Lecture 3 CPSC 447/547 - Intro to QC

From Bits to Qubits (in computation)

Outline.

- Boolean Circuits
- Reversible circuits
- Randomized circuits
- Quantum circuits

Recall from the first lecture:

Information

	Bit	Qubit	Random bit
Possible State	0 or 1	$\alpha_0\|0\rangle + \alpha_1\|1\rangle$ $\alpha_0, \alpha_1 \in \mathbb{C}$ $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$	p_0 "0" + p_1 "1" $p_0, p_1 \in [0,1]$ $p_0 + p_1 = 1$.

Multiple bits (e.g. 3 bits)

Joint State	000 or 001 or 010 or ⋮ or 111	$\alpha_{000}\|000\rangle + \alpha_{001}\|001\rangle + \alpha_{010}\|010\rangle + \cdots + \alpha_{111}\|111\rangle$	p_{000} "000" + p_{001} "001" + p_{010} "010" + ⋮ + p_{111} "111"
8 possibilities:		$\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \vdots \\ \alpha_{111} \end{bmatrix}$	$\begin{bmatrix} p_{000} \\ p_{001} \\ p_{010} \\ \vdots \\ p_{111} \end{bmatrix}$

State vector

Computation

(Deterministic, reversible, randomized, quantum)

Computational tasks can be modeled as transitions of states.

Or mathematically as Boolean Functions.

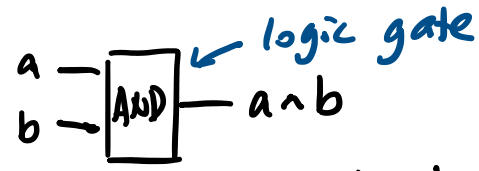
<u>Example</u>: AND function: $\{0,1\}^2 \to \{0,1\}$ maps 2 bits to 1 bit.

$$AND(a,b) = a \wedge b$$

Truth table to represent all transitions from input state to output state:

input		output
a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

We can also conveniently use a circuit diagram for this function:



This way, we can represent very complex computational tasks as sequence of logic gates.

<u>Proposition</u>: Any Boolean function $f: \{0,1\}^m \to \{0,1\}^n$ can be computed by a Boolean circuit that consists of AND, OR, and NOT gates. "Universality".

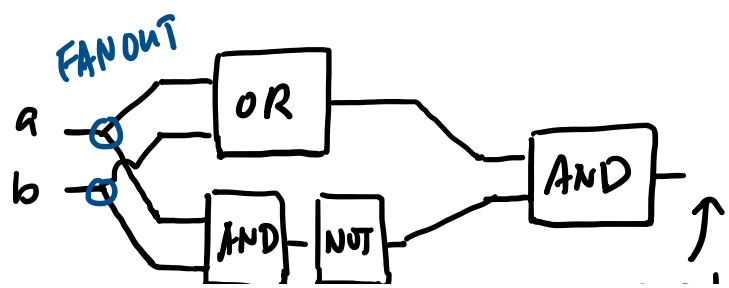
<u>Example</u>: XOR function: $XOR(a,b) = a \oplus b$

Truth table

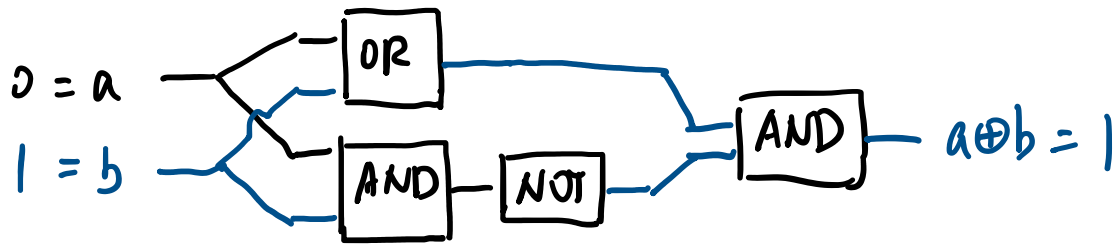
a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

"parity"

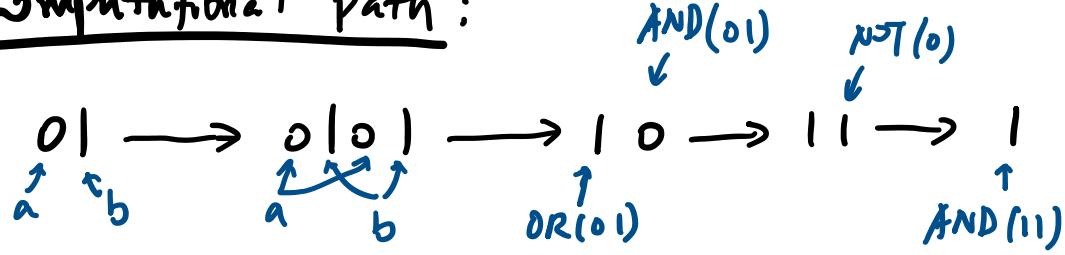
Boolean circuit



E.g. $a=0$, $b=1$ $\qquad a \oplus b$



Computational path:



Reversible Computation.

Logical reversibility: A logic gate is reversible if the mapping from input to output is a bijection.

" Given the output, the input is not uniquely determined."

Example: NOT gate is reversible.

Given output, we can always negate back to input.

Example: XOR function is not reversible.

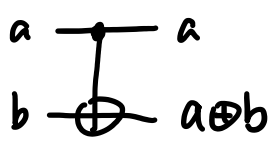
Given $a \oplus b = 1$, we cannot determine if we had:

$(a=0, b=1)$ or $(a=1, b=0)$.

Q: Is there a reversible version of XOR?

A: Introducing controlled-Not gate (CNOT)

Circuit diagram



(trick: save the input)

Truth table

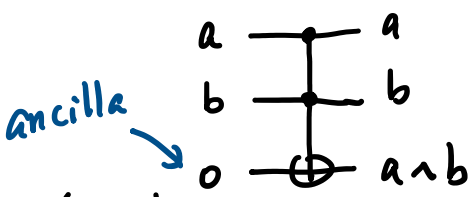
input	output
00	00
01	01
10	11
11	10

"Apply NOT to b if and only if a=1."

Bijection?

Q: Is the a reversible version of AND?

A: Introducing **Toffoli** gate.



(trick: add ancilla input)

In general, third bit can be anything

output: $(a \wedge b) \oplus c$.

"Apply NOT to c if and only if both a and b are 1."

Q: Is there a reversible version for <u>any</u> Boolean function?

A: <u>**Theorem**</u> Any Boolean function $f: \{0,1\}^m \to \{0,1\}^n$ can be computed by a reversible circuit that consists of only Toffoli gates.*

k bits in, k out

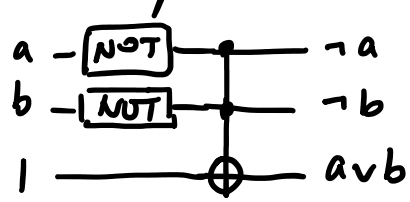
$k > m$, $k > n$.

"Reversibility + Universality".

(* assuming we allow extra ancilla inputs and some garbage outputs.)

How to show universality? (assume previous proposition)

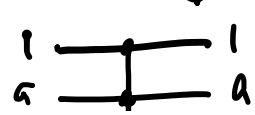
Reversible OR:



de Morgan's Law

$a \vee b = \neg(\neg a \wedge \neg b)$

Reversible FANOUT:



Later lecture: How many ancilla inputs needed? $0 \longrightarrow \oplus \longrightarrow a$

How to clean up garbage bits?

Randomized Computation (random inputs, random gates)

A random bit r can be represented as a probabilistic state vector

state of r: $\begin{bmatrix} p \\ 1-p \end{bmatrix}$ ← prob. of "0" ← prob. of "1" $\quad 0 \le p \le 1$

What if we apply NOT gate to the random bit?

Matrix representation for this transition:

$$r \longrightarrow \boxed{\text{NOT}} \longrightarrow \bar{r}$$

$$\begin{bmatrix} p \\ 1-p \end{bmatrix} \qquad \begin{bmatrix} 1-p \\ p \end{bmatrix}$$

$$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{Pauli-}X} \begin{bmatrix} p \\ 1-p \end{bmatrix} = \begin{bmatrix} 1-p \\ p \end{bmatrix}.$$

What about a random gate?

E.g. Randomized NOT gate: "Flips a coin; negate input if the outcome is tails."

$$r \longrightarrow \boxed{\$\text{-NOT}} \longrightarrow ?$$

$\begin{bmatrix} p \\ 1-p \end{bmatrix}$ $\qquad \begin{bmatrix} q \\ 1-q \end{bmatrix}$ ← heads prob. ← tails prob.

$$\begin{bmatrix} ? \end{bmatrix} \begin{bmatrix} p \\ 1-p \end{bmatrix} = \begin{bmatrix} pq + (1-p)(1-q) \\ p(1-q) + q(1-p) \end{bmatrix}$$

$$q \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + (1-q) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} q & 1-q \\ 1-q & q \end{bmatrix}$$

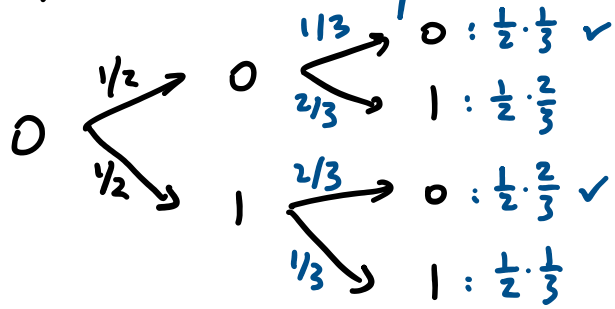
Example:

$$0 \longrightarrow \boxed{\$\text{-NOT}} \longrightarrow \boxed{\$\text{-NOT}} \longrightarrow$$

$\begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$ $\qquad \begin{bmatrix} 1/3 \\ 2/3 \end{bmatrix}$

What is the probability that its output is 0?

This time, let's use computational path method:



$$\boxed{\frac{1}{2}\cdot\frac{1}{3}+\frac{1}{2}\cdot\frac{2}{3}=\frac{1}{2}}$$

"Adding the probability of each correct path"

Quantum Computation

A quantum bit $|\psi\rangle$ can be represented as a superposition state vector:

Quantum State: $|\psi\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$ α ← amplitude of $|0\rangle$, β ← amplitude of $|1\rangle$.

$\alpha, \beta \in \mathbb{C}$

$|\alpha|^2 + |\beta|^2 = 1$

Let's see what happens if amplitudes are <u>negative</u>:

Introducing quantum gate: Hadamard gate (H)

Circuit Diagram

Truth Table

in	out
$\lvert 0\rangle$	$\frac{\lvert 0\rangle+\lvert 1\rangle}{\sqrt{2}} = \lvert +\rangle$
$\lvert 1\rangle$	$\frac{\lvert 0\rangle-\lvert 1\rangle}{\sqrt{2}} \equiv \lvert -\rangle$
$\alpha\lvert 0\rangle+\beta\lvert 1\rangle$	$\alpha\lvert +\rangle+\beta\lvert -\rangle$

Matrix

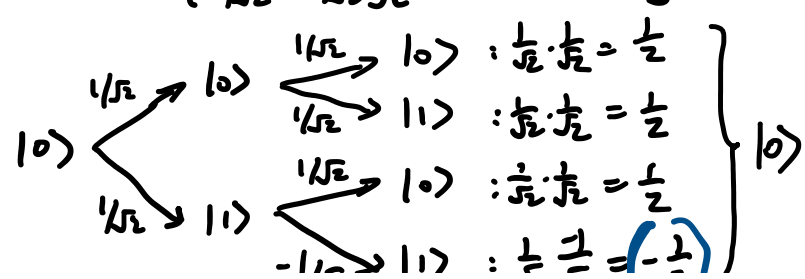
$$\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{bmatrix}$$

Examples:

$\begin{bmatrix}0\\1\end{bmatrix} = |1\rangle$ — H — ?

$$\begin{bmatrix}1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2}\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1/\sqrt{2} \\ -1/\sqrt{2}\end{bmatrix}$$

$\begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$ — H — H — ?



Adding the <u>amplitude</u> of each path".

$|0\rangle : \frac{1}{2}+\frac{1}{2} = 1$: constructive interference

$|1\rangle : \frac{1}{2}-\frac{1}{2} = 0$: destructive interference.

Negative amplitudes can <u>cancel</u> with positive amplitudes.

This is another hint of the power of quantum computation.

- In fact, real (positive and negative) amplitudes are usually enough in most quantum algorithms.
- Complex amplitudes are need, however, to fully describe a quantum process. (See Aaronson's blog for sutlety)

Another (non-classical) gate : Square-root of NOT gate. ($\sqrt{X}$ gate).

What is a gate U, such that $U^2 = X$ gate ?

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = (+1)|+\rangle\langle+| + (-1)|-\rangle\langle-| \quad \text{(Spectral)}$$

$$X^{1/2} = \sqrt{+1}\,|+\rangle\langle+| + \sqrt{-1}\,|-\rangle\langle-|$$

$$= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot \frac{\langle 0|+\langle 1|}{\sqrt{2}} + i \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}} \cdot \frac{\langle 0|-\langle 1|}{\sqrt{2}}$$

$$= \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix}.$$

Measurement (Quantum information readout)

A qubit (e.g. photon) stores two amplitudes $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

To readout the information, we need to perform a physical experiment, called measurement, on the qubit.

(e.g. shining lasers at photon)

- Measurement outcome is probabilistic!

$$\text{Measure } |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \begin{cases} \text{Outcome: } |0\rangle \text{ with prob. } |\alpha|^2 \\ \text{Outcome: } |1\rangle \text{ with prob } |\beta|^2 \end{cases}$$

- Measurement is irreversible!

$$\text{Quantum state } |\psi\rangle \xrightarrow{\text{collapses}} \begin{cases} |0\rangle \\ |1\rangle. \end{cases}$$

Example:

$$|\psi\rangle = \sqrt{X}\cdot|0\rangle = \begin{bmatrix} \frac{1+i}{2} \\ \frac{1-i}{2} \end{bmatrix}$$

$$\text{Measurement collapses } |\psi\rangle \text{ to } \begin{cases} |0\rangle \text{ with prob: } \frac{1}{2} \\ |1\rangle \text{ with prob: } \frac{1}{2} \end{cases}$$

- It's like opening a black box, the amplitudes inside is revealed, but in the form of a random bit.
- But once opened, the state of the box is altered to the collapsed state.