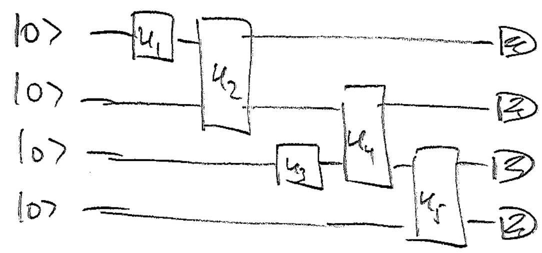


Measurement based quantum computation

(Review: quant-ph/0508124)

Standard model of quantum computation: <u>Circuit model:</u>



* N-qubit "quantum register" $(\mathbb{C}^2)^{\otimes N}$

1. initialize to $|0\rangle^{\otimes N}$

2. apply one- and two-qubit "gates" (= unitaries) from "universal gate set", e.g. $R_X(\phi) = e^{-i\phi/2\, X}$, $R_Z(\phi) = e^{-i\phi/2\, Z}$,

   $CZ = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$ ("Controlled-phase")

3. measure (a subset of) qubits in Z-basis $\{|0\rangle, |1\rangle\}$

   $\rightarrow$ output of computation!

Requires to keep register <u>coherent</u> and ability to apply two-qubit unitaries (and interactions are typ. complicated)

$\rightarrow$ alternative models: adiabatic QC, topological QC, dissipative QC, measurement based QC, ...

Measurement based q. computation (MBQC):

1. Prepare special 2D state ("cluster state"): ground state of gapped local Ham.!

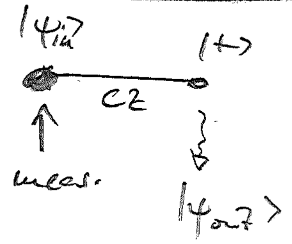
2. Perform a sequence of (adaptive) one-qubit meas.

3. Output of QC function of meas. outcome

→ No interactions needed after cluster state is prepared!

(Note: Also known as "one-way quantum computing")

Elementary "gadget":



- Consider $|\psi_{in}\rangle_1 |+\rangle_2$ $\quad (|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle)$
- Apply a CZ
- measure 1 in basis $\left(e^{+i\phi/2}|0\rangle \pm e^{-i\phi/2}|1\rangle\right)/\sqrt{2}$

Outcome:

$$|\psi_{in}\rangle_1 |+\rangle_2 = \alpha|0\rangle_1|+\rangle + \beta|1\rangle|+\rangle$$

$$\xrightarrow{CZ} \alpha|0\rangle|+\rangle + \beta|1\rangle|-\rangle$$

$$\xrightarrow{meas.} |\psi_{out}\rangle = \alpha e^{-i\phi/2}|+\rangle \pm \beta e^{+i\phi/2}|-\rangle$$

with m the measurement outcome,

and $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ the <u>Hadamard gate</u>, we find...

Note: H changes betw. X and Z basis:

$$H|+\rangle = |0\rangle, \quad H|0\rangle = |+\rangle$$

$$H|-\rangle = |1\rangle, \quad H|1\rangle = |-\rangle$$

$$HXH = Z, \quad HZH = X$$

$$H^2 = \mathbb{1}$$

$$|\psi_{out}\rangle = \alpha e^{-i\phi/2}|+\rangle \pm \beta e^{+i\phi/2}|-\rangle$$

$$= H\left[\alpha e^{-i\phi/2}|0\rangle \pm \beta e^{+i\phi/2}|1\rangle\right]$$

$$= H Z^m R_z(\phi)|\psi_{in}\rangle$$

$$= X^m H R_z(\phi)|\psi_{in}\rangle$$

$\Rightarrow$ Protocol implement 1-qubit-gate $HR_z(\phi)$ up to a Pauli error!

Concatenate two steps:

<u>Step 1</u>: Angle ϕ_1 $\longrightarrow$ Outcome m_1

<u>Step 2</u>: Angle $(-1)^{m_1}\phi_2$ $\rightarrow$ Outcome m_2

$$\Rightarrow |\psi_{out,2}\rangle = X^{m_2} \underbrace{H \underbrace{R_z((-1)^{m_1}\phi_2) X^{m_1}}_{= X^{m_1} R_z(\phi_2)}}_{= Z^{m_1} H} H R_z(\phi_1)|\psi_{in}\rangle$$

$$= X^{m_2} Z^{m_1} \underbrace{H R_Z(\phi_2) H}_{= R_X(\phi_2)} R_Z(\phi_1) |\psi_{in}\rangle$$

$$= X^{m_2} Z^{m_1} R_X(\phi_2) R_Z(\phi_1) |\psi_{in}\rangle .$$

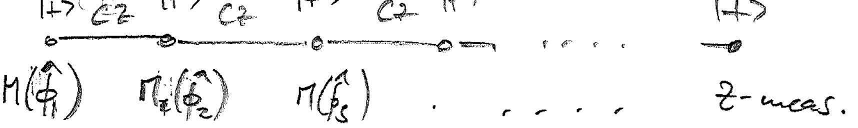
Can be iterated:

$$X^{m_4} Z^{m_3} R_X(\tilde{\phi}_4) R_Z(\tilde{\phi}_3) X^{m_2} Z^{m_1} R_X(\phi_2) R_Z(\phi_1) |\psi_{in}\rangle$$

$$= X^{m_4 \oplus m_2} Z^{m_3 \oplus m_1} R_X(\underbrace{(-1)^{m_1} \tilde{\phi}_4}_{\phi_4}) R_Z(\underbrace{(-1)^{m_2} \tilde{\phi}_3}_{\phi_3}) R_X(\phi_2) R_Z(\phi_1) |\psi_{in}\rangle$$

Read-out: We can simply measure in the Z basis (and correct for the X error!).

Protocol for 1-qubit computation, starting in state $|+\rangle$:



But: We can as well first do all CZ and then measure.
Moreover, the CZ commute – order irrelevant.

$\longrightarrow$ "cluster state"

This is the <u>unique ground state</u> of

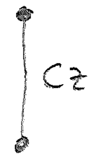
$$H = -\sum h_i \,, \qquad h_i = Z_{i-1} \otimes X_i \otimes Z_{i+1}$$

(<u>Proof</u>: Homework)

→ computation based on G.S. & 1-qubit-meas.

How can we go <u>beyond 1 qubit</u>?

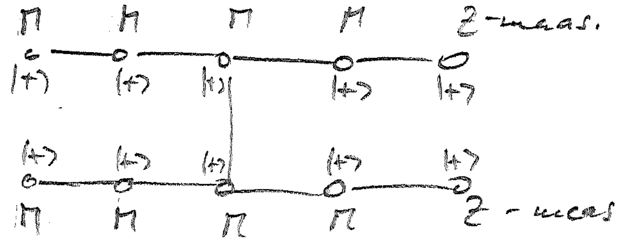
two-qubit input $|\psi_{in}\rangle$ $\xrightarrow{CZ}$



$\longrightarrow |\psi_{out}\rangle = CZ\,|\psi_{in}\rangle$

(without measurement!)

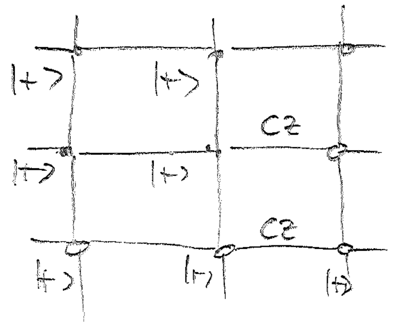
→ two-qubit operations in a circuit via



⇒ Can again be based on <u>cluster state</u> on the right underlying graph! (This is <u>again</u> G.S. of L.H. $H = -\sum h_i$ with $h_i = X_i \otimes \bigotimes_{j \in \mathrm{neigh}(i)} Z_j$ → homework!)

→ Any q. computation can be implemented by first preparing a cluster state & then doing 1-qubit-meas!

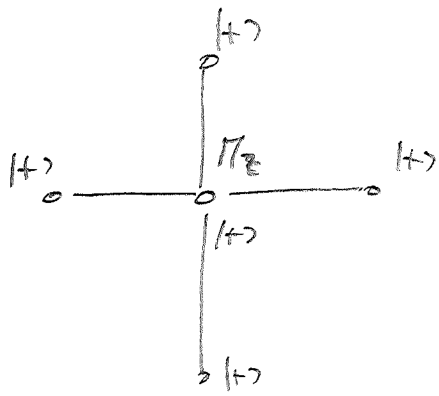
Can we also do this on e.g. a square lattice:



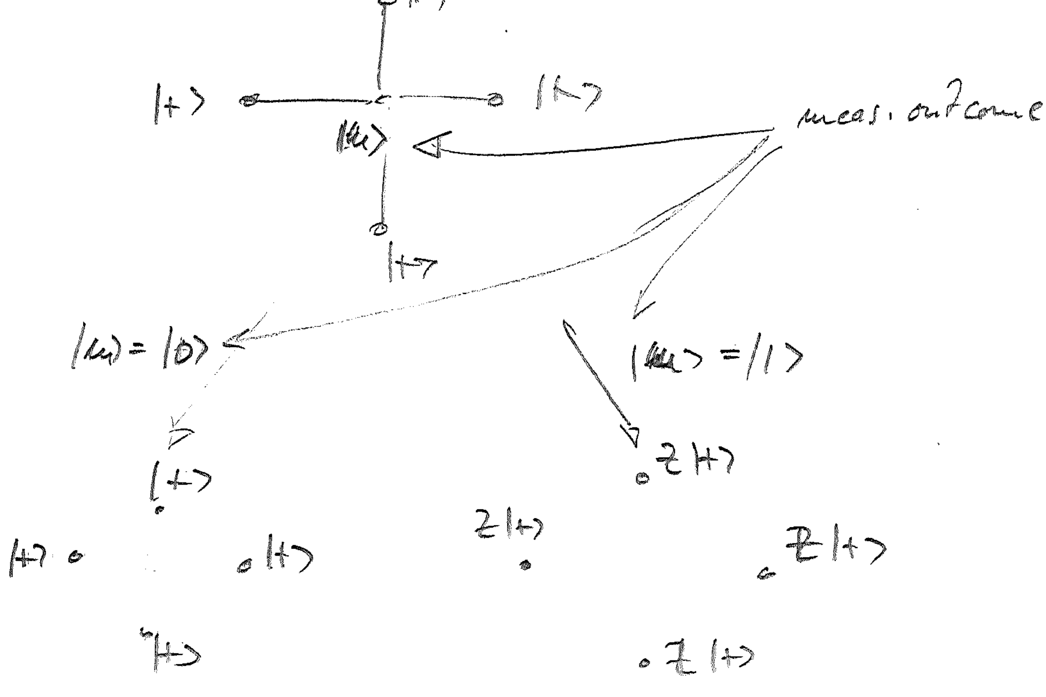
↔ $H = -\sum h_i$,

$$h_i = \begin{array}{ccc} & Z & \\ Z & X & Z \\ & Z & \end{array}$$

→ Z-meas. allow to erase sites from a cluster state:



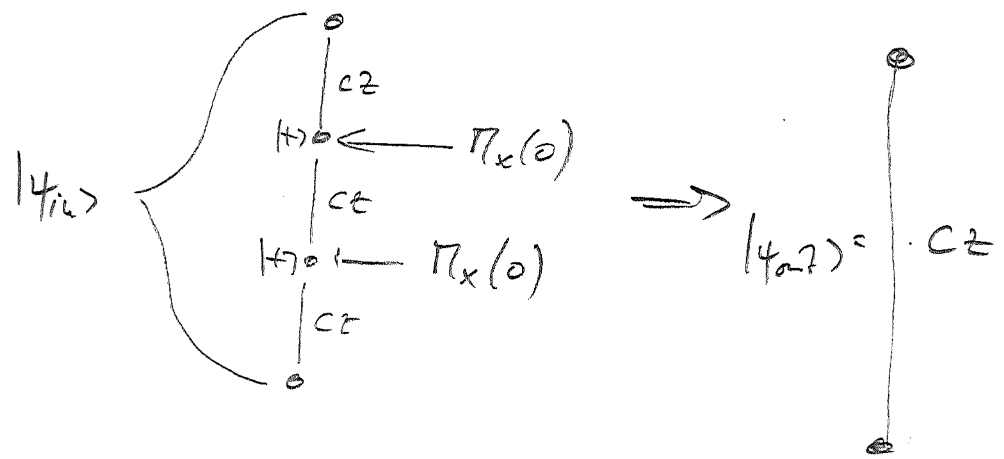
Meas. commutes w/ CZ → equiv. to



→ qubit <u>removed</u> & Z-errors on neighbors

→ Z err. commute w/ CZ ⟹ we can use this to "etch" a circuit into a regular (e.g. 2D square lattice) cluster state! (only need to adapt meas. bases to Z errors)

<u>But</u>: We need a different way to do 2-qubit gates (on the square lattice, at least):



(up to Pauli errors)

(→ homework!)

<u>Full protocol:</u>

- Start from cluster state
- "etch" circuit via Z meas.
- perform sequence of XY-plane-meas. to implement circuits (adaptive basis!)
- measure output in Z basis & interpret according to prev. meas. outcomes (≡ X/Z errors)

Remarks:

- adaptive meas. only requires comp. of parities
  - → computationally very easy
- many meas. patterns can be implemented non-adaptively
- in part.: any Clifford circuit (generated by $\{H, S, CZ\}$, with $S = \begin{pmatrix} 1 & \\ & i \end{pmatrix}$) can be implemented by non-adaptive measurements

- non-adaptive measurements can be done in parallel – potential parallelization of Q. Comp.
- in certain cases, a logarithmic number of layers is enough. (Note: class. side-processing still requires poly time!)

- MBQC has a particularly nice interpretation in terms of teleportation and PEPS (→ homework)

<u>A beautiful application</u> of <u>MBQC</u> : "<u>Blind q. computation</u>"
(Broadbent, Fitzsimons, Kashefi, arXiv: 0807.4154)

Bob has full QC, Alice can only prepare single qubits. Can Bob perform a QC for Alice w/out knowing comp. & outcome?

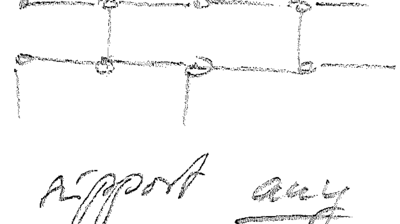
<u>Idea:</u> A prepares $|+\rangle$ states and sends them to Bob, who entangles them w/ CZ & performs the meas. A tells him.

<u>Trick:</u> A prepares $|\phi\rangle = |0\rangle + e^{i\phi}|1\rangle$ instead w/ different rand. ϕ for each qubit $\longrightarrow$ cluster has random Z rotations at each site.

<u>Alice</u> can <u>adapt</u> the meas. basis to the rotation, while for <u>Bob</u>, the meas. looks completely random. Bob reports outcomes & Alice adapts the meas. $\rightarrow$ no info revealed!

The <u>final Z meas.</u> is also random to Bob since he does not know the X errors!

Bob could still learn sth. from the <u>shape</u> of the cluster $\longrightarrow$ use universal "brickwork state"



which can support <u>any</u> Q.C. !