ACCQ 206 - Entanglement and quantum algorithms

Alex Bredariol Grilo
Alex.Bredariol-Grilo@lip6.fr

Product states vs. entangled states

EPR pair

$|\psi_{00}\rangle$

Product states

Can be written as $|\psi\rangle \otimes |\phi\rangle$

Example: $|+\rangle \otimes |+\rangle$, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle$

$|+\rangle \otimes |+\rangle \otimes |+\rangle$

$\frac{1}{\sqrt{2}}\left(|000\rangle + |110\rangle\right)$

Entangled states

Can**not** be written as $|\psi\rangle \otimes |\phi\rangle$

Examples: $\frac{1}{\sqrt{2}}(|0\rangle_A |00\rangle_B + |1\rangle_A |10\rangle_B)$

$$\text{Bell basis} \begin{cases} |\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{cases}$$

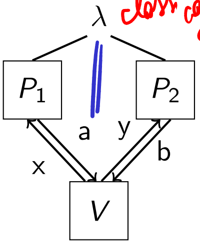
$|\psi_{ab}\rangle = (X^a Z^b \otimes I)|\psi_{00}\rangle$

CHSH

Bell inequality non-local game

Classical strategies

classical string



$x, y \in_R \{0, 1\}$

$x \cdot y = a \oplus b$

$a \neq b$ iff $x = y = 1$

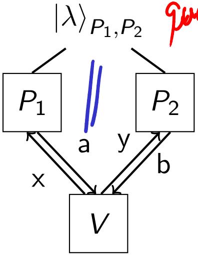
Optimal winning value

$\omega(CHSH) = 3/4$

$<$

Quantum strategies

quantum state



$x, y \in_R \{0, 1\}$

$x \cdot y = a \oplus b$

$a \neq b$ iff $x = y = 1$

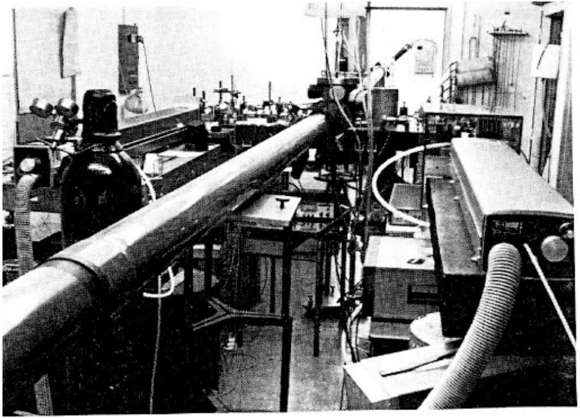
Optimal winning value

$\omega^*(CHSH) = \cos^2(\pi/8) \simeq 0.85$

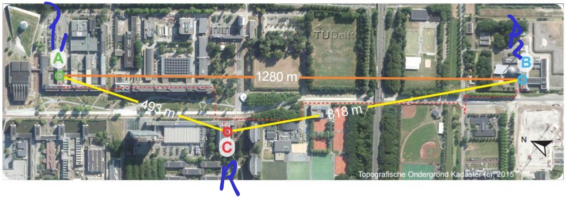
Bell inequalities

Experimental way of testing "quantumness" (or at least "super-classicality")

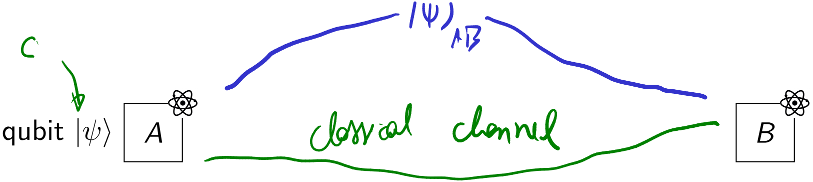
Alain Aspect (1982, Institut d'Optique)



QuTech group (2015, TU Delft)



Quantum teleportation D



Problem: Alice wants to send a qubit $|\psi\rangle$ to Bob.

If they have a quantum channel to communicate: Trivial (non-interesting)

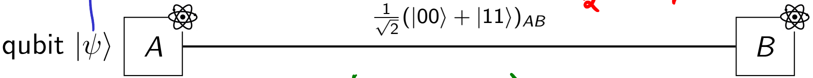
If they have a classical channel to communicate: loss of information due quantum measurements => not possible

If they have a classical channel to communicate + pre-shared quantum state:

Alice can send qubit $|\psi\rangle$ using just classical channel

Quantum teleportation

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$



$|00\rangle = \frac{1}{\sqrt{2}}(|\psi_{00}\rangle + |\psi_{01}\rangle) \left(= \frac{1}{2}\left(\underbrace{\frac{1}{\sqrt{2}}|00\rangle + \cancel{\frac{1}{\sqrt{2}}|11\rangle}}_{|\psi_{00}\rangle} + \frac{1}{\sqrt{2}}|00\rangle - \cancel{\frac{1}{\sqrt{2}}|11\rangle}\right)\right)$

$|11\rangle = \frac{1}{\sqrt{2}}(|\psi_{00}\rangle - |\psi_{01}\rangle)$

$|01\rangle = \frac{1}{\sqrt{2}}(|\psi_{10}\rangle + |\psi_{11}\rangle)$

$|10\rangle \quad \frac{1}{\sqrt{2}}(|\psi_{10}\rangle - |\psi_{11}\rangle)$

global state $\quad |\psi\rangle_{A'} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \rightsquigarrow |\psi\rangle \quad |junk\rangle_{A'A}|\psi\rangle_B$

$$\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)_{A'}(|00\rangle + |11\rangle)_{AB} = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{A'AB} + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)$$

$$= \frac{1}{2}\Big(\alpha(|\psi_{00}\rangle + |\psi_{01}\rangle)|0\rangle + \alpha(|\psi_{10}\rangle + |\psi_{11}\rangle)|1\rangle + \beta(|\psi_{10}\rangle - |\psi_{11}\rangle)|0\rangle + \beta(|\psi_{00}\rangle - |\psi_{01}\rangle)|1\rangle\Big)$$

$$= \frac{1}{2}\Big(|\psi_{00}\rangle_{A'A}(\alpha|0\rangle + \beta|1\rangle) + |\psi_{01}\rangle(\alpha|0\rangle - \beta|1\rangle) + |\psi_{10}\rangle(\alpha|1\rangle + \beta|0\rangle) + |\psi_{11}\rangle(\alpha|1\rangle - \beta|0\rangle)\Big)$$

Quantum teleportation

$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $Z|b\rangle = (-1)^b |b\rangle$

$Z^\dagger = Z$

qubit $|\psi\rangle$ A —— $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ —— B $|\psi\rangle$

w.p. 1/4 outcome $|\Psi_{00}\rangle$ then B holds $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

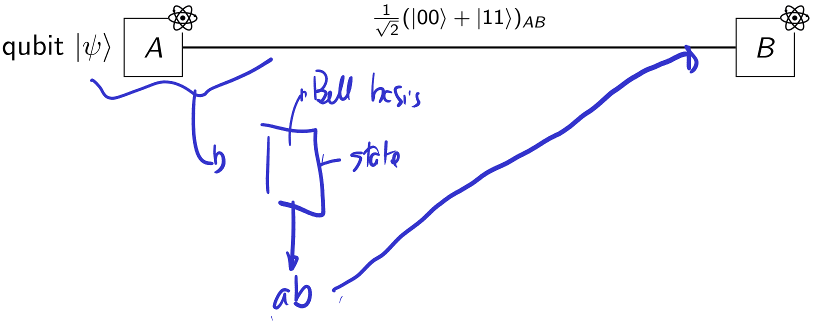
w.p. 1/4 outcome $|\Psi_{01}\rangle$ ~ $\alpha|0\rangle - \beta|1\rangle = Z|\psi\rangle$

↳ A tells Bob: outcome was $|\Psi_{01}\rangle$, Bob applies $Z^\dagger$ on $Z|\psi\rangle \Rightarrow$ he has $|\psi\rangle$

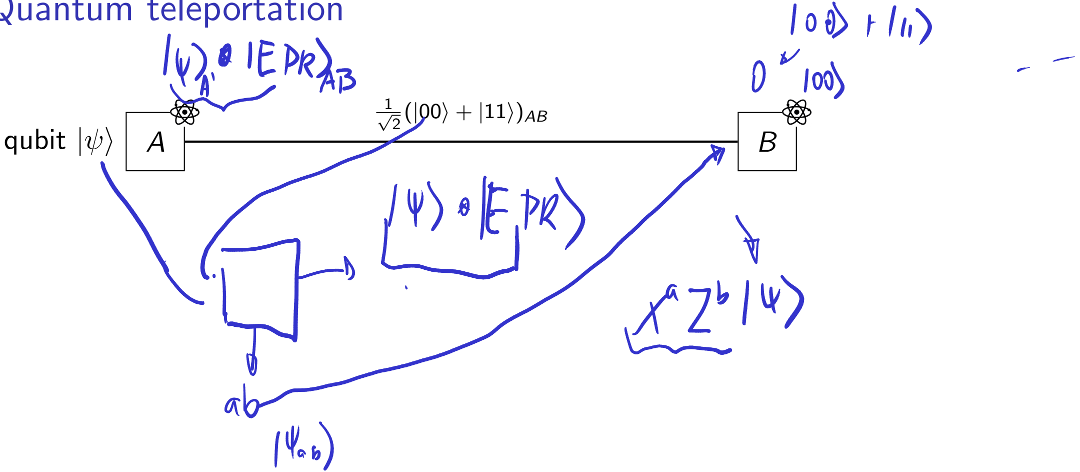
w.p. 1/4 outcome $|\Psi_{10}\rangle$ $\alpha|1\rangle + \beta|0\rangle \Rightarrow$ Bob has to apply X

w.p. 1/4 outcome $|\Psi_{11}\rangle$ $\alpha|1\rangle - \beta|0\rangle \Rightarrow$ Bob applies X and Z gate

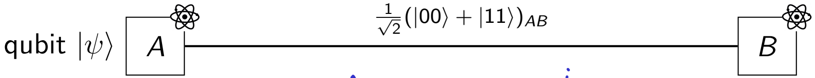
Quantum teleportation



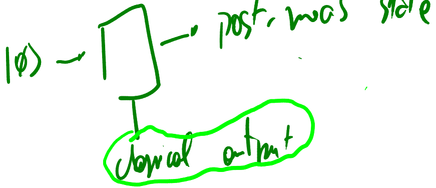
Quantum teleportation



Quantum teleportation



If A measures her 2 qubits in the Bell basis
w.p. 1/4 the outcome is $|\Phi_{00}\rangle$ and post-meas. state
is $|\Phi_{00}\rangle(\alpha|0\rangle + \beta|1\rangle) = |\Phi_{00}\rangle\underbrace{|\psi\rangle}$



Protocol:

1. Alice measures her qubits in Bell basis
2. A sends the outcome to Bob
3. B performs correction

Super-dense coding

Alice receives two random bits a and b and she wants Bob to learn both of them.

If Alice sends a single classical bit:

If Alice sends a single qubit:

Super-dense coding

$a,b \in \{0,1\}$

A ——— $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ ——— B

① Send a and b classically: 2 bits are necessary

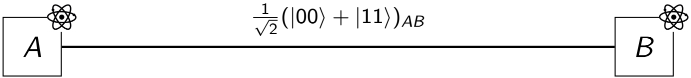
② If they share an EPR pair: 1 qubit suffices

↳ $(\underbrace{X^a Z^b}_{\text{Alice applies gates}} \otimes I)|\Psi_{00}\rangle_{AB} = |\Psi_{ab}\rangle$

↳ measure the state on Bell basis

↳ Bob recovers a and b

Super-dense coding



$|00\rangle + |11\rangle$ cannot write $|\phi_0\rangle \otimes |\phi_1\rangle$

$|\psi_{00}\rangle_{AB}$

$A \xrightarrow[\text{1 qubit}]{} B$

Mixed states

- Mixed states: probabilistic distribution of quantum states

Examples

$((\frac{1}{2}, |0\rangle), (\frac{1}{2}, |+\rangle))$, $((\frac{1}{3}, |0\rangle), (\frac{2}{3}, |1\rangle))$

- Density matrices: mathematical representation of mixed states
  $(1, |\psi\rangle)$

  $((p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), ..., (p_k, |\psi_k\rangle))$

- Properties of density matrices
  - Its trace is 1 (The trace of a square matrix is $\sum_i a_{i,i}$)
  - Positive semi-definitive (all its eigenvalues are non-negative)
- Definition of evolution and measurements can be extended to density matrices

"Parts" of quantum states

- Trace-out: ignore qubits of a larger quantum state

$$Tr_B(|a_1, b_1\rangle\langle a_2, b_2|_{A,B}) = \langle b_1|\, b_2\rangle\, |a_1\rangle\langle a_2|$$

Quantum algorithms

Quantum operations

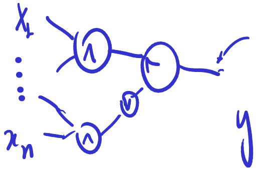
Evolution of quantum states is described by unitary operators

- $UU^\dagger = U^\dagger U = I$
  - For every quantum state $|\psi\rangle$, $U|\psi\rangle$ is also a quantum state
  - Reversible: no information loss $U|\psi\rangle \xrightarrow{U^\dagger} |\psi\rangle$
- Equivalent models of quantum computation:
  - Quantum Turing Machines
  - Quantum circuits
  - Adiabatic quantum computation
  - Measurement-based quantum computation
  - ...

Classical circuits

Problem Π $\qquad \{C_n\}_{n\in\mathbb{N}}$

↳ C_n solve problem for inputs of size n

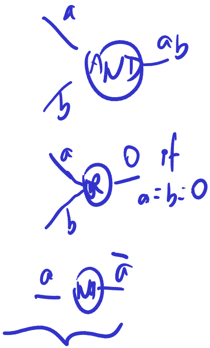


solution to your problem on input $x_1, \dots, x_n$

$$AND(0,1) = AND(1,0) = 1$$

$\wedge, \vee, \neg$ are sufficient to compute all functions

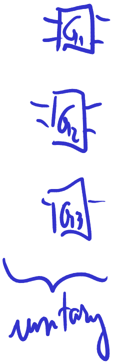
Classical circuits



construct larger circuits by connecting gates

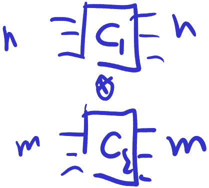
are sufficient to compute <u>all</u> possible functions

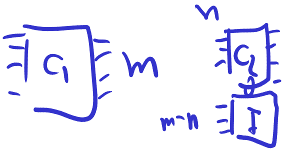
Quantum circuits



composing gates

· tensor product





n + m input/output

· sequential composition

n input/outputs

Universal gateset

Definition

~~ε-approximation~~ An n-qubit unitary U ε-approximates an n-qubit unitary U' if

$$\max_{|\psi\rangle\in\mathbb{C}^{2^n}} \| U|\psi\rangle - U'|\psi\rangle \| \leq \varepsilon.$$

most general operation allowed by Q. Machines

Definition

// $\{G_1, \ldots, G_k\}$ $\forall \varepsilon$

Universal gateset A gateset $\mathcal{G}$ is universal if for every unitary U, there exists a unitary U' composed by gates in $\mathcal{G}$ such that U' ε-approximates U.

$2^n \times 2^n$

Tensor product + sequential composition

Lemma

The following gatesets are universal:

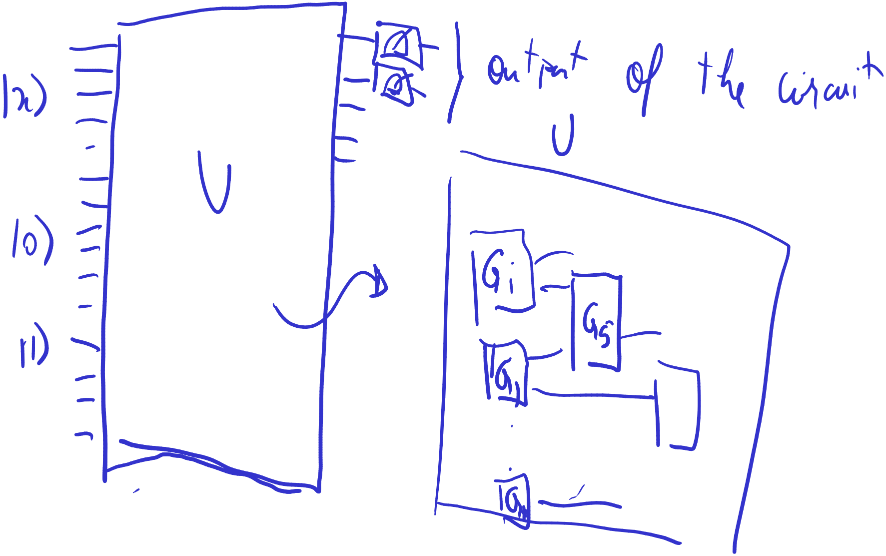
$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \text{unitary} \right\} \cup \{ CNOT : CNOT|a\rangle|b\rangle = |a\rangle|b \oplus a\rangle \}$

flips 3rd qubit if $a=b=1$

- $\{1\text{-qubit gates}, CNOT\}$
- $\{CNOT, H, T\}$ $H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$ $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
- $\{H, CCNOT\}$ *(for unitaries with real entries)*

$CCNOT|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|c \oplus ab\rangle$

Template for quantum circuits



Template for quantum circuits

$|\psi_0\rangle$ $|\psi_1\rangle$ $|\psi_2\rangle \cdots |\psi_T\rangle$

measure them

wp P_i output 1

Oracle gates

$\mathcal{F}$ - known family of functions

Pick $f \in \mathcal{F}$ but keep it unknown

Classical oracles

$$x \to \boxed{f} \to f(x)$$

How many queries do we need to learn properties of this box?

Quantum oracles

unitary

$$\begin{array}{l} |x\rangle \\ |b\rangle \end{array} \boxed{U_f} \begin{array}{l} |x\rangle \\ |b \oplus f(x)\rangle \end{array}$$

How many quantum queries do we need to learn properties of f?

Deutsch-Josza algorithm

Problem

Given oracle access to $f : \{0,1\}^n \to \{0,1\}$ with the promise that:

- f is constant $f(x)=0$ or $f(x)=1$
- f is balanced $|f^{-1}(0)| = |f^{-1}(1)|$

Find out which is the case.

Deutsch-Josza algorithm

Problem

Given oracle access to $f : \{0,1\}^n \to \{0,1\}$ with the promise that:

- f is constant
- f is balanced → first $2^n/2$ inputs have output 0, ..

Find out which is the case.

Deterministic algorithms: need $2^n/2+1$ queries to solve it in worst case

Randomized algorithms: pick k inputs uniformly at random

. f is constant ⇒ always see the same output

. f is balanced ⇒ $\exists$ two different outputs except w.p. $\frac{1}{2^{k-1}}$

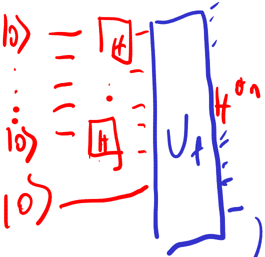
Quantum algorithms: 1 quantum query is sufficient w.p. 1

Quantum parallelism

$$H|b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b |1\rangle\right)$$

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$



$$|0\ldots0\rangle = (H|0\rangle) \otimes (H|0\rangle) \ldots \otimes (H|0\rangle)$$

$$= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes n} =$$

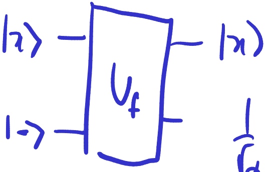
$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Quantum parallelism

$|x\rangle \to \boxed{\tilde{U}_f} \to (-1)^{f(x)}|x\rangle$ – phase oracle

(1)



$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$

$$\frac{1}{\sqrt{2}}|f(x)\rangle - \frac{1}{\sqrt{2}}|1 \oplus f(x)\rangle$$

→ if $f(x) = 0$

$\to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$

→ if $f(x) = 1$

$\to \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle = -|-\rangle$

$= -\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

$$U_f\left(\sum_x \alpha_x |x\rangle|-\rangle\right) = \sum_x \alpha_x \cdot (-1)^{f(x)}|x\rangle|-\rangle$$

Quantum parallelism

(2) $H^{\otimes n}\left(|x_1\rangle \dots |x_n\rangle\right) = \left(H|x_1\rangle\right) \otimes \left(H|x_2\rangle\right) \dots \left(H|x_n\rangle\right) =$

$$= \frac{1}{\sqrt{2}}\Big(\underbrace{|0\rangle + (-1)^{x_1}|1\rangle}_{y_1}\Big) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_2}|1\rangle\right) \dots \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_n}|1\rangle\right)$$

inner product

$$= \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x_1 y_1}(-1)^{x_2 y_2}\dots(-1)^{x_n y_n}|y\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle$$

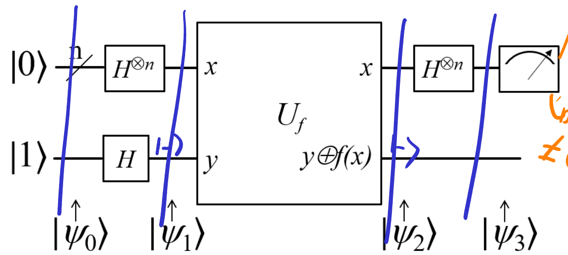
$y_1 = 1$ and $x_1 = 1 \Rightarrow$ have phase -1

$$\frac{1}{2}\left(|0\rangle + (-1)^{x_1}|1\rangle\right)\left(|0\rangle + (-1)^{x_2}|1\rangle\right) = \frac{1}{2}\Big(|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_1}|10\rangle + (-1)^{x_1+x_2}|11\rangle\Big)$$

$$\sum_{y\in\{0,1\}^2} (-1)^{y_1 x_1}(-1)^{y_2 x_2}|y_1\rangle|y_2\rangle$$

Deutsch-Josza algorithm

$|0\rangle^{\otimes n}$



$0\ldots0$ f is constant

or

$\neq 0\ldots0$ f is balanced

Analysis

$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$ before $H^{\otimes n+1}$

$|\psi_1\rangle = H^{\otimes(n+1)}|\psi_0\rangle = \left(H^{\otimes n}|0\rangle^{\otimes n}\right)\otimes\left(H|1\rangle\right) =$ after $H^{\otimes n+1}$

$= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \otimes |-\rangle$

Deutsch-Josza algorithm

Analysis

After the oracle call. $U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|-\rangle\right) =$

$$= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-\rangle$$

After $H^{\otimes n}$ $\quad (H^{\otimes n}\otimes I)\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-1\rangle\right)$

$$\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}H^{\otimes n}|x\rangle|-1\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_x(-1)^{f(x)}\sum_y\frac{1}{\sqrt{2^n}}(-1)^{x\cdot y}|y\rangle|-\rangle$$

Deutsch-Josza algorithm

Analysis

$$= \frac{1}{2^n} \sum_x \sum_y \underbrace{(-1)^{f(x)+x\cdot y}}\ |y\rangle|-\rangle$$

Amplitude of: $y = \underbrace{0 \cdot 0}_{n \text{ times}}$

$$\alpha_y = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x\cdot(0..0)} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$$

a) f is constant: $\alpha_0 = (-1)^{f(0)} \frac{2^n}{2^n} = (-1)^{f(0)}$

b) f is balanced: $\alpha_0 = 0$

$$\Pr[\text{output } \underbrace{0 . 0}_{n}] = |\alpha_0|^2$$

$((-1)^{f(0)})^2 = 1$ constant

$(0)^2 = 0$ balanced

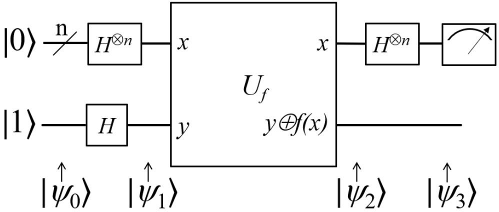
Deutsch-Josza algorithm

Problem

Given oracle access to $f : \{0,1\}^n \to \{0,1\}$ with the promise that:

- f is constant
- f is balanced

Find out which is the case.



Simon's algorithm

Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

$$\exists s \neq 0^n \text{ such that } f(x) = f(y) \text{ iff } y \in \{x, s \oplus y\}.$$

Find s.

Simon's algorithm

Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

$$\exists s \neq 0^n \text{ such that } f(x) = f(y) \text{ iff } y \in \{x, s \oplus y\}.$$

Find s.

Deterministic algorithms:

Randomized algorithms:

Simon's algorithm

Lemma

With a single quantum query, we can compute a random $d \in \{0,1\}^n$ such that

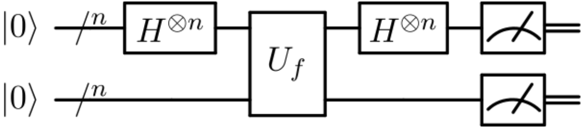
$$d \cdot s = 0.$$

Theorem

There is a quantum algorithm that retrieves s with high probability with $O(n)$ queries.

Proof

Simon's algorithm - sampling d s.t. $d \cdot s = 0$



Analysis

Simon's algorithm

Analysis (cont.)

Simon's algorithm - recap

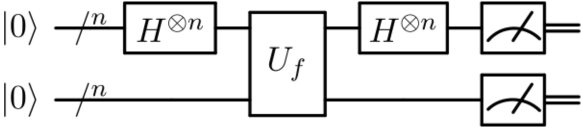
Problem

Given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

$$\exists s \neq 0^n \text{ such that } f(x) = f(y) \text{ iff } y \in \{x, s \oplus y\}.$$

Find s.

The following circuit samples random d such that



Sampling it $O(n)$ times, with high probability we have n linearly independent d_i's and we can solve the following linear system of equations to compute s

$$\forall 1 \leq i \leq n, d_i \cdot s = 0.$$