Quantum Gates

Operations are constrained: transformations are unitary

- No info loss

Identifying $e_0 \mapsto |0\rangle$, $e_1 \mapsto |1\rangle$,

<u>Simple</u>

I	Identity	$\begin{array}{l} \lvert 0\rangle \to \lvert 0\rangle \\ \lvert 1\rangle \to \lvert 1\rangle \end{array}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
X	Swap	$\begin{array}{l} \lvert 0\rangle \to \lvert 1\rangle \\ \lvert 1\rangle \to \lvert 0\rangle \end{array}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Y	$= ZX$	$\begin{array}{l} \lvert 0\rangle \to -\lvert 1\rangle \\ \lvert 1\rangle \to \lvert 0\rangle \end{array}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
Z	Phase shift	$\begin{array}{l} \lvert 0\rangle \to \lvert 0\rangle \\ \lvert 1\rangle \to -\lvert 1\rangle \end{array}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Unitarity proof:

1. Self inverse
2. Maps $e_i \rightleftarrows e_j$ (symmetric)

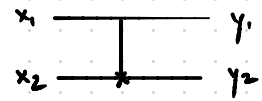
Quantum Gates

Classical Computation Gates

Cnot — Controlled NOT

$|00\rangle \to |00\rangle$
$|01\rangle \to |01\rangle$

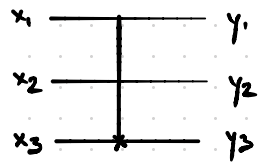
$|10\rangle \to |11\rangle$
$|11\rangle \to |10\rangle$



T — Toffoli (Double C_{not})

$|11x\rangle \to |11\neg x\rangle$

$|ab\,x\rangle \to |ab\,x\rangle$ for $ab \neq 11$



Unitarity: both self inverse & ~~complete~~ symm.

Prop. Toffoli is logically complete

Proof, NOT: $T|11\,x\rangle \to |11\,\neg x\rangle$

AND: $T|x\,y\,0\rangle \to |x\,y\,x\wedge y\rangle$

Quantum Gates

Using superposition:

H — Walsh-Hadamard Gate

$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

* Unitarity:

check by def $U^* U = I$

Prop. Hadamard Identity: $H_n |x\rangle = \overbrace{HH\ldots H}^{\text{on separate bits}} |x\rangle = \frac{1}{\sqrt{2}^n} \sum_{y=0}^{2^n-1} (-1)^{x \odot y} |y\rangle$

Proof: for $|01\rangle$:

$$HH|01\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

for nth bit of y,

1. If it is a zero, contributes $1/\sqrt{2}$
2. If it is a one, then factor depends on parent bit in x:

   $1/\sqrt{2}$ if parent 0 $\quad -1/\sqrt{2}$ if parent 1

Quantum Gates

Thm. No Cloning

No unitary U satisfies $U|a0\rangle = |aa\rangle$ for $a \in \{0,1\}$

Proof: set $|c\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$

Entanglement contradiction:

$$|c0\rangle = |c\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \qquad (1)$$

Then,

$$U|c0\rangle = |cc\rangle = \underbrace{\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)}_{\text{product}} = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

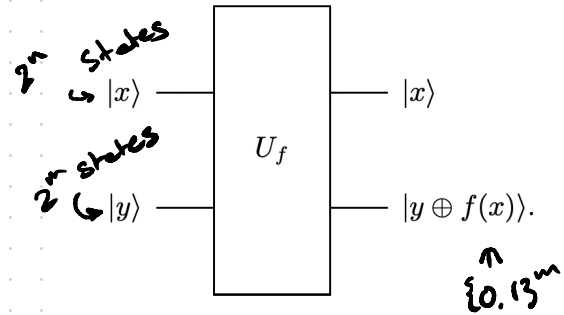
$$U|c0\rangle \overset{(1)}{=} \frac{1}{\sqrt{2}}\left(U|00\rangle + U|10\rangle\right) = \underbrace{\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)}_{\text{entangled}}$$

which is impossible

★ Entangled $\rightarrow$ product vs entangled $\wedge$ product

Quantum Gate Array

An arbitrary (possibly lossy) computable function f has an associated gate array.



Easy to see it is self inverse:

$$|x\rangle \to |x\rangle \to |x\rangle = |x\rangle$$

$$|y\rangle \to |y \oplus f(x)\rangle \to |y \oplus f(x) \oplus f(x)\rangle = |y\rangle$$

Full unitarity not obvious

EPR Paradox

An EPR Pair: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Permits "communication" over great distance.

Setup:

Dfn. Parity Game

Alice and Bob are separated. They receive random input bits x, y.
After receiving their bits, they must output bits a, b so

$$a \oplus b = x \wedge y$$

ie A&B must <u>agree</u> unless $x \wedge y = 1$.

Best classical strategy is to always disagree.

Classical assumption: A&B are too far apart to conspire, so their disagreement is random and independent of $x \wedge y$.

So, suppose A&B disagree. By independence,

$\Pr(\text{win} \mid \text{disagree}) = \Pr(x \wedge y = 1 \mid \text{dis.}) = \Pr(x \wedge y = 1) = 1/4$

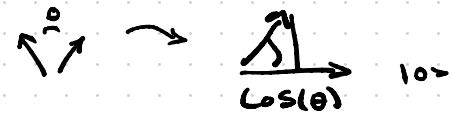
$\Pr(\text{lose} \mid \text{disagree}) = 3/4$

$\Longrightarrow$ more expected wins by disagreeing less

EPR Paradox

Quantum Case: suppose A & B share an EPR Qubit

Notation: $|\rightarrow\rangle$ is $|0\rangle$, $|\uparrow\rangle$ is $|1\rangle$, so $|\overset{\theta}{\nwarrow\nearrow}\rangle$ has Pr(measured equal) $= \cos^2(\theta)$



1. Construct $\frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$
2. Give Alice first Qubit and Bob the second
3. Alice receives her qubit. If it's 1, Alice rotates by 22.5°, otherwise stays the same.

   $0 \rightarrow \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$ $\qquad$ $1 \rightarrow \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$
4. Bob receives his qubit. If 1, he rotates −22.5° in opposite direction.
5. A&B measure & output their measurements.

EPR

This strategy allows some disagreement, correlated with $x \wedge y$:

(1) $x=0,\ y=0$, surely agree

(2) $x=1,\ y=0$
$x=0,\ y=1$ agree 85%

(3) $x=1,\ y=1$ agree 50%

$$\Pr(\text{agree}) = (1/4)(1) + (1/2)(.85) + (1/4)(.5)$$
$$= \underline{80\%}$$

Dense Coding via EPR Bit

Transmit 2 classical bits with 1 qubit

1. A&B each get one half of EPR state

2. Alice wants to send a number $\{0, 1, 2, 3\}$. She encodes this with one of the basic gates, $\{I, X, Y, Z\}$:

$$\varphi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Value	Transformation	New State
0	$\varphi_0 = (I \otimes I)\varphi_0$	$(1/\sqrt{2})(\|00\rangle + \|11\rangle)$
1	$\varphi_1 = (I \otimes X)\varphi_0$	$(1/\sqrt{2})(\|10\rangle + \|01\rangle)$
2	$\varphi_2 = (I \otimes Y)\varphi_0$	$(1/\sqrt{2})(-\|10\rangle + \|01\rangle)$
3	$\varphi_3 = (I \otimes Z)\varphi_0$	$(1/\sqrt{2})(\|00\rangle - \|11\rangle)$

10 → 11

01 → 01

3. Alice sends her qubit to Bob. Bob runs Cnot on the two qubits:

Initial State	After C_{not}	Independent State
$\varphi_0 = (1/\sqrt{2})(\|00\rangle + \|11\rangle)$	$(1/\sqrt{2})(\|00\rangle + \|10\rangle)$	$(1/\sqrt{2})(\|0\rangle + \|1\rangle) \otimes \|0\rangle$
$\varphi_1 = (1/\sqrt{2})(\|10\rangle + \|01\rangle)$	$(1/\sqrt{2})(\|11\rangle + \|01\rangle)$	$(1/\sqrt{2})(\|0\rangle + \|1\rangle) \otimes \|1\rangle$
$\varphi_2 = (1/\sqrt{2})(-\|10\rangle + \|01\rangle)$	$(1/\sqrt{2})(-\|11\rangle + \|01\rangle)$	$(1/\sqrt{2})(\|0\rangle - \|1\rangle) \otimes \|1\rangle$
$\varphi_3 = (1/\sqrt{2})(\|00\rangle - \|11\rangle)$	$(1/\sqrt{2})(\|00\rangle - \|10\rangle)$	$(1/\sqrt{2})(\|0\rangle - \|1\rangle) \otimes \|0\rangle$

Converts entangled ↓ independent

4. Bob measures qubit 2, and is left with Hadamard output states.
   To undo this, Bob applies Hadamard again.

5. Bob measures the final bit to recover the message.

BQP

BPP uses exponentially many computation paths, all correct with high likelihood.

Each path depends on a "random seed" and we can encode all seeds in a superimposed input

Dfn. BQP

$L \in BQP$ iff there exists a polynomial time uniform circuit family of quantum circuits $\{Q_n : n \in \mathbb{N}\}$

1. For $n \in \mathbb{N}$, Q_n takes n qubits and outputs 1 bit
2. For $x \in L$, $\Pr(Q_{|x|}(x) = 1) \geq 2/3$
3. For $x \notin L$, $\Pr(Q_{|x|}(x) = 0) \geq 2/3$

Circuit uniformity: computable by TM.

BQP

What we know:

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

tree enumeration

Relationship to NP is not known.