Alice sends measurement to Bob. If it's 1, Bob applies Z to ...

Julia Kempe : kempe@post.tau.ac.il

4 homework assignments.

Axioms of quantum:

① States - vectors in complex Hilbert space

② Dynamics - unitary matrices, $U \cdot U^{\dagger} = \mathbb{1}$ $(U^{\dagger} = \bar{U}^{T})$ complex conjugate [So the ... are ...

③ Measurements - "collapse" the state

ket: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

bra: $\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^{\dagger} = (1\ 0)$

bra-ket $\langle 0|0\rangle = (1\ 0) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$

$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$. $\Rightarrow$ Probability of seeing "0" is $|\alpha|^2 = |\langle 0|\Psi\rangle|^2$

We can choose in what basis to measure. For example, the $|\pm\rangle$ basis: $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

In this basis, the probability of seeing "+" when measuring $|\langle + |\Psi\rangle|^2$.

Say U is a unitary, such that $U|+\rangle = |0\rangle$, $U|-\rangle = |1\rangle$

$$|\langle + |\Psi\rangle|^2 = |\langle + | \underbrace{U^{\dagger} U}_{\mathbb{1}} |\Psi\rangle|^2 = |\langle 0 | U\Psi\rangle|^2$$

[In this case we have $U = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H^{\dagger}$]

Partial measurement: measuring only a part of the qubits of ...

$|\varphi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$. "0" $\rightarrow |00\rangle$. "1" $\rightarrow |11\rangle$

If we want to measure it over a different basis, say $|\pm\rangle$:

$H \otimes \mathbb{1} \, |\varphi\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle - |11\rangle)$

"0" $\rightarrow |0\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ "1" $\rightarrow |1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

BB84 (Bennett - Brassard) [Quantum Cryptography]

Key distribution, for one-time pad.

① Alice sends randomly one of the following u to Bob: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$

② Bob chooses a random basis from $\{\underset{\text{"0"}}{|0\rangle}, \underset{\text{"1"}}{|1\rangle}\}, \{\underset{\text{"1"}}{|+\rangle}, \underset{\text{"0"}}{|-\rangle}\}$.

* Notation: $|0\rangle : \uparrow$, $|1\rangle : \rightarrow$, $|+\rangle \searrow$, $|-\rangle : \nearrow$, $\{|0\rangle, |1\rangle\} : +$, $\{|+\rangle, |-\rangle\} : \times$

names	A	B	Result	Announce	
"0"	$\uparrow$	$+$	0	$+$	✓
"1"	$\searrow$	$\times$	1	$\times$	✓
"0"	$\nearrow$	$+$	assume 1	$\times$	discard
"0"	$\uparrow$	$\times$	0	$+$	discard
"1"	$\rightarrow$	$+$	1	$+$	✓
"0"	$\nearrow$	$+$	1	$\times$	discard
"1"	$\rightarrow$	$\times$	assume→1	$+$	discard
"1"	$\searrow$	$\times$	~~assum~~ 1	$\times$	✓
"0"	$\uparrow$	$+$	0	$+$	✓
"0"	$\nearrow$	$+$	assume→0	$\times$	discard

③ Bob measures the random bit in his basis

④ Alice publicly announces if the state of the bit she send was in $+$ or in $\times$. Bob sais ~~[illegible]~~ whether he measured in the right basis.

⑤ Alice and Bob discard bits measured in a different basis.

- In expectation, they keep half the bits.
- If Eve measures the bits in the middle, with probability $\frac{1}{4}$ she will change Bob's result. To ensure they would catch her:

⑥ Alice and Bob verify consistency on half of the key.

* It is impossible to clone quantum states – <u>No-Cloning Principle</u>

Assume, we have a unitary U that can clone a state $|\psi\rangle$, for all $|\psi\rangle$

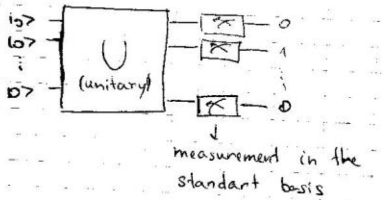
$$|\psi\rangle|0\rangle \xrightarrow{U} |\psi\rangle|\psi\rangle$$

$$|0\rangle|0\rangle \xrightarrow{U} |0\rangle|0\rangle, \quad |1\rangle|0\rangle \xrightarrow{U} |1\rangle|1\rangle$$

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \xrightarrow{U} \begin{array}{l} \xrightarrow{\text{want}} (\alpha|0\rangle + \beta|1\rangle)\otimes(\alpha|0\rangle + \beta|1\rangle) \\ \qquad\qquad \neq \\ \xrightarrow{\text{get}} \alpha|00\rangle + \beta|11\rangle \end{array}$$

–radiction! □

Quantum Computer



All quantum dynamics are unitary, and therefore reversible, whereas classical gates are not reversible. So we want to show that a quantum computer can simulate a classical computer.

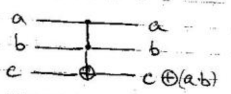
We will first show that a classical computer can be simulated by a classical reversible computer.

A classical computer can be built only by 2 gates.

NAND: $a \cdot b \to 1 \oplus (a \cdot b)$

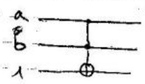
FANOUT: $a \to a, a$

Toffoli gate (classical):

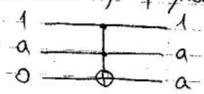


This gate is reversible (it is the inverse of itself)

We can use Toffoli gate to simulate both NAND and FANOUT (and thus any classical computer), with only polynomial overhead!



$1 \oplus ab = \text{NAND}(a,b)$



$>$ FANOUT(a)

The Toffoli gate is unitary, and we can therefor use it to simulate a classical computer with a quantum one.

Universality

(Classicaly: any function can be built from elementary gates)

① Any unitary can be built from CNOT and one-qubit unitaries.

② Any unitary can be approximated to any accuracy by $\{H, \text{CNOT}, \frac{\pi}{8}\text{-gate}\}$.

- $\frac{\pi}{8}$-gate: $\begin{pmatrix} e^{i\pi/8} & 0 \\ 0 & e^{-i\pi/8} \end{pmatrix}$ (or, up to phase $\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}$) $\left(\frac{\pi}{8}\right)^2 = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$

$\left(\frac{\pi}{8}\right)^4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z = \sigma_z$

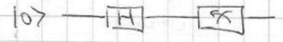
Def.: Norm of ~~matrices~~: $\|U\| = \max_{\||v\rangle\|=1} |U|v\rangle|$ (for unitaries: always 1)

- When we say "approximate unitary U", we mean we can build a ~~th~~ unitary U_b such that $\|U - U_b\| \le \varepsilon$, for any ε.
- There are many universal gate sets.

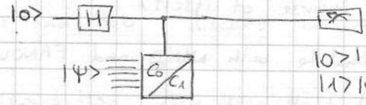
Theorem (Solovay-Kitaev): Any universal gate set can be efficiently approximated by any other.

Def.: BQP = the class of languages L that can be decided correctly with probability 75% by a polynomial size quantum computer.

We can simulate a random classical computer by:



* It is possible to postpone measurements: instead of measuring inside the computer and using a unitary C_0 or C_1 according to the result we can use a special controlled unitary C_0/C_1, and measure later.

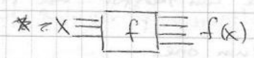


$|0\rangle|\psi\rangle \to |0\rangle C_0|\psi\rangle$
$|1\rangle|\psi\rangle \to |1\rangle C_1|\psi\rangle$

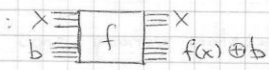
Example: CNOT =

Black-box / Oracle:

classical:



classical reversible:
(with Toffoli)



quantum: