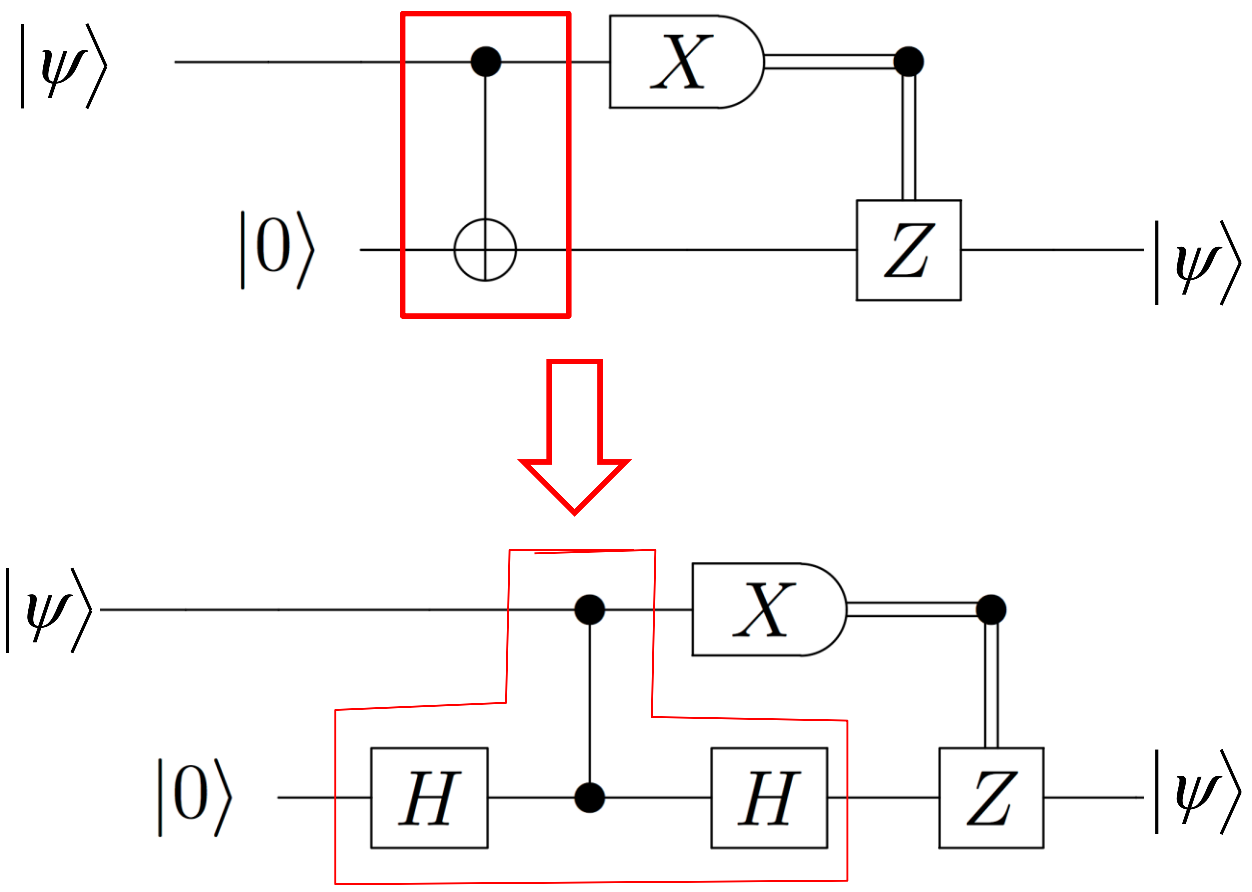
3 versions of the "1-bit *Z* teleportation" circuit:



- X measurement result controls Z gate
- Direct calculation shows this works

MBQC: step-by-step

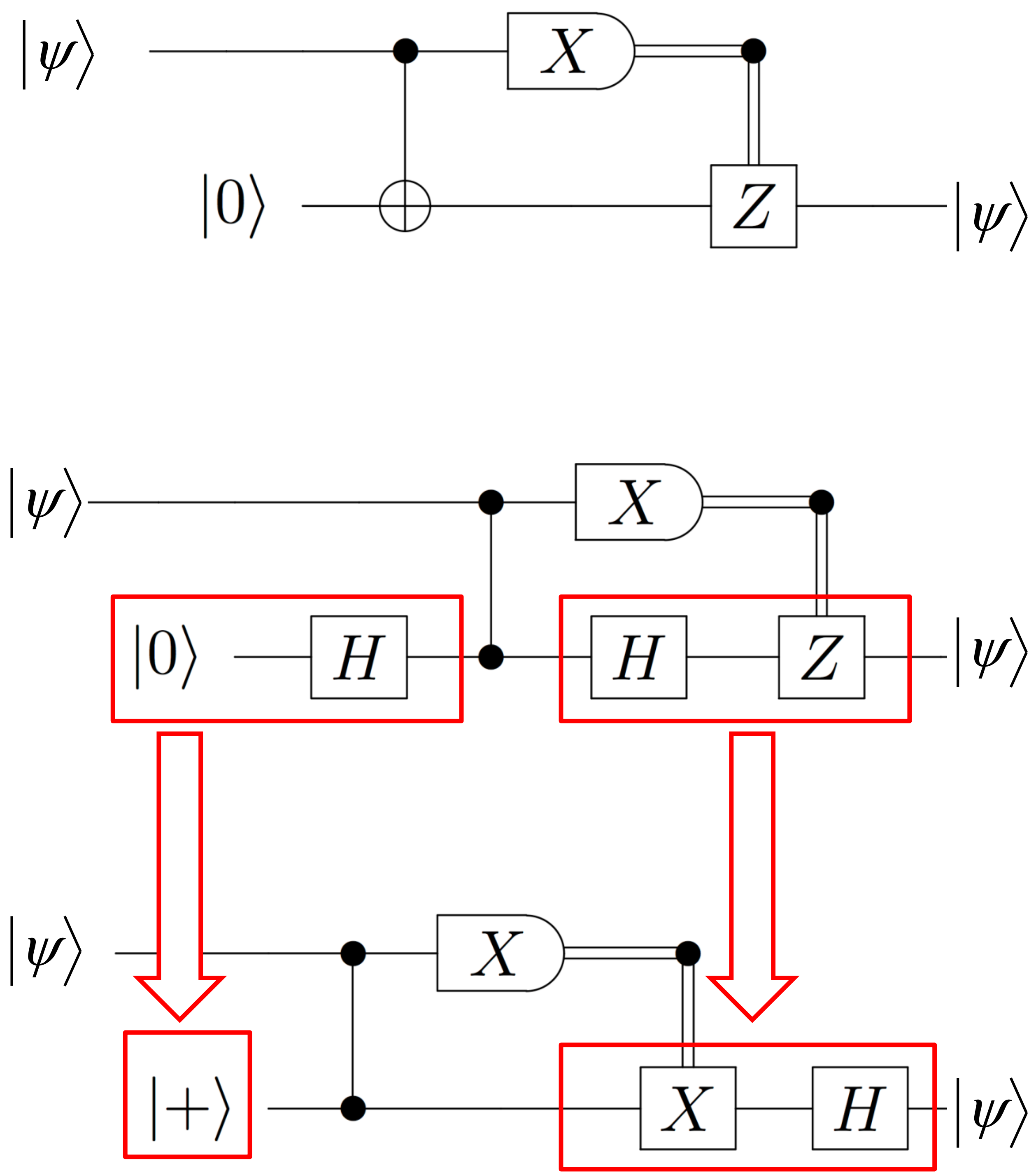
3 versions of the “1-bit *Z* teleportation” circuit:



- X measurement result controls Z gate
- Direct calculation shows this works
- Identity transforms CNOT into CZ

MBQC: step-by-step

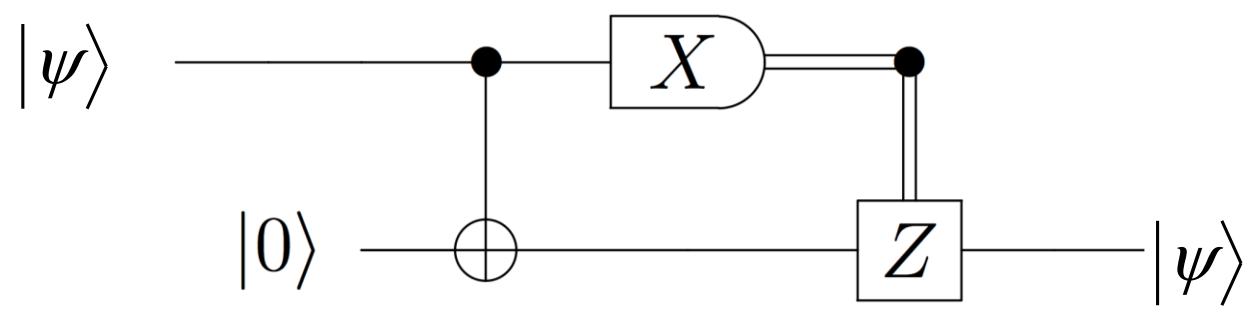
3 versions of the "1-bit *Z* teleportation" circuit:



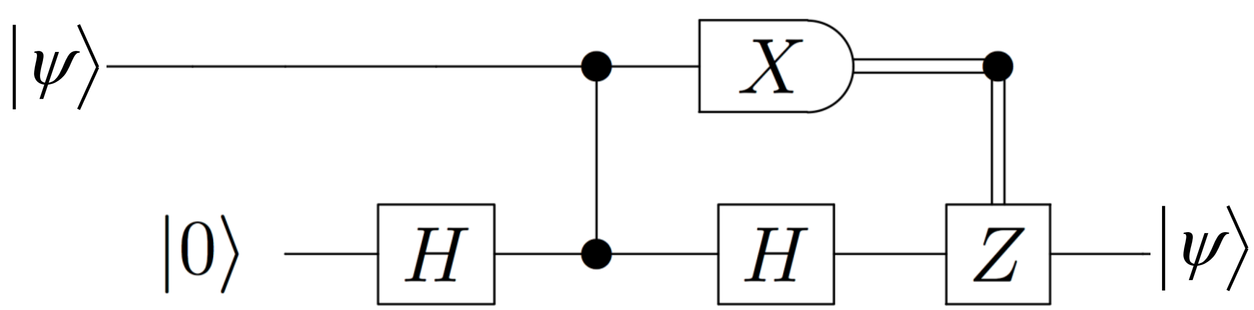
- X measurement result controls Z gate
- Direct calculation shows this works
- Identity transforms CNOT into CZ
- Left H incorporated in input $|+\rangle$
- HZ = XH identity

MBQC: step-by-step

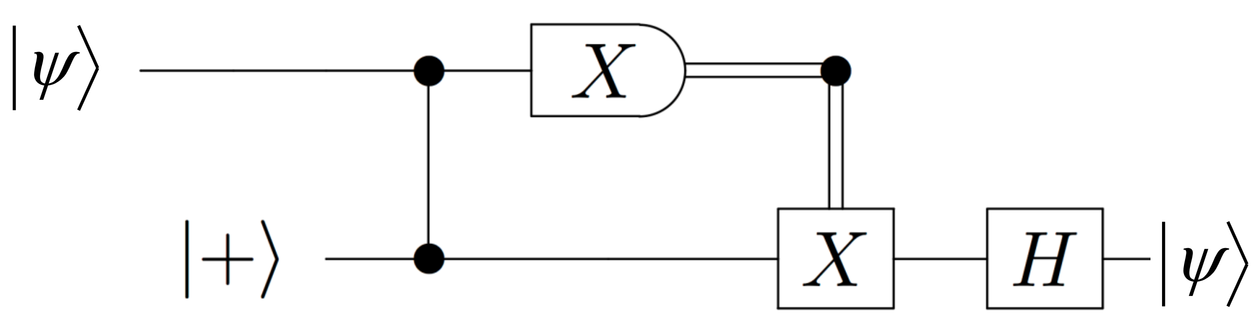
3 versions of the "1-bit *Z* teleportation" circuit:



- X measurement result controls Z gate
- Direct calculation shows this works



- Identity transforms CNOT into CZ

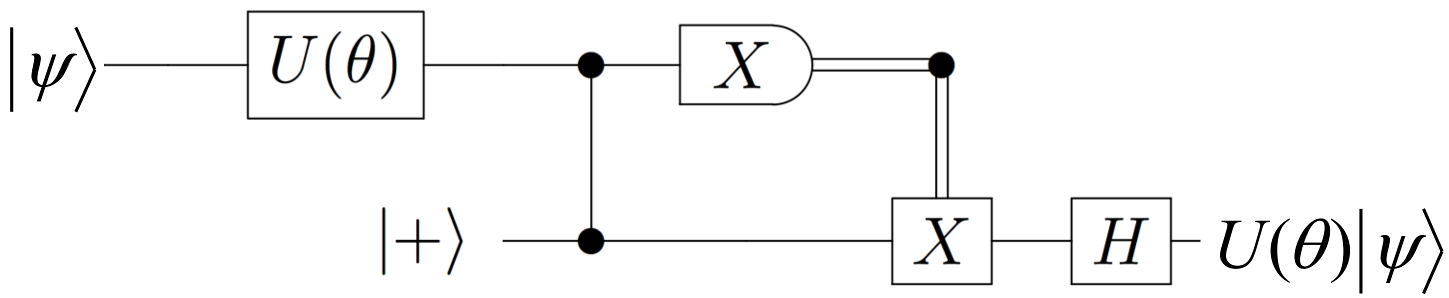


- Left H incorporated in input $|+\rangle$
- HZ = XH identity

So far: no computation, but: ancilla initialized in $|+\rangle$ state; CZ gate creates entanglement

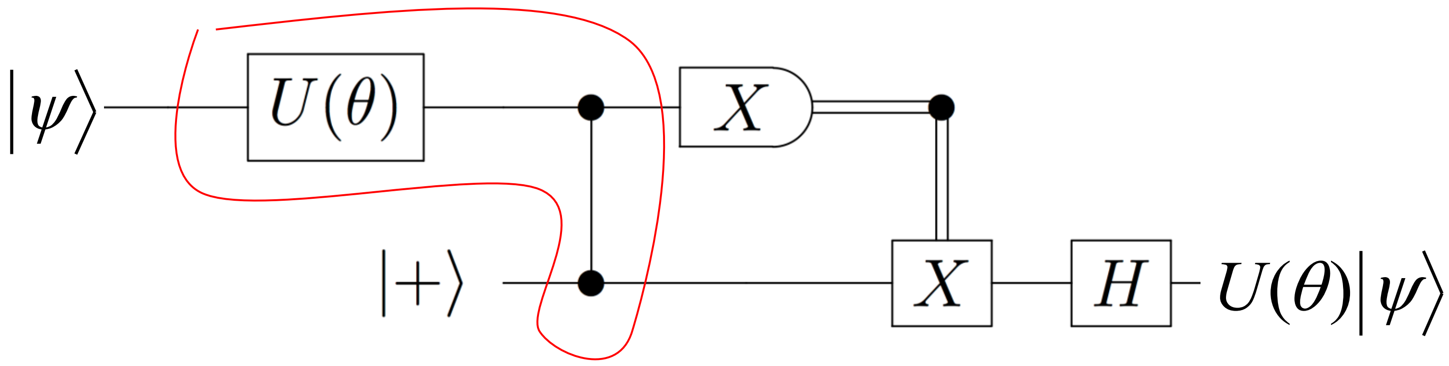
MBQC: step-by-step

Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$**:**



MBQC: step-by-step

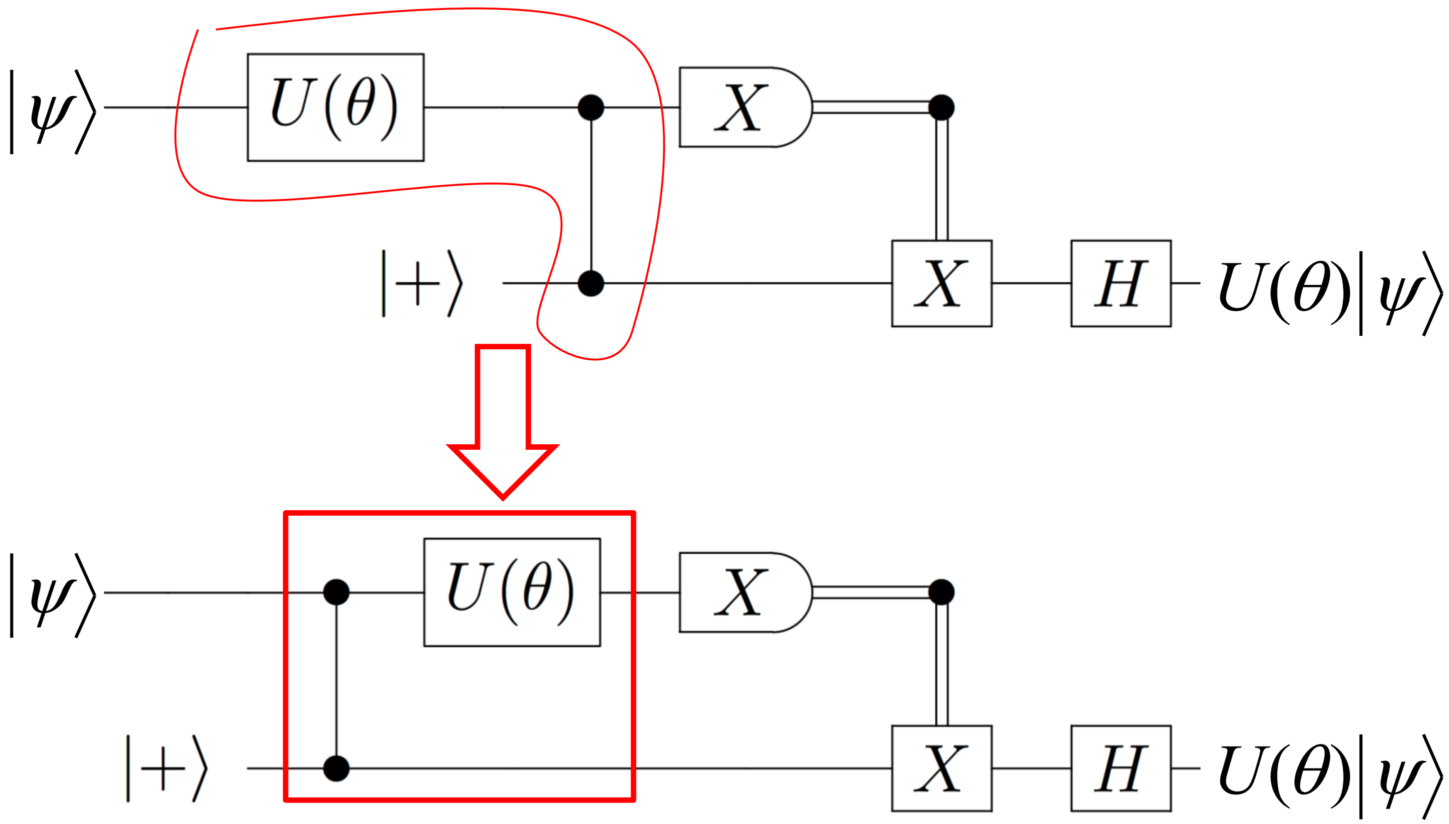
Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$



- U commutes with CZ

MBQC: step-by-step

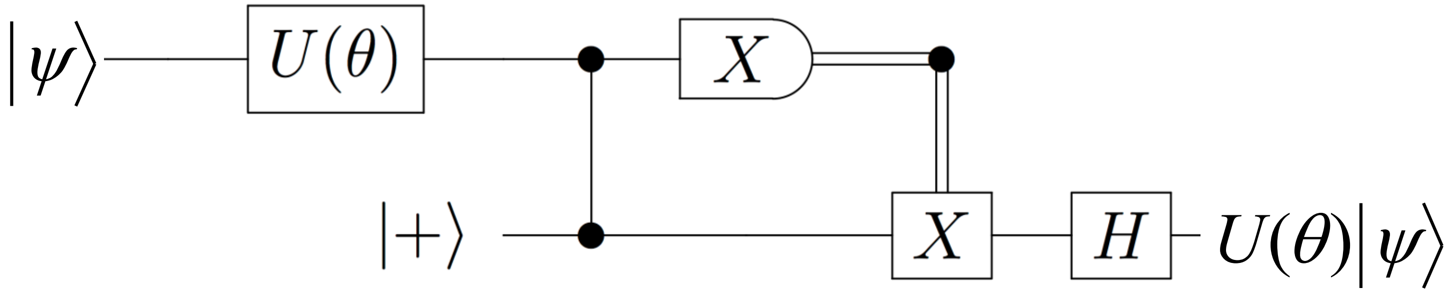
Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$**:**



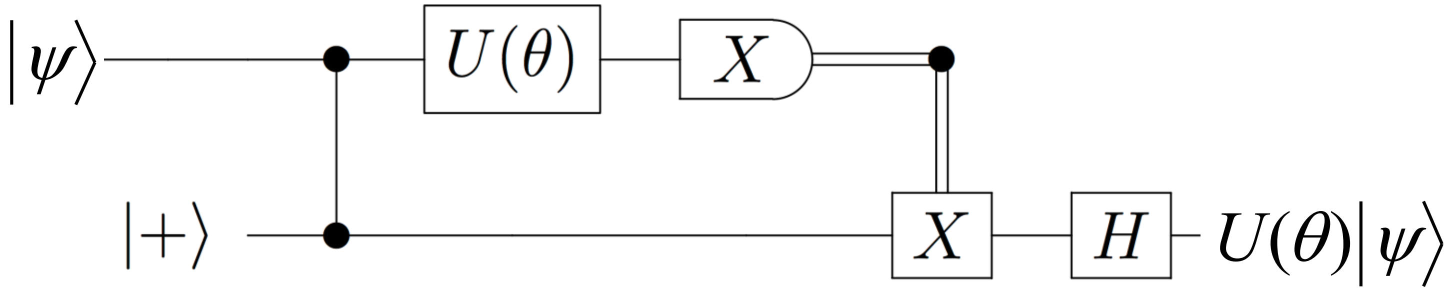
- U commutes with CZ

MBQC: step-by-step

Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$**:**

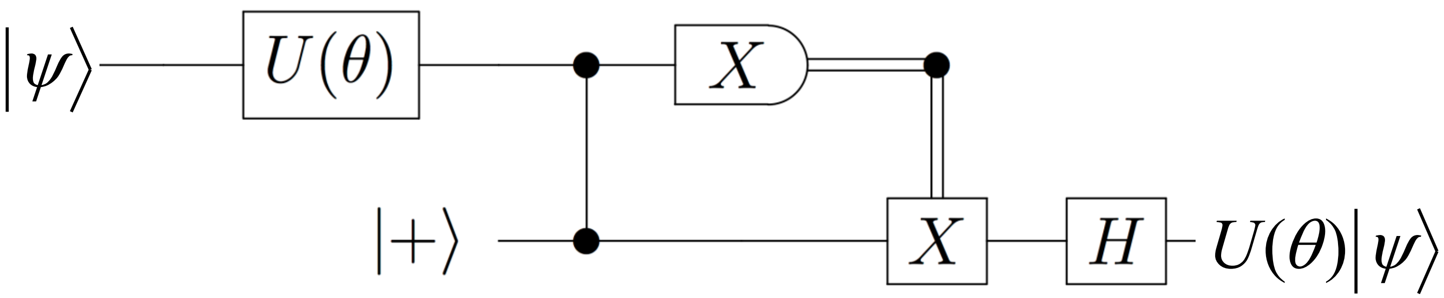


- U commutes with CZ

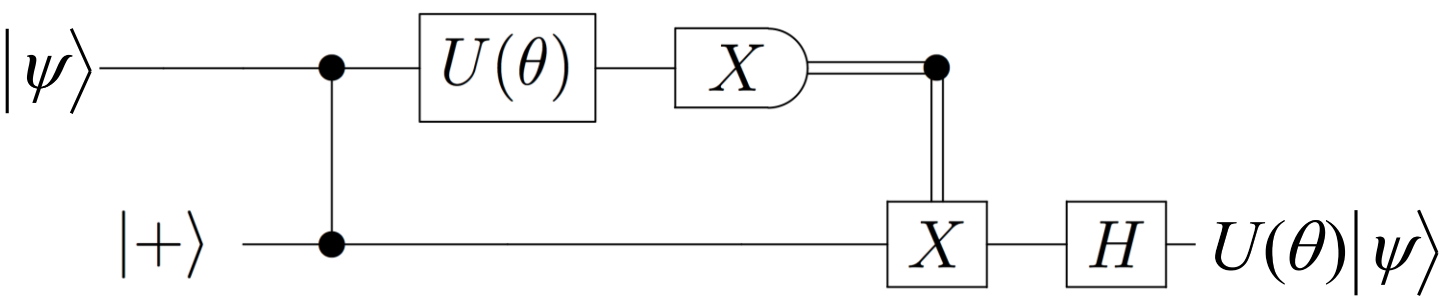


MBQC: step-by-step

Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$:

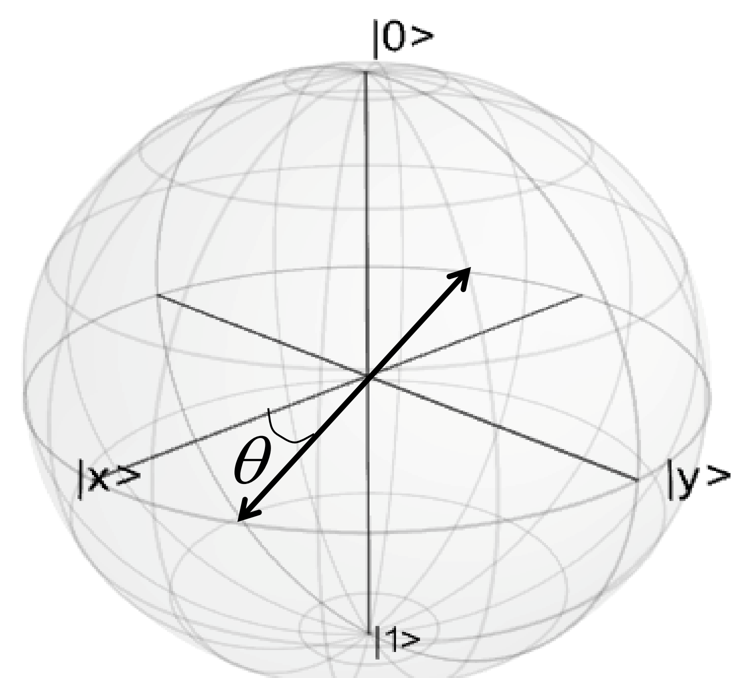


- U commutes with CZ



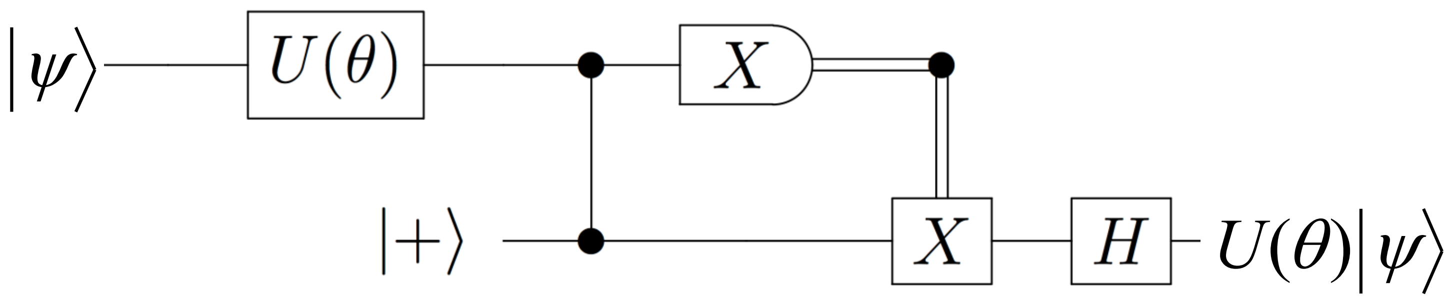
- U followed by X-measurement = measurement in *x-y* plane of Bloch sphere:

$$U^{+}XU = R(\theta) = \cos(\theta)X + \sin(\theta)Y$$

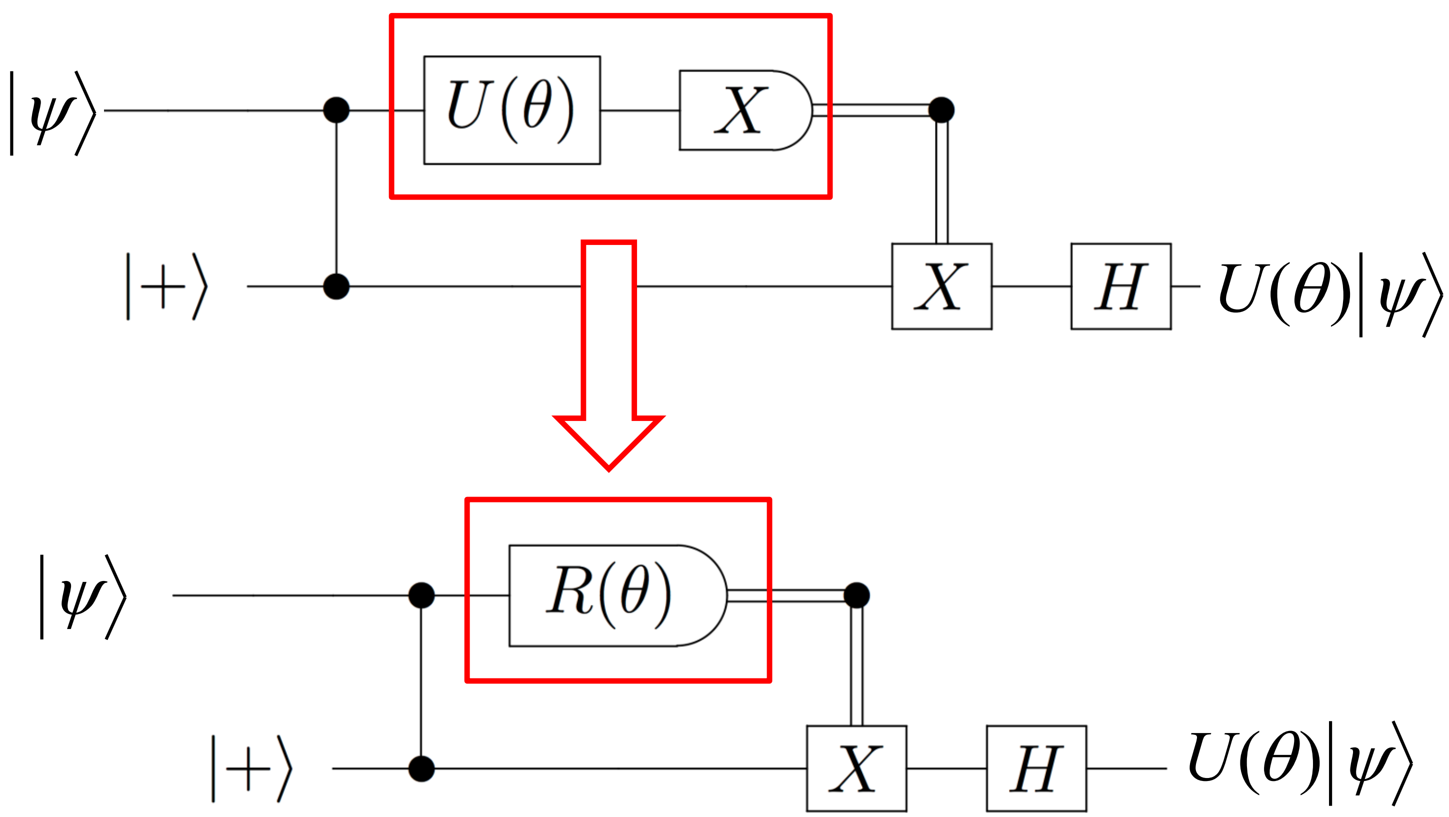


MBQC: step-by-step

Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$:

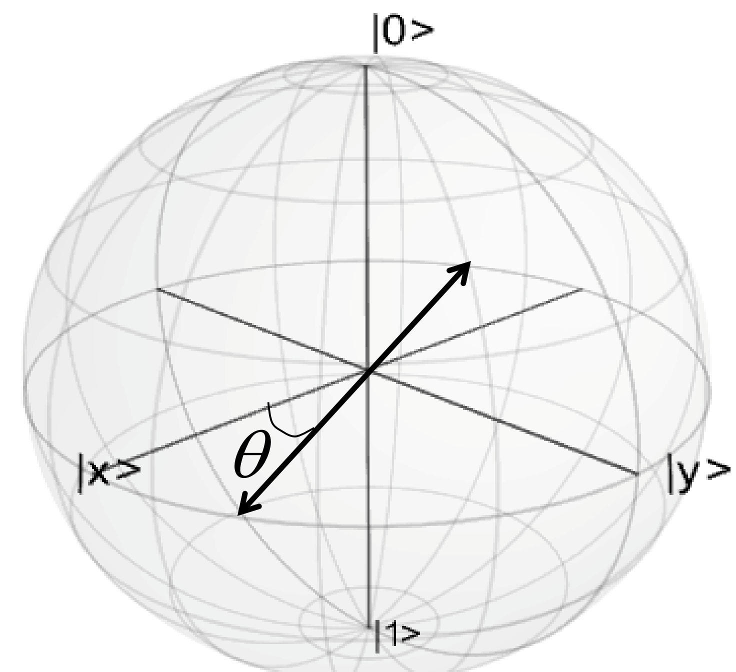


- U commutes with CZ



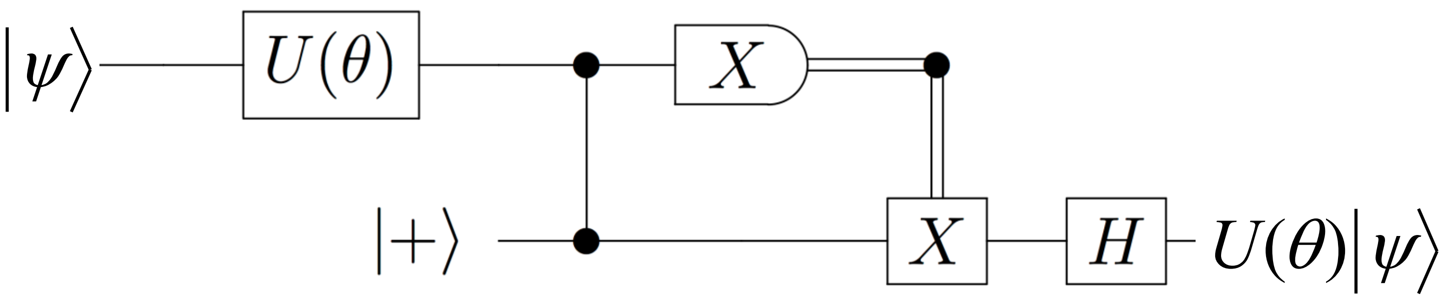
- U followed by X-measurement = measurement in *x*-*y* plane of Bloch sphere:

$$U^{+}XU = R(\theta) = \cos(\theta)X + \sin(\theta)Y$$

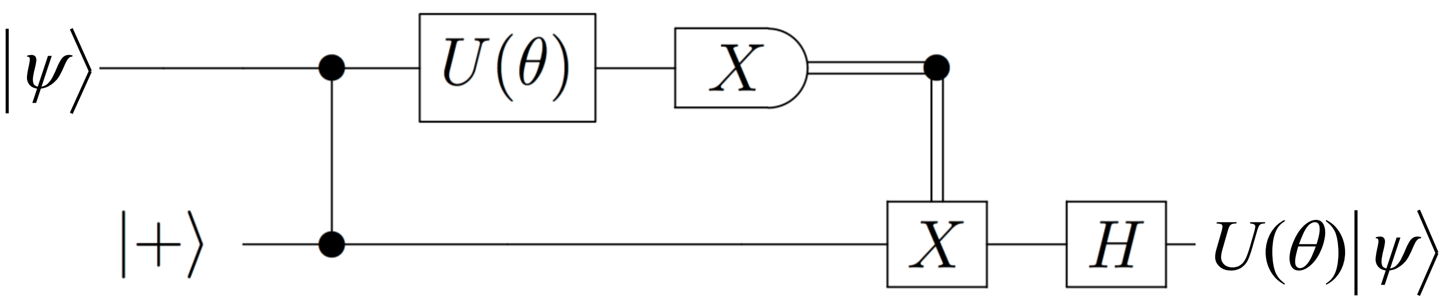


MBQC: step-by-step

Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$:

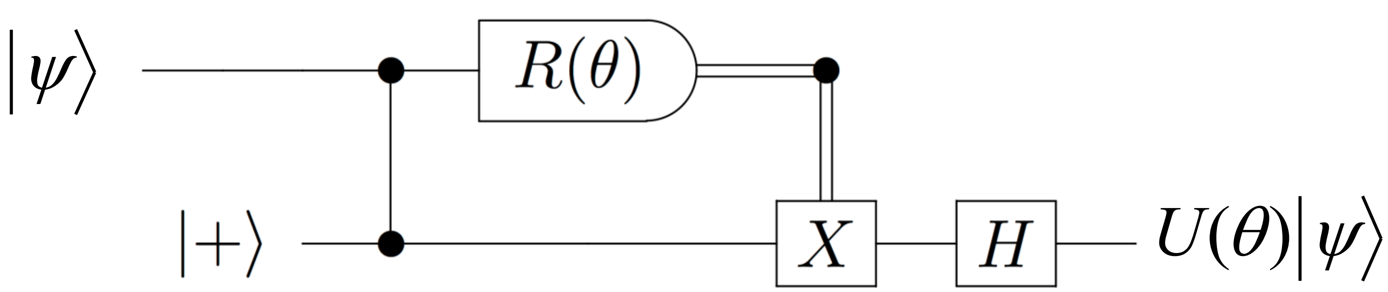


- U commutes with CZ



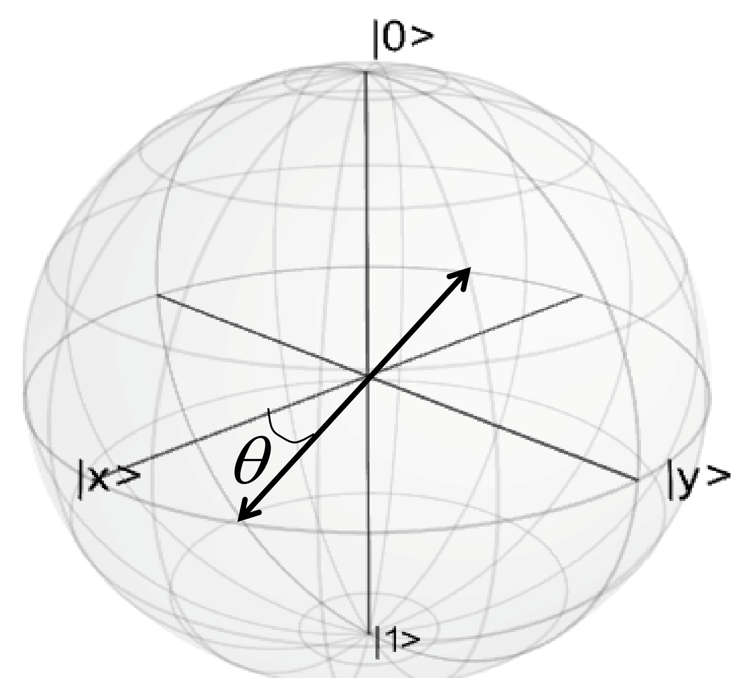
- U followed by X-measurement = measurement in *x-y* plane of Bloch sphere:

$$U^{+}XU = R(\theta) = \cos(\theta)X + \sin(\theta)Y$$



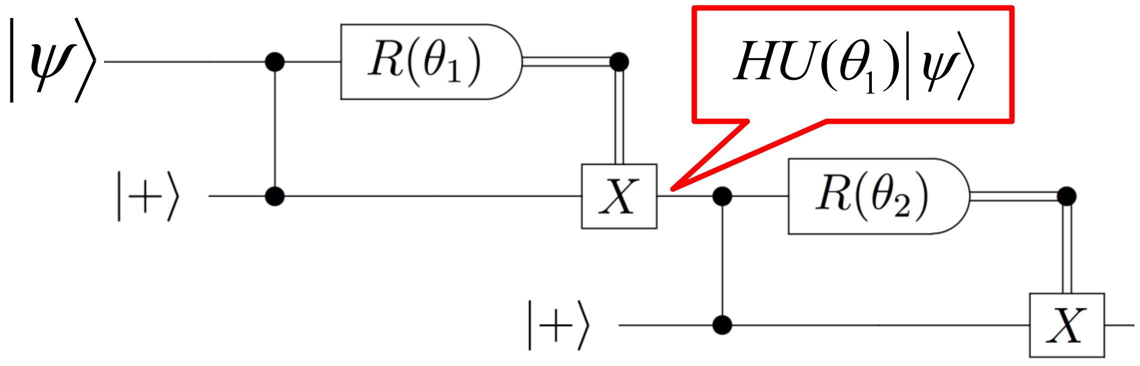
Evolved state $U(\theta)|\psi\rangle$ is teleported, via entanglement and right choice of measurement basis of top qubit

(*gate teleportation* idea of Gottesman and Chuang)



MBQC: step-by-step

Now two different unitaries in sequence:

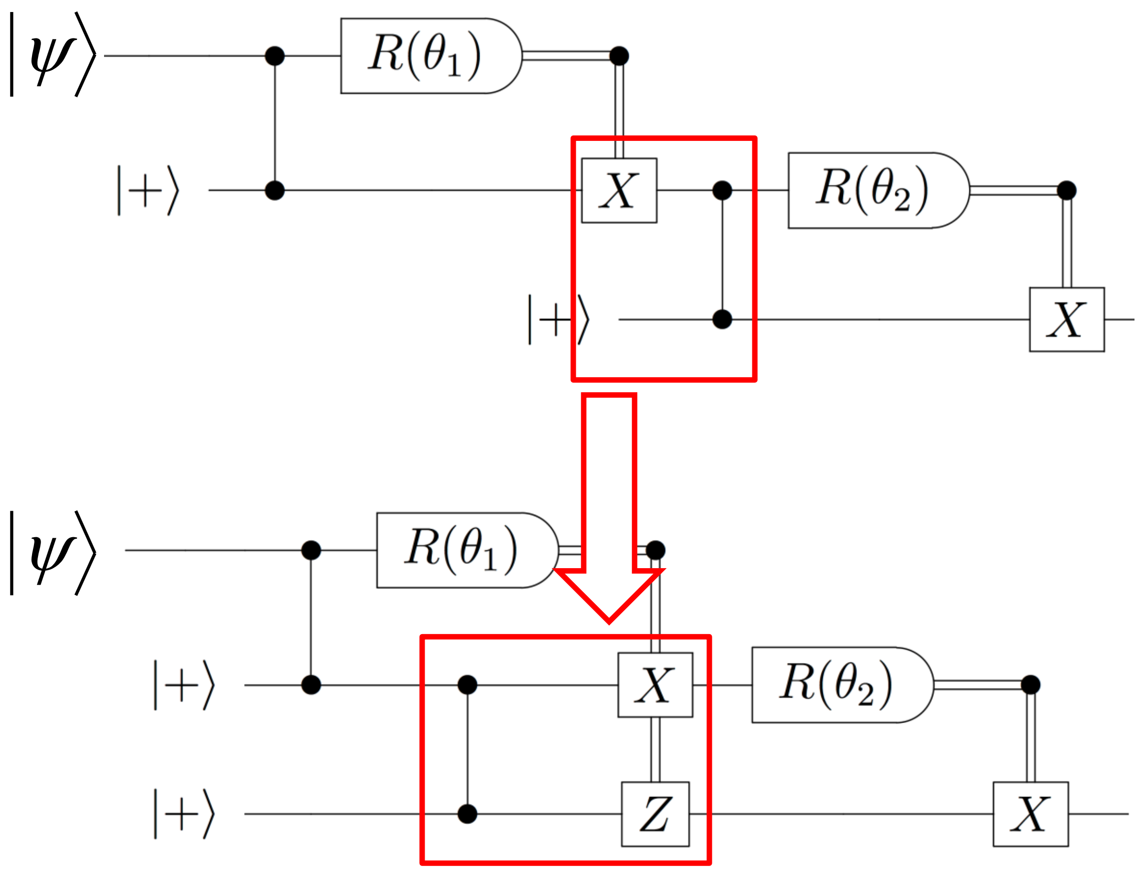


- Two gate teleportations, without final H gates, result in final state

$$HU(\theta_2)HU(\theta_1)|\psi\rangle$$

MBQC: step-by-step

Now two different unitaries in sequence:



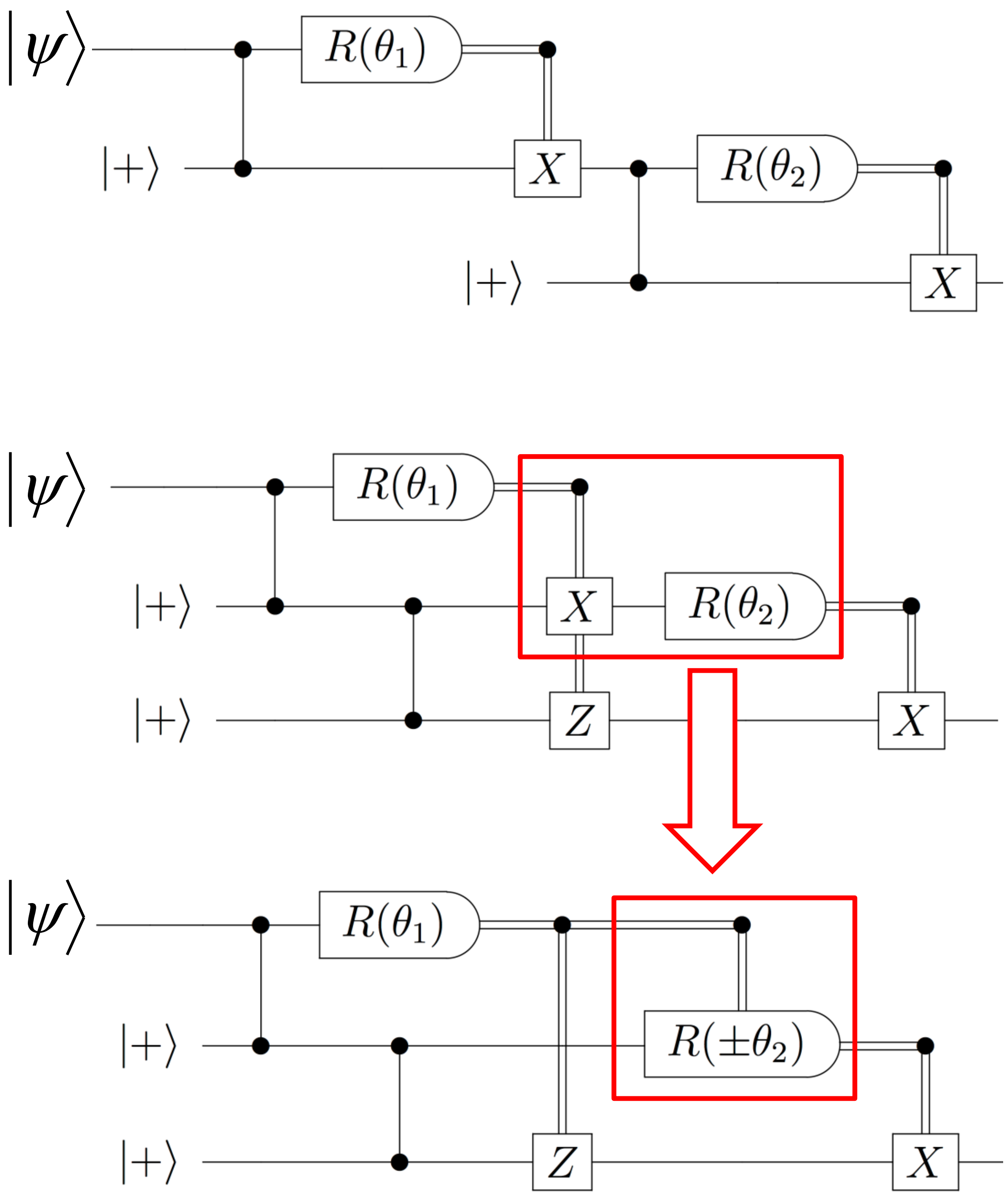
- Two gate teleportations, without final H gates, result in final state

$$HU(\theta_2)HU(\theta_1)|\psi\rangle$$

- Now commute X and CZ, which requires adding Z gate controlled by measurement 1

MBQC: step-by-step

Now two different unitaries in sequence:



- Two gate teleportations, without final H gates, result in final state

$$HU(\theta_2)HU(\theta_1)|\psi\rangle$$

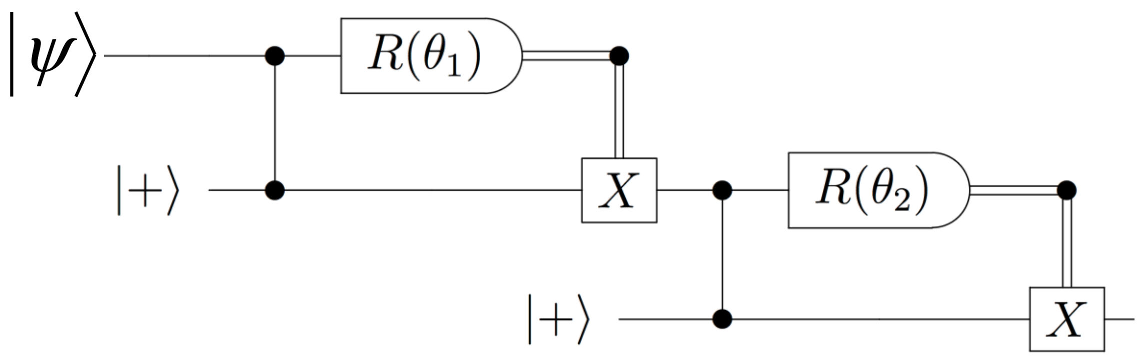
- Now commute X and CZ, which requires adding Z gate controlled by measurement 1

- Incorporate X correction into measurement angle of 2. When X is applied because:

$$\theta_2 \rightarrow -\theta_2 \quad XR(\theta)X = R(-\theta)$$

MBQC: step-by-step

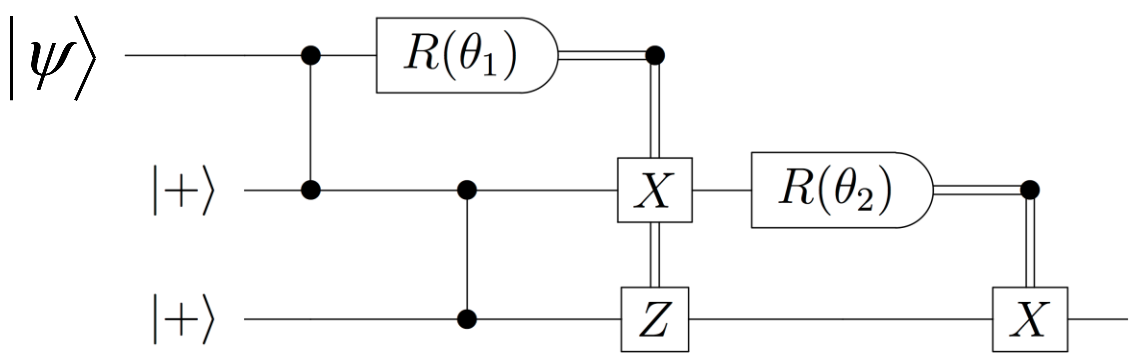
Now two different unitaries in sequence:



- Two gate teleportations, without final H gates, result in final state

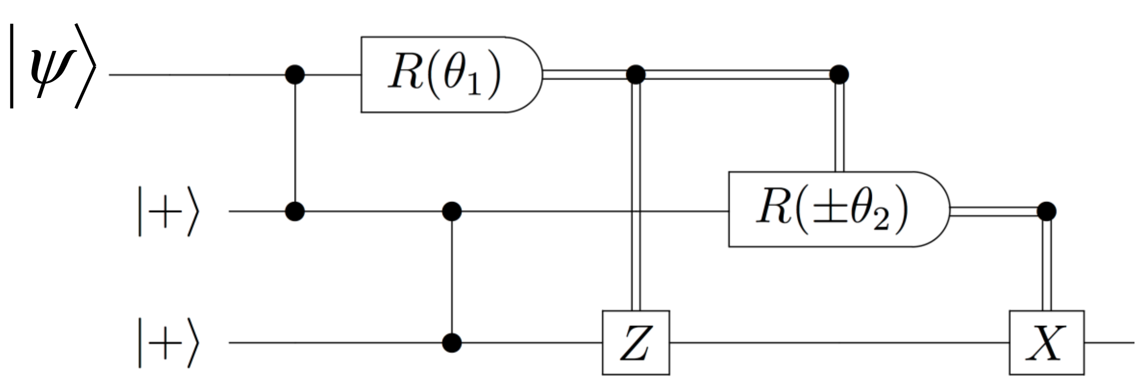
$$HU(\theta_2)HU(\theta_1)|\psi\rangle$$

- Now commute X and CZ, which requires adding Z gate controlled by measurement 1



- Incorporate X correction into measurement angle of 2. When X is applied because:

$$\theta_2 \rightarrow -\theta_2 \qquad XR(\theta)X = R(-\theta)$$



- By adapting measurement 2 according to outcome of 1, we can apply

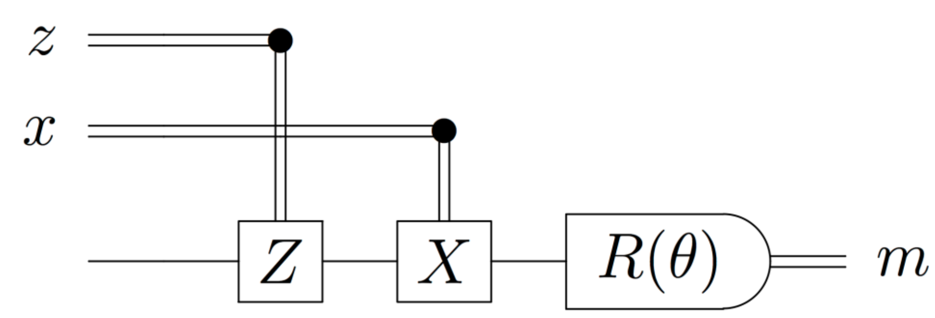
$$HU(\theta_2)HU(\theta_1)|\psi\rangle$$

- Easy to extend to multiple single-qubit unitaries, and $\{HU(\theta)\}$ is universal set for 1 qubit

Adaptivity allows for any single-qubit unitary to be implemented in the one-way model
CZ gates can be implemented similarly, propagation to beginning induces extra corrections

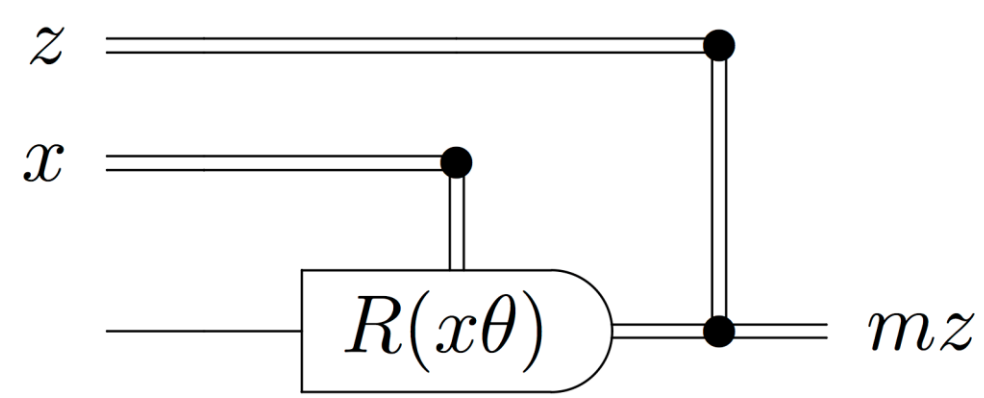
MBQC: step-by-step

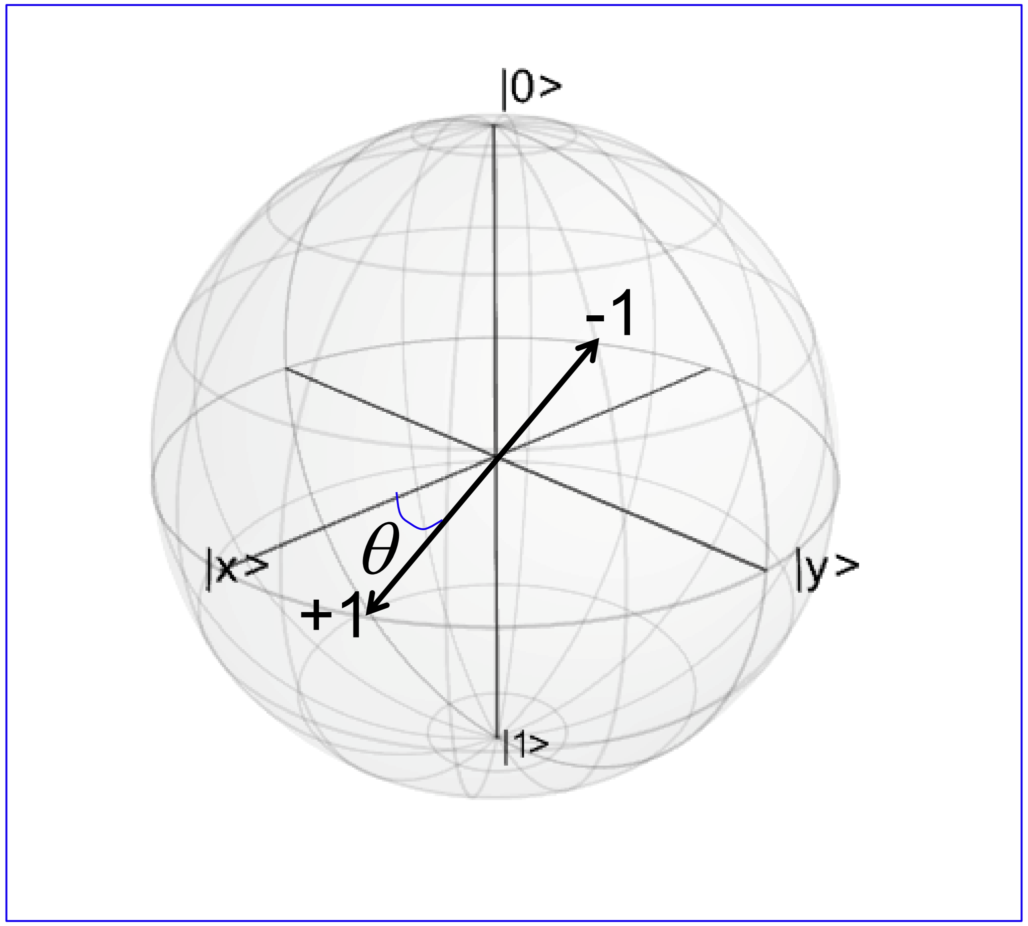
- How do corrections affect future measurements? We can have both X and Z corrections:
  Outcomes of previous measurements:
  $$z, x \in \{-1, 1\}$$



- As $XR(\theta)X = R(-\theta)$, X corrections turn $\theta \rightarrow -\theta$

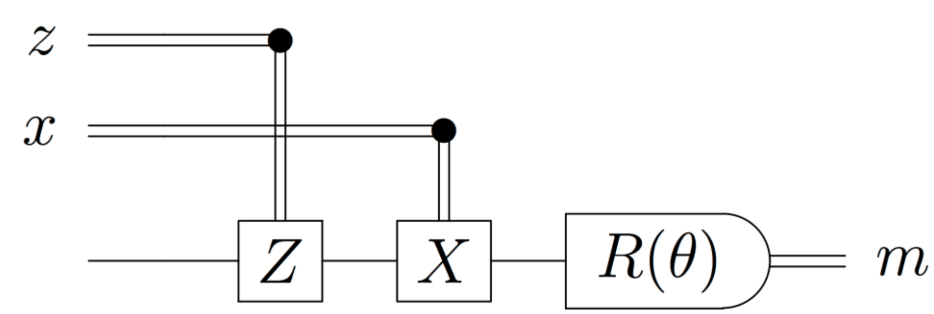
- As $ZR(\theta)Z = -R(\theta)$, Z corrections invert the output





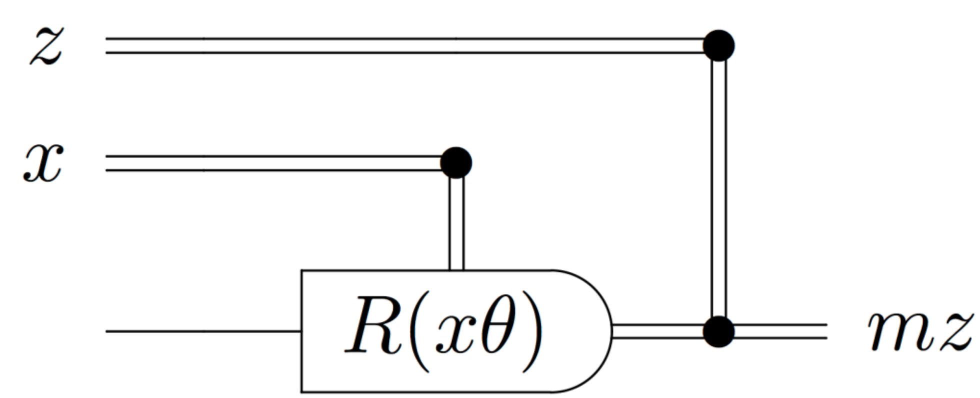
MBQC: step-by-step

- How do corrections affect future measurements? We can have both X and Z corrections:
  Outcomes of previous measurements:
  $$z, x \in \{-1, 1\}$$

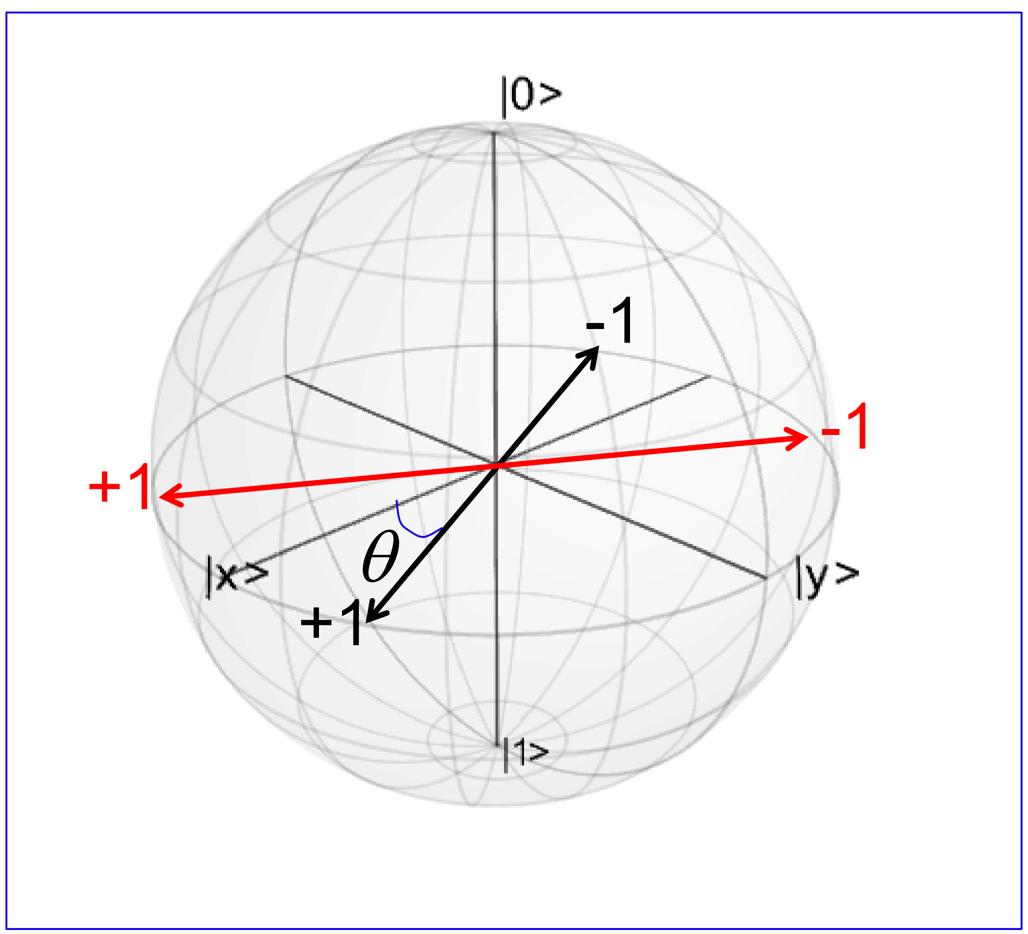


- As $XR(\theta)X = R(-\theta)$, X corrections turn $\theta \to -\theta$

- As $ZR(\theta)Z = -R(\theta)$, Z corrections invert the output



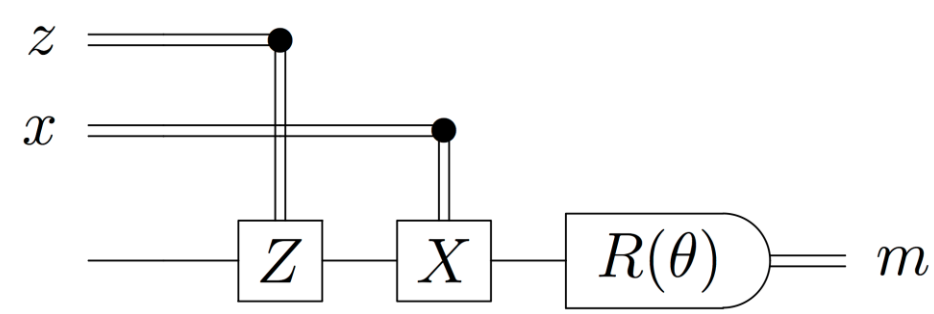
X correction



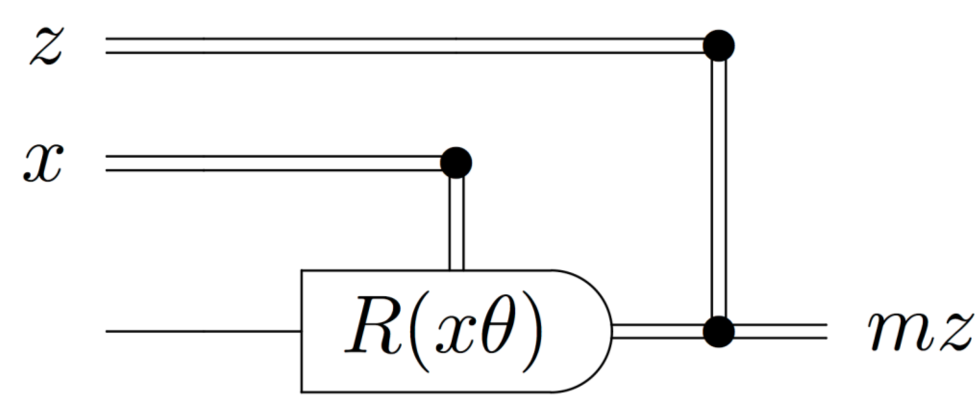
MBQC: step-by-step

- How do corrections affect future measurements? We can have both X and Z corrections:
  Outcomes of previous measurements:

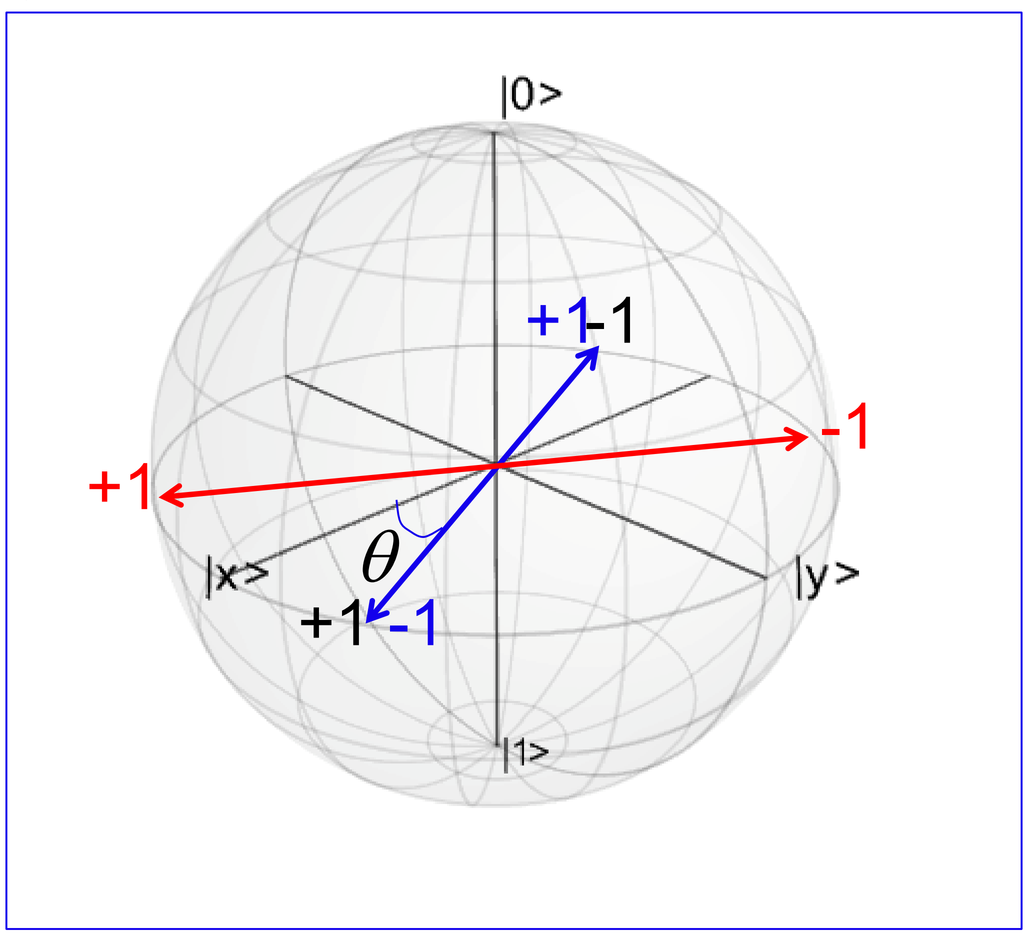
$$z, x \in \{-1,1\}$$



- As $XR(\theta)X = R(-\theta)$, X corrections turn $\theta \rightarrow -\theta$
- As $ZR(\theta)Z = -R(\theta)$, Z corrections invert the output

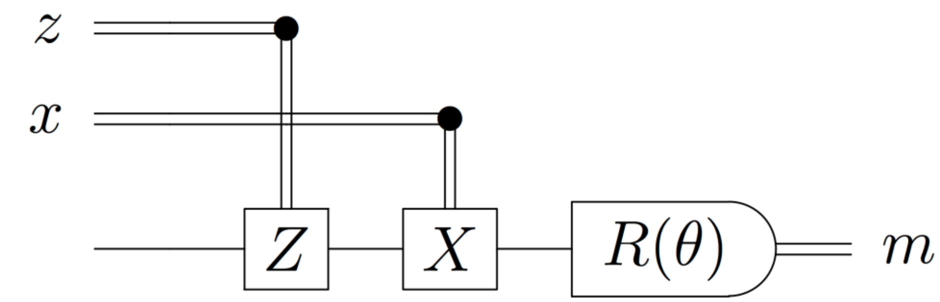


X correction
Z correction

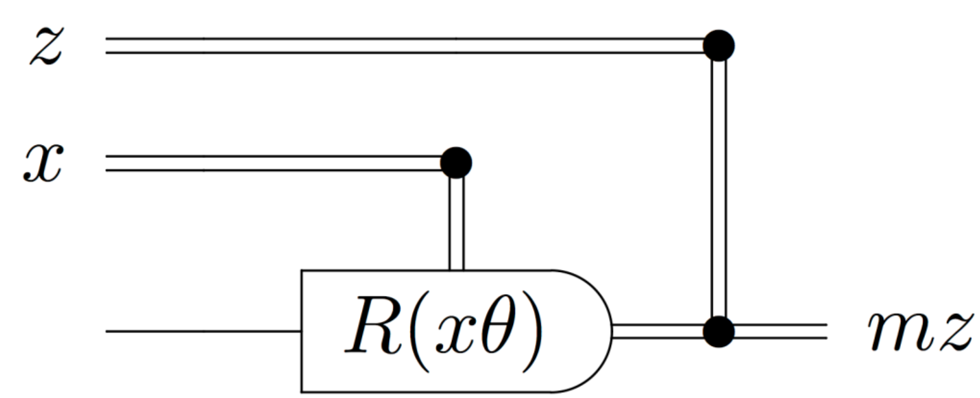


MBQC: step-by-step

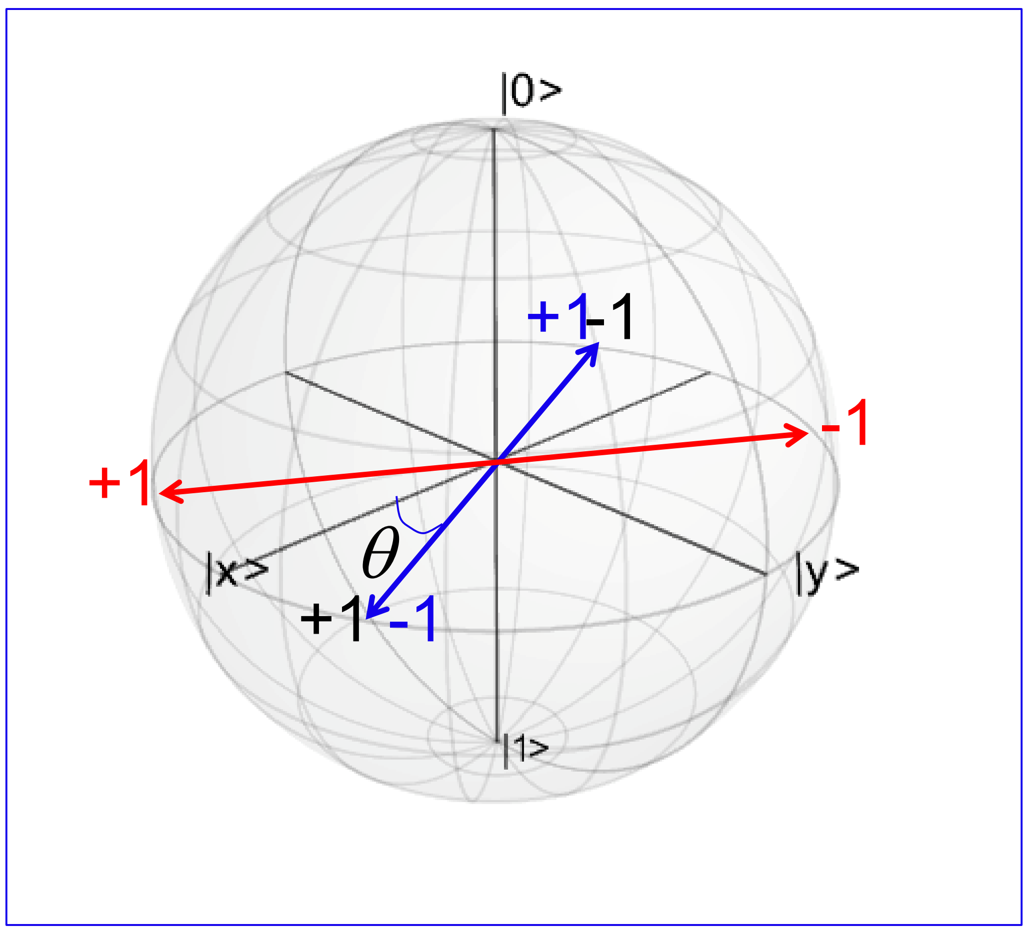
- How do corrections affect future measurements? We can have both X and Z corrections:
  Outcomes of previous measurements:
  $$z, x \in \{-1, 1\}$$



- As $XR(\theta)X = R(-\theta)$, X corrections turn $\theta \rightarrow -\theta$
- As $ZR(\theta)Z = -R(\theta)$, Z corrections invert the output



X correction
Z correction



Classical control computer needs only store&update **sum modulo 2** of X and Z corrections of each qubit

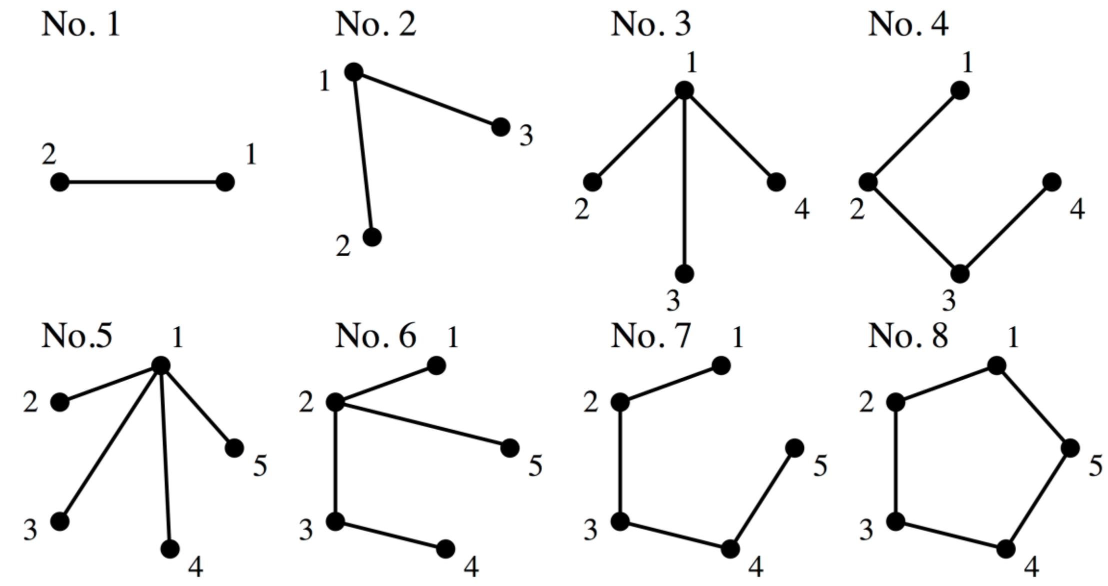
This **parity computer** is quite simple, but together with the quantum resource yields universal QC

Entanglement resources for MBQC

- **Graph states**: class of states obtainable by

  1. Initialization of a set of qubits in $|+\rangle$ states
  2. CZ gates between neighboring vertices in a graph

- Examples:



- No. 7 (5 qubits): sufficient for any single qubit unitary
- No. 3 (4 qubits): sufficient for CNOT

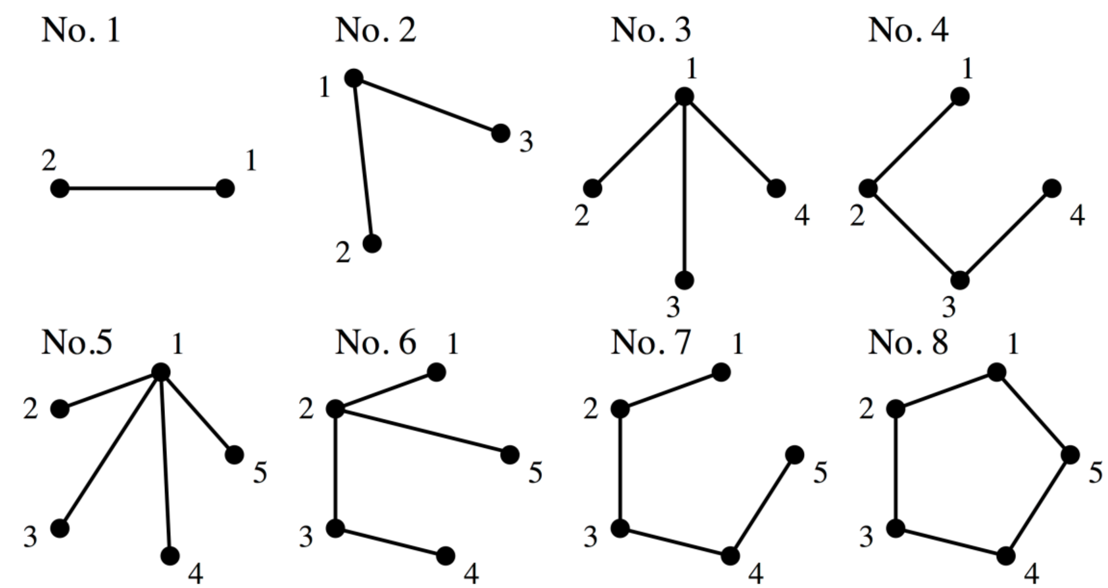
Entanglement resources for MBQC

- **Graph states**: class of states obtainable by

  1. Initialization of a set of qubits in $|+\rangle$ states
  2. CZ gates between neighboring vertices in a graph

- Examples:

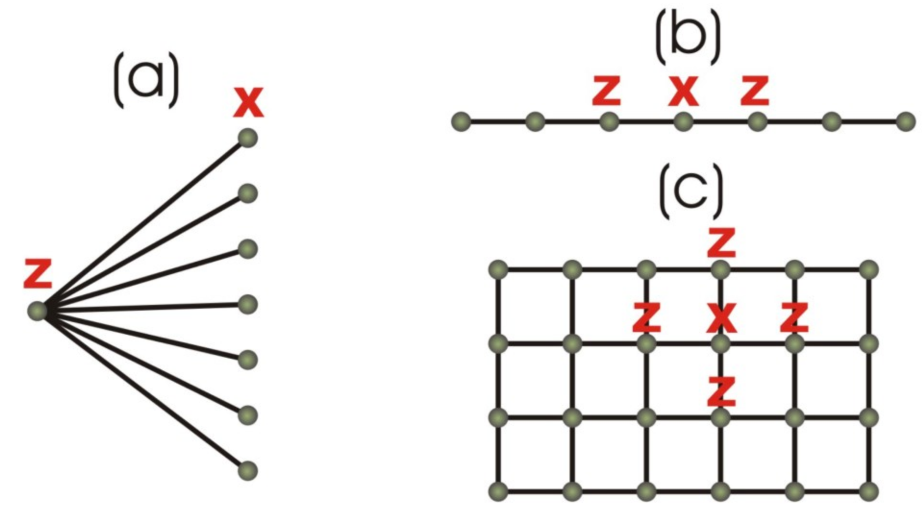
- No. 7 (5 qubits): sufficient for any single qubit unitary
- No. 3 (4 qubits): sufficient for CNOT



- Alternative characterization of graph states:

- Unique state which is simultaneous eigenstate (with eigenvalue 1) of set of operators

$$K_i = X_i \prod_{j \text{ neighbor of i}} Z_j$$

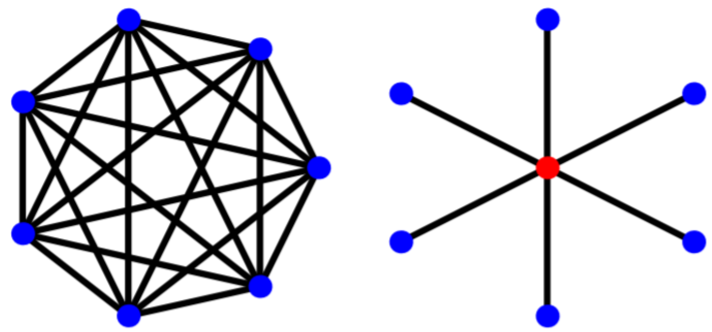


- Are there families of graph states which are universal for QC?

Entanglement resources for MBQC

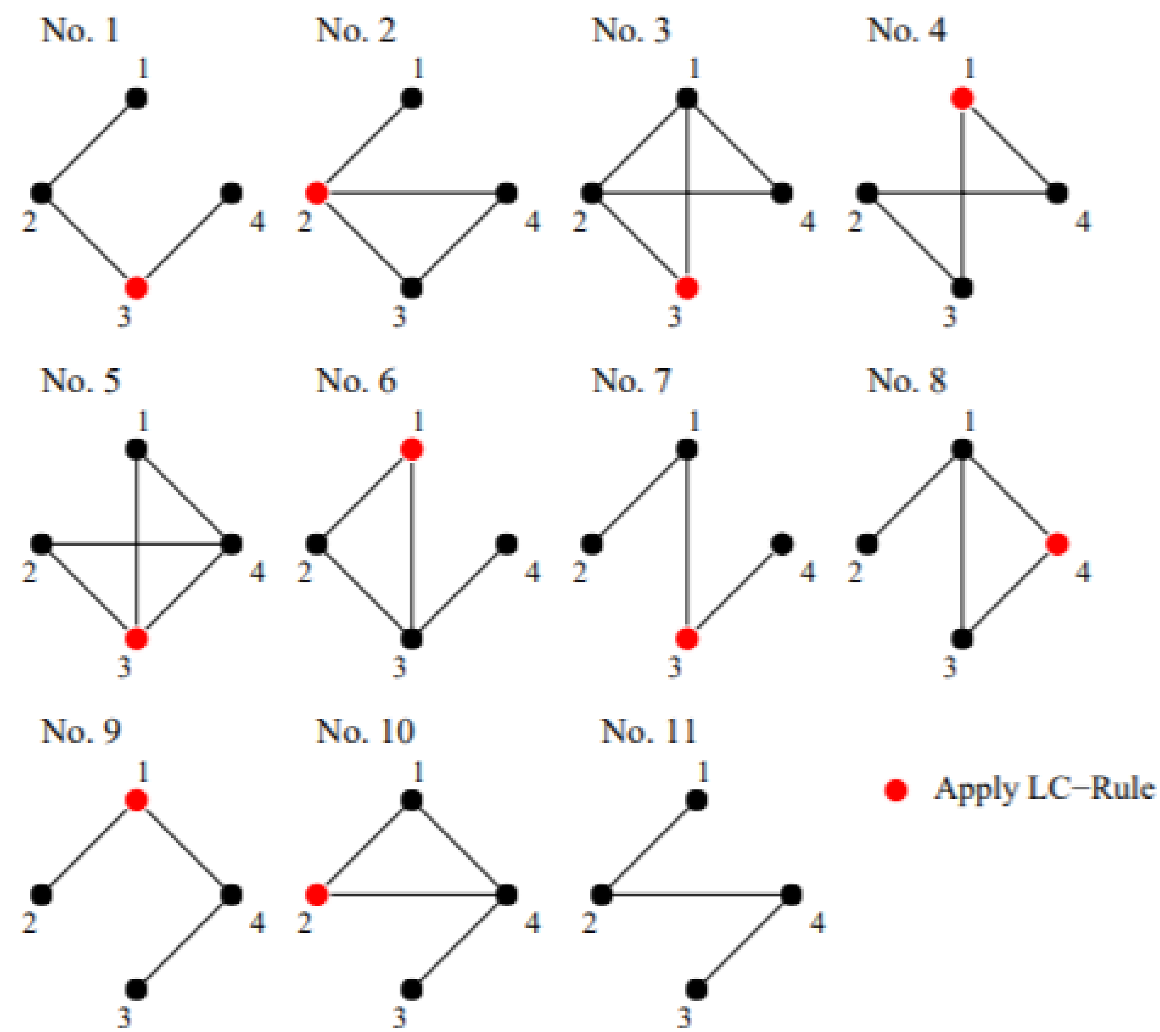
- **Graph states**: different graphs may be local-unitary equivalent.

Example: GHZ states



- **Local complementation:** local Clifford unitaries that map a given graph state to all its Clifford LU equivalent graph states

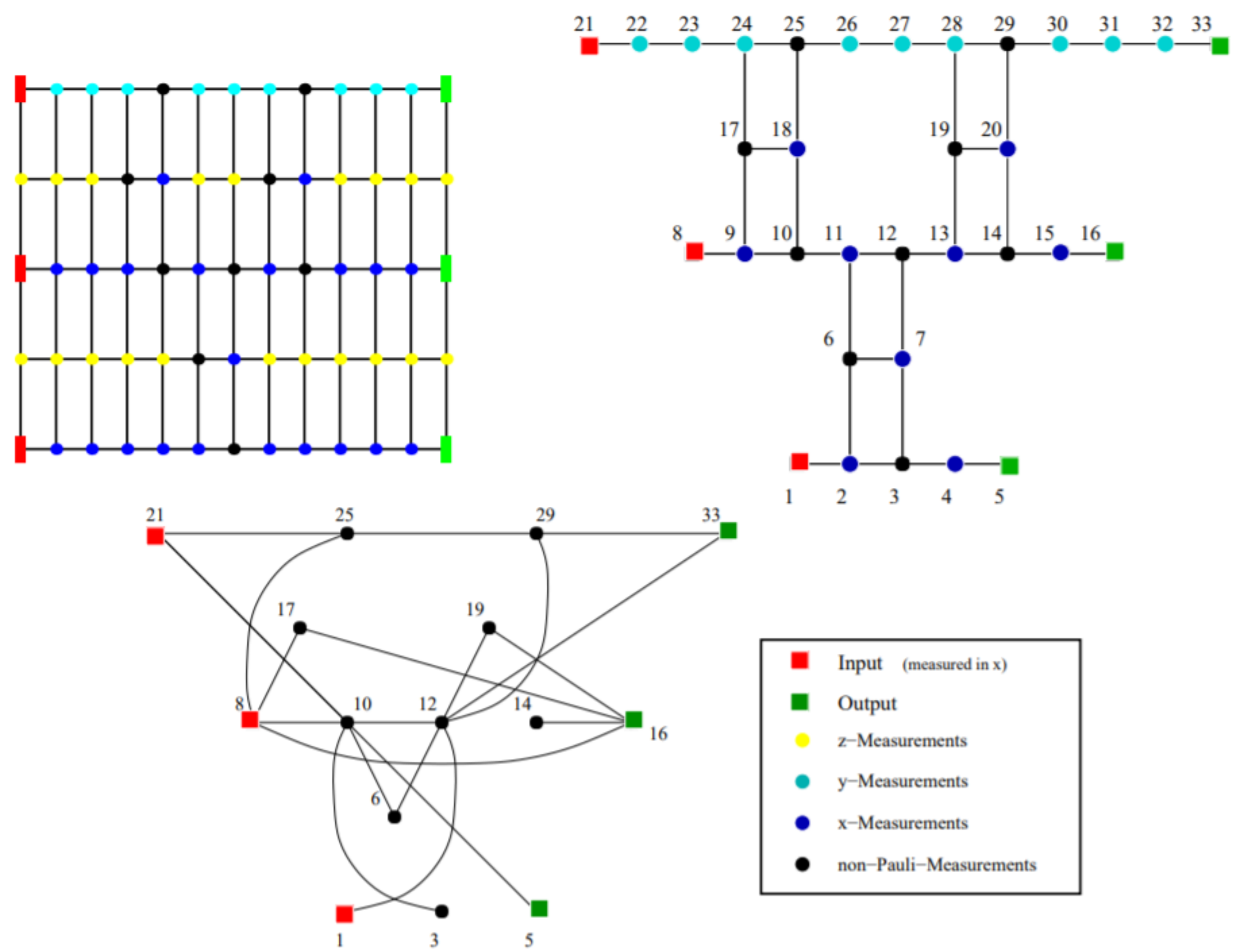
- Simple interpretation in terms of graph change: choose vertex, complement subgraph of neighbors



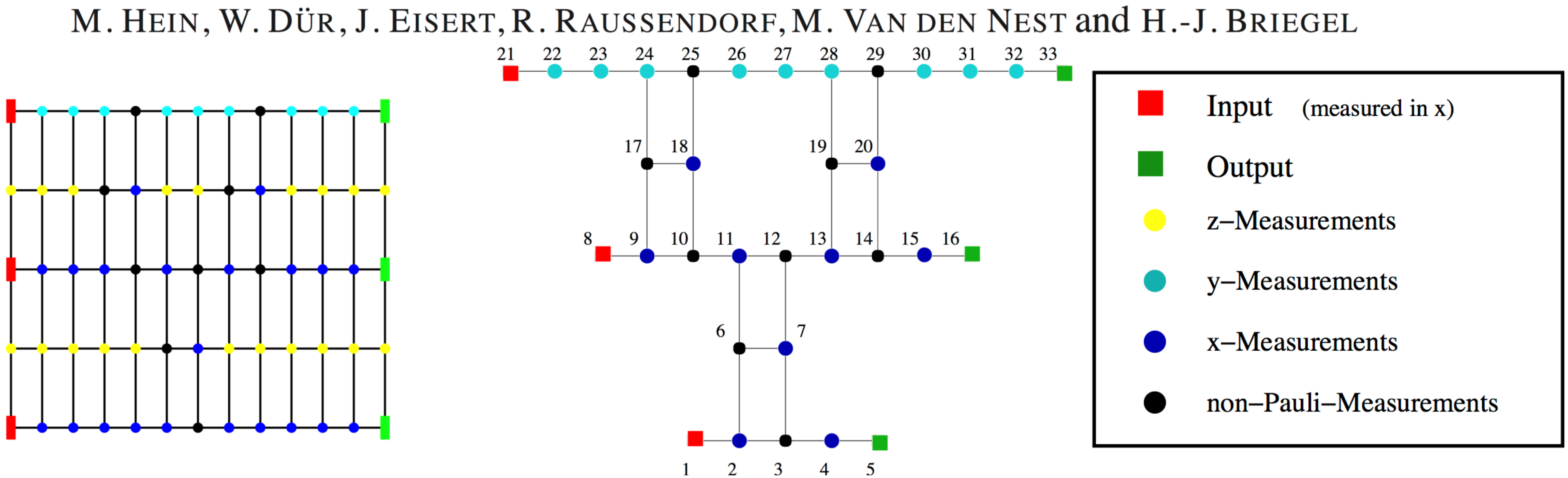
$$\text{No. } 1 \xrightarrow{3} \text{No. } 2 \xrightarrow{2} \text{No. } 3 \xrightarrow{3}$$
$$\text{No. } 4 \xrightarrow{1} \text{No. } 5 \xrightarrow{3} \text{No. } 6 \xrightarrow{1}$$
$$\text{No. } 7 \xrightarrow{3} \text{No. } 8 \xrightarrow{4} \text{No. } 9 \xrightarrow{1}$$
$$\text{No. } 10 \xrightarrow{2} \text{No. } 11$$

Entanglement resources for MBQC

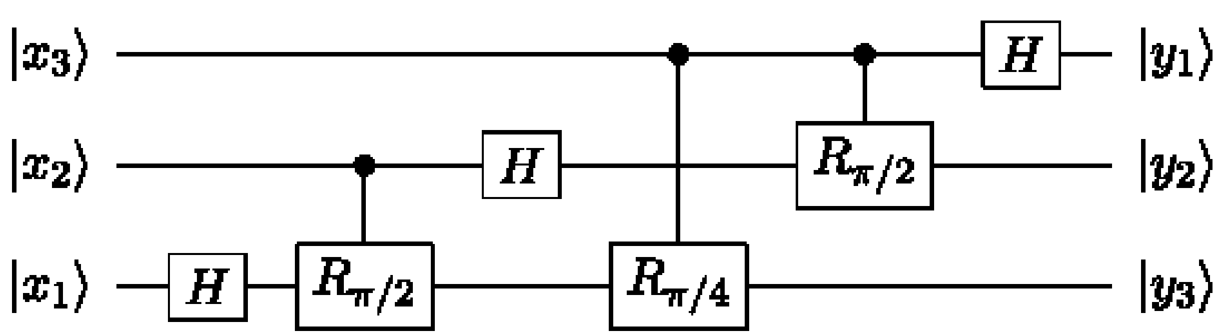
- **Stabilizer measurements** take graph states to graph states:



Entanglement resources for MBQC



from: Proc. Int. School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos", Varenna, Italy (2005)

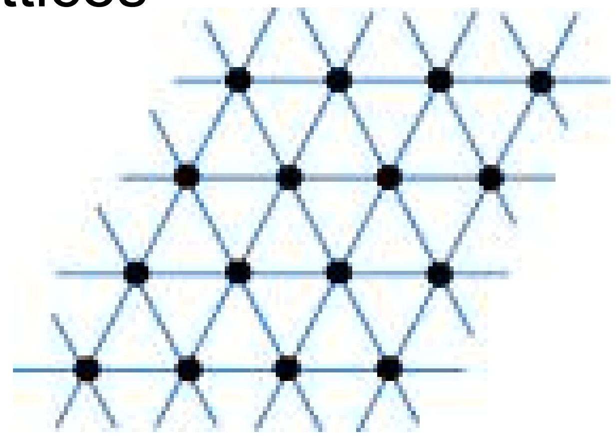


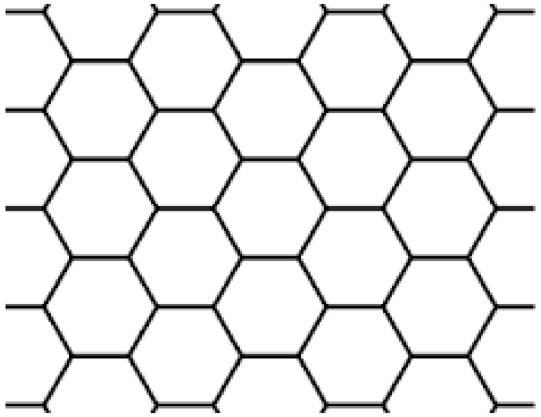
3-qubit QFT

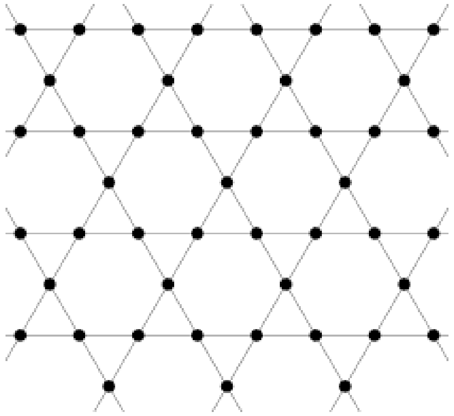
- Example of universal graph: 2D square lattice (called **cluster state**)
  - Above: MBQC implementation of 3-qubit discrete Fourier Transform
  - “Unwanted” vertices deleted by Z-measurements; resulting corrections must be taken into account

Entanglement resources for MBQC

- Some known universal resources for MBQC: 2D triangular, hexagonal, Kagome lattices







  - These resources are "universal state preparators" = strong notion of universality

- Other resource states enable simulation of classical measurement statistics of any universal quantum computer = weaker notion of universality
  - Some of these require a universal classical computer (instead of a parity computer)

[Gross *et al.*, PRA 76, 052315 (2007)]

- Universality also for ground state of 2D Affleck-Kennedy-Lieb-Tasaki (AKLT) model

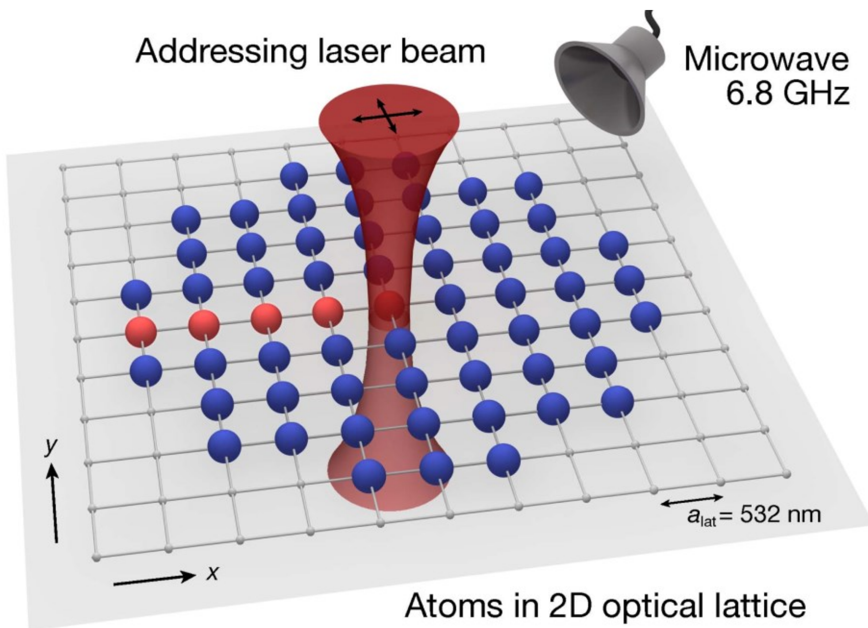
[Wei, Affleck, Raussendorf PRL 106, 070501 (2011)]

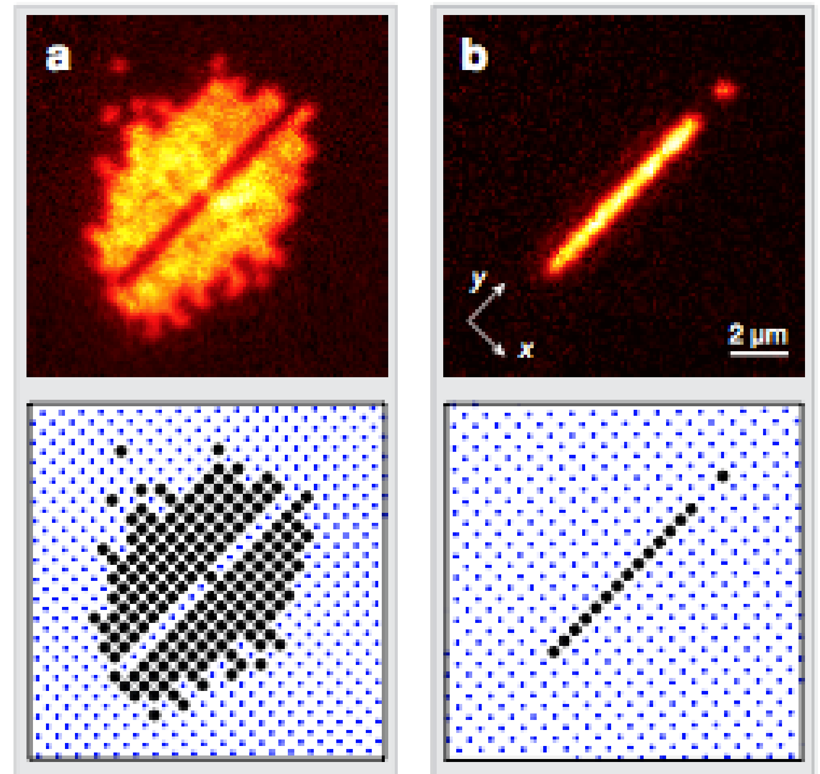
- MBQC on some resource states is known to be simulable, e.g. on 1D chain

[Markov, Shi, SIAM J. Comput. 38, 963 (2008)]

MBQC - implementations

- Optical lattices – counter-propagating laser beams trap cold neutral atoms
    - Challenge: single-site addressing

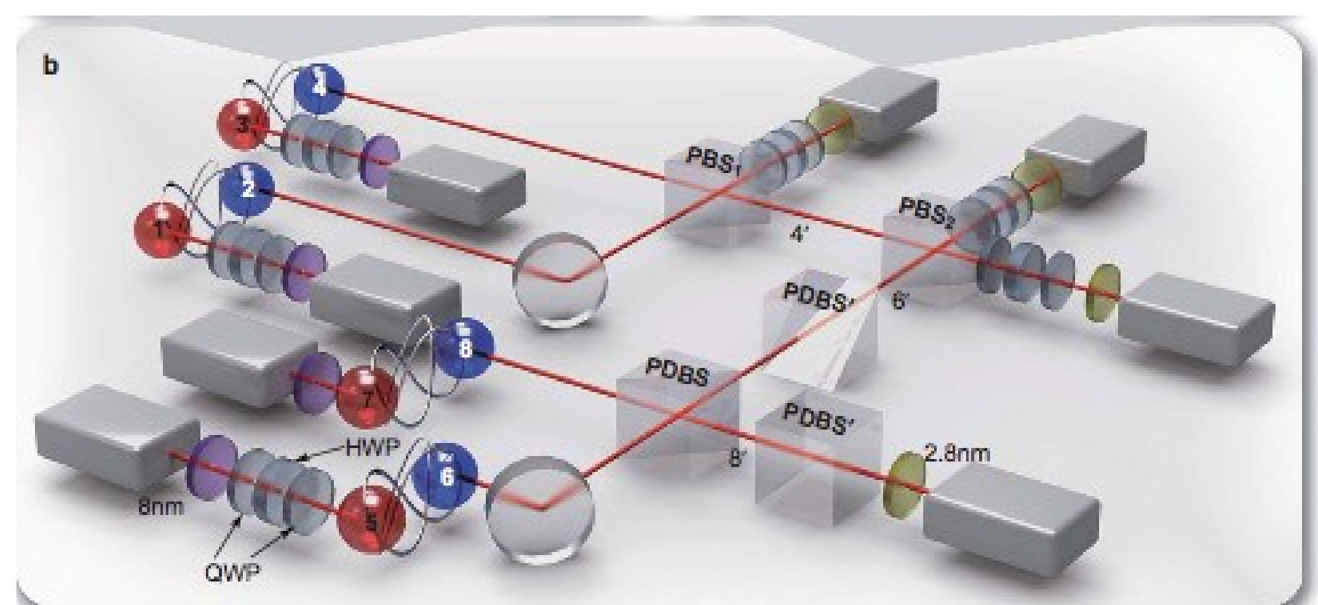




from: Weintenberg et al., *Nature* 471, 319 (2011)

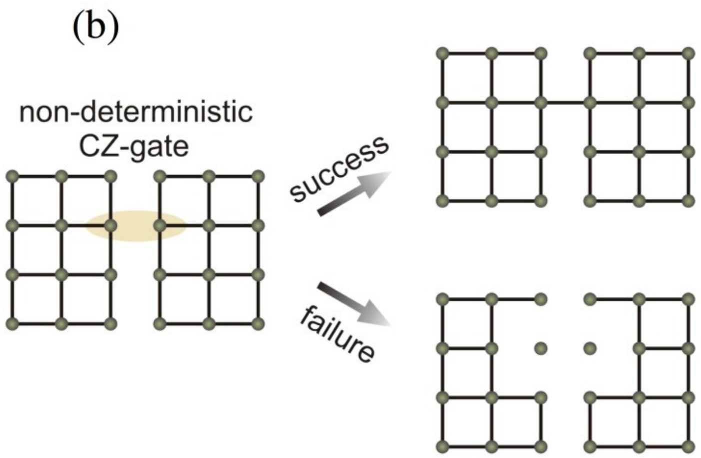
- Proof-of-principle implementations using photons
    - Topological error-correction using eight-photon cluster states

from: Yao et al., *Nature* 482, 489 (2012)

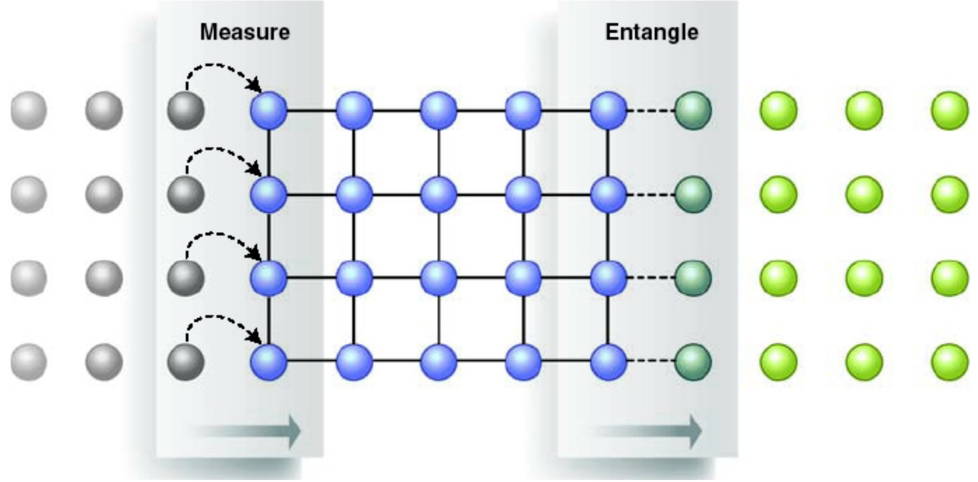


MBQC - implementations

- Using one-way model to advantage: building large resource states from probabilistic operations; at once or on the go



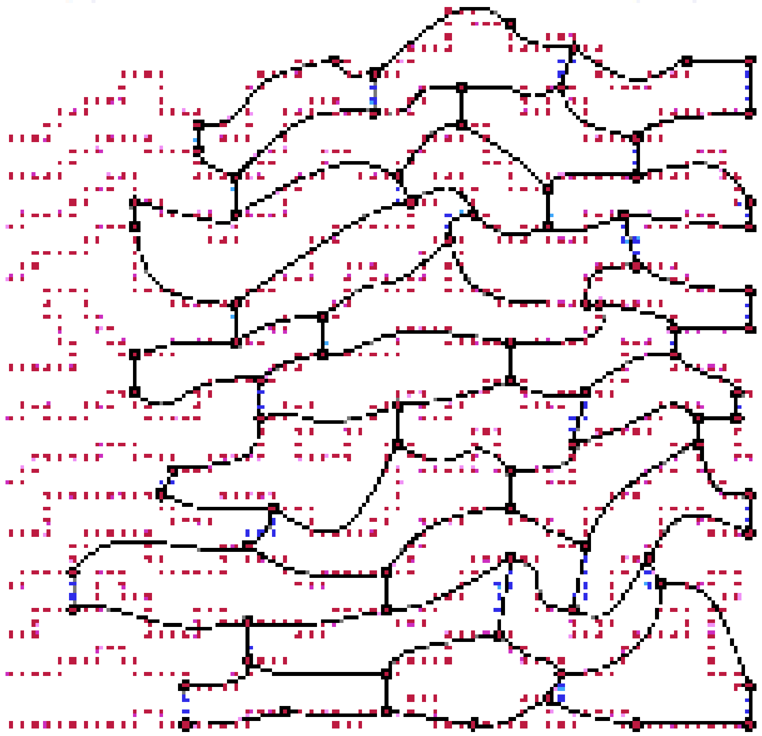
from: Briegel *et al., Nat. Phys.* 5 (1), 19 (2009)



from: O'Brien, Science 318, 1467 (2007)

- Schemes for adapting imperfect clusters for MBQC

(a) initial faulty square lattice

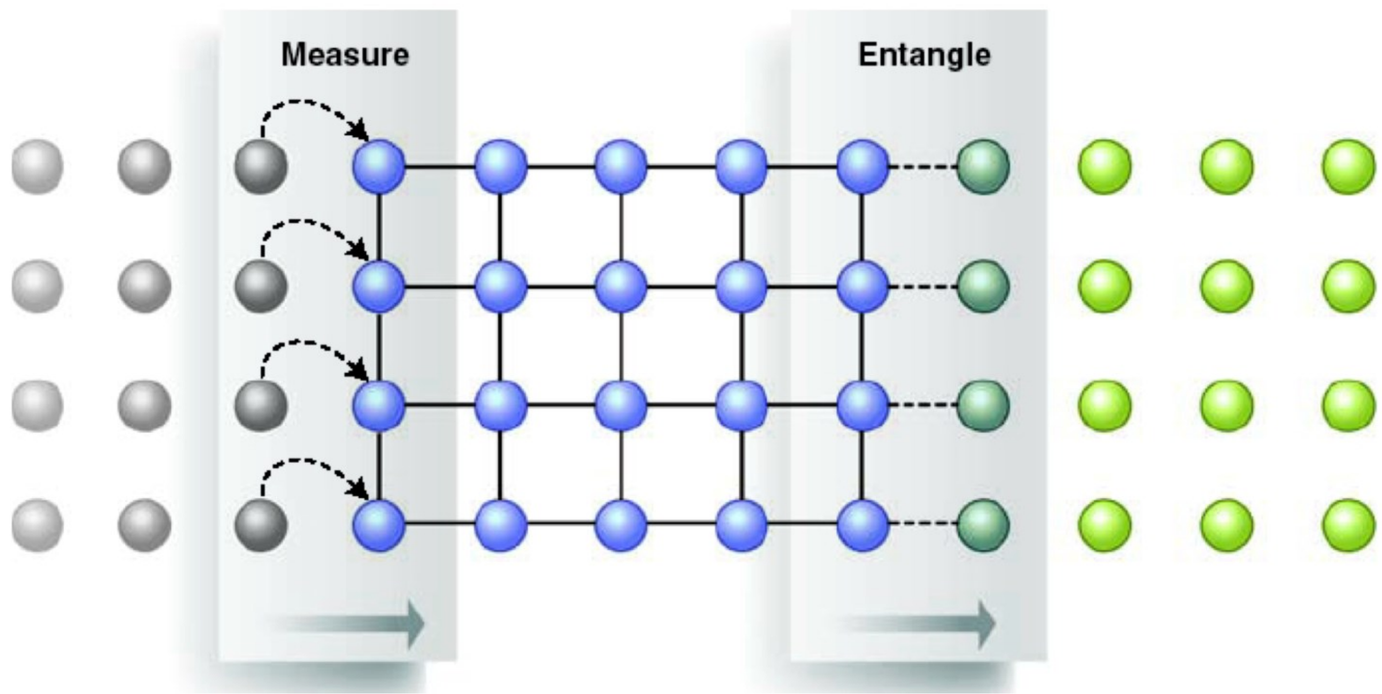


(f) deletion and contraction (Q.1 & Q.2)

from: Browne *et al., New J. Phys.* 10, 023010 (2008)

Universal QC with measurement-based quantum computation

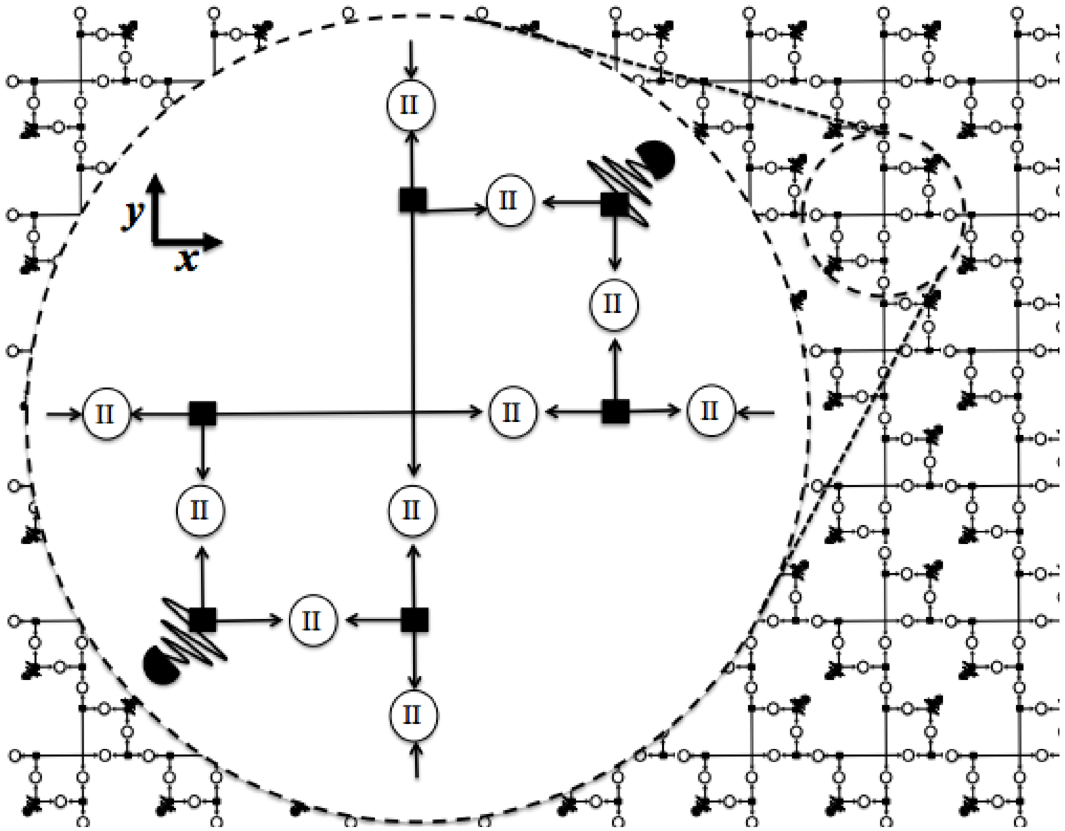
- Measurement-based quantum computation (MBQC) relies only on
  - entangling gates;
  - adaptive single-qubit measurements.
- Teleportation-based gates – states are teleported (and transformed) step by step

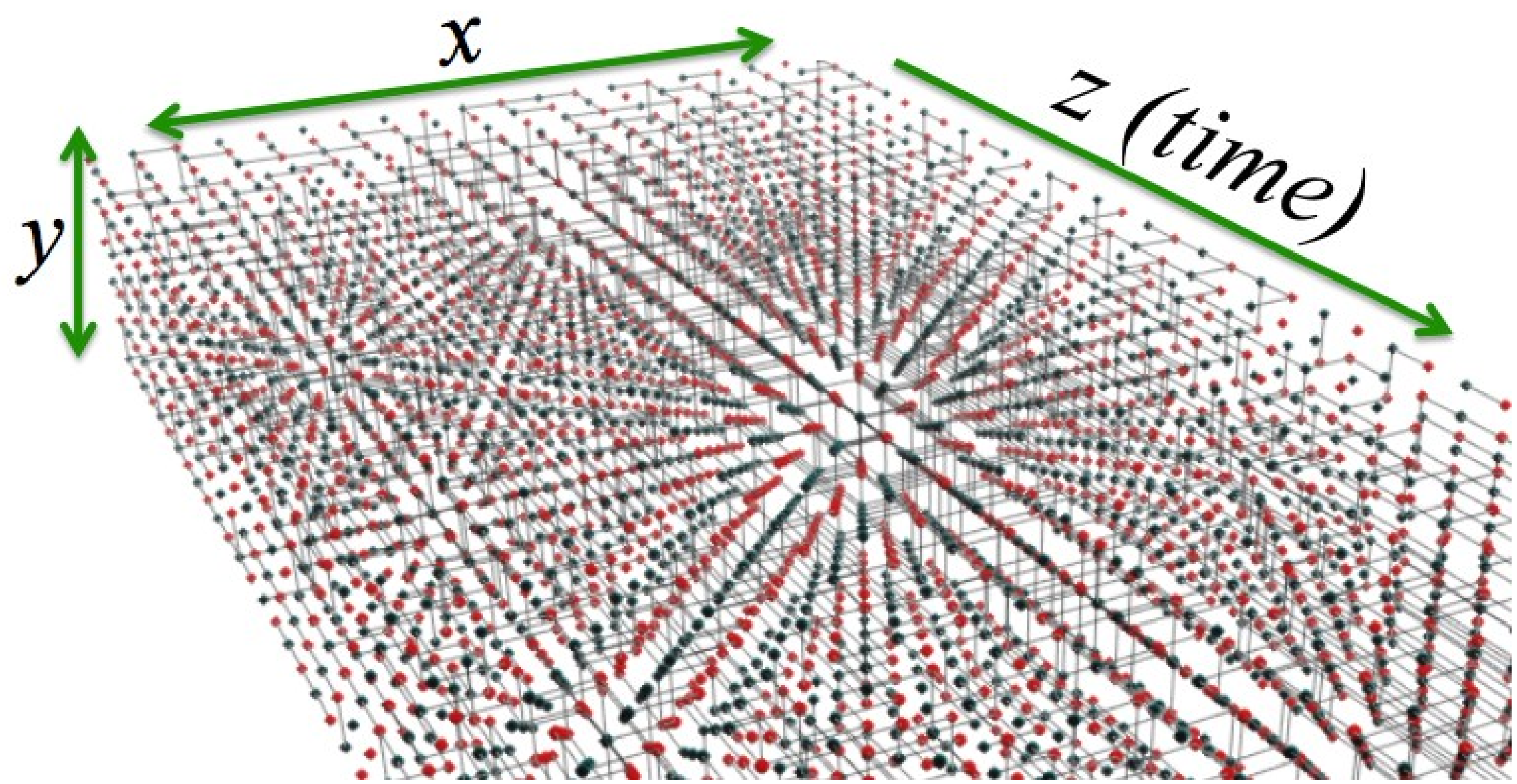


from: O'Brien, *Science* 318, 1467 (2007)

- MBQC is uniquely suited to photonic quantum computation:
  - Photons fly away fast…
  - …so they are stored for short times, measured, and information teleported to fresh photons.
- Approach being pursued by US company PsiQuantum (> 3 billion US$ valuation)

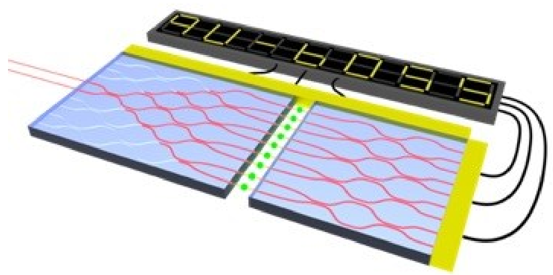
Universal QC with measurement-based quantum computation





- MBQC using 3-photon GHZ-state sources on-chip: [Rudolph, arXiv:160708535]
  - (2+1)-dimensional architecture
  - probabilistic entangling gates sufficient, if above percolation threshold (essential use of error correction)
  - adaptive single-qubit measurements (delay lines)
- Key advantages: room-temperature chips (small cryo units for e.g. detectors), compatible with major chip foundry techniques, i.e. potentially scalable

INL in 2 EC-funded projects on photonic quantum computation



ERC Advanced Grant QU-BOSS ("Quantum advantage via non-linear Boson Sampling") 2020-2025

- PI: Fabio Sciarrino (Univ. of Rome, La Sapienza)
- Partners: Istituto de Fotonica e Nanotecnologie (IFN-CNR – Milan), INL

H2020 FETOPEN PHOQUSING ("Photonic Quantum Sampling Machine")

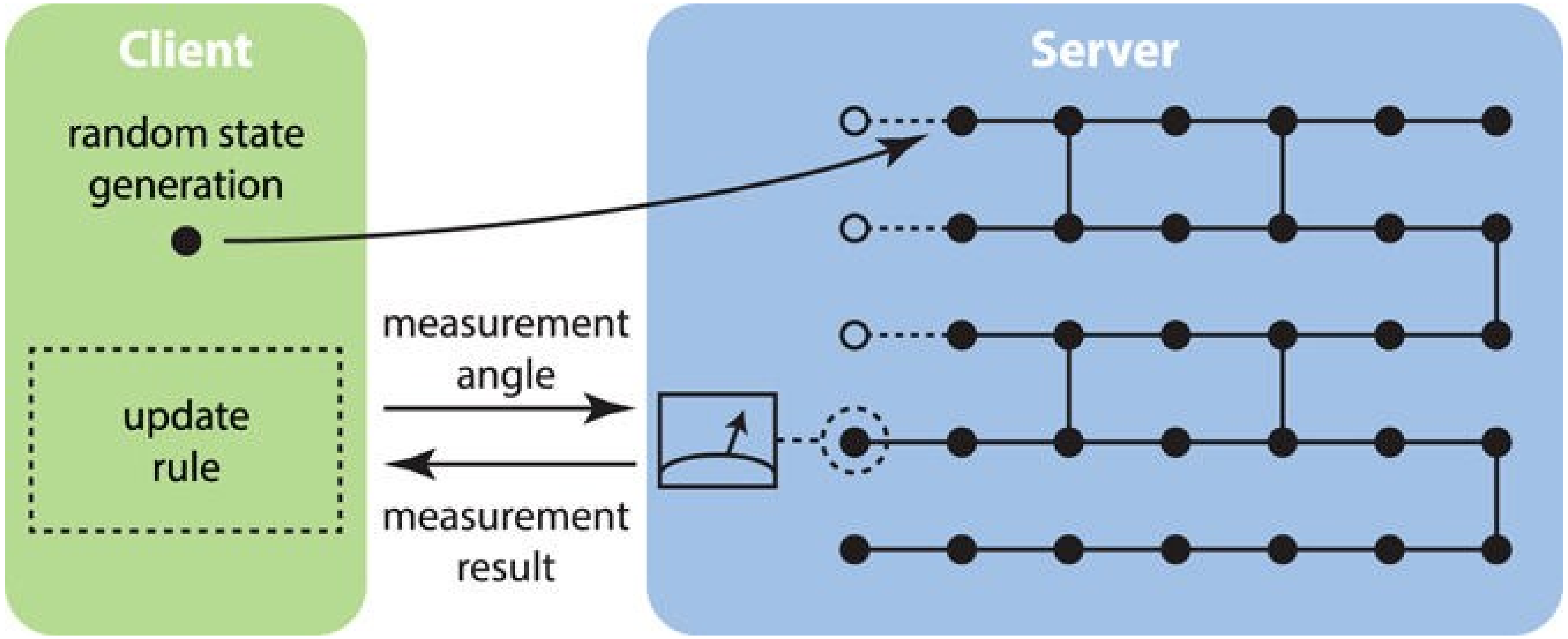
2020-2024

- PI: Fabio Sciarrino (Univ. of Rome, La Sapienza)
- Partners: CNR (IT), CNRS (FR), Sorbonne Univ. (FR), Veriqloud (FR), QuiX BV (NL), INL

- Development of complex linear and non-linear interferometers
    - Theoretical characterization of photonic indistinguishability, resources such as contextuality and coherence
    - Scalability of photonic QC, MBQC ideas
- Noisy, Intermediate-Scale Quantum (NISQ) computational applications: variational algorithms, randomness manipulation, cryptography, quantum chemistry

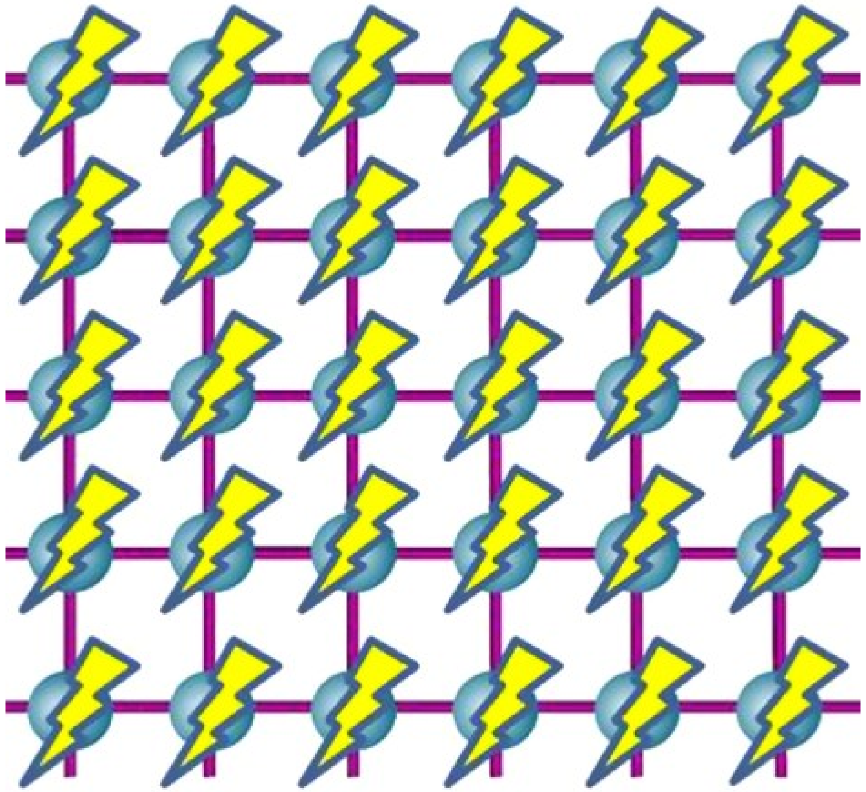
Application: blind quantum computation

- Classical/quantum separation in MBQC allow for implementation of novel protocols – such as blind quantum computation
- Here, client has limited quantum capabilities, and uses a server to do computation for her.
- Blind = server doesn't know what's being computed.



Broadbent, Fitzsimons, Kashefi, axiv:0807.4154 [quant-ph]

Which resource gives MBQC its power?



- Clearly, the correlations in the resource state.

- Analysis of MBQC protocols in terms of Bell inequalities:
  - Anders/Browne PRL 102, 050502 (2009)
  - Hoban et al., New J. Phys. 13, 023014 (2011)

- …but measurements are usually not space-like separated:
  ⇨ quantum contextuality

  - Raussendorf, PRA 88, 022322 (2013)

Quantum contextuality

- Context of an observable A = set of commuting observables measured together with A
- Non-contextuality hypothesis: outcomes of observables are context-independent
- Violated by quantum mechanics!

- Famously proved by Kochen and Specker (1967). Let's see a proof by Mermin (1990).

$\mathbb{1} \otimes \sigma_z$	$\sigma_z \otimes \mathbb{1}$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes \mathbb{1}$	$\mathbb{1} \otimes \sigma_x$	$\sigma_x \otimes \sigma_x$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$

- Operators in each row and column commute;

Moreover, they are the product of the other two in same row/column

- EXCEPTION: third column:

$$\sigma_y \otimes \sigma_y = -\sigma_z \otimes \sigma_z \cdot \sigma_x \otimes \sigma_x$$

- So it's impossible to assign +1 or -1 values to each observable in a context-independent way. $\Rightarrow$ QM is contextual.

Contextuality is necessary for magic state distillation

Howard et al., Nature 310, 351 (2014)

- The Mermin square proof of quantum contextuality is state-independent – any state violates the non-contextuality hypothesis.
- For Hilbert space dimension d>2, all contextuality proofs are *state-dependent*.
- So what's special about states revealing contextuality?

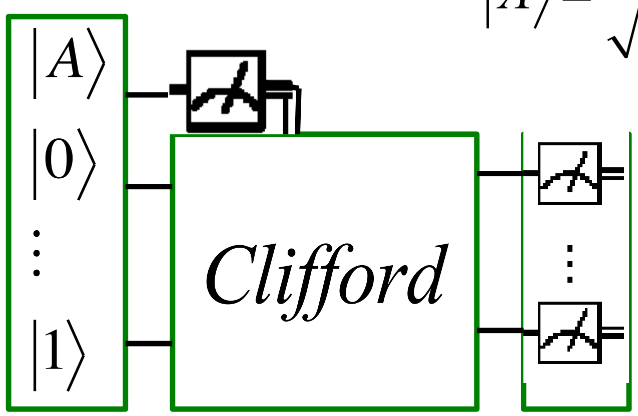
Contextuality is necessary for magic state distillation

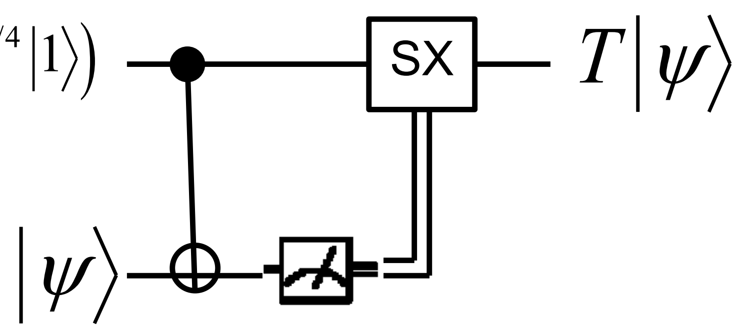
Howard et al., Nature 310, 351 (2014)

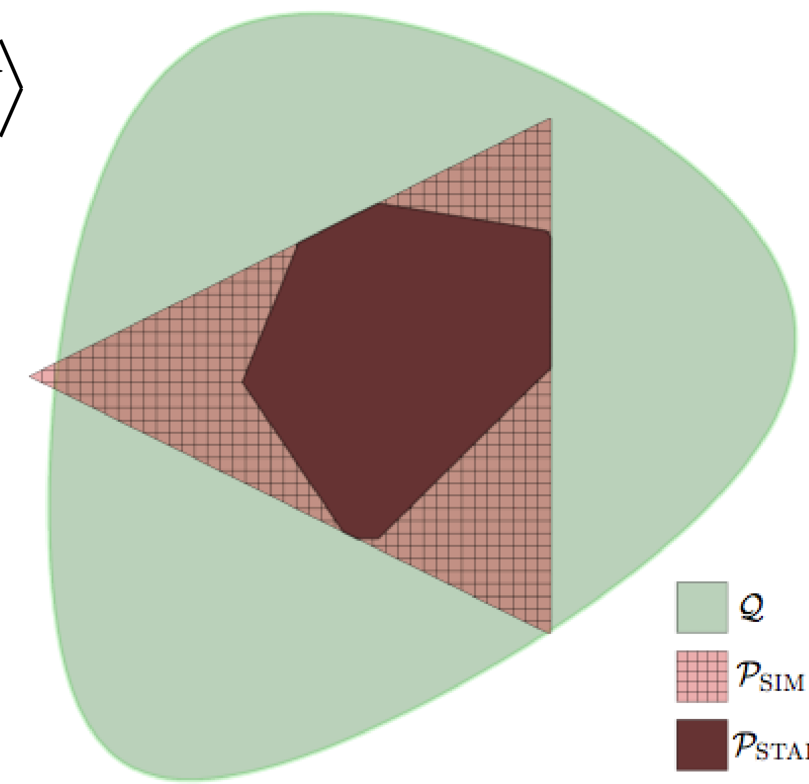
- The Mermin square proof of quantum contextuality is state-independent – any state violates the non-contextuality hypothesis.
- For Hilbert space dimension d>2, all contextuality proofs are *state-dependent*.
- So what's special about states revealing contextuality?

- Howard et al. (2014) looked at that problem in the QC model of Clifford computer + magic states:

$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$







from Howard et al., Nature 310, 351 (2014)

PSIM = simulable under stabilizer measurements
PSTAB = stabilizer states
Q = general quantum states

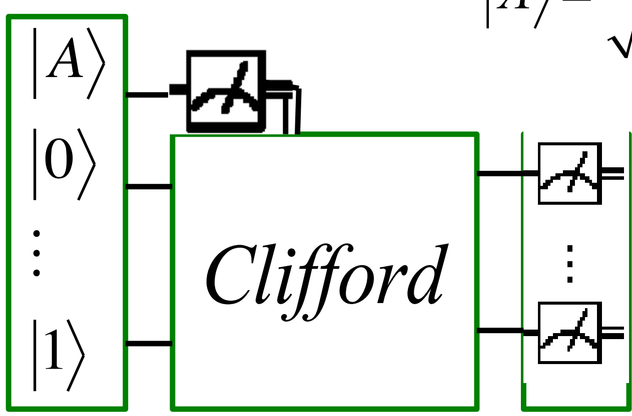
Contextuality is necessary for magic state distillation

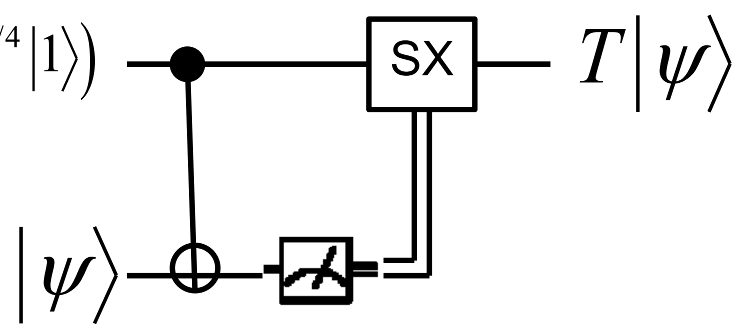
Howard et al., Nature 310, 351 (2014)

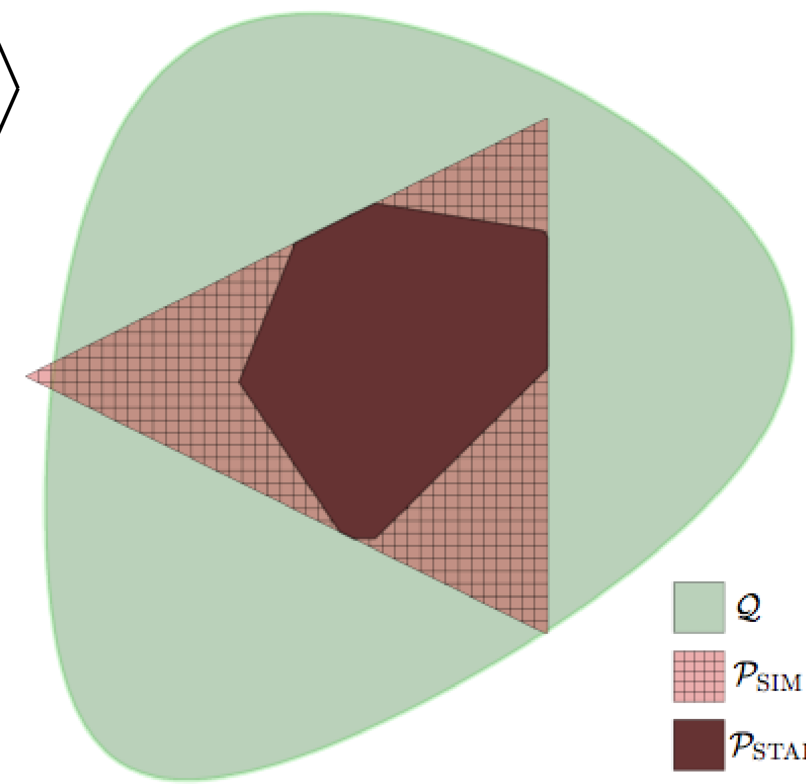
- The Mermin square proof of quantum contextuality is state-independent – any state violates the non-contextuality hypothesis.
- For Hilbert space dimension d>2, all contextuality proofs are *state-dependent*.
- So what's special about states revealing contextuality?

- Howard et al. (2014) looked at that problem in the QC model of Clifford computer + magic states:

$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$







from Howard et al., Nature 310, 351 (2014)

- Result: any state out of PSIM violates a state-dependent non-contextuality inequality, using stabilizer measurements. States in PSIM are non-contextual.

→ contextuality is necessary for magic-state computation

PSIM = simulable under stabilizer measurements
PSTAB = stabilizer states
Q = general quantum states

Application: model for quantum spacetime

- MBQC can serve as a discrete toy model for quantum spacetime:

quantum space-time	MBQC
quantum substrate	graph states
events	measurements
principle establishing global space-time structure	determinism requirement for computations

[Raussendorf *et al.*, arxiv:1108.5774]

- Even closed timelike curves (= time travel) have analogues in MBQC!

[Dias da Silva, Kashefi, Galvão PRA 83, 012316 (2011)]