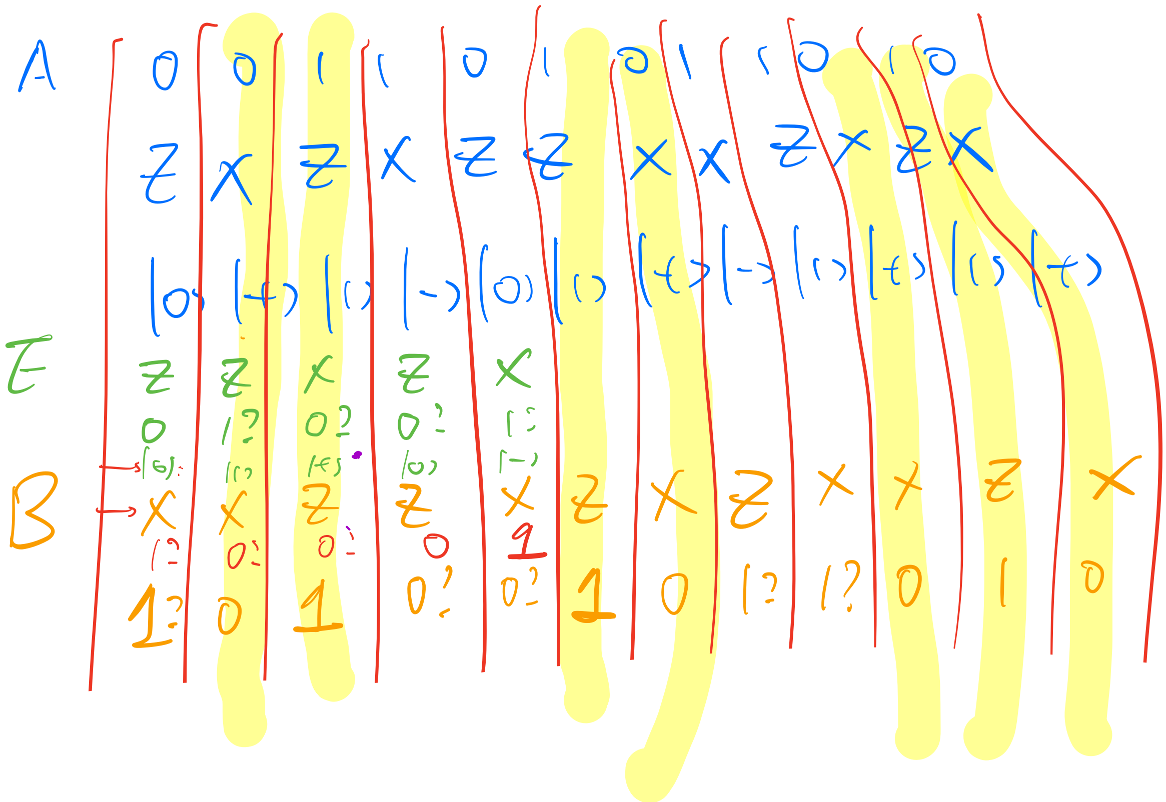
Basic quantum algorithms: Key exchange / Bell's inequality

Yipeng Huang

Rutgers University

February 2, 2024

Table of contents



A
0 0 1 1 0 1 0 1 1 0 1 0
Z X Z X Z Z X X Z X Z X
|0⟩ |+⟩ |1⟩ |−⟩ |0⟩ |1⟩ |+⟩ |−⟩ |1⟩ |+⟩ |1⟩ |+⟩
E
Z Z X Z X
B
X X Z Z X Z X Z X X Z X
1 0 1 0 0 1 0 1 1 0 1 0

Table of contents

Bell states form an orthogonal basis set

1. $|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = |\Phi^+\rangle$
2. $|01\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|01\rangle + |11\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) = |\Psi^+\rangle$
3. $|10\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle - |10\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) = |\Phi^-\rangle$
4. $|11\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|01\rangle - |11\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) = |\Psi^-\rangle$

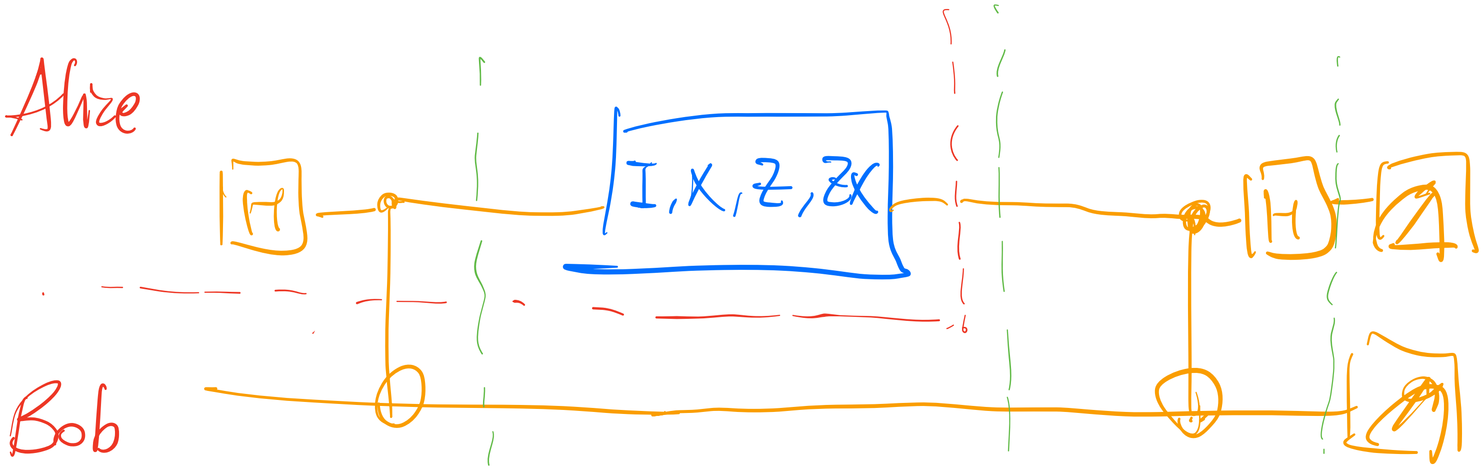
Superdense coding

Transmit 2 bits of classical information by sending 1 qubit

1. Alice wishes to tell Bob two bits of information: 00, 01, 10, or 11.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$.
3. Alice performs I, X, Z, or ZX on her qubit; she then sends her qubit to Bob.
4. Bob measures in the Bell basis to receive 00, 01, 10, or 11.

Superdense coding circuit

`https://github.com/quantumlib/Cirq/blob/master/examples/superdense_coding.py`



$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

$$\begin{cases} I & \frac{|00\rangle+|11\rangle}{\sqrt{2}} \\ X & \frac{|10\rangle+|01\rangle}{\sqrt{2}} \\ Z & \frac{|00\rangle-|11\rangle}{\sqrt{2}} \\ ZX & \frac{|10\rangle-|01\rangle}{\sqrt{2}} \end{cases}$$

$$\begin{cases} I & |00\rangle \\ X & |01\rangle \\ Z & |10\rangle \\ ZX & |11\rangle \end{cases}$$

Superdense coding

Transmit 2 bits of classical information by sending 1 qubit

1. Alice wishes to tell Bob two bits of information: 00, 01, 10, or 11.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$.
3. Alice performs I, X, Z, or ZX on her qubit; she then sends her qubit to Bob.
4. Bob measures in the Bell basis to receive 00, 01, 10, or 11.

Alice applies different operators on her qubit so Bob measures the message

1. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \xrightarrow{I\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle\Big) \xrightarrow{H\otimes I} |00\rangle$
2. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \xrightarrow{X\otimes I} \frac{1}{\sqrt{2}}\Big(|10\rangle + |01\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|11\rangle + |01\rangle\Big) \xrightarrow{H\otimes I} |01\rangle$
3. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \xrightarrow{Z\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle - |10\rangle\Big) \xrightarrow{H\otimes I} |10\rangle$
4. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \xrightarrow{ZX\otimes I} \frac{1}{\sqrt{2}}\Big(-|10\rangle + |01\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(-|11\rangle + |01\rangle\Big) \xrightarrow{H\otimes I} |11\rangle$

Table of contents

Quantum teleportation

"Teleport" a qubit state by transmitting classical information

1. Alice wishes to give Bob a qubit state $|Q\rangle$.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle$.
3. Alice first entangles $|Q\rangle$ and $|P\rangle$; then, she measures her local two qubits.
4. Alice tells Bob (via classical means) her two-bit measurement result.
5. Bob uses Alice's two bits to perform I, X, Z, or ZX on his qubit to obtain $|Q\rangle$.

Depending on if Alice measures 00, 01, 10, or 11, Bob applies I, X, Z, or ZX to recover $|Q\rangle$

$$|Q\rangle \otimes |P\rangle = \left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$= \frac{\alpha}{\sqrt{2}}|0\rangle\left(|00\rangle + |11\rangle\right) + \frac{\beta}{\sqrt{2}}|1\rangle\left(|00\rangle + |11\rangle\right) \quad (1)$$

$$\xrightarrow{CNOT_{0,1}} \frac{\alpha}{\sqrt{2}}|0\rangle\left(|00\rangle + |11\rangle\right) + \frac{\beta}{\sqrt{2}}|1\rangle\left(|10\rangle + |01\rangle\right) \quad (2)$$

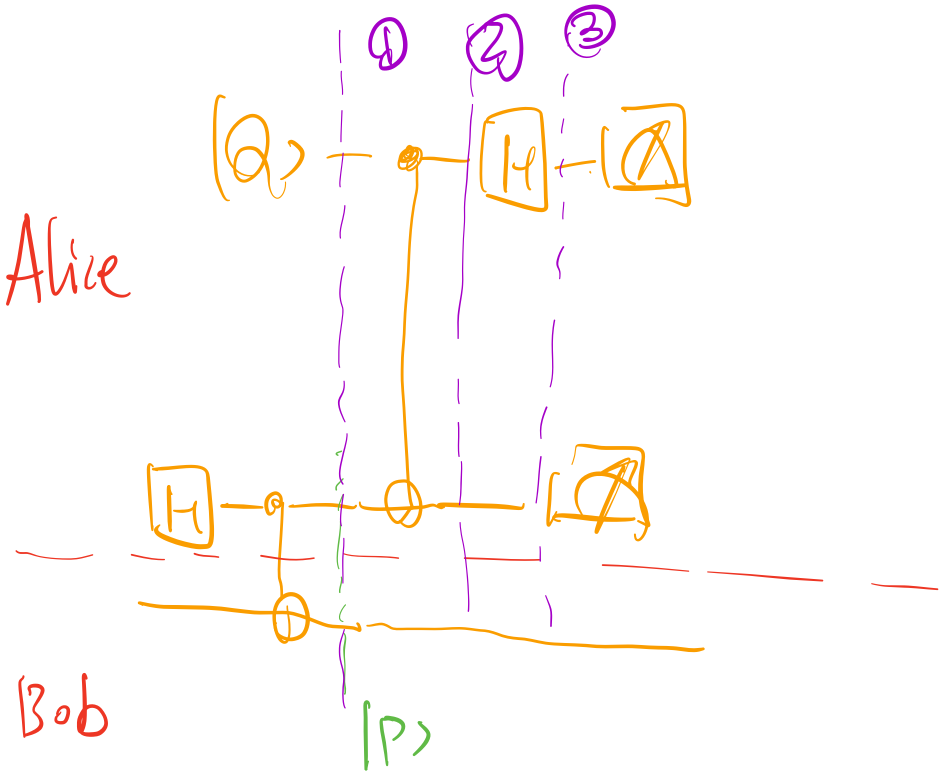
$$\xrightarrow{H\otimes I\otimes I} \frac{\alpha}{2}\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + \frac{\beta}{2}\left(|0\rangle - |1\rangle\right)\left(|10\rangle + |01\rangle\right) \quad (3)$$

$$= \frac{1}{2}|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right)$$ Alice measures 00 so Bob applies I

$$+ \frac{1}{2}|01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right)$$ Alice measures 01 so Bob applies X

$$+ \frac{1}{2}|10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right)$$ Alice measures 10 so Bob applies Z

$$+ \frac{1}{2}|11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)$$ Alice measures 11 so Bob applies ZX



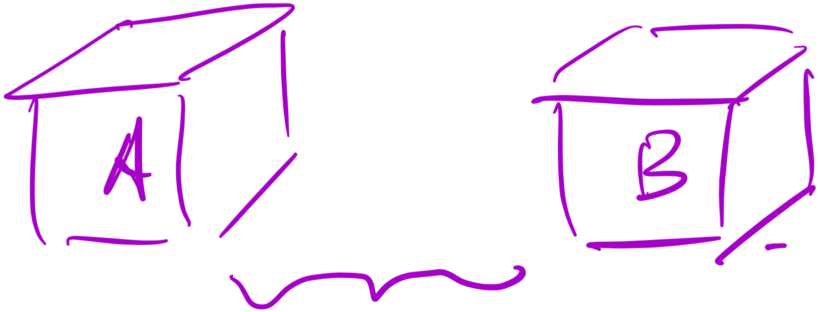
1
2
3
|Q⟩
H
Alice
H
Bob
|P⟩

Table of contents

EPR paradox

- When quantum physics was first discovered, the mathematics of entanglement led to shocking conclusions.
- If you can keep systems coherent (isolated), they can exhibit superposition and entanglement.
- Einstein and others: there shouldn't be "spooky action at a distance" so there must be some local hidden-variable. The task was then to prove or disprove local hidden-variables.
- But protocols and experiments like Hardy's, GHZ, CHSH, and Aspect experimentally rejected local hidden-variable theory.

CHSH game: Test of entanglement



Two isolated parties Alice and Bob

- Alice gets coin toss x, replies a
- Bob gets coin toss y, replies b

Goal: maximize $a \oplus b = x \wedge y$

x	y	$x \wedge y$	$a \oplus b$	winning options for (a, b)
0	0	0	0	(0,0) or (1,1)
0	1	0	0	(0,0) or (1,1)
1	0	0	0	(0,0) or (1,1)
1	1	1	1	(0,1) or (1,0)

Best classical strategy to maximize $a \oplus b = x \wedge y$

Proof that any assignment to a and b cannot always satisfy $a \oplus b = x \wedge y$

1. Let a_0 be Alice's response if she sees $x = 0$
2. Let a_1 be Alice's response if she sees $x = 1$
3. Let b_0 be Bob's response if she sees $y = 0$
4. Let b_1 be Bob's response if she sees $y = 1$

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

1. $a_0 \oplus b_0 = 0$
2. $a_0 \oplus b_1 = 0$
3. $a_1 \oplus b_0 = 0$
4. $a_1 \oplus b_1 = 1$

Sum (mod 2) of left side

$$(a_0 \oplus b_0) \oplus (a_0 \oplus b_1) \oplus (a_1 \oplus b_0) \oplus (a_1 \oplus b_1) =$$
$$(a_0 \oplus a_0) \oplus (a_1 \oplus a_1) \oplus (b_0 \oplus b_0) \oplus (b_1 \oplus b_1) = 0$$

Sum (mod 2) of right side

1

Best classical strategy to maximize $a \oplus b = x \wedge y$

- Even if the two shared randomness, the random coin toss of x and y prevents use of shared randomness.
- Best you can do is 3/4.
- Give a couple ways of getting 3/4

A quantum strategy to maximize $a \oplus b = x \wedge y$

Alice and Bob share entangled pair $|\Phi\rangle$

$$|\Phi\rangle = \frac{1}{\sqrt{12}}\Big(3|00\rangle + |01\rangle + |10\rangle - |11\rangle\Big)$$

$(x, y) = (0, 0)$ So Alice and Bob both apply I:

$$(I \otimes I)|\Phi\rangle = \frac{1}{\sqrt{12}}\begin{bmatrix} 3 \\ 1 \\ 1 \\ -1 \end{bmatrix}$$

Measurement yields

$$\begin{cases} (a, b) = (0, 0), \text{ a win, with probability } \frac{9}{12} \\ (a, b) = (0, 1), \text{ a loss, with probability } \frac{1}{12} \\ (a, b) = (1, 0), \text{ a loss, with probability } \frac{1}{12} \\ (a, b) = (1, 1), \text{ a win, with probability } \frac{1}{12} \end{cases}$$

A quantum strategy to maximize $a \oplus b = x \wedge y$

Alice and Bob share entangled pair $|\Phi\rangle$

$$|\Phi\rangle = \frac{1}{\sqrt{12}}\Big(3\,|00\rangle + |01\rangle + |10\rangle - |11\rangle\Big)$$

$(x, y) = (0, 1)$ So Alice applies I, Bob applies H:

$$(I \otimes H)\,|\Phi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{bmatrix}\frac{1}{\sqrt{12}}\begin{bmatrix}3\\1\\1\\-1\end{bmatrix} = \frac{1}{2\sqrt{6}}\begin{bmatrix}4\\2\\0\\2\end{bmatrix}$$

Measurement yields

$$\begin{cases}(a,b) = (0,0), \text{ a win, with probability } \frac{4}{6}\\ (a,b) = (0,1), \text{ a loss, with probability } \frac{1}{6}\\ (a,b) = (1,0), \text{ a loss, with probability } 0\\ (a,b) = (1,1), \text{ a win, with probability } \frac{1}{6}\end{cases}$$

A quantum strategy to maximize $a \oplus b = x \wedge y$

Alice and Bob share entangled pair $|\Phi\rangle$

$$|\Phi\rangle = \frac{1}{\sqrt{12}}\Big(3\,|00\rangle + |01\rangle + |10\rangle - |11\rangle\Big)$$

$(x, y) = (1, 0)$ So Alice applies H, Bob applies I:

$$(H \otimes I)\,|\Phi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \frac{1}{\sqrt{12}}\begin{bmatrix} 3 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2\sqrt{6}}\begin{bmatrix} 4 \\ 0 \\ 2 \\ 2 \end{bmatrix}$$

Measurement yields

$$\begin{cases} (a, b) = (0, 0), \text{ a win, with probability } \frac{4}{6} \\ (a, b) = (0, 1), \text{ a loss, with probability } 0 \\ (a, b) = (1, 0), \text{ a loss, with probability } \frac{1}{6} \\ (a, b) = (1, 1), \text{ a win, with probability } \frac{1}{6} \end{cases}$$

A quantum strategy to maximize $a \oplus b = x \wedge y$

Alice and Bob share entangled pair $|\Phi\rangle$

$$|\Phi\rangle = \frac{1}{\sqrt{12}}\Big(3|00\rangle + |01\rangle + |10\rangle - |11\rangle\Big)$$

$(x, y) = (1, 1)$ So Alice and Bob both apply H:

$$(H \otimes H)|\Phi\rangle = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \frac{1}{\sqrt{12}} \begin{bmatrix} 3 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{4\sqrt{3}} \begin{bmatrix} 4 \\ 4 \\ 4 \\ 0 \end{bmatrix}$$

Measurement yields

$$\begin{cases} (a, b) = (0, 0), \text{ a loss, with probability } \frac{1}{3} \\ (a, b) = (0, 1), \text{ a win, with probability } \frac{1}{3} \\ (a, b) = (1, 0), \text{ a win, with probability } \frac{1}{3} \\ (a, b) = (1, 1), \text{ a loss, with probability } 0 \end{cases}$$

A quantum strategy to maximize $a \oplus b = x \wedge y$

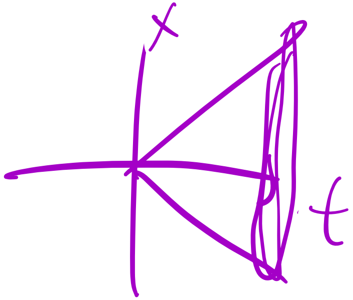
Sum of winning chances?

83%

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

"(0,0), (1,1), (0,1), (0,0)"

Philosophical interpretations of quantum mechanics



Cannot have both locality and realism

- Locality: "means that information and causation act locally, not faster than light"
- Realism: "means that physical systems have definite, well-defined properties (even if those properties may be unknown to us)"

Source: de Wolf. Quantum Computing: Lecture Notes

Unpalatable choices

- Keep locality and sacrifice realism: no definite narrative of the world
- Keep realism and sacrifice locality: spooky-action-at-a-distance

Table of contents

Deutsch-Jozsa algorithm: simplest quantum algorithm showing advantage vs. classical

A Heist

- You break into a bank vault. The bank vault has 2^n bars. Three possibilities: all are gold, half are gold and half are fake, or all are fake.
- Even if you steal just one gold bar, it is enough to fund your escape from the country, forever evading law enforcement.
- You do not want to risk stealing from a bank vault with only fake bars.
- You have access to an oracle $f(x)$ that tells you if gold bar x is real.
- Using the oracle sounds the alarm, so you only get to use it once.

Deutsch-Jozsa algorithm: simplest quantum algorithm showing advantage vs. classical

More formal description

- The 2^n bars are either fake or gold. $f : \{0,1\}^n \to \{0,1\}$.
- Three possibilities:
  1. All are fake. f is constant. $f(x) = 0$ for all $x \in \{0,1\}^n$.
  2. All are gold. f is constant. $f(x) = 1$ for all $x \in \{0,1\}^n$.
  3. Half fake half gold. f is balanced.

     $$\Big|\{x \in \{0,1\}^n : f(x) = 0\}\Big| = \Big|\{x \in \{0,1\}^n : f(x) = 1\}\Big| = 2^{n-1}$$
- The oracle U works as follows: $U|c\rangle|t\rangle = |c\rangle|t \oplus f(c)\rangle$
- Try deciding if f is constant or balanced using oracle U only once.

What is in the oracle

For $n = 1$, four possibilities

	f_0	f_1	f_2	f_3
f(0)	0	0	1	1
f(1)	0	1	0	1
	f is constant 0	f is balanced	f is balanced	f is constant 1

Demonstration of Deutsch-Jozsa for the $n = 1$ case

Output of circuit is $c = 0$ iff f is constant

1. Initial state: $|c\rangle \otimes |t\rangle = |0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle$
2. After first set of Hadamards: $H \otimes H\Big(|0\rangle \otimes |1\rangle \Big) = H|0\rangle \otimes H|1\rangle = |+\rangle \otimes |-\rangle =$

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

From here, let's take an aside via matrix-vector multiplication to build intuition with interference and phase kickback.

Demonstration of Deutsch-Jozsa for the $n = 1$ case

Output of circuit is $c = 0$ iff f is constant

1. Initial state: $|c\rangle \otimes |t\rangle = |0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle$
2. After first set of Hadamards: $H \otimes H\Big(|0\rangle \otimes |1\rangle \Big) = |+\rangle |-\rangle =$
$$\Big(\tfrac{1}{\sqrt{2}} |0\rangle + \tfrac{1}{\sqrt{2}} |1\rangle \Big)\Big(\tfrac{1}{\sqrt{2}} |0\rangle - \tfrac{1}{\sqrt{2}} |1\rangle \Big) = \tfrac{1}{2}\Big(|0\rangle \left(|0\rangle - |1\rangle \right) + |1\rangle \left(|0\rangle - |1\rangle \right) \Big)$$
3. After applying oracle U:
$$U\tfrac{1}{2}\Big(|0\rangle \left(|0\rangle - |1\rangle \right) + |1\rangle \left(|0\rangle - |1\rangle \right) \Big) = \tfrac{1}{2}\Big(|0\rangle \left(|f(0) \oplus 0\rangle - |f(0) \oplus 1\rangle \right) +$$
$$|1\rangle \left(|f(1) \oplus 0\rangle - |f(1) \oplus 1\rangle \right) \Big) = \tfrac{1}{2}\Big(|0\rangle \left(|f(0)\rangle - |f(\bar{0})\rangle \right) + |1\rangle \left(|f(1)\rangle - |f(\bar{1})\rangle \right) \Big)$$

Demonstration of Deutsch-Jozsa for the $n = 1$ case

Output of circuit is $c = 0$ iff f is constant

1. Initial state: $|c\rangle \otimes |t\rangle = |0\rangle \otimes |1\rangle = |0\rangle\,|1\rangle = |01\rangle$
2. After first set of Hadamards: $\frac{1}{2}\Big(|0\rangle\,(|0\rangle - |1\rangle) + |1\rangle\,(|0\rangle - |1\rangle)\Big)$
3. After applying oracle U: $U\frac{1}{2}\Big(|0\rangle\,(|0\rangle - |1\rangle) + |1\rangle\,(|0\rangle - |1\rangle)\Big) =$
   $\frac{1}{2}\Big(|0\rangle\,\big(\,|f(0)\rangle - |\bar{f}(0)\rangle\,\big) + |1\rangle\,\big(\,|f(1)\rangle - |\bar{f}(1)\rangle\,\big)\Big)$
4. This last expression can be factored depending on f:
   $U\frac{1}{2}\Big(|0\rangle\,(|0\rangle - |1\rangle) + |1\rangle\,(|0\rangle - |1\rangle)\Big) =$
   $$\begin{cases} \frac{1}{2}\big(\,|0\rangle + |1\rangle\,\big)\big(\,|f(0)\rangle - |\bar{f}(0)\rangle\,\big) \text{ if } f(0) = f(1) \\ \frac{1}{2}\big(\,|0\rangle - |1\rangle\,\big)\big(\,|f(0)\rangle - |\bar{f}(0)\rangle\,\big) \text{ if } f(0) \neq f(1) \end{cases} = \begin{cases} |+\rangle\,|-\rangle \ \text{ if } f(0) = f(1) \\ |-\rangle\,|-\rangle \ \text{ if } f(0) \neq f(1) \end{cases}$$

The trick where oracle's output on $|t\rangle$ affects phase of $|c\rangle$ is called phase kickback.

Demonstration of Deutsch-Jozsa for the $n = 1$ case

Output of circuit is $c = 0$ iff f is constant

1. Initial state: $|c\rangle \otimes |t\rangle = |0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle$
2. After first set of Hadamards: $\frac{1}{2}\Big(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)\Big)$
3. After applying oracle U:
$$U\frac{1}{2}\Big(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)\Big) = \begin{cases} |+\rangle|-\rangle & \text{if } f(0) = f(1) \\ |-\rangle|-\rangle & \text{if } f(0) \neq f(1) \end{cases}$$
4. After applying second H on top qubit:
$$\begin{cases} H \otimes I\big(|+\rangle|-\rangle\big) = |0\rangle|-\rangle & \text{if } f(0) = f(1) \\ H \otimes I\big(|-\rangle|-\rangle\big) = |1\rangle|-\rangle & \text{if } f(0) \neq f(1) \end{cases}$$

Deutsch-Jozsa programs and systems

Algorithm

David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. 1992.

Programs

Google Cirq programming example.

Implementation

- Mach-Zehnder interferometer implementation. `https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/SinglePhotonLab/SinglePhotonLab.html`
- Ion trap implementation. Gulde et al. Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer. Letters to Nature. 2003.

Mach-Zehnder interferometer implementation of Deutsch's algorithm

$$|0\rangle \xrightarrow{H} |+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \begin{cases} \xrightarrow{I} |+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \xrightarrow{H} |0\rangle \\ \xrightarrow{Z} |-\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} & \xrightarrow{H} |1\rangle \\ \xrightarrow{-Z} -|-\rangle = \begin{bmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \xrightarrow{H} -|1\rangle \\ \xrightarrow{-ZZ=-I} -|+\rangle = \begin{bmatrix} \frac{-1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} & \xrightarrow{H} -|0\rangle \end{cases}$$