ACCQ 206 - Entanglement and quantum algorithms

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

Product states vs. entangled states

Product states

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

Example: $|+\rangle \otimes |+\rangle$, $(|00\rangle + |11\rangle) \otimes |0\rangle$

Entangled states

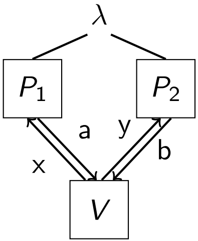
Can**not** be written as $|\psi\rangle \otimes |\phi\rangle$

Examples: $(|0\rangle_A |00\rangle_B + |1\rangle_A |10\rangle_B)$

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

CHSH

Classical strategies

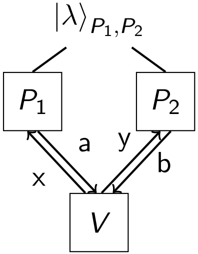


$$x, y \in_R \{0,1\}$$
$$x \cdot y = a \oplus b$$
$$a \neq b \text{ iff } x = y = 1$$

Optimal winning value

$$\omega(CHSH) = 3/4$$

Quantum strategies



$$x, y \in_R \{0,1\}$$
$$x \cdot y = a \oplus b$$
$$a \neq b \text{ iff } x = y = 1$$

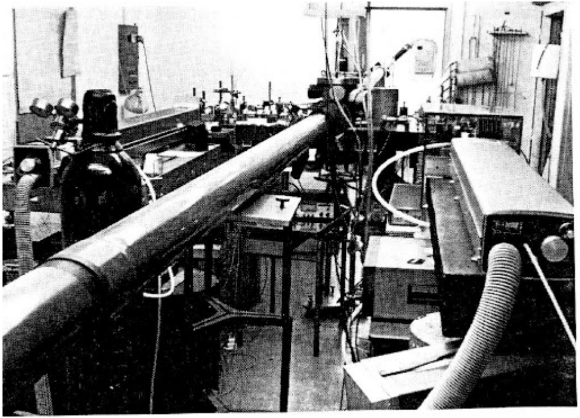
Optimal winning value

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

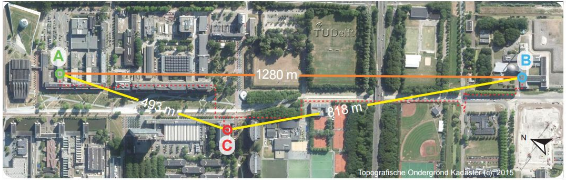
Bell inequalities

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

Alain Aspect (1982, Institut d'Optique)



QuTech group (2015, TU Delft)



Quantum teleportation

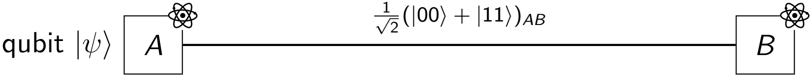
Problem: Alice wants to send a qubit $|\psi\rangle$ to Bob.

If they have a quantum channel to communicate:

If they have a classical channel to communicate:

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

Quantum teleportation



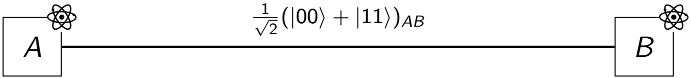
Super-dense coding

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



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
  $(1, |\psi\rangle)$

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

- 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
- Equivalent models of quantum computation:
  - Quantum Turing Machines
  - Quantum circuits
  - Adiabatic quantum computation
  - Measurement-based quantum computation
  - ...

Classical circuits

Quantum circuits

Universal gateset

Definition

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

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

Definition

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.

Lemma

The following gatesets are universal:

- $\{1\text{-}qubit\ gates, CNOT\}$
- $\{CNOT, H, T\}$
- $\{H, CCNOT\}$ *(for unitaries with real entries)*

Template for quantum circuits

Oracle gates

Classical oracles

Quantum oracles

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.

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.

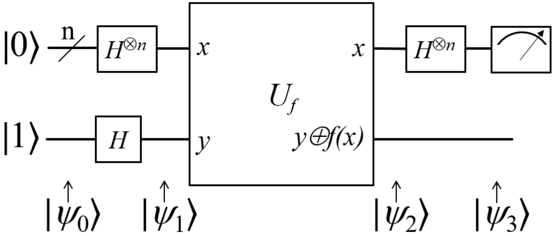
Deterministic algorithms:

Randomized algorithms:

Quantum algorithms:

Quantum parallelism

Deutsch-Josza algorithm



Analysis

Deutsch-Josza algorithm

Analysis

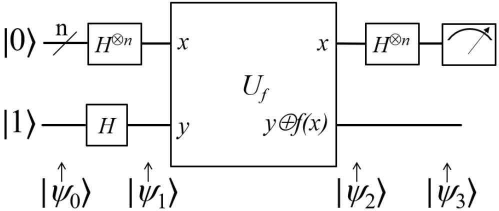
Deutsch-Josza algorithm

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

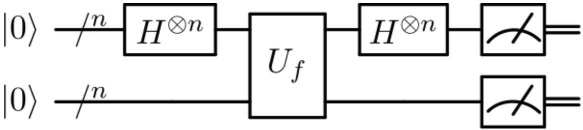
$$d \cdot s = 0.$$

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

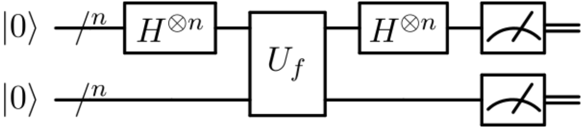
Problem

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

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