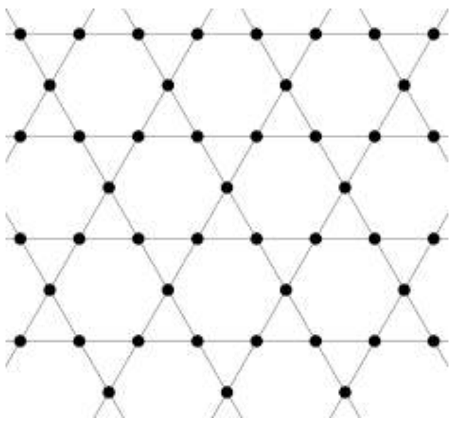
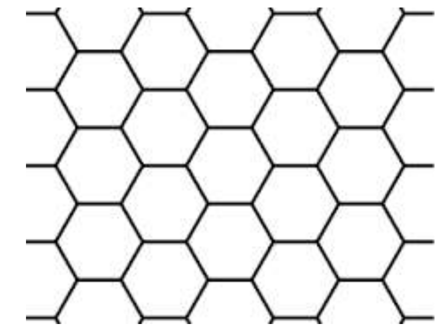
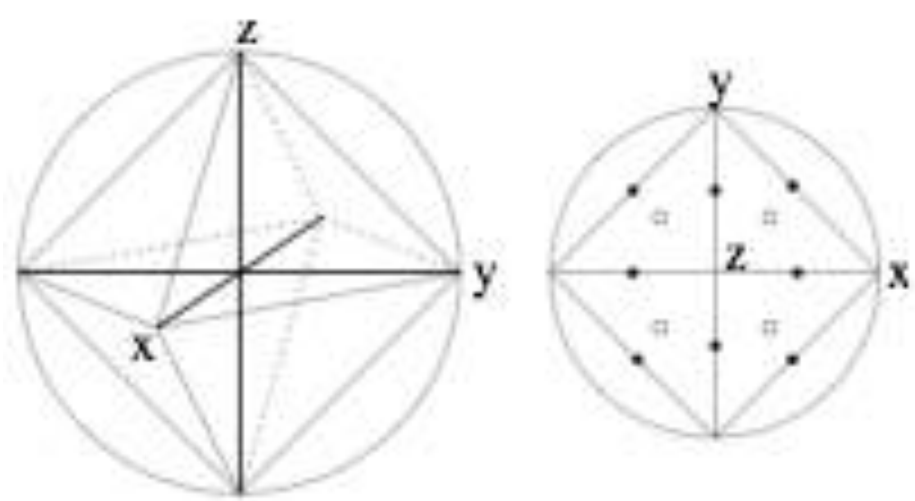


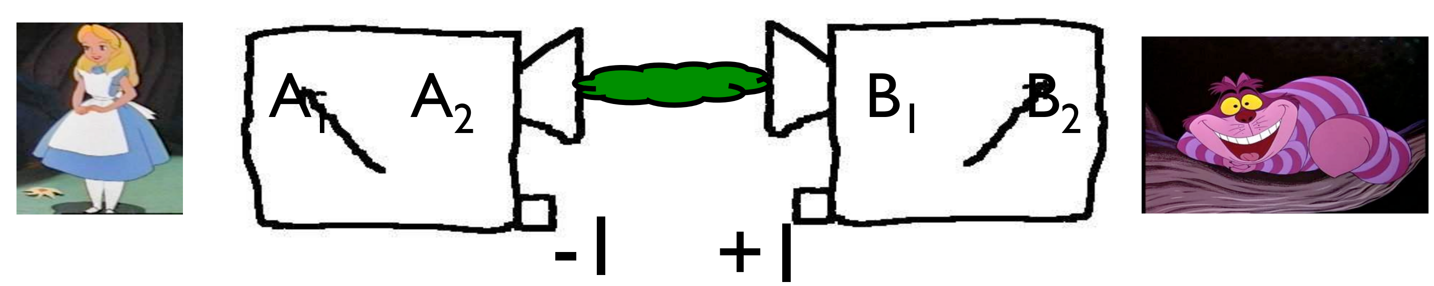
Introduction to quantum computation and simulability



Daniel J. Brod (UFF)
Leandro Aolita (UFRJ/ICTP-SAIFR)
Ernesto F. Galvão (UFF)

Instituto de Física
Universidade Federal Fluminense





ICTP-SAIFR – IFT/UNESP , October 15th-19th, 2018

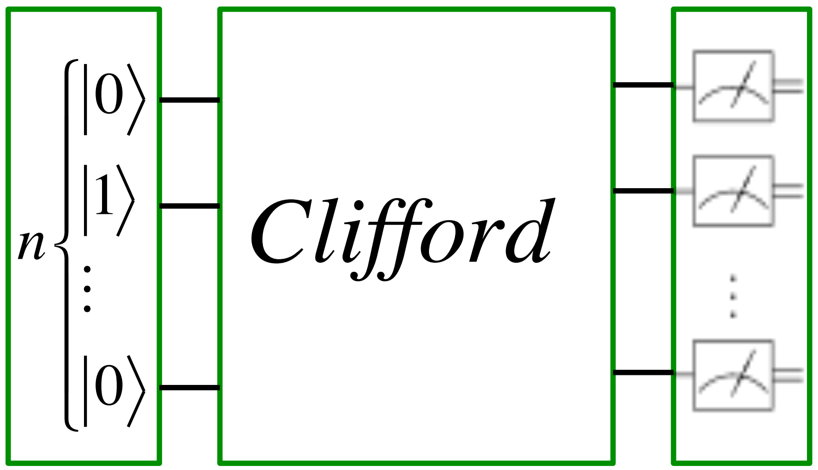
Lecture 5 : Clifford circuits, measurement-based QC (MBQC) I

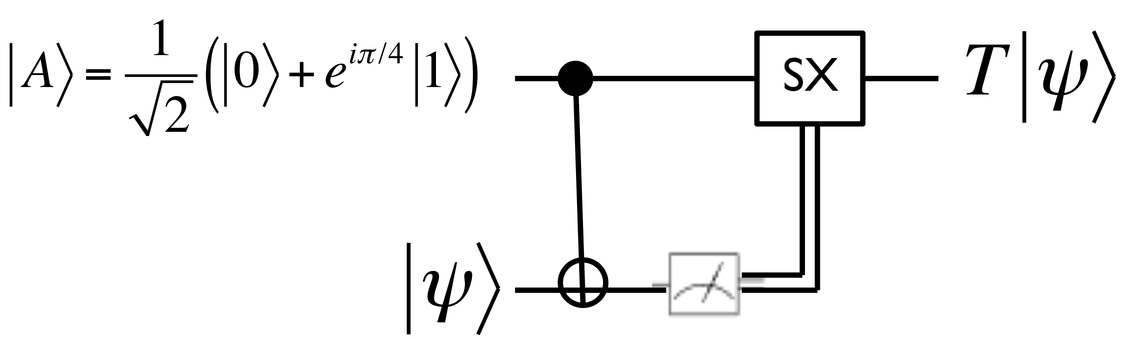
Outline:

- Clifford circuits
  - Pauli and Clifford groups
  - Simulability of Clifford circuits
  - Upgrading Clifford circuits to universal QC
- Introduction to Bell non-locality
- How MBQC works
  - One-bit teleportation circuit
  - Gate teleportation
  - Concatenating MBQC gates
- Resources for MBQC: graph and cluster states
- Experimental implementations

- For slides and links to related material, see

Clifford circuits





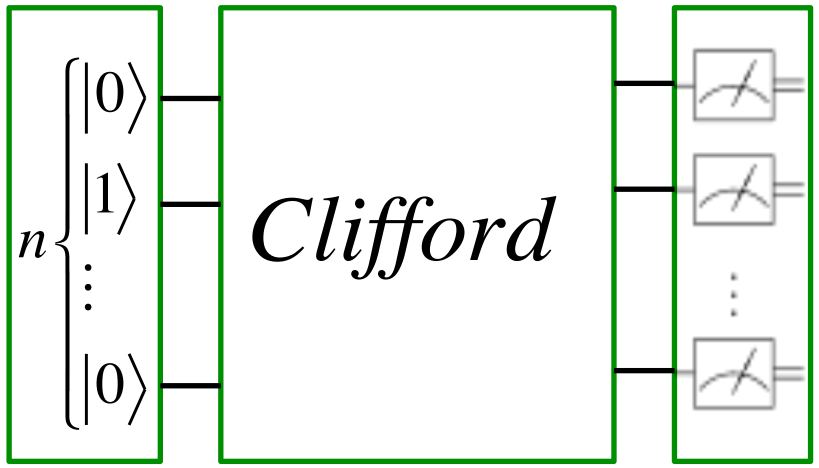
Clifford circuits

- **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:

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



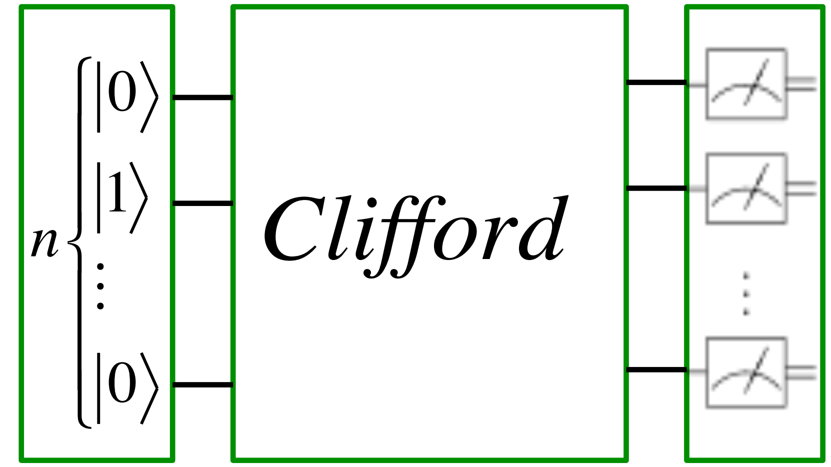
- Clifford group is generated by $\{H, P, CNOT\}$

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

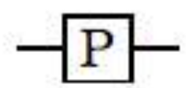
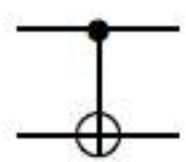
…but are **efficiently simulable**.

Clifford circuits

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



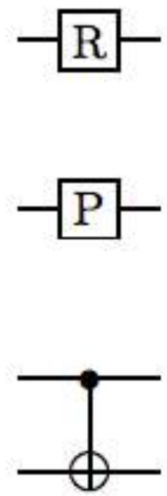
$$CP_iC^{+} = P_j \Leftrightarrow CP_i = P_jC$$

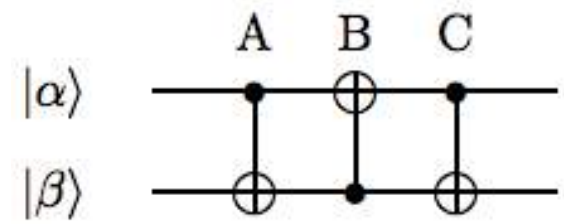
R	$X \rightarrow Z$ $Z \rightarrow X$	
P	$X \rightarrow Y$ $Z \rightarrow Z$	
CNOT	$X \otimes I \rightarrow X \otimes X$ $I \otimes X \rightarrow I \otimes X$ $Z \otimes I \rightarrow Z \otimes I$ $I \otimes Z \rightarrow Z \otimes Z$	

- 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$(1 \to 2)$	$\overline{X}_1$	$I \otimes X$
	$\overline{X}_2$	$X \otimes I$
	$\overline{Z}_1$	$I \otimes Z$
	$\overline{Z}_2$	$Z \otimes I$

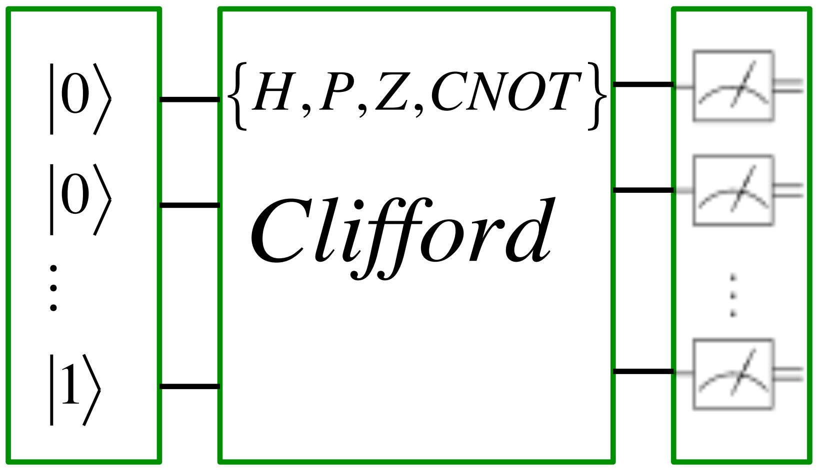
- The key simulation idea is to use Heisenberg picture:
  - initial state is eigenstate of Pauli operator
  - each Clifford gate maps it into a new Pauli (efficient computation)
  - keep track of the Pauli transformation until end, when measurement outcomes can be efficiently computed.

“Upgrading” a Clifford computer

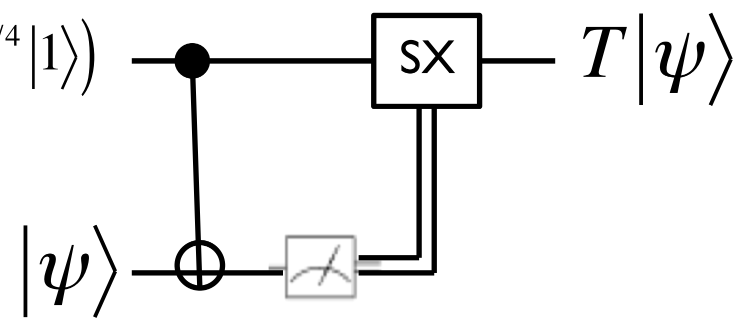
- Clifford: $\{H, P, Z, CNOT\}$, all that’s missing is *T* gate

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

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

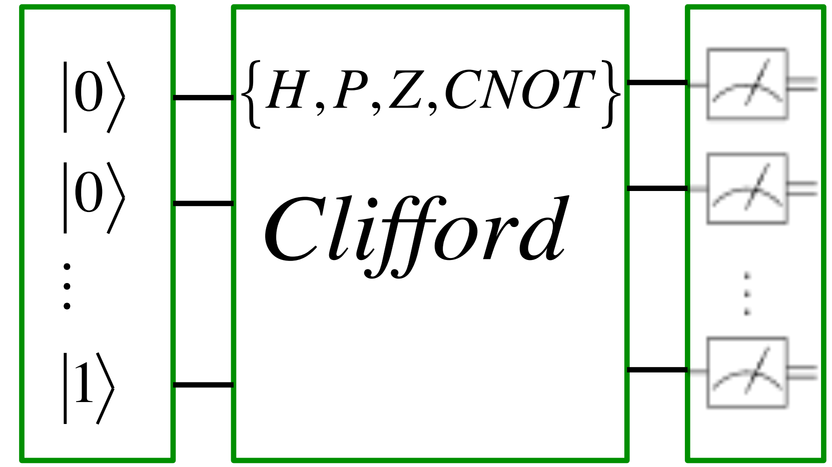


$$|A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$$



“Upgrading” a Clifford computer

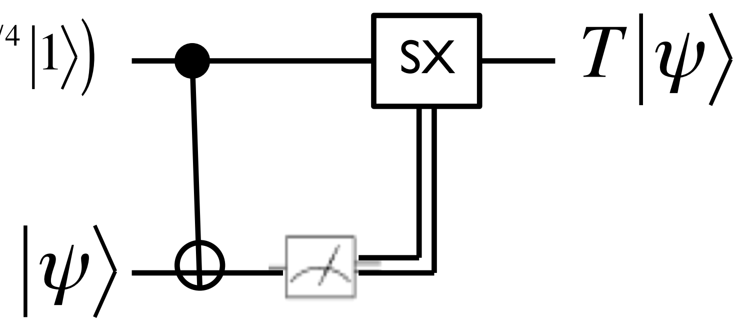
- Clifford: $\{H, P, Z, CNOT\}$, all that’s missing is T gate

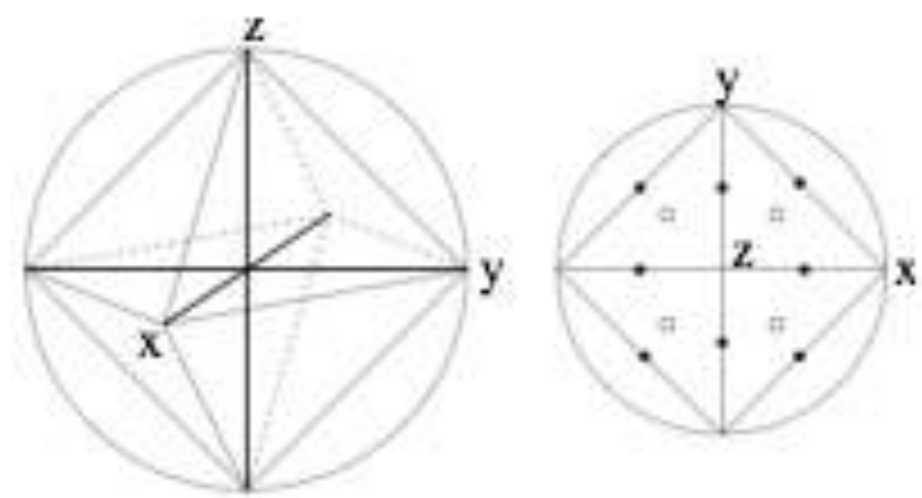


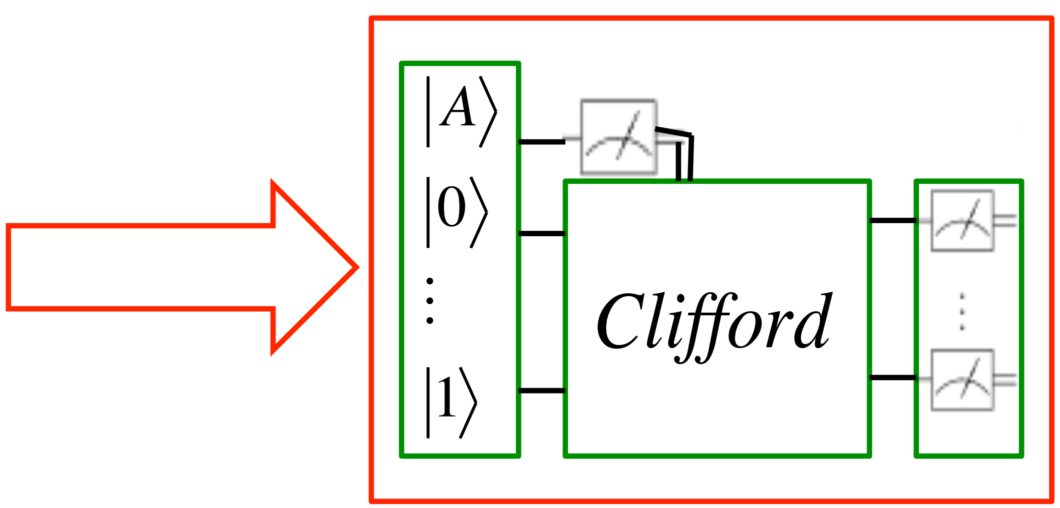
- There’s a work-around using:
  - **magic input states** and
  - **adaptativity**

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

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





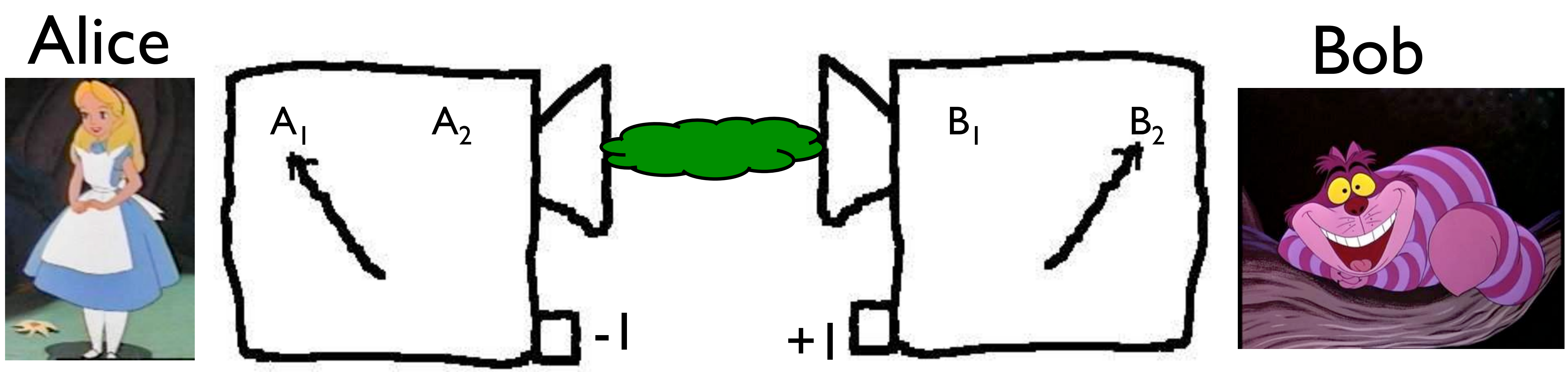


is universal for QC

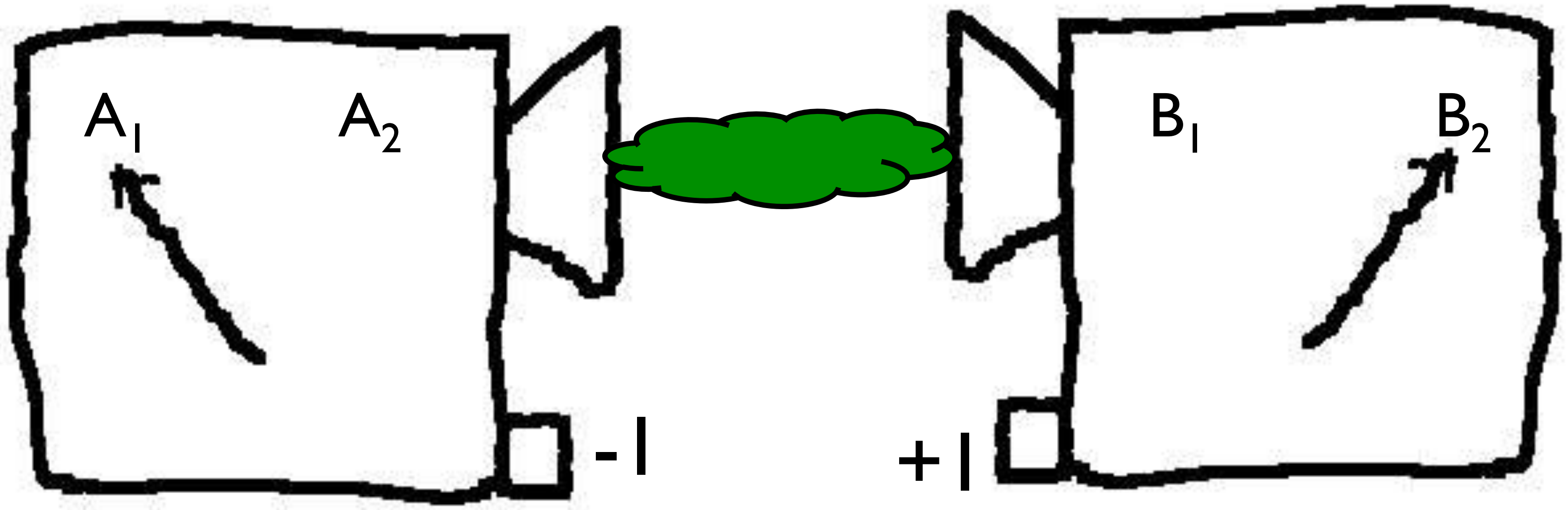
- Relevant for topological quantum computation with anyons, as for example Ising model implements Clifford operations in a topologically protected way

Bell non-locality

- Bell inequalities (Bell 1964) are limits on the correlation of distant systems
- Example: **Clauser-Horn-Shimony-Holt (CHSH) inequality** (1969):
  - Alice e Bob measure dychotomic properties (results +1 or -1)
  - Each chooses randomly which property to measure:
    - Alice measures A_1 or A_2; result a_1 or a_2
    - Bob measures B_1 or B_2; result b_1 or b_2.



CHSH inequality



- Hypotheses:
  - Pre-determined value for experimental outcomes (realism)
  - Result of A doesn't depend on what B does (and vice-versa) (locality)

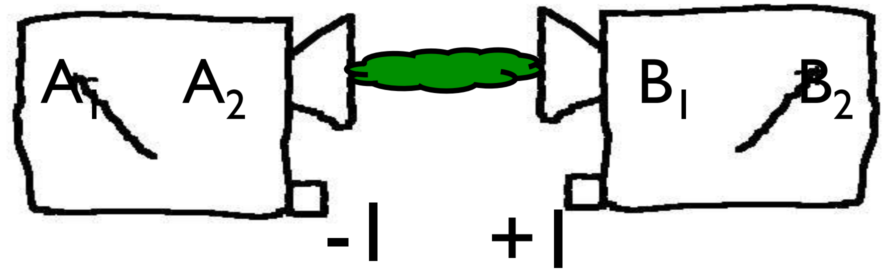
→ local realism

- CHSH inequality:

$$\left|\langle a_1 b_1\rangle + \langle a_2 b_1\rangle + \langle a_2 b_2\rangle - \langle a_1 b_2\rangle\right| \leq 2$$

CHSH inequality

- Alice and Bob compare notes and jointly prepare spreadsheet:



a_1	a_2	b_1	b_2	a_1b_1	a_1b_2	a_2b_1	a_2b_2
+1		-1		-1			
	-1		+1				-1
	+1	+1				+1	
-1			+1		-1		

$$\langle a_1b_1\rangle \quad \langle a_1b_2\rangle \quad \langle a_2b_1\rangle \quad \langle a_2b_2\rangle$$

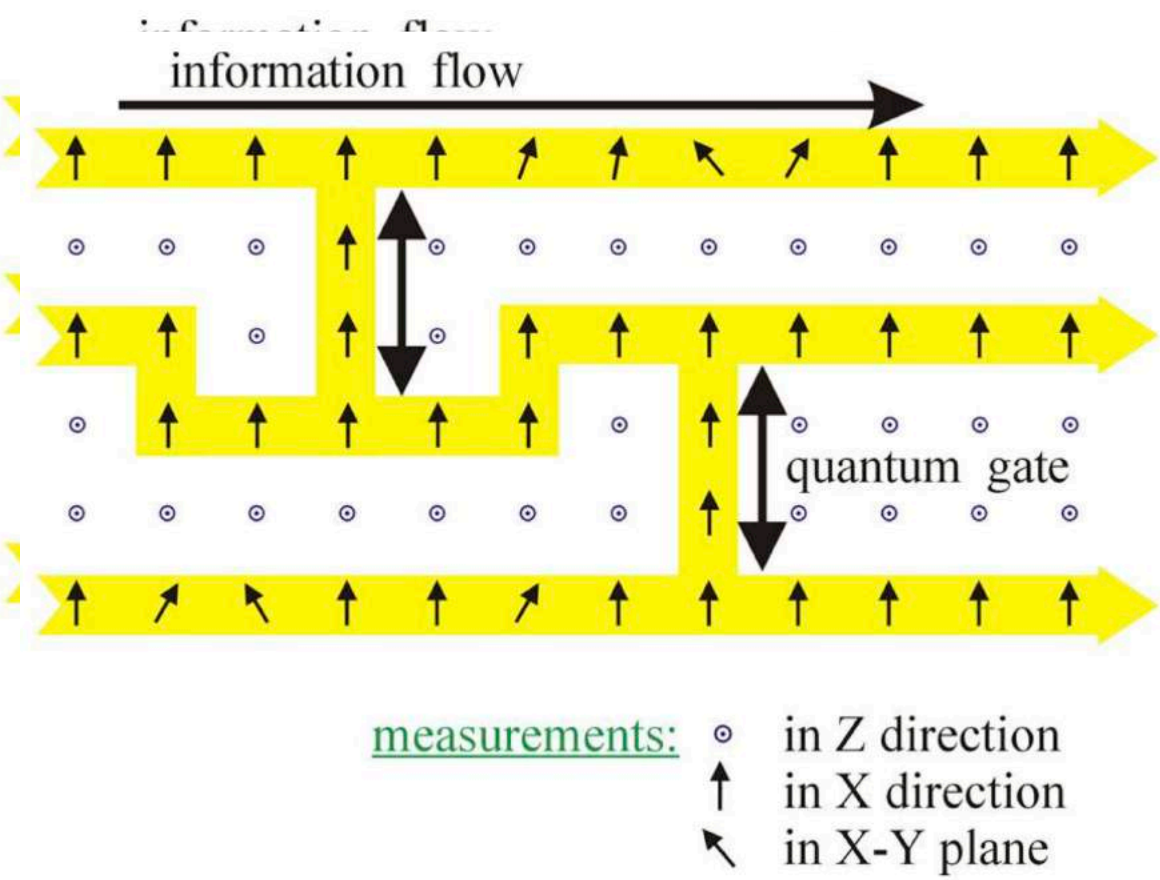
- If local realism holds, then: $$\left|\langle a_1b_1\rangle + \langle a_2b_1\rangle + \langle a_2b_2\rangle - \langle a_1b_2\rangle\right| \leq 2$$

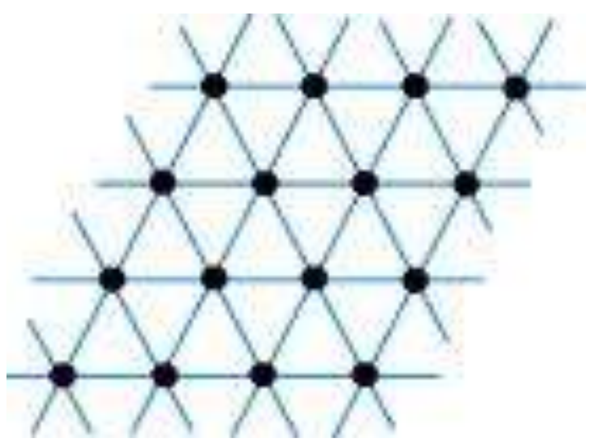
- But local measurements on particles in entangled state $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\downarrow\rangle_A|\uparrow\rangle_B - |\uparrow\rangle_A|\downarrow\rangle_B\right)$

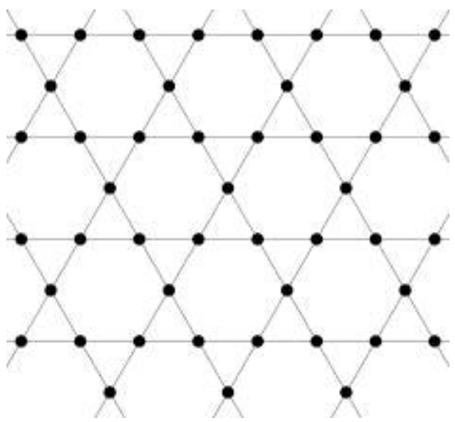
give $$\left|\langle a_1b_1\rangle + \langle a_2b_1\rangle + \langle a_2b_2\rangle - \langle a_1b_2\rangle\right| = 2\sqrt{2} > 2$$

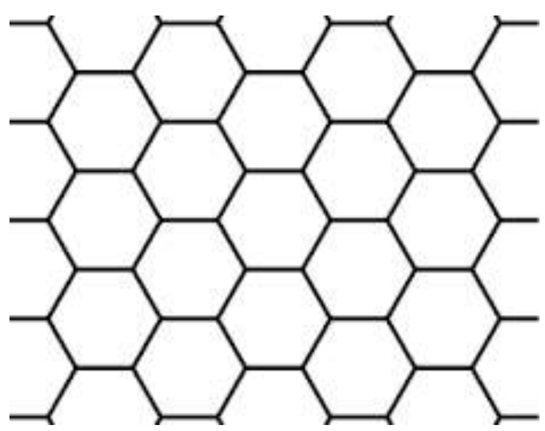
QM violates local realism!

Measurement-based quantum computation (MBQC)



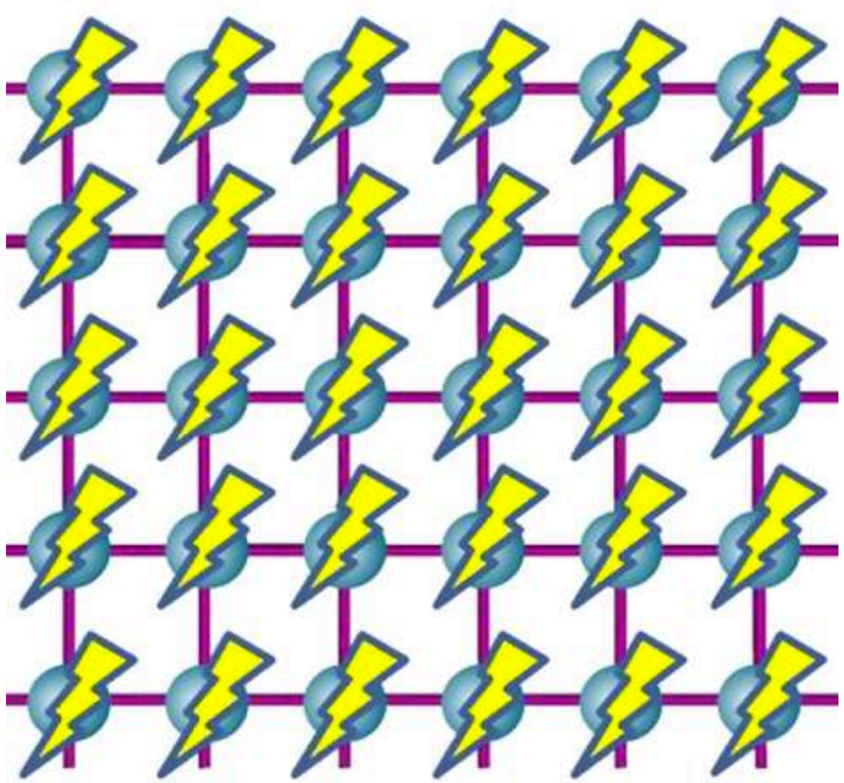






MBQC: basic ingredients

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



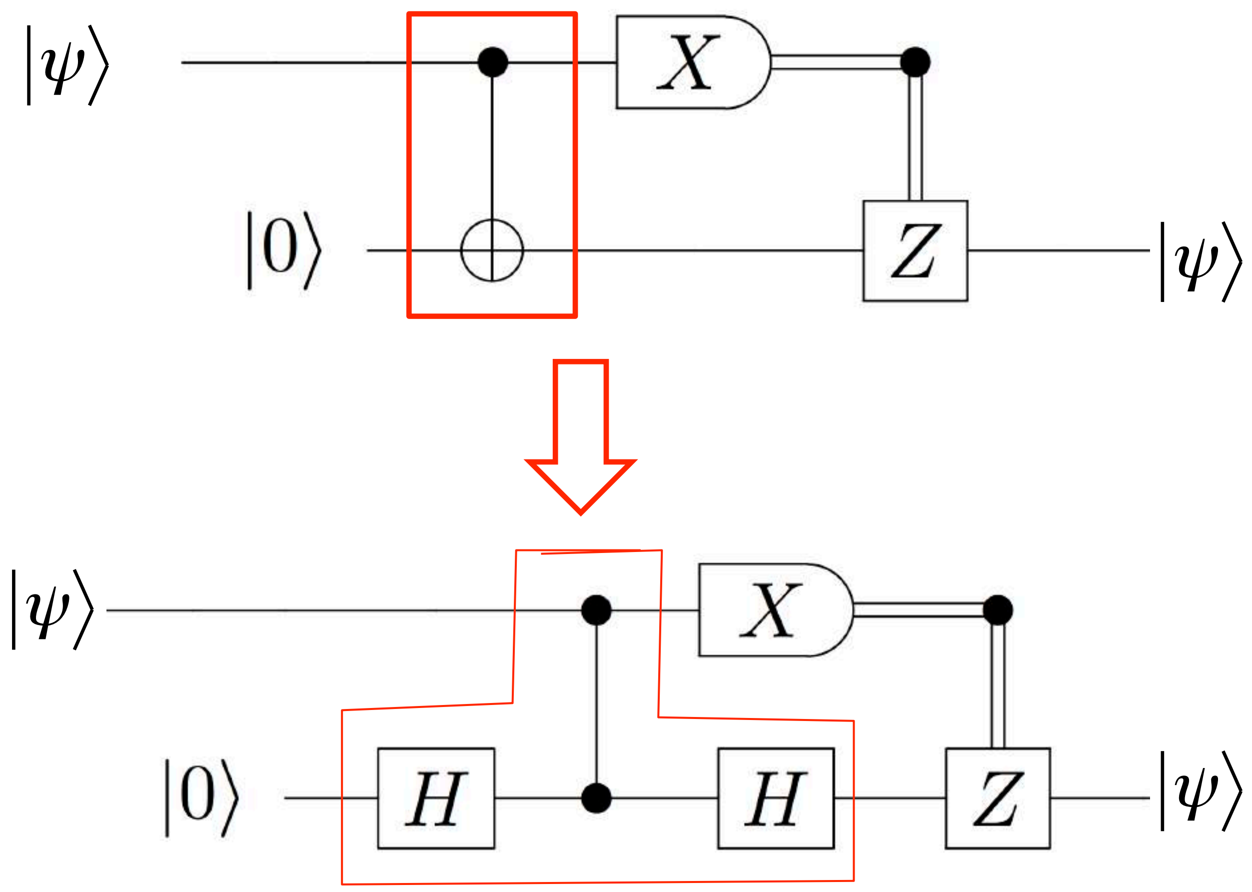
1- Initialization by CZ gates on $|+\rangle$ states;

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

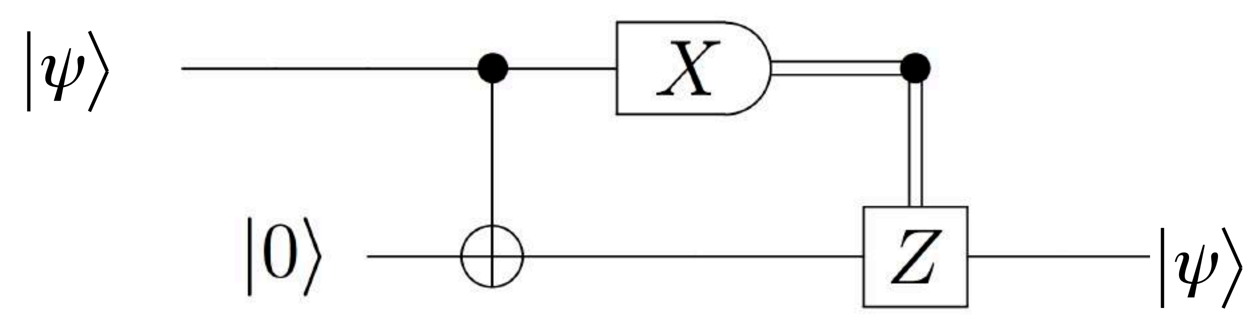
3 versions of the "1-bit *Z* teleportation" circuit:



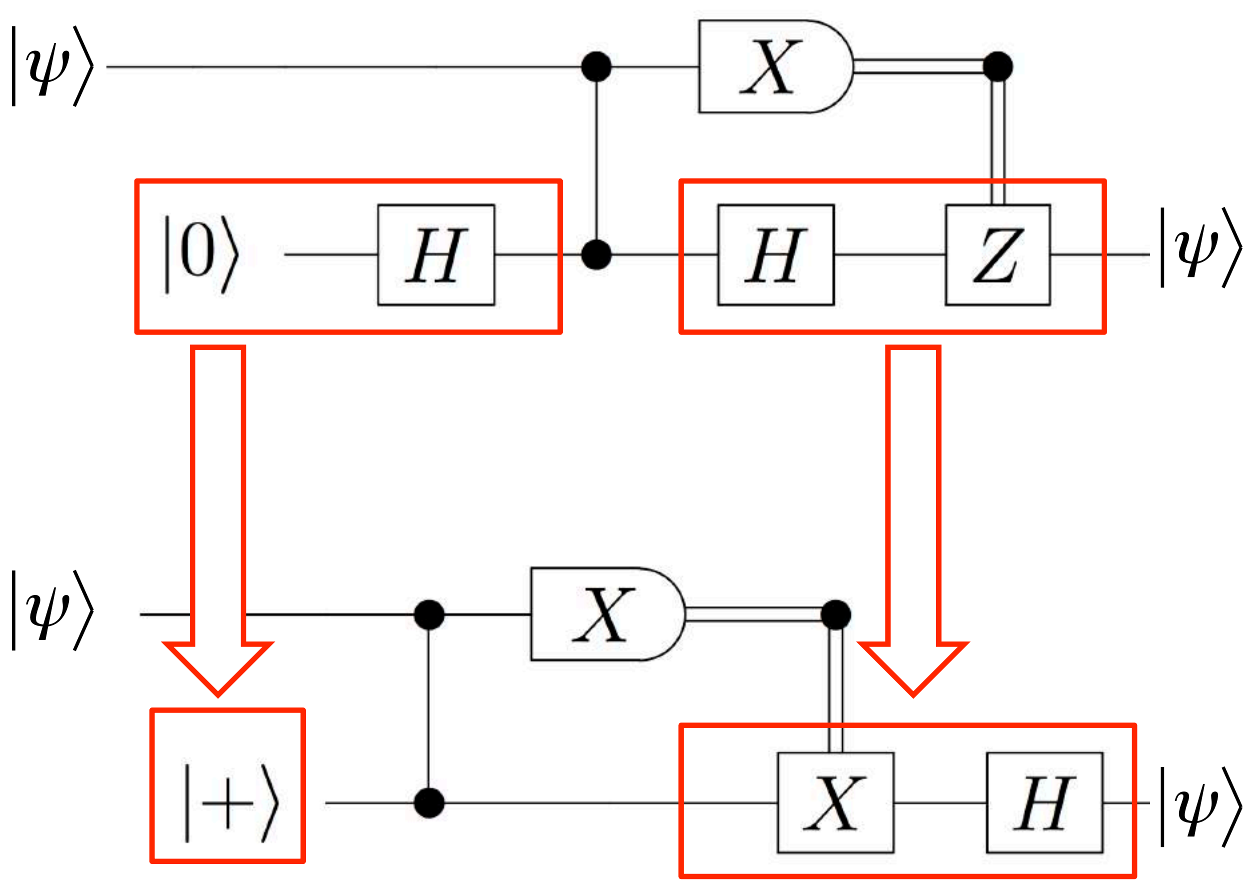
- X measurement result controls Z gate
- Direct calculation shows this works
- Identity transforms CNOT into CZ

MBQC: step-by-step

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



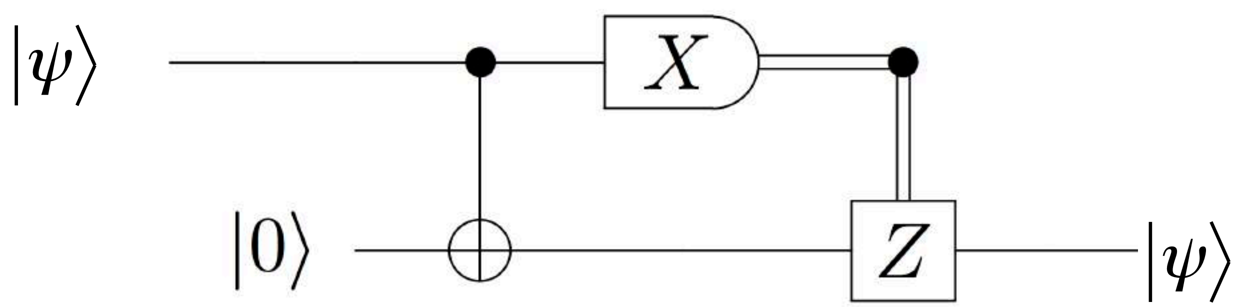
- X measurement result controls Z gate
- Direct calculation shows this works



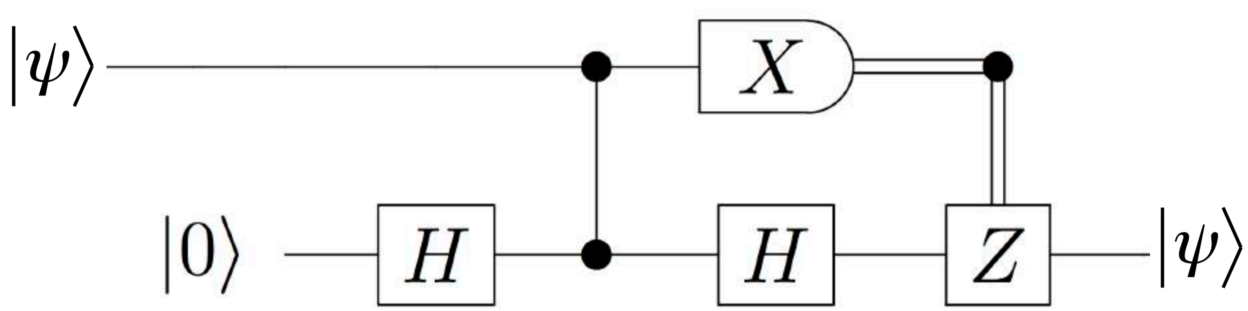
- Identity transforms CNOT into CZ
- Left H incorporated in input $|+\rangle$
- HZ = XH identity

MBQC: step-by-step

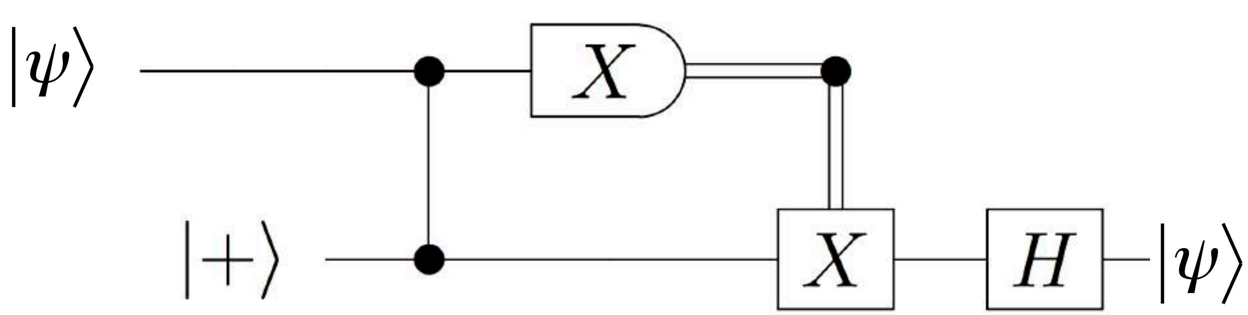
3 versions of the “1-bit *Z* teleportation” circuit:



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



- Identity transforms CNOT into CZ

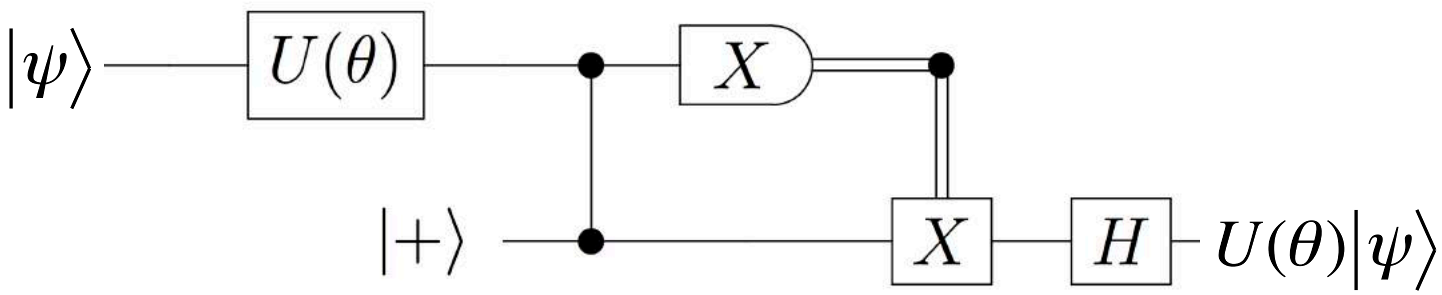


- Left H incorporated in input $|+\rangle$
- HZ = XH identity

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

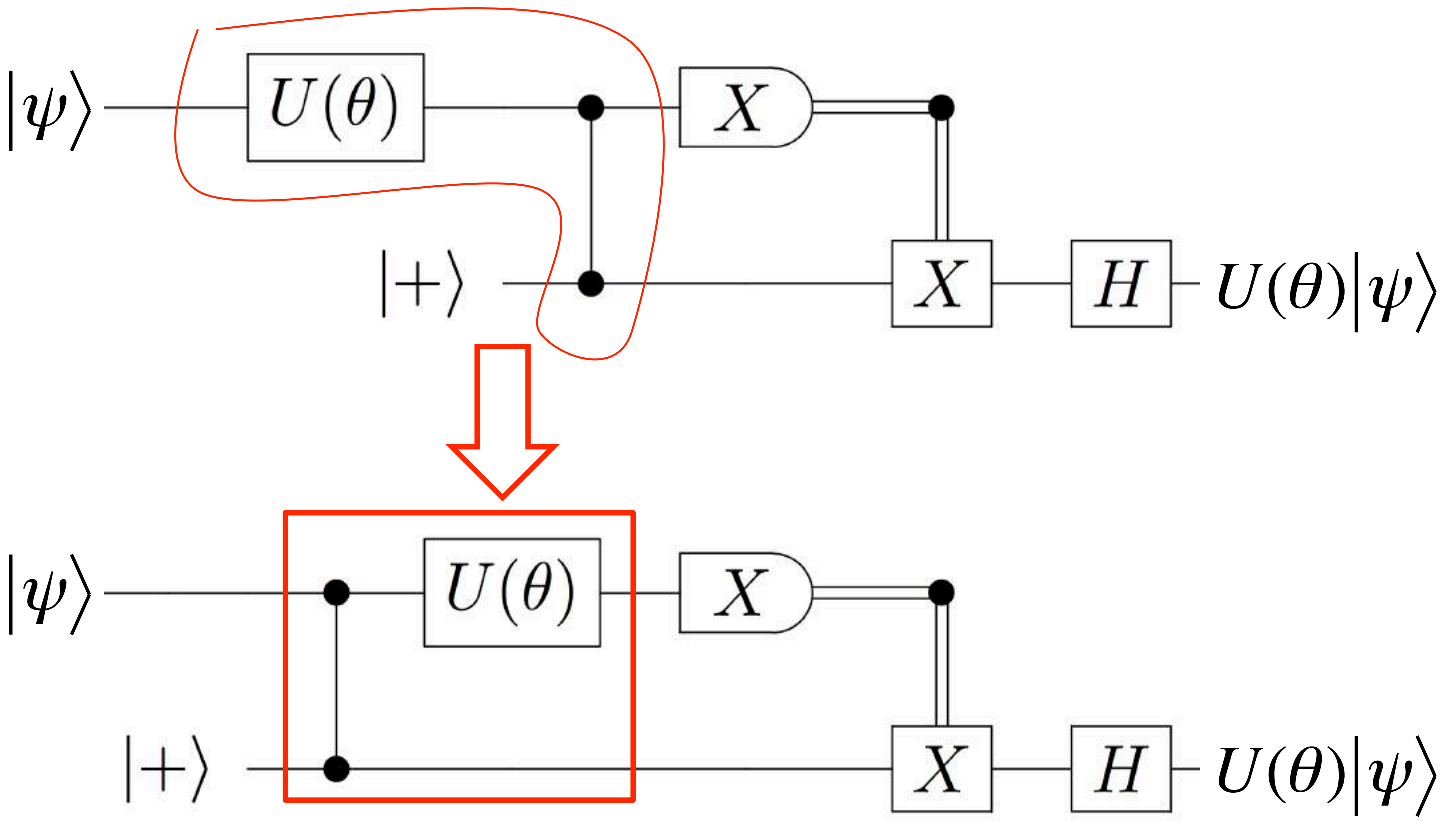
MBQC: step-by-step

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



MBQC: step-by-step

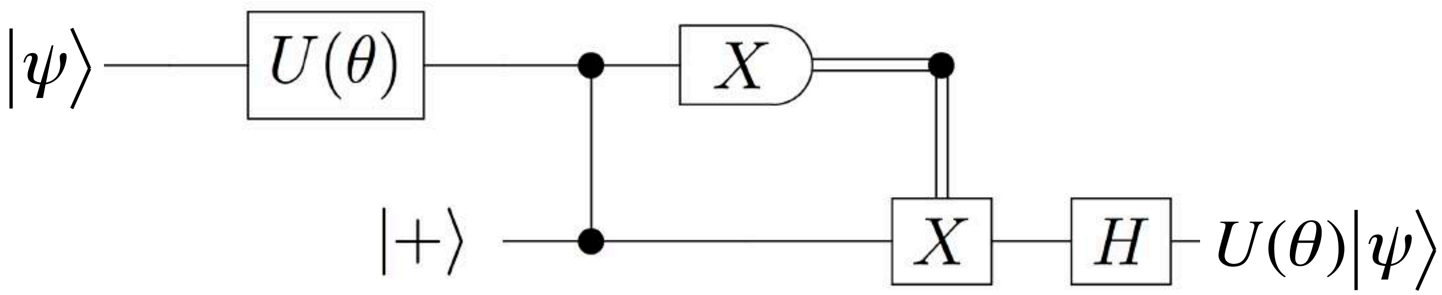
Now let's teleport the unitary $U(\theta) = \exp(i\theta Z/2)$ **:**



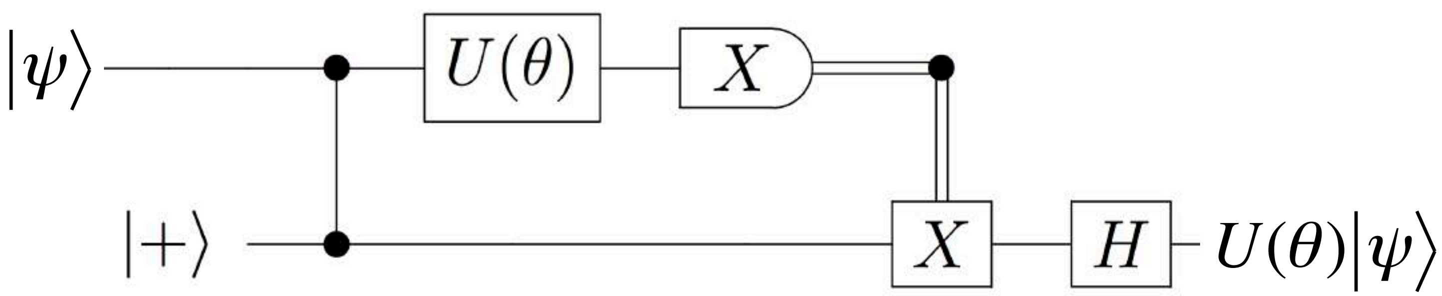
- U commutes with CZ

MBQC: step-by-step

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

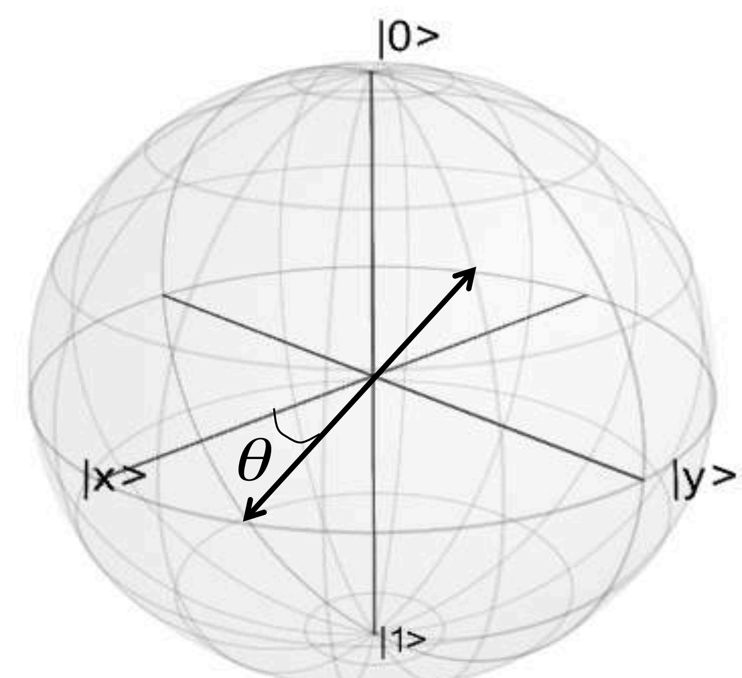


- U commutes with CZ



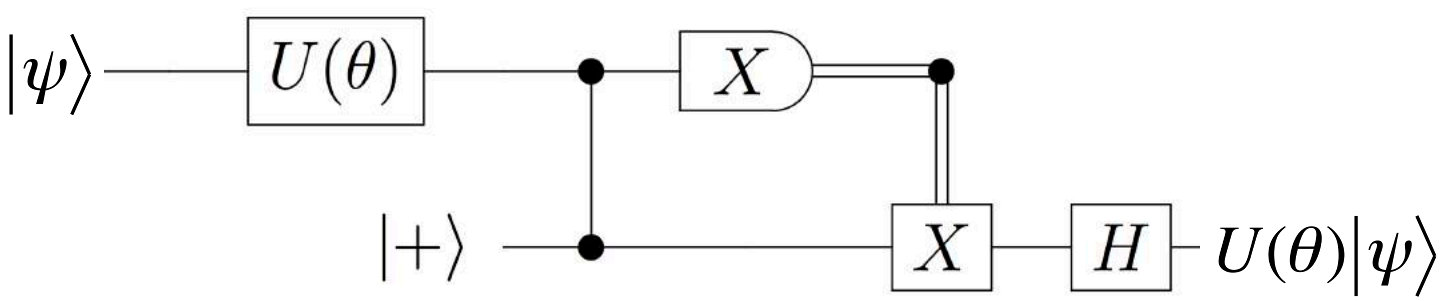
- U followed by X-measurement = measurement in *x-y* plane of Bloch sphere:

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

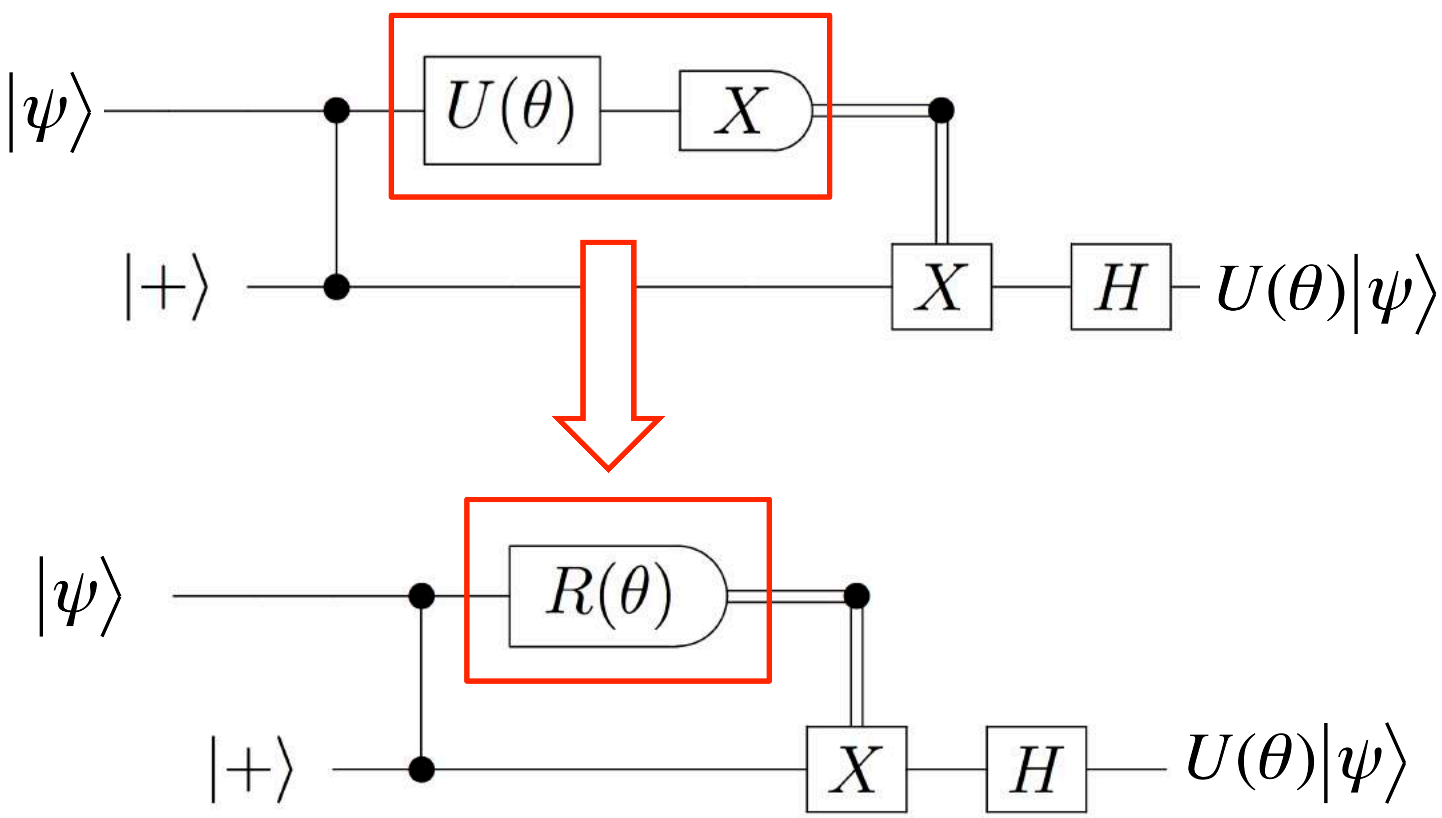


MBQC: step-by-step

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

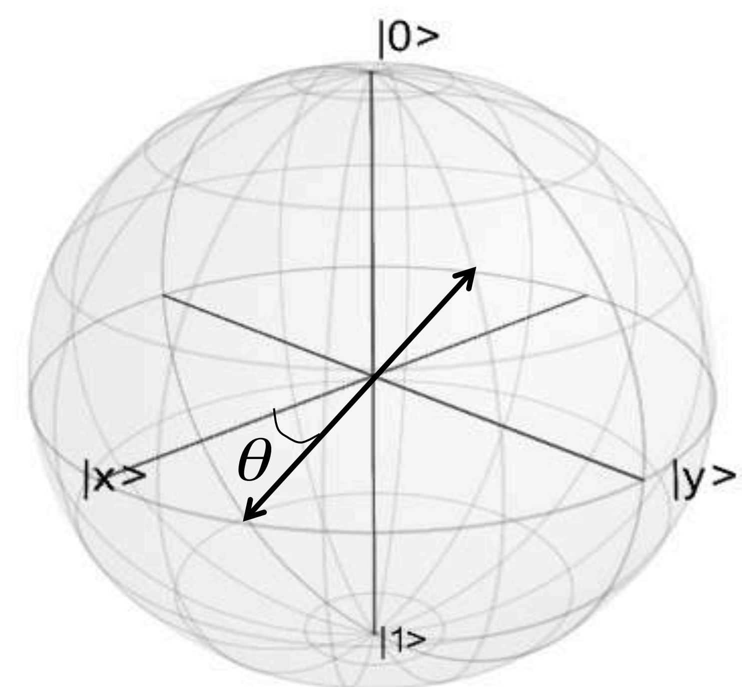


- U commutes with CZ



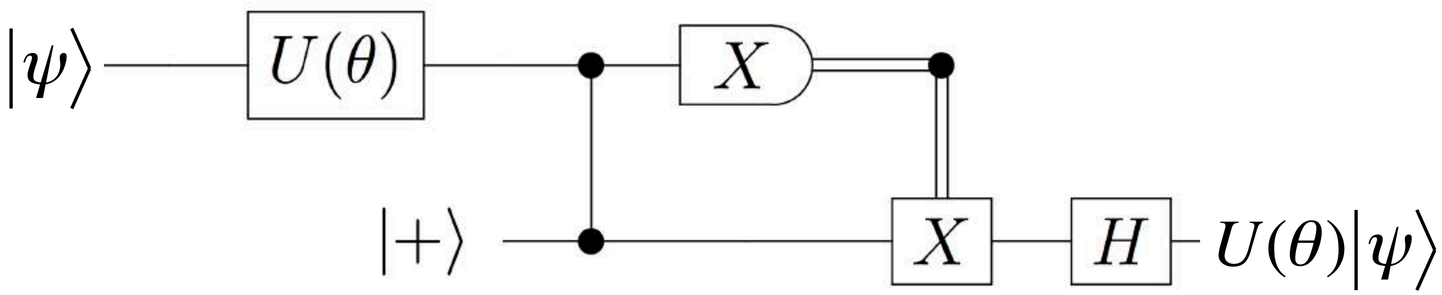
- U followed by X-measurement = measurement in *x-y* plane of Bloch sphere:

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

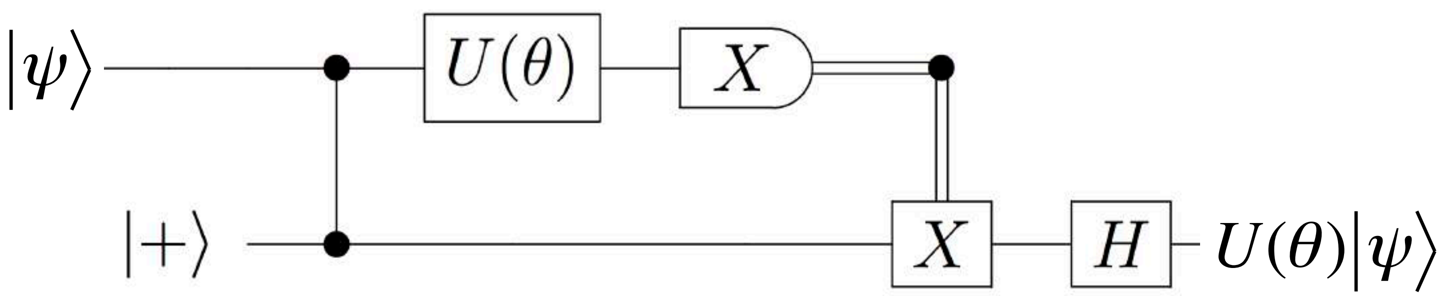


MBQC: step-by-step

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

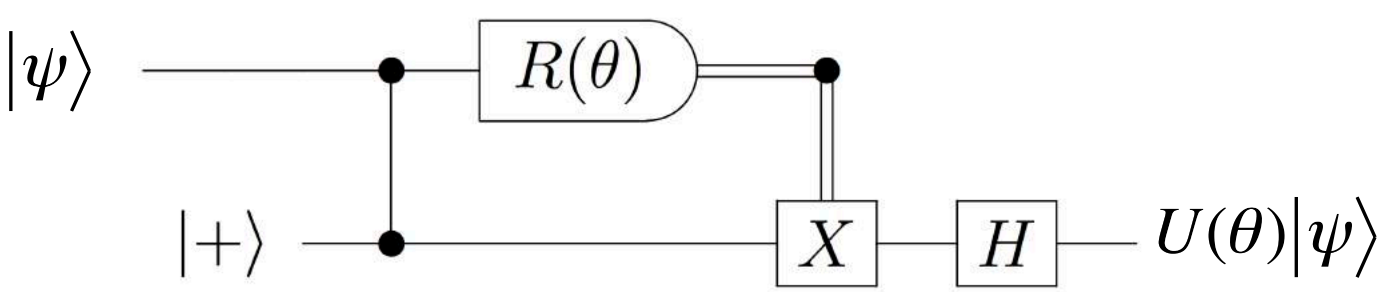


- U commutes with CZ



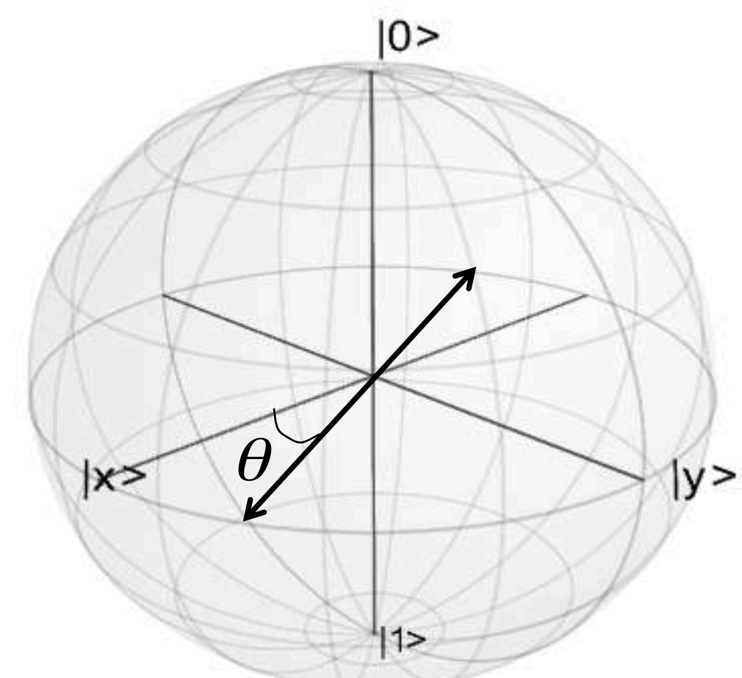
- U followed by X-measurement = measurement in *x-y* plane of Bloch sphere:

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



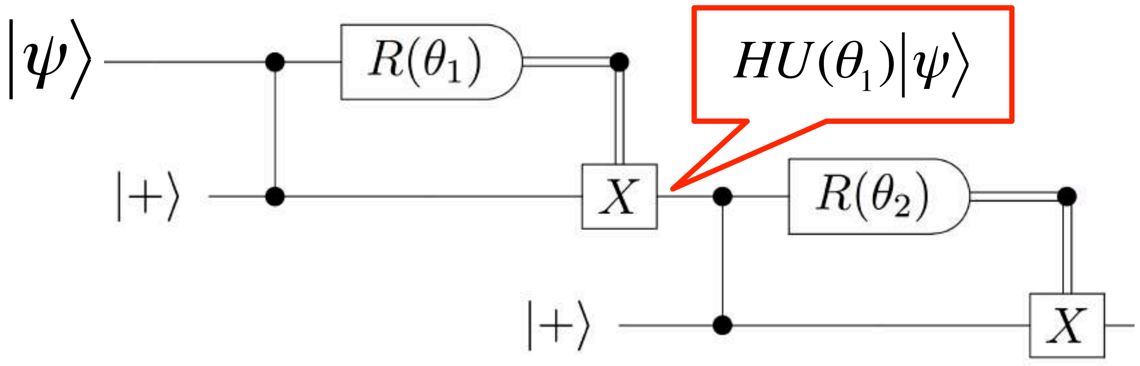
Evolved state $U(\theta)|\psi\rangle$ is teleported, via entanglement and right choice of measurement basis of top qubit

(*gate teleportation* idea of Gottesman and Chuang)



MBQC: step-by-step

Now two different unitaries in sequence:

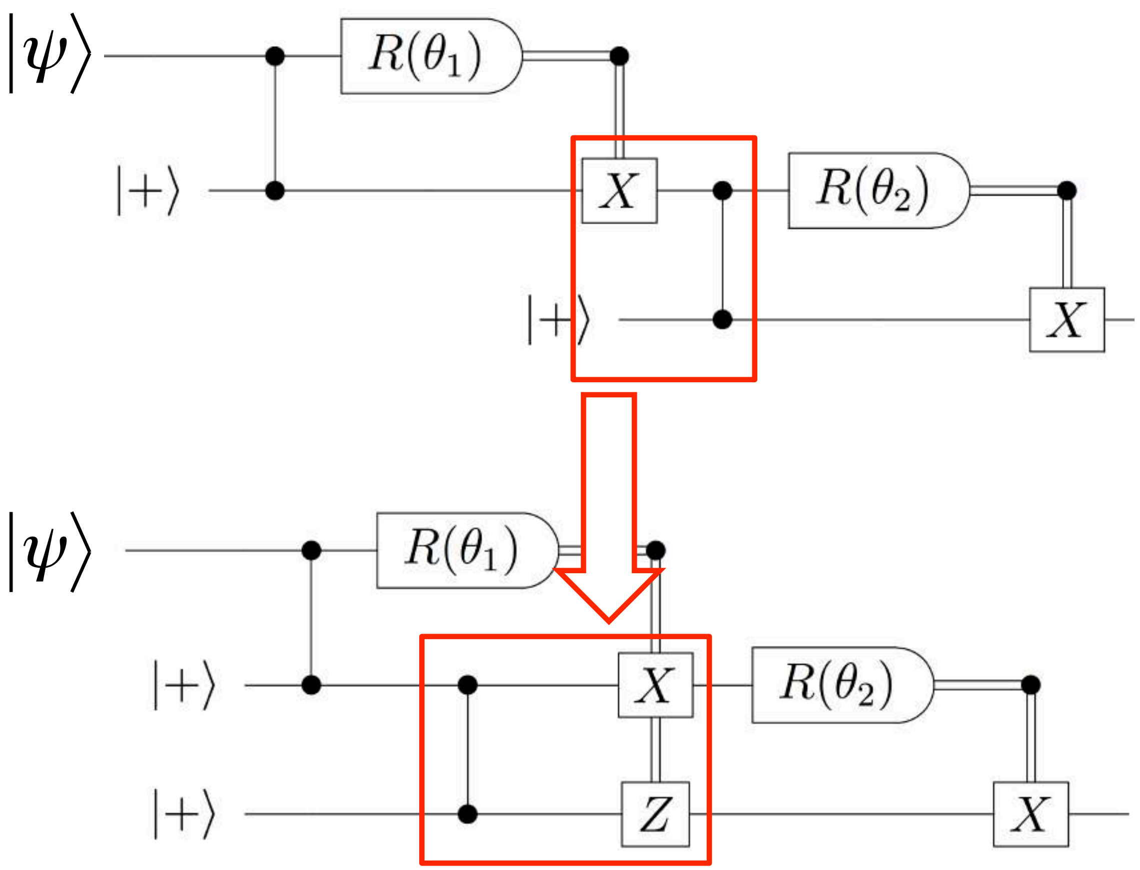


- Two gate teleportations, without final H gates, result in final state

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

MBQC: step-by-step

Now two different unitaries in sequence:



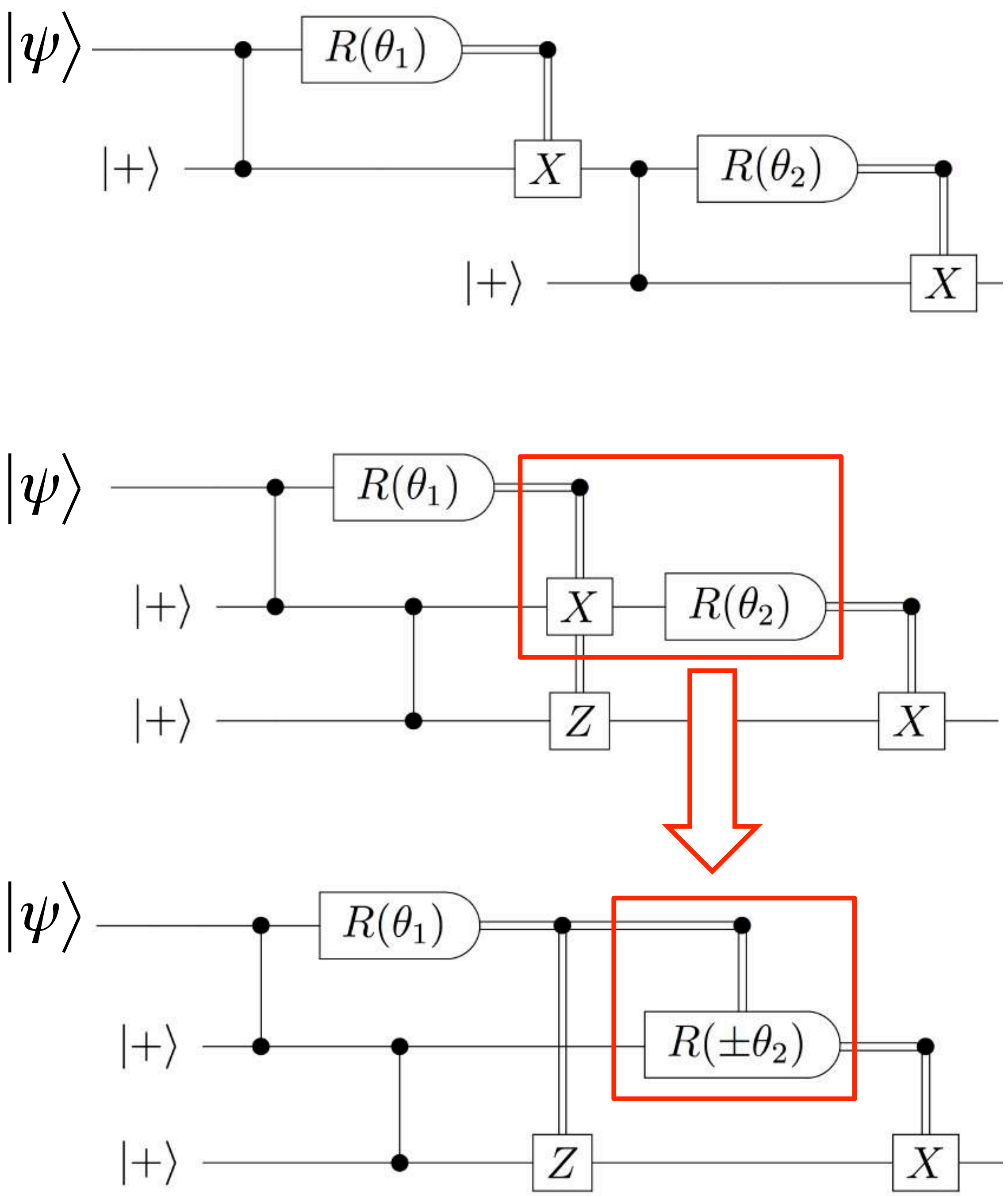
- Two gate teleportations, without final H gates, result in final state

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

- 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

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

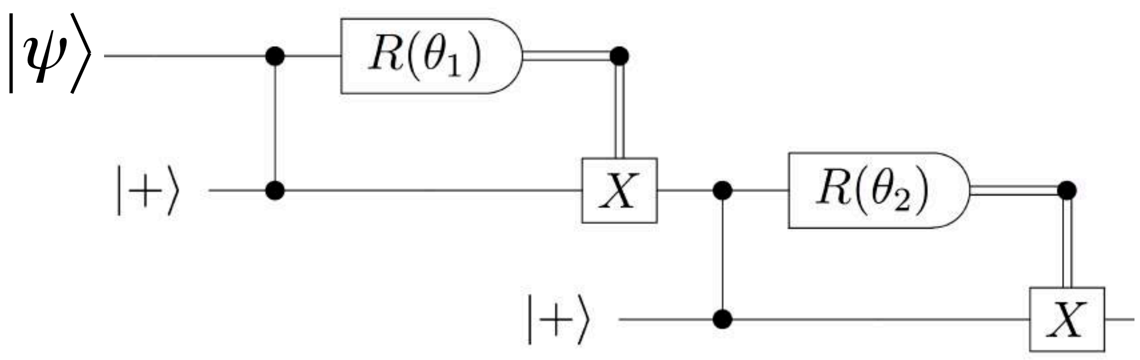
- Now commute X and CZ, which requires adding Z gate controlled by measurement 1

- Incorporate X correction into measurement angle of 2. When X is applied $\theta_2 \to -\theta_2$ because:

$$XR(\theta)X = R(-\theta)$$

MBQC: step-by-step

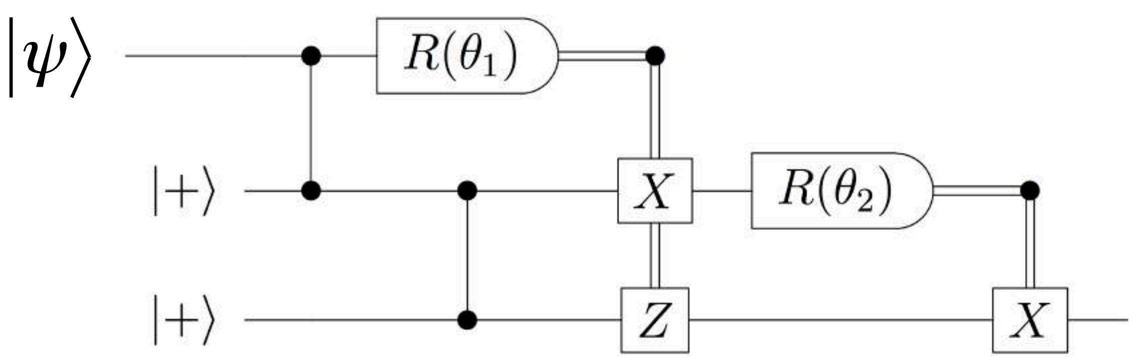
Now two different unitaries in sequence:



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

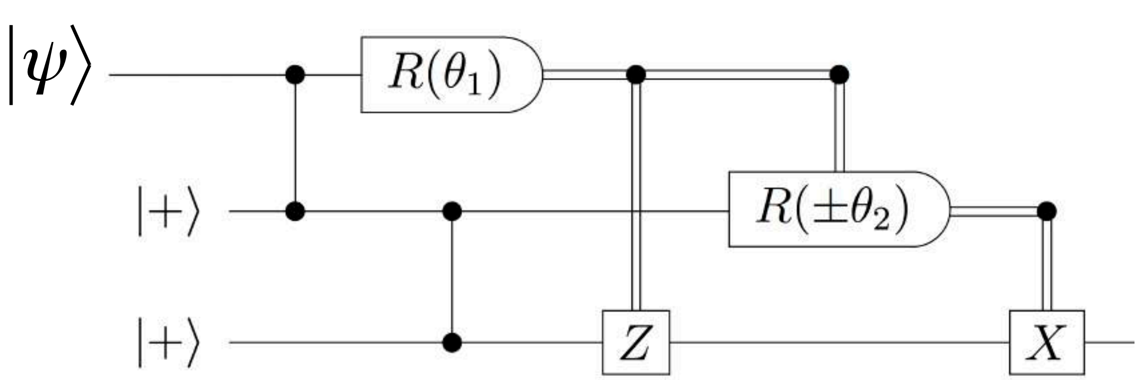
$$HU(\theta_2)HU(\theta_1)|\psi\rangle$$

- 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 $\theta_2 \rightarrow -\theta_2$ because:

$$XR(\theta)X = R(-\theta)$$



- By adapting measurement 2 according to outcome of 1, we can apply $HU(\theta_2)HU(\theta_1)|\psi\rangle$

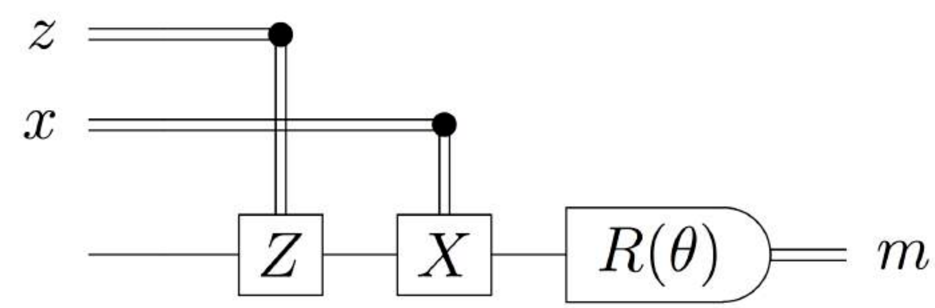
- Easy to extend to multiple single-qubit unitaries, and $\{HU(\theta)\}$ is universal set for 1 qubit

Adaptativity 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

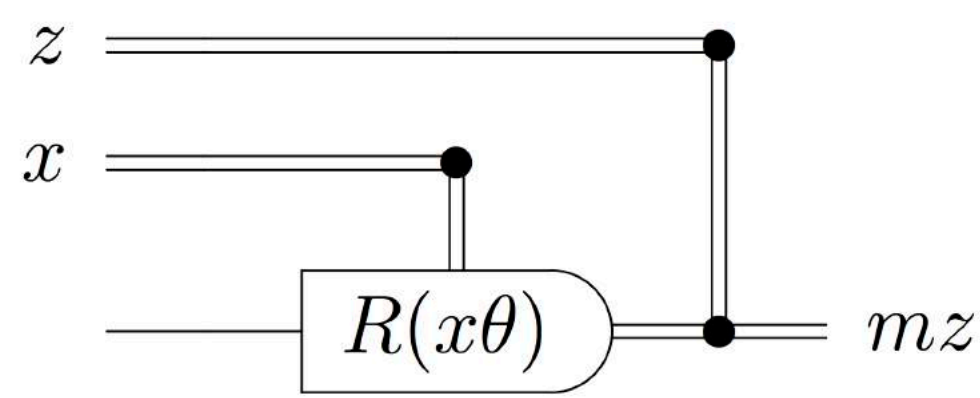
MBQC: step-by-step

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

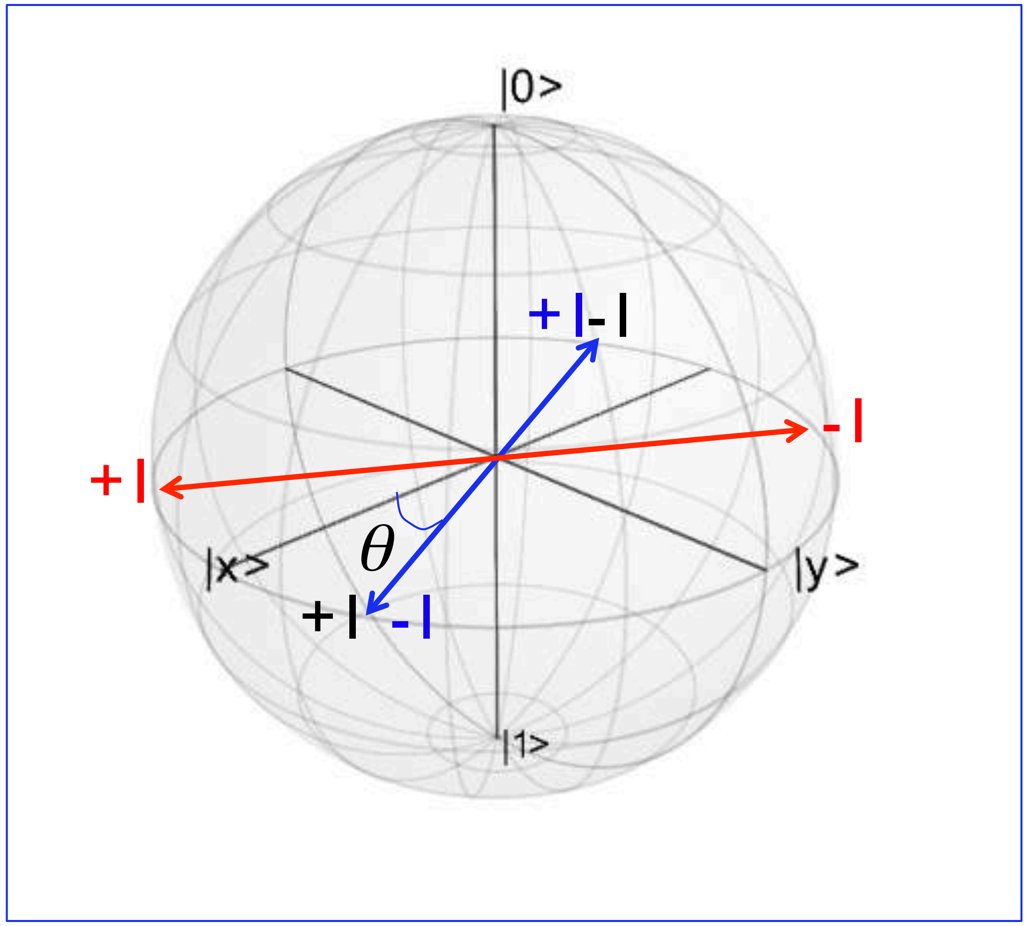
$$z, x \in \{-1, 1\}$$



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



X correction
Z correction

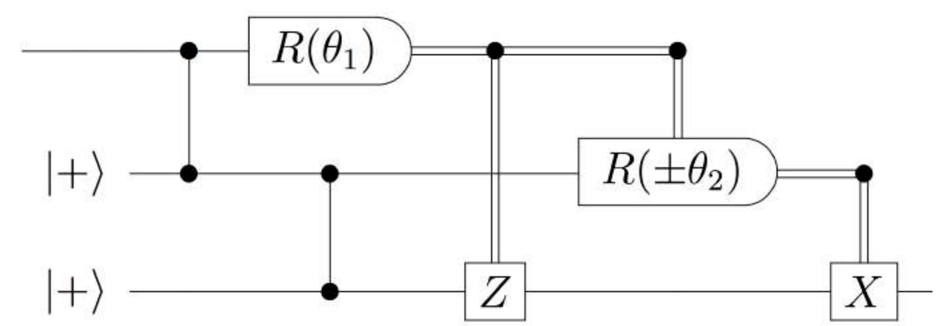


Classical control computer needs only store&update **sum modulo 2** of X and Z corrections of each qubit

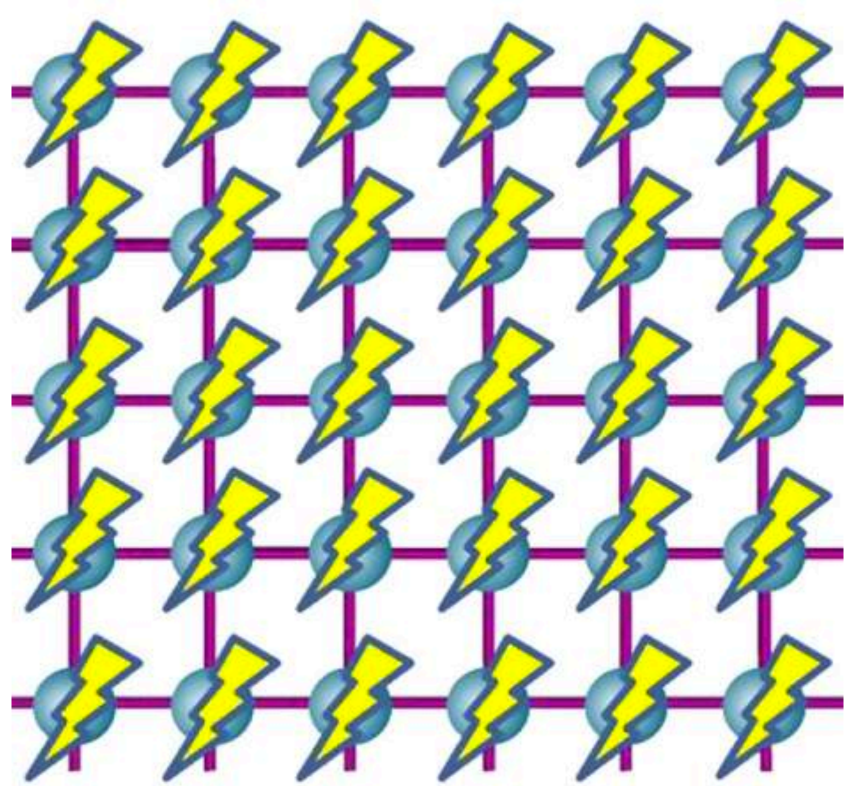
This **parity computer** is quite simple, but together with the quantum resource yields universal QC

MBQC: step-by-step

- Single-qubit inputs can be prepared from $|+\rangle$ by MBQC computation, so all qubits are initialized in $|+\rangle$ state



- Now the have all the ingredients for the **one-way model of MBQC**:



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

2- Sequence of single-qubit, adaptive measurements.

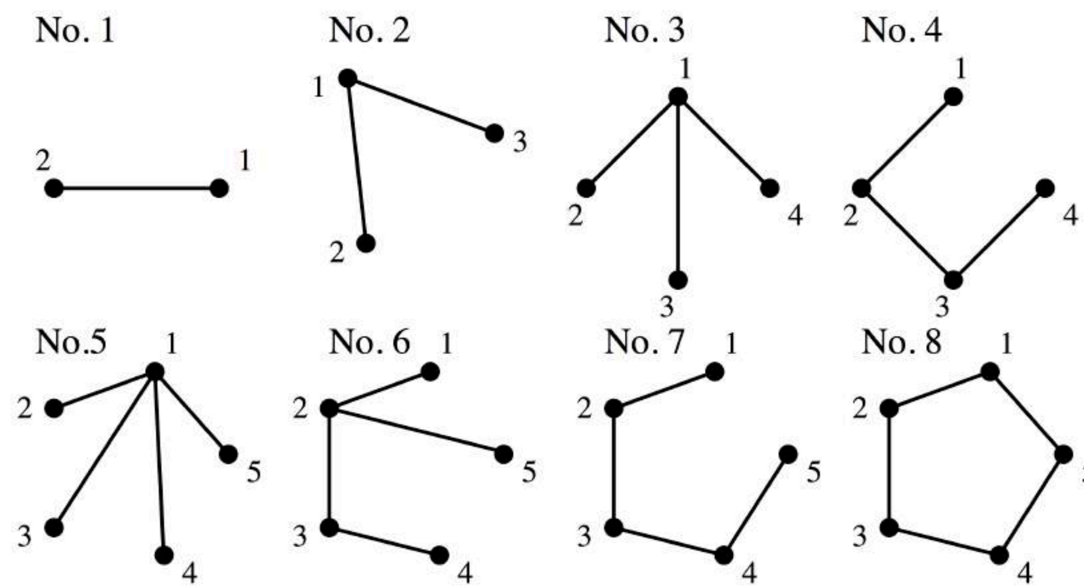
- Different algorithms may differ by the required entanglement structure, and by the sequence of different bases measured

Entanglement resources for MBQC

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

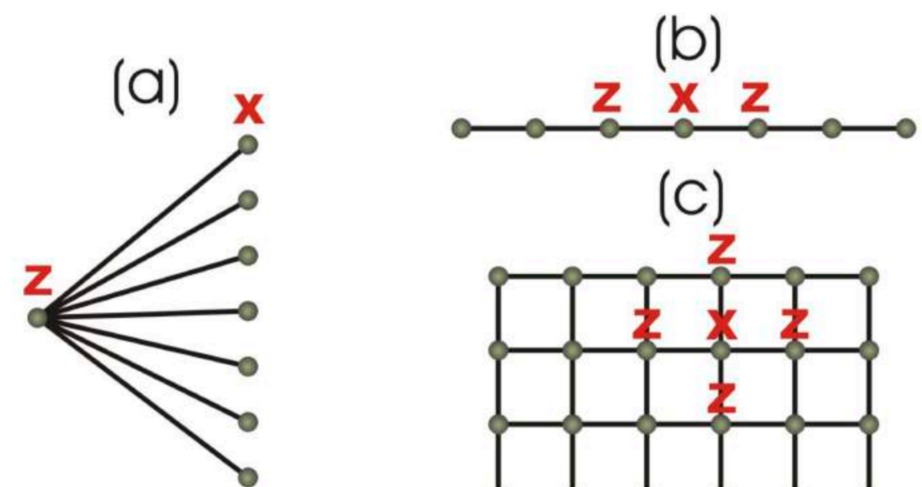
    1. Initialization of a set of qubits in $|+\rangle$ states
    2. CZ gates between neighboring vertices in a graph

- Examples:



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

- Alternative characterization of graph states:



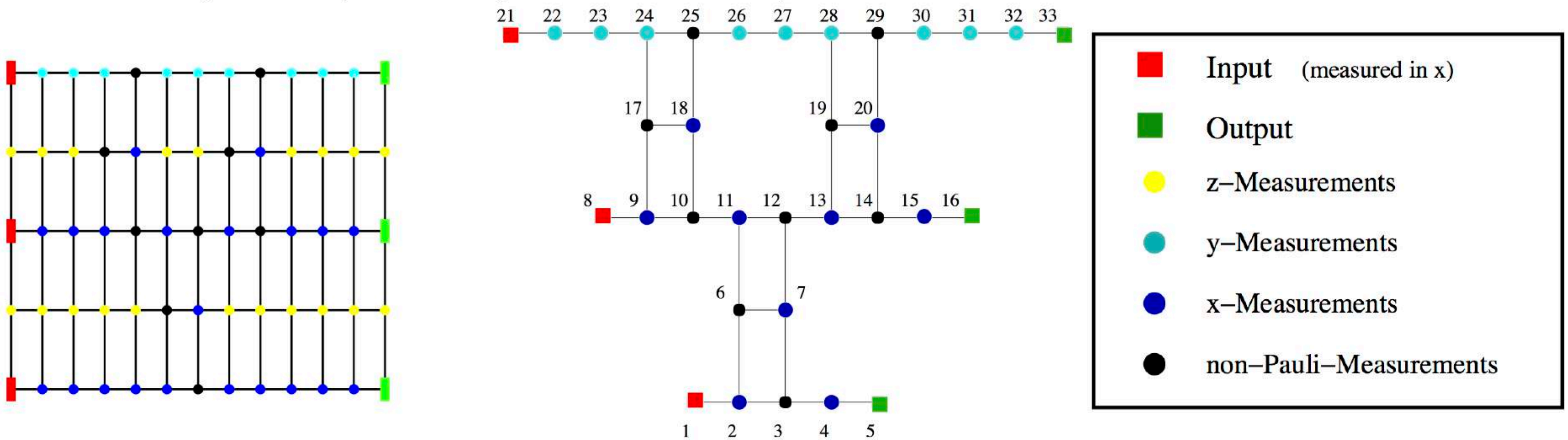
- Unique state which is simultaneous eigenstate (with eigenvalue 1) of set of operators

$$\left\{K_i = X_i \bigotimes_{j \text{ neighbor of i}} Z_j\right\}$$

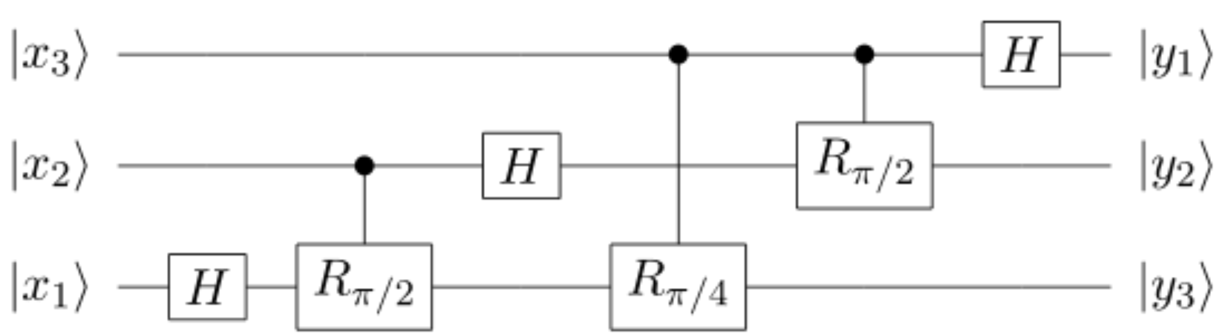
- Are there families of graph states which are universal for QC?

Entanglement resources for MBQC

M. HEIN, W. DÜR, J. EISERT, R. RAUSSENDORF, M. VAN DEN NEST and H.-J. BRIEGEL



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

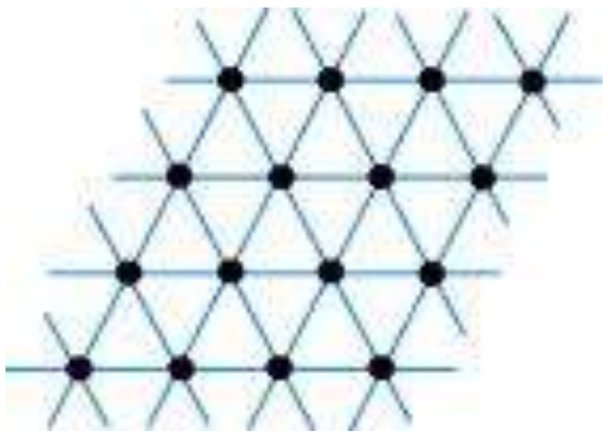
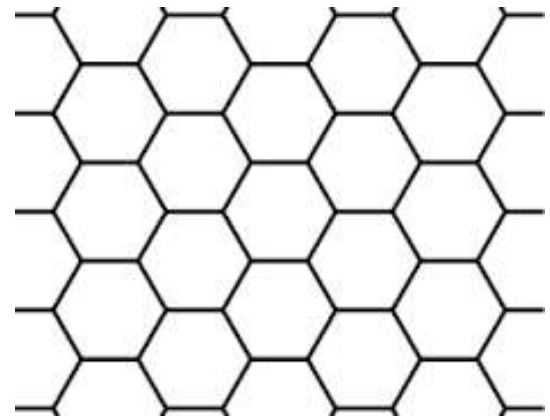
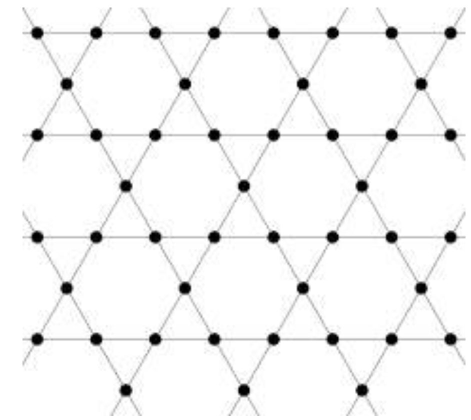


3-qubit QFT

- 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

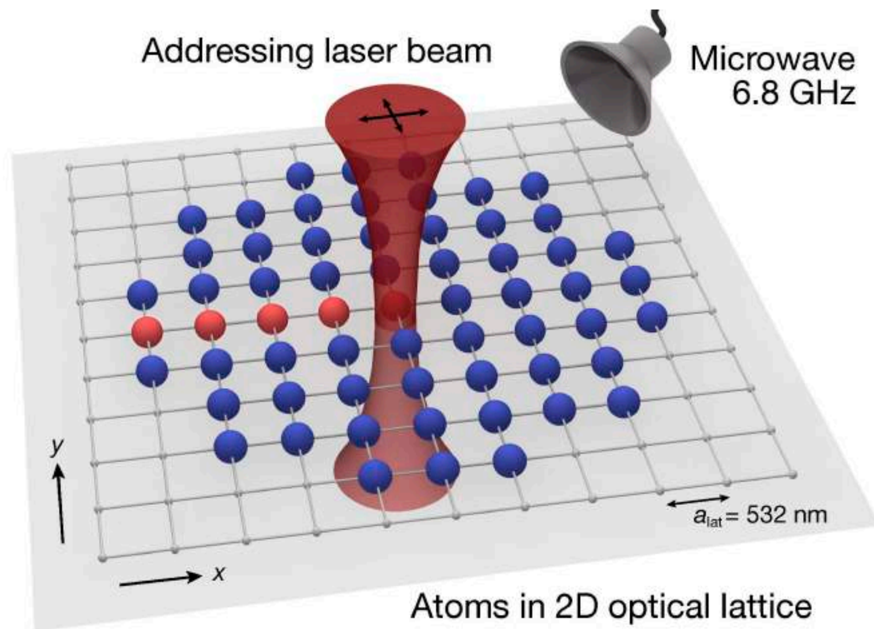
[Wei, Affleck, Raussendorf PRL 106, 070501 (2011)]

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

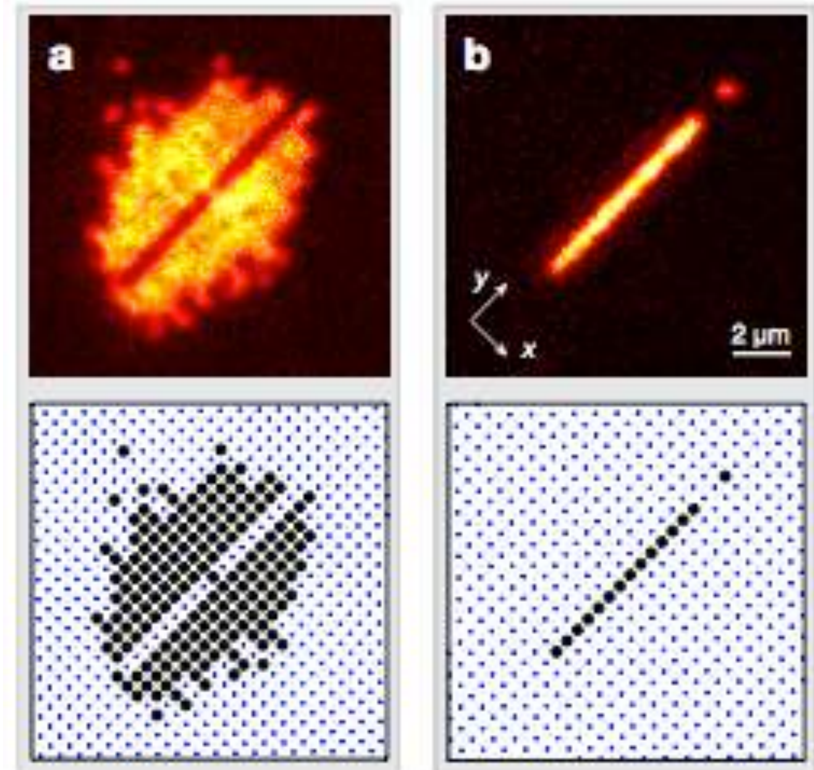
[Markov, Shi, SIAM J. Comput. 38, 963 (2008)]

MBQC - implementations

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

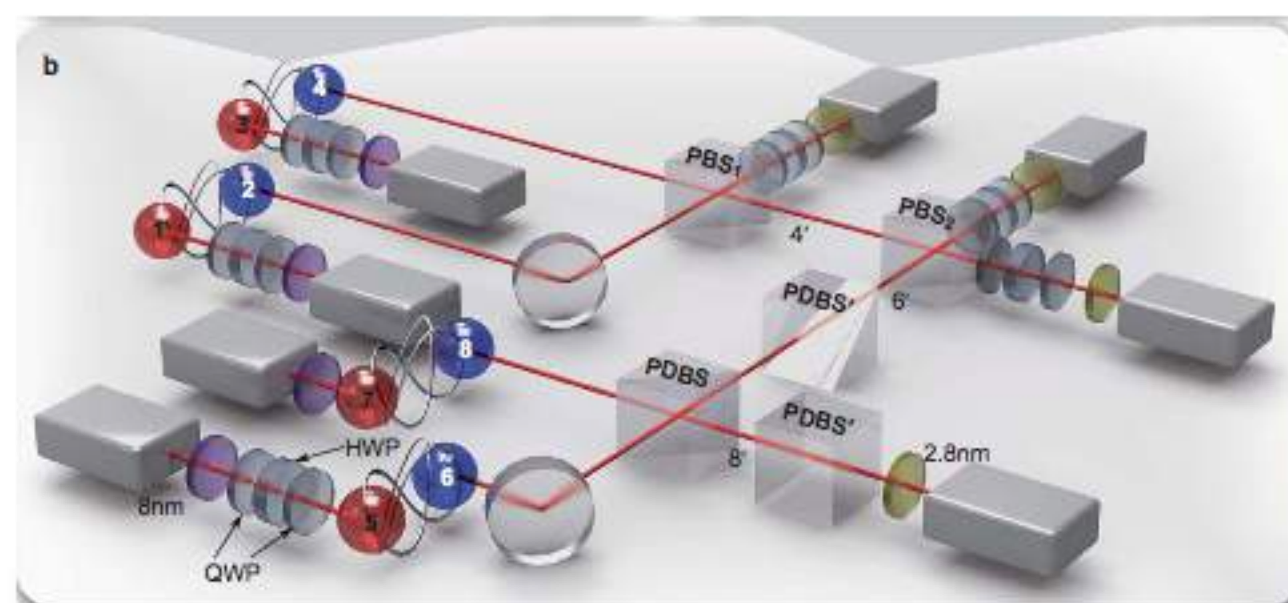


from: Weintenberg et al., *Nature* 471, 319 (2011)



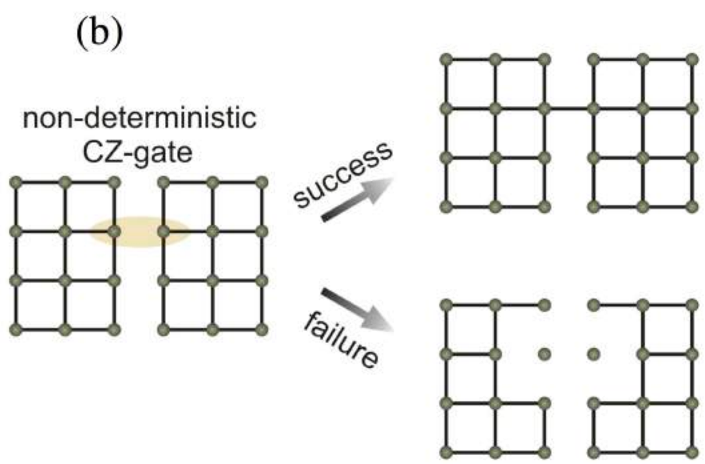
- Proof-of-principle implementations using photons
  - Topological error-correction using eight-photon cluster states

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

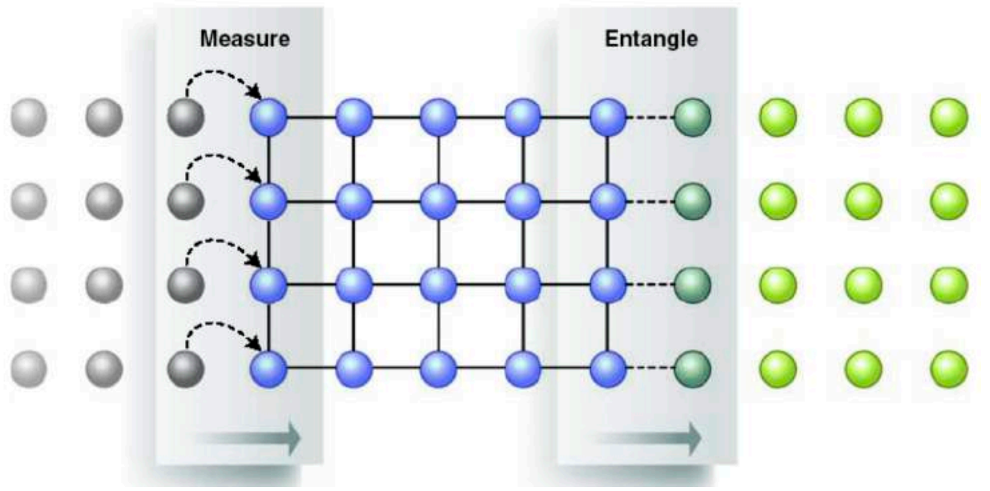


MBQC - implementations

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



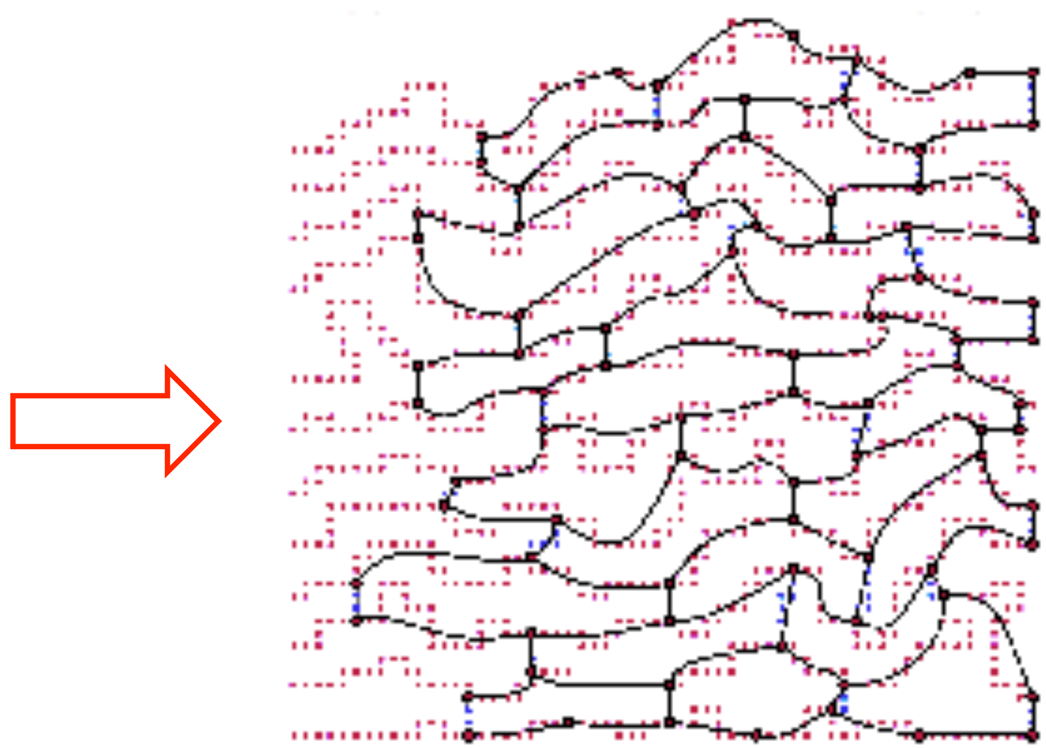
from: Briegel *et al.*, *Nat. Phys.* 5 (1), 19 (2009)



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

- Schemes for adapting imperfect clusters for MBQC

(a) initial faulty square lattice

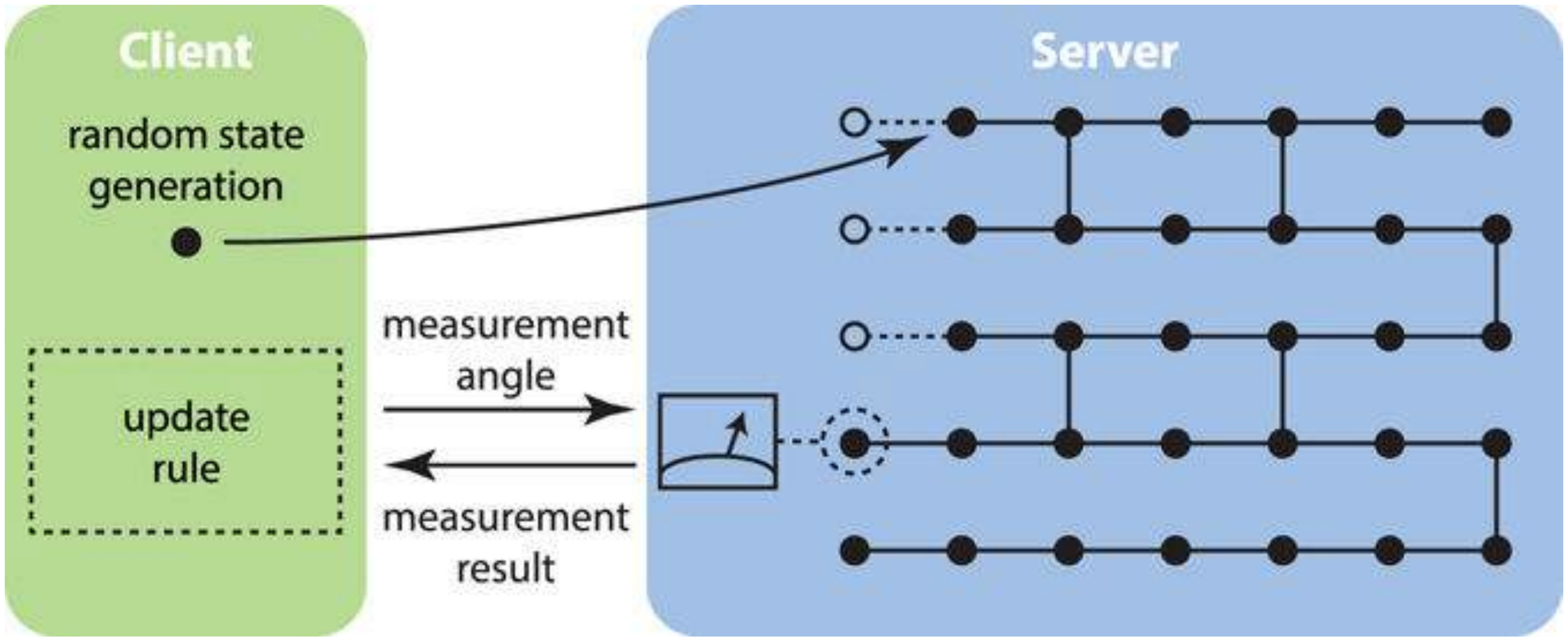


(f) deletion and contraction (Q.1 & Q.2)

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

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]

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)]