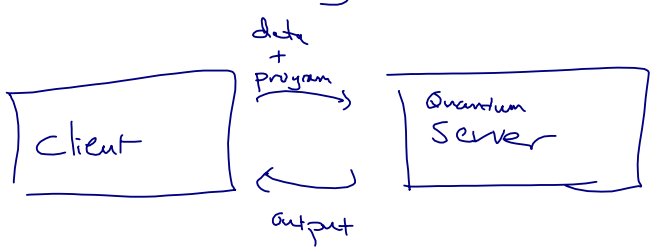
Blind Quantum Computing



Blind means the quantum serve must not know:

- the input data (hidden input quantum state)
- the operations being performed (e.g. the gates of the program)
- the output data (hidden output quantum state)
- any intermediate data (any classical data collected by the server must not be correlated w/ the input data, output data, or with the computation.

Some data must still be leaked: the time & space resources used for the computation (as an upper bound).

We introduce BQC protocols within a model of quantum comp. called measurement based quantum computing.

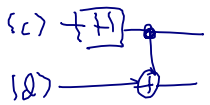
MBQC $\Longleftrightarrow$ Gate model quantum computing.

In MBQC you begin w/ entangling operations to generate a large state. Computations are then performed only by making measurements in different bases. This means that entangling operations can be performed seperately for any particular program.

This is done w/ a generalized version of quantum teleportation.

Quantum Teleportation

Uses entanglement and then measurements to move a quantum state between registers.



for $|c\rangle = |d\rangle = |0\rangle$ produces $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

For other input basis states it produces:

Bell states $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = X \otimes I\, |B_{00}\rangle$

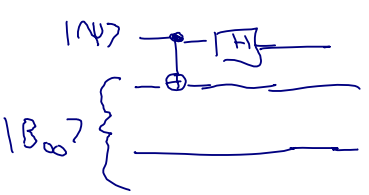
$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = Z \otimes I\, |B_{00}\rangle$

$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = iY \otimes I\, |B_{00}\rangle$

$\Big\} |B_{cd}\rangle = Z^c X^d \otimes I\, |B_{00}\rangle$

Start in state $|\Psi_0\rangle = |\psi\rangle |B_{00}\rangle \xrightarrow{\text{teleport}} |\Psi_f\rangle = |c\rangle |d\rangle |\psi\rangle$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$



$= |\Psi_2\rangle = \frac{1}{2}\Big\{ |00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \Big\}$

$= |c\rangle|d\rangle (X^d Z^c |\psi\rangle)$

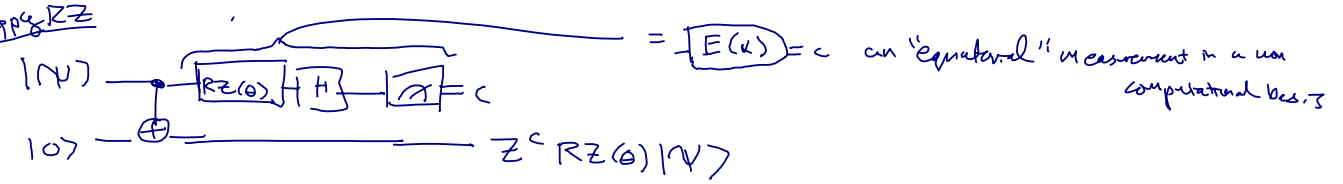
Measuring the first two qubits tells us what corrections to apply as

$|c\rangle|d\rangle Z^c X^d (X^d Z^c) |\psi\rangle = |c\rangle|d\rangle|\psi\rangle$

This is a kind of SWAP operation. Note we could have stored c & d classically and applied the corrections later.

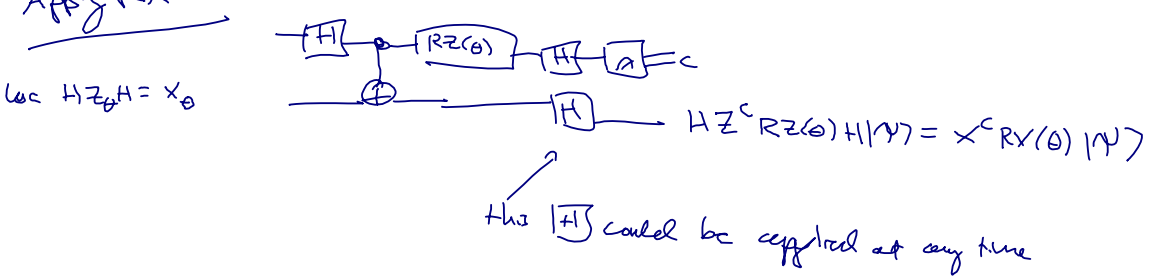
It turns out that any gate can be implemented as a simple entangle then measure and track corrections structure.

Apply RZ



can "equivalent" measurement in a non computational basis.

Apply RX



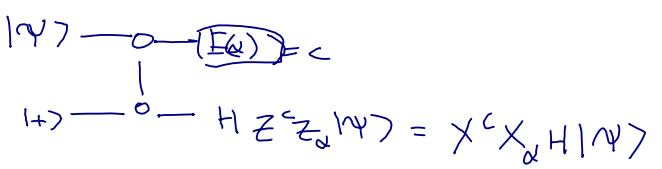
Use $HZ_\theta H = X_\theta$

this H could be applied at any time

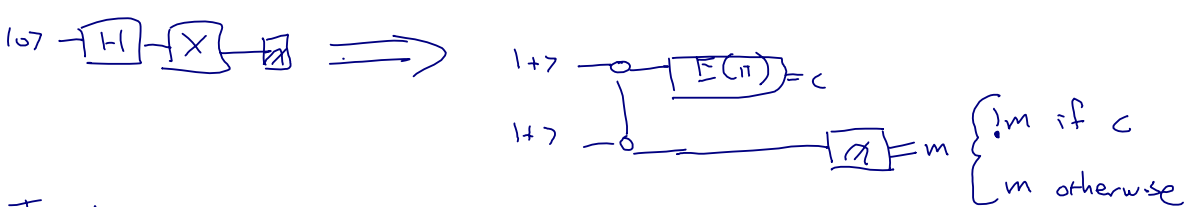
Thus we are universal for single qubit gates because any

$$U = R_X(\alpha) R_Z(\beta) R_X(\gamma) \text{ for some } \alpha, \beta, \gamma$$

In MBQC literature the above examples are typically rewritten in terms of CZ using with all initial states as $|+\rangle$.



Example



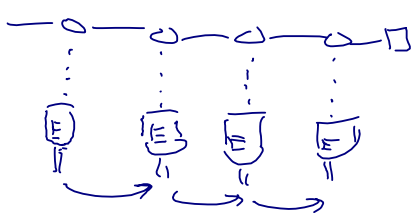
In MBQC a condensed notation is used where we represent this as a graph:

- Vertices are qubits initialized in the $|+\rangle$ state.
- Edges are CZ operations
- Labels are the angles to measure

} These are called "graph states"

An ordering is applied to the graph that indicates how feed-forward should work.

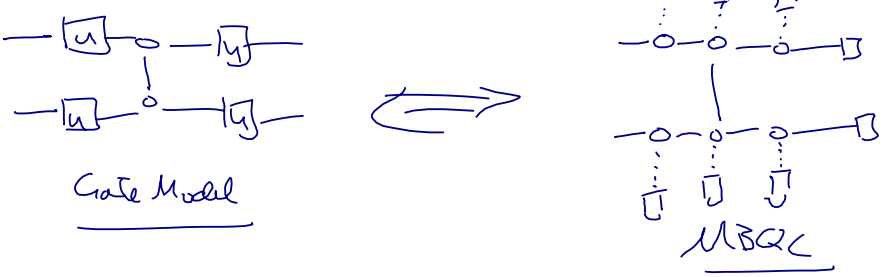
This notation allows us to describe chaining operations:



for composing single qubit unitaries.

We also have a CZ in MBQC between qubits by just using the CZ from the initial state prep.

Ex

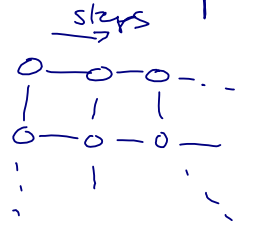


CZ is equivalent to CNOT w/ some single qubit gates and so

arbitrary 1Q unitaries + CNOT $\Rightarrow$ MBQC is universal

Note that CZ's commute e.g. $CZ_{ab} = CZ_{ba}$ and so the order in which the CZ's are applied to make the original state doesn't matter.

This one can do universal computation w/ a "cluster state"



where the first step is to apply CZ's to "undo" the CZ's that don't happen in the computation

Blind QC Protocol (Broadbent, Fitzsimons, Kashefi 2009)

Client Alice

Classical computer
+
can prepare and send single qubits with randomly chosen states from $\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right) \mid \theta = 0, \pi/4, 2\pi/4, \ldots 7\pi/4\right\}$

Server Bob

Quantum Computer

The idea "distributed MBQC"

Alice

① prepares qubits → **Bob** ② Entangles a "brickwork state"

③ computes feedforward → ④ measures

w/ randomness added to obscure Bob's view

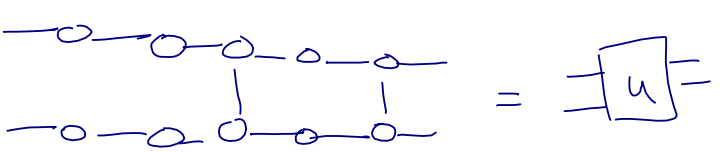
Alice can also detect interference from Bob w/ high prob or correct it w/o detection

Authentication is done by Alice encoding her input in a Quantum error correcting code w/ some "trap" qubits that detect interference.

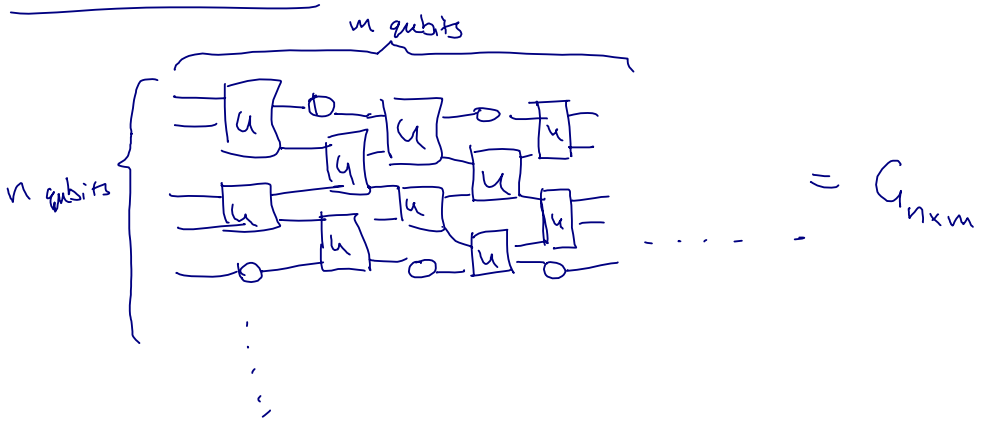
Input security

The first MBQC step w/ a cluster state is to knock out certain CZ gates. We need to prevent Bob reading this info by choosing a single graph state for Bob to entangle that works for any computation Alice wants to do.

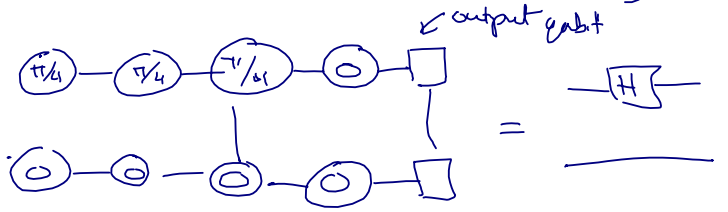
Let "brickwork" unit cell be:

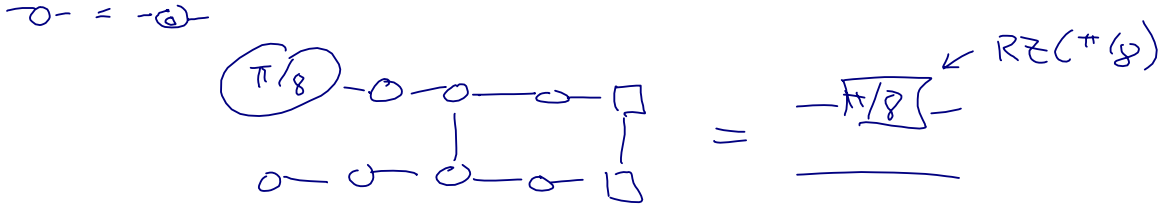


The brickwork state is:

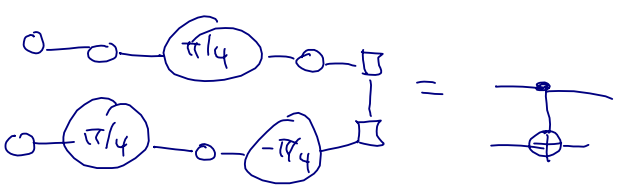


This state is universal w/ only changing the choices of the measurements applied to each qubit. We show this by constructing the set $\{H, CNOT, \pi/8\}$



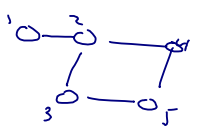


CNOT we saw before



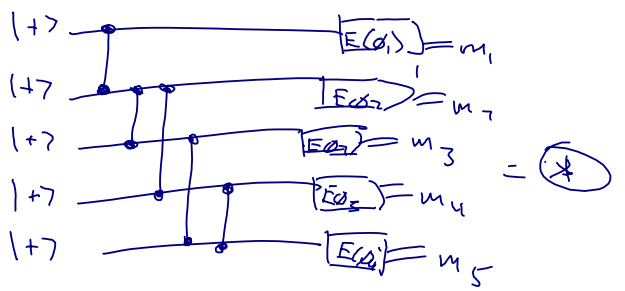
Thus if Bob entangles a brickwork state he knows nothing about the protocol Alice wants to implement and yet he can still perform (approximately) universal quantum computation.

Hiding information example,

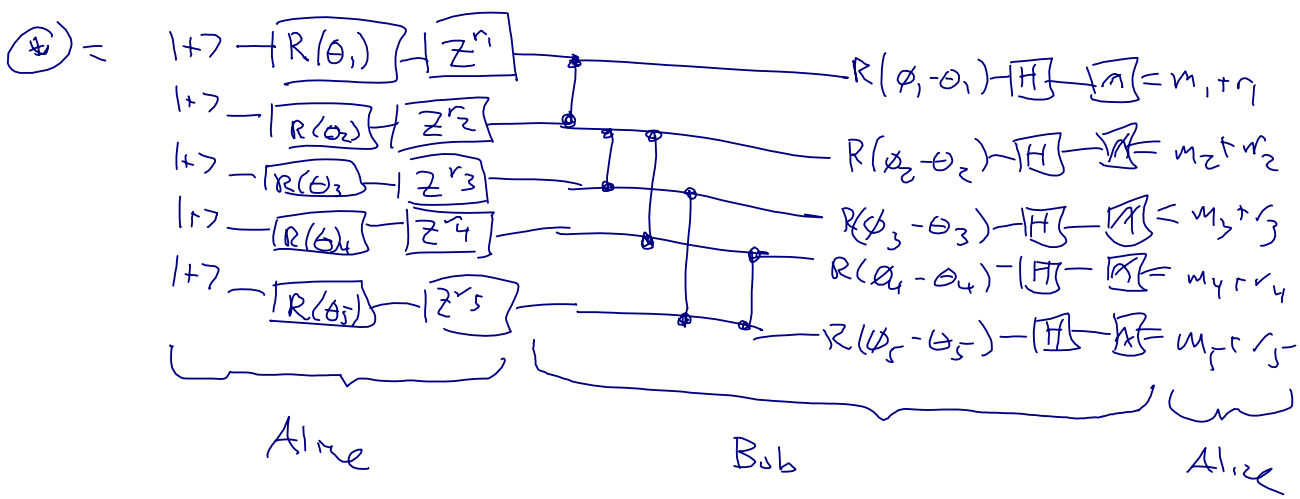


by MBQC def

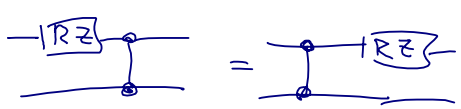
$\Rightarrow$



We are going to "randomize" the ϕ_i and m_i to encrypt the computation.



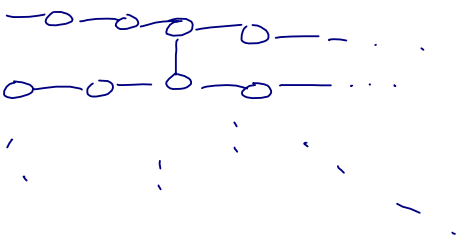
Where we have used the fact that RZ and Z commute through:



Uniform random θ_i and r_i

Protocol sketch

Alice $\xrightarrow{|\psi_i\rangle}$ Bob



For each qubit i:

(1) Alice computes $\delta_i = \phi_i + \theta_i + \pi r_i$

(2) Bob measures b_i

(3) Alice computes $m_i = b_i \oplus r_i$

And in this way Alice performs a MBQC w/ Bob's qubits.

Claim Bob learns nothing during execution;
(except the size $n \times m$)

Bob gets for each qubit $|\psi_i\rangle = \left(|0\rangle + e^{i(\theta_i + r_i \pi)}|1\rangle\right)/\sqrt{2}$ $r \in_R \{0,1\}$

and $\delta_i = \phi_i + \theta_i + \pi r_i$ $\theta_i \in \{0, \ldots \pi/4\}$

Define Blindness as

(1) The classical info (δ_i's) that Bob has are independent from the quantum states

(2) Given Bob's classical info, the state Bob obtains is fixed and independent of Alice's input.

(1) θ_i is uniform random and so $\theta_i + \pi r_i$ is also and so δ_i is also

(2) Each qubit Bob has is in the state:

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{r_i} e^{i(\delta_i - \phi_i)}|1\rangle\right)$$

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{r_i} e^{i(\delta_i - \phi_i)}|1\rangle\right)$$

Lets look at the density matrix for the second where r_i is chosen uniformly from $\{0,1\}$ then

$$r_i = 0 \Rightarrow |\psi_i(r_i=0)\rangle\langle\psi_i(r_i=0)| = \frac{1}{2}\begin{pmatrix} 1^2 & e^{-i(\delta_i-\phi_i)} \\ e^{i(\delta_i-\phi_i)} & 1 \end{pmatrix} = \rho_0$$

$$r_i = 1 \Rightarrow \frac{1}{2}\begin{pmatrix} 1 & -e^{-i(\delta_i-\phi_i)} \\ -e^{i(\delta_i-\phi_i)} & 1 \end{pmatrix} = \rho_1$$

$$\rho = (\rho_0 + \rho_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \underline{\mathbb{1}}$$ ← this is a coin flip on outcomes

Thus Bob has a maximally mixed state, with no info.

The proves blindness,

Authentication and fault-tolerance are also possible.