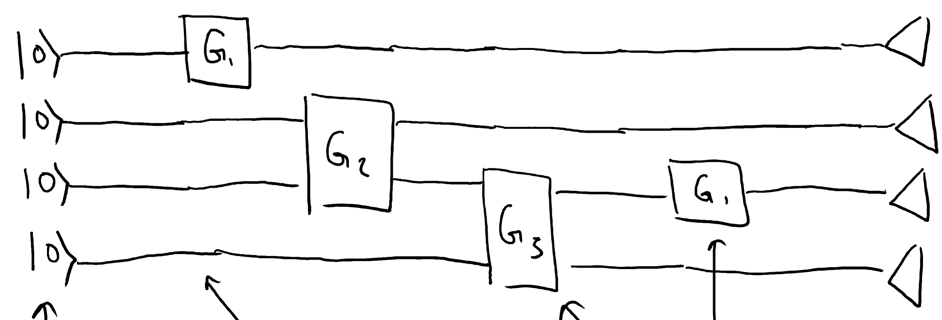
S.KIMMEL

Quantum Circuits

Standard Q. Circuit Model



Measurement is always in standard basis $\{|0\rangle, |1\rangle\}$ for each individual qubit

Outcome is string in $\{0,1\}^n$ e.g. 001100

Initial state is composite system (tensor) of n qubits, all in $|0\rangle$ standard basis states.

Time runs left to right, wires represent qubits

Unitaries Can only come from a specific set

Labelling: $|0\rangle_{top}|0\rangle \cdots |0\rangle_{bottom}$

Measure of Circuit Complexity

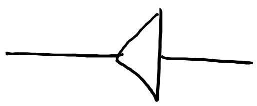
- # of qubits needed (size)
- # of gates needed (gate count) (depends on gate set)
- time/depth - depends on whether can apply in parallel

Why is circuit model good?

- Build computer out of many small systems (like a computer out of bits)
- Physically difficult to create gates on multiple qubits
- Physically easy to measure all at once

Remarks on Measurements

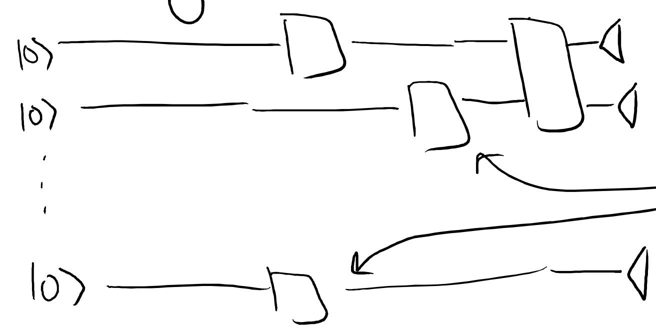
- Intermediate measurements:

 = Measure qubit in $\{|0\rangle, |1\rangle\}$.
If get outcome 0, outgoing $= |0\rangle$
" 1, " $= |1\rangle$

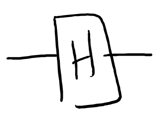
- Commonly see  as measurement symbol

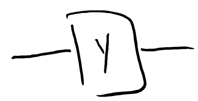
S. KIMMEL

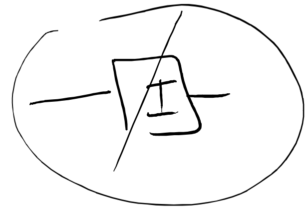
Commonly Used Single Qubit Gates



What are these gates

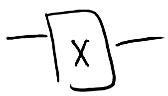


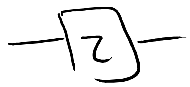


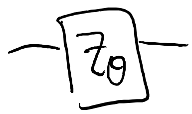


Why don't we use this?

Wire already is "don't change"







$$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i \theta} \end{pmatrix}$$

$$Z_{\pi} = Z$$

$$Z_{\pi/2} = P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$Z_{\pi/4} = T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{(1+i)}{\sqrt{2}} \end{pmatrix}$$

S. KIMMEL

Commonly Used Gates Con't: Control Gates

- Quantum Control Gate:
  - 2-Qubit Controlled Not "CNOT"

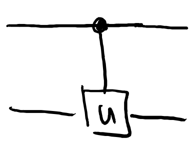
"controlled on first qubit, apply X to second qubit"

Acts on standard basis states like CNOT

$$\left.\begin{aligned}
|00\rangle &\to |00\rangle \\
|01\rangle &\to |01\rangle \\
|10\rangle &\to |1\rangle X|0\rangle = |1\rangle|1\rangle = |11\rangle \\
|11\rangle &\to |1\rangle X|1\rangle = |1\rangle|0\rangle = |10\rangle
\end{aligned}\right\} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CNOT: $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$

More generally, controlled U operation

- $C\text{-}U =$ 

$$|0\rangle|i\rangle \to |0\rangle|i\rangle \qquad : |0\rangle\langle 0| \otimes I$$
$$|1\rangle|i\rangle \to |1\rangle U|i\rangle \qquad + |1\rangle\langle 1| \otimes U$$

S.KIMMEL

Universality

Classically

OR, AND, NOT,
↓
can combine to create any Boolean function

Quantumly

Small set of ≤ 2 qubit unitaries
↓
can combine to create any unitary?

Universal Discrete Gate Set

For ease of computing, need a discrete set of gates;

$G_1, G_2 \ldots G_t$

$\underbrace{R_z(\theta)}_{\text{uncountably } \infty \text{ set of unitaries}}$

Problem: can form countably ∞ unitaries

Can't hope to do many unitaries exactly, but if approximate, is OK.

Approximate?

- Want: $\underset{\text{Ideal } U}{U}|0\rangle^{\otimes n} = |\psi\rangle$, $\underset{\text{Approximate } U}{U'}|0\rangle^{\otimes n} = |\psi'\rangle \Rightarrow |\psi\rangle \underset{?}{\approx} |\psi'\rangle$

≈?

- Want: $|\psi\rangle \approx |\psi'\rangle \Rightarrow$ Small probability that any measurement can distinguish $|\psi\rangle$ from $|\psi'\rangle$.

Claim:
- H, T, CNOT are a universal gate set.
- Toffoli, H are a universal gate set

Claim: No quantum universal gate set is any better than any other in terms of efficiency.

2 Frequent Errors

- $(A+B)^2 \neq A^2 + 2AB + B^2$ ↑↑ matrices $= A^2 + AB + BA + B^2$ } Matrices do not necessarily <u>commute</u>

$$A, B \text{ commute} \iff AB = BA$$

- Subscripts

Bob: outcome 1
Eve: outcome 0

Prob:

<u>Not Correct</u>

$$\left|\langle 01 | \psi \rangle\right|^2 = \left|(0\,1\,0\,0)\left(\quad\right)\right|^2$$

EB ↑ ↑ BE

<u>Correct</u>:

$$\left|{}_{BE}\langle 10 | \psi \rangle_{BE}\right|^2 = \left|(0\,0\,1\,0)\left(\quad\right)\right|^2$$

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = |\psi\rangle_{AB} \quad \text{what is } |\psi\rangle_{BA}?$$

(Physically the same, but mathematically different. Either choice is OK, but need to stay consistent.)

<u>A</u> $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ <u>B</u> $\begin{pmatrix} c \\ d \\ a \\ b \end{pmatrix}$ <u>C</u> $\begin{pmatrix} a \\ c \\ b \\ d \end{pmatrix}$ ⟸ Correct! (See next page)