Qubit 2003

Quantum Computation Without Entanglement

Eli Biham	Technion
Gilles Brassard	Université de Montréal
Dan Kenigsberg	Technion
Tal Mor	Technion

Where Does The Power of Quantum Computation Come From?

- ◇ Superposition?

Where Does The Power of Quantum Computation Come From?

- ◇ Superposition?
- ◇ Linearity?

Where Does The Power of Quantum Computation Come From?

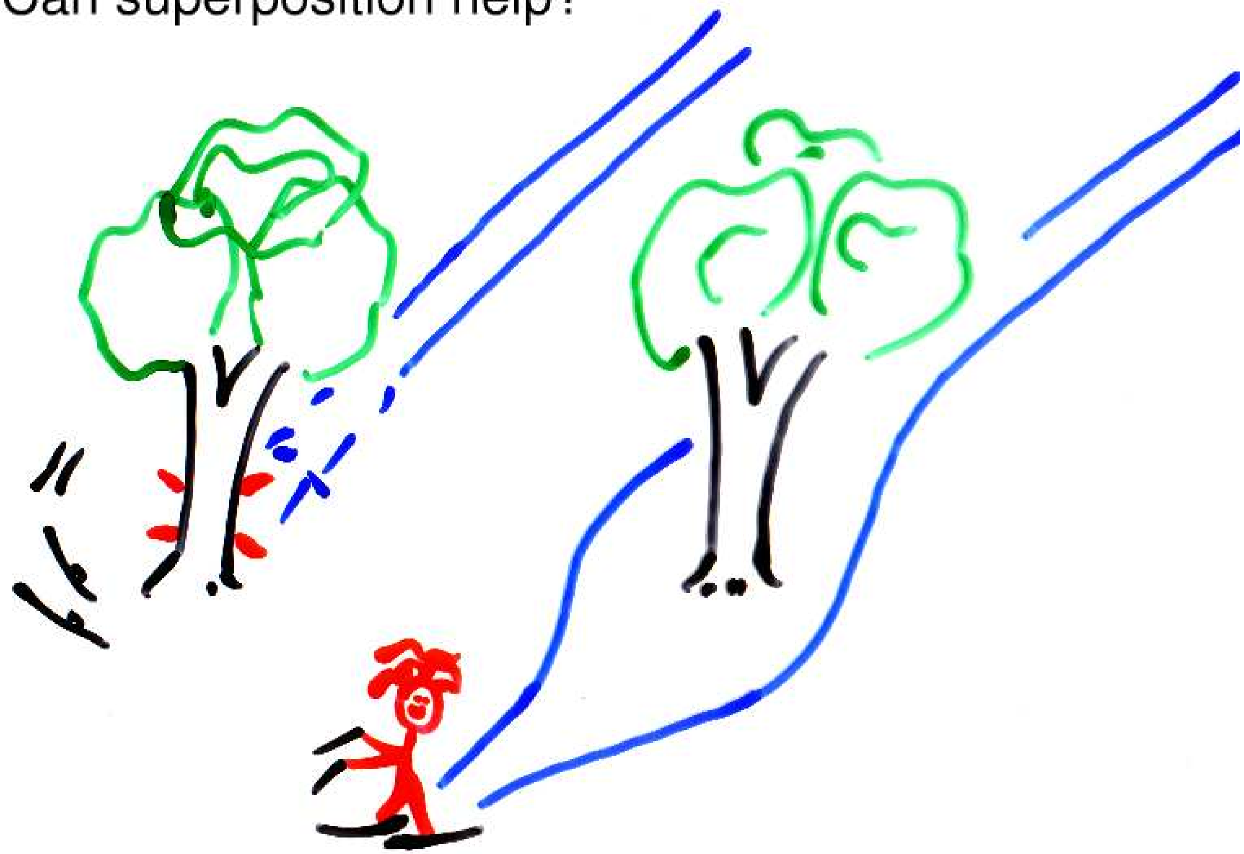
- ◇ Superposition?
- ◇ Linearity?
- ◇ Entanglement?

Where Does The Power of Quantum Computation Come From?

- ◇ Superposition?
- ◇ Linearity?
- ◇ Entanglement?
- ◇ $\cdots$?

Superposition Can Be Useful

Can superposition help?



Is Entanglement Necessary?

"For any quantum algorithm operating on pure states we prove that the presence of multi-partite entanglement [. . .] is necessary if the quantum algorithm is to offer an exponential speed-up over classical computation."

— Jozsa and Linden, quant-ph/0201143

Separable Pure States

Definition: *Separable* pure states can be factored as the tensor product of a state of qubit A and a state of qubit B.

Separable Pure States

Definition: *Separable* pure states can be factored as the tensor product of a state of qubit A and a state of qubit B;
Entangled states are those that are not separable.

Separable Pure States

Definition: *Separable* pure states can be factored as the tensor product of a state of qubit A and a state of qubit B;
Entangled states are those that are not separable.

Example: State $|\Phi^+\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$ is entangled.

Separable Pure States

Definition: *Separable* pure states can be factored as the tensor product of a state of qubit A and a state of qubit B;
Entangled states are those that are not separable.

Example: State $|\Phi^+\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$ is entangled.

Proof: Separable two-qubit pure states can be written as

$$\begin{aligned} & (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ = \quad & \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \, . \end{aligned}$$

Separable Pure States

Definition: *Separable* pure states can be factored as the tensor product of a state of qubit A and a state of qubit B;
Entangled states are those that are not separable.

Example: State $|\Phi^+\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$ is entangled.

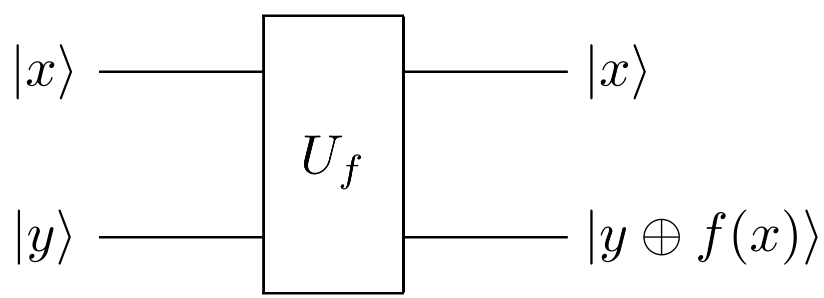
Proof: Separable two-qubit pure states can be written as

$$\begin{aligned} & (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ = \quad & \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \,. \end{aligned}$$

No choice of $\alpha, \beta, \gamma, \delta$ can induce $\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}}$ and $\alpha\delta = \beta\gamma = 0$ because the first equation requires that $\alpha\gamma\beta\delta = \frac{1}{2}$ and the second requires that $\alpha\delta\beta\gamma = 0$.

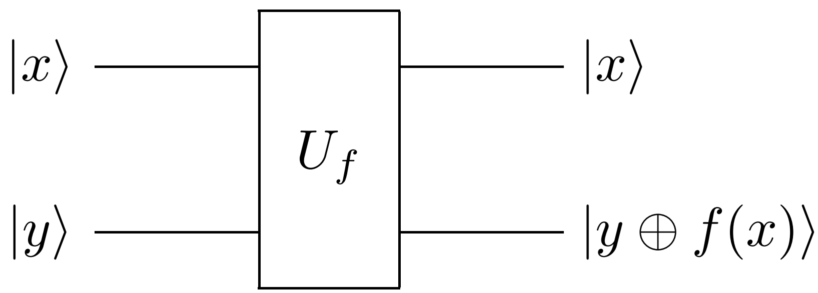
Quantum Computation

Consider function $f : \{0,1\}^n \rightarrow \{0,1\}^m$.



Quantum Computation

Consider function $f : \{0,1\}^n \rightarrow \{0,1\}^m$.



Exponentially many values can be computed simultaneously if we start with a superposition.

$$U_f \sum_{i=1}^{2^n} \alpha_i |x_i\rangle |y\rangle = \sum_{i=1}^{2^n} \alpha_i |x_i\rangle |y \oplus f(x_i)\rangle$$

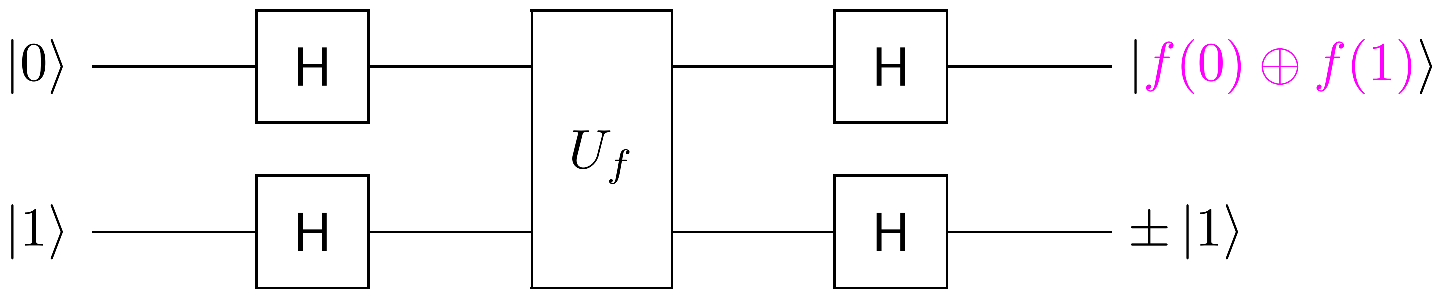
Deutsch's Problem

Consider function $f : \{0, 1\} \rightarrow \{0, 1\}$.

We want to know whether or not $f(0) = f(1)$.

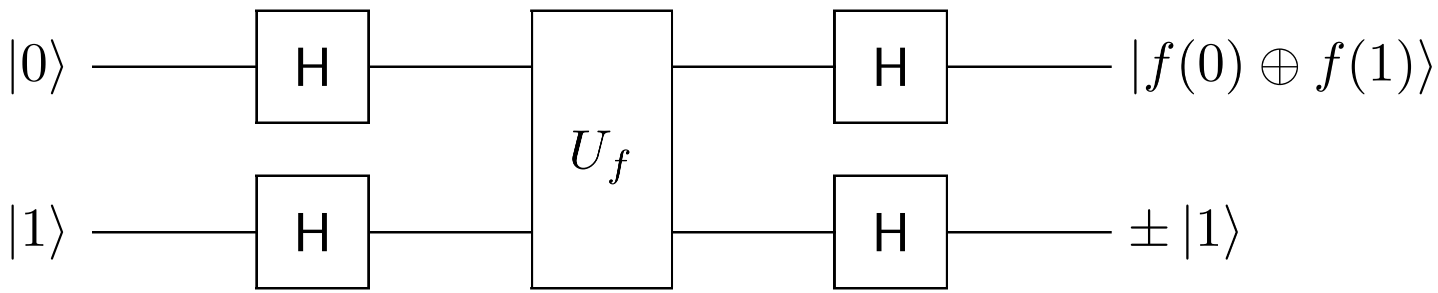
Deutsch's Algorithm

Consider function $f : \{0, 1\} \rightarrow \{0, 1\}$.
We want to know whether or not $f(0) = f(1)$.



Deutsch's Algorithm

Consider function $f : \{0,1\} \to \{0,1\}$.
We want to know whether or not $f(0) = f(1)$.

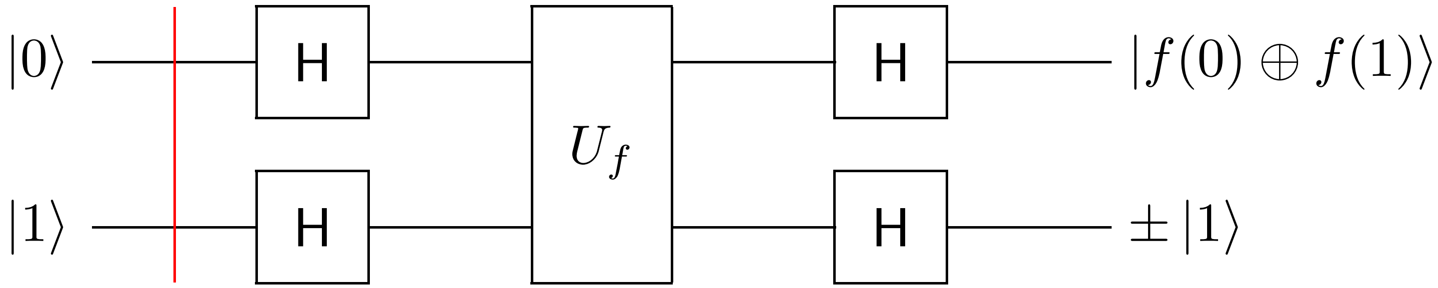


We can determine whether or not $f(0) = f(1)$ with a single call on a circuit that computes function f.

This would be impossible for a classical computer!

Deutsch's Algorithm

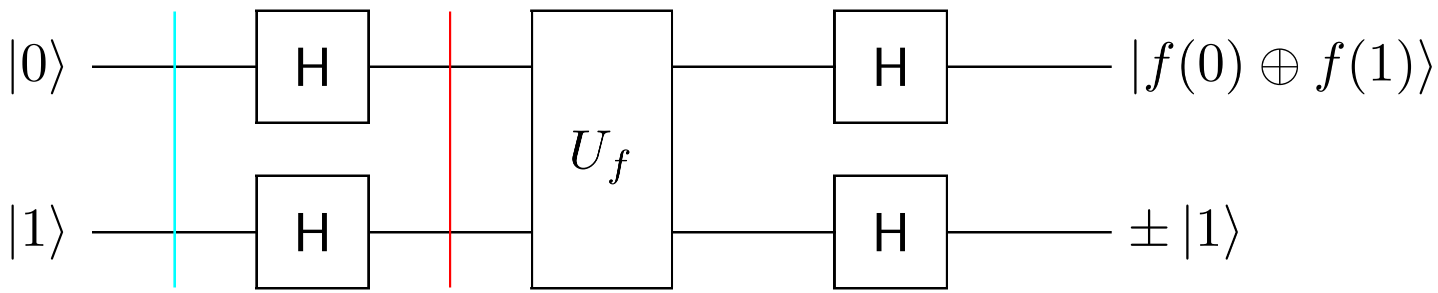
Consider function $f : \{0,1\} \to \{0,1\}$.
We want to know whether or not $f(0) = f(1)$.



No entanglement here.

Deutsch's Algorithm

Consider function $f : \{0,1\} \to \{0,1\}$.
We want to know whether or not $f(0) = f(1)$.

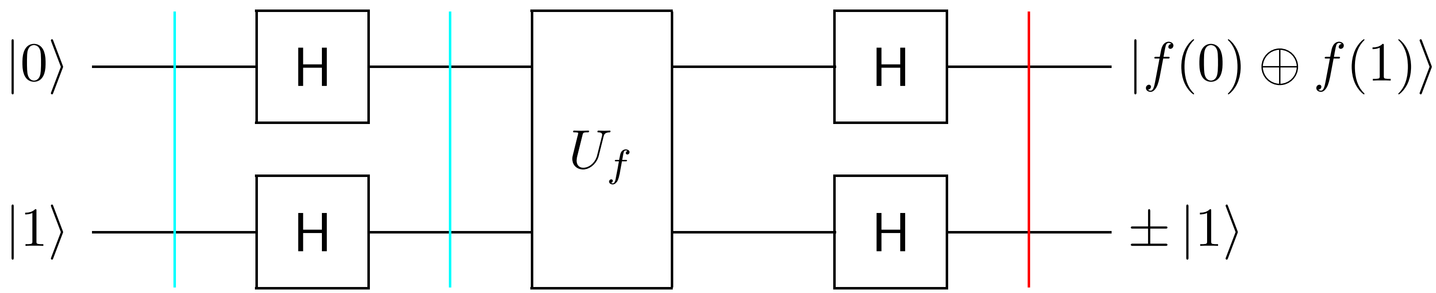


No entanglement here.

No entanglement here either.

Deutsch's Algorithm

Consider function $f : \{0,1\} \to \{0,1\}$.
We want to know whether or not $f(0) = f(1)$.

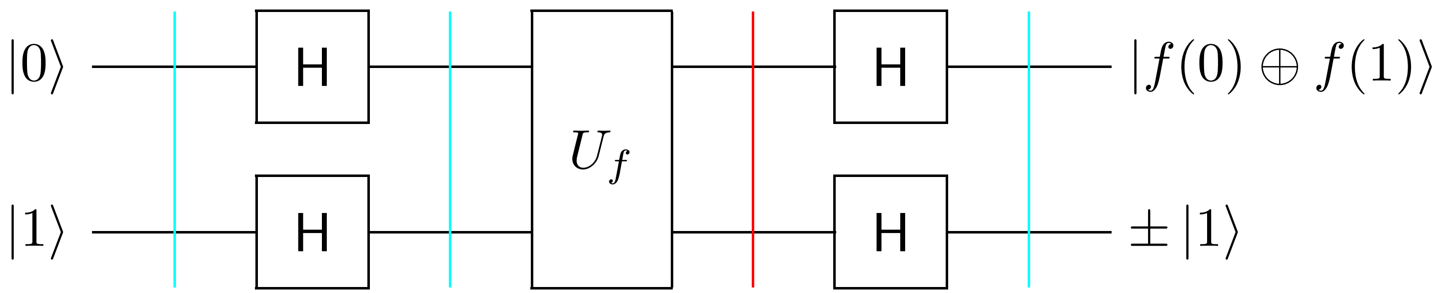


No entanglement here.

No entanglement here either.

Deutsch's Algorithm

Consider function $f : \{0, 1\} \to \{0, 1\}$.
We want to know whether or not $f(0) = f(1)$.

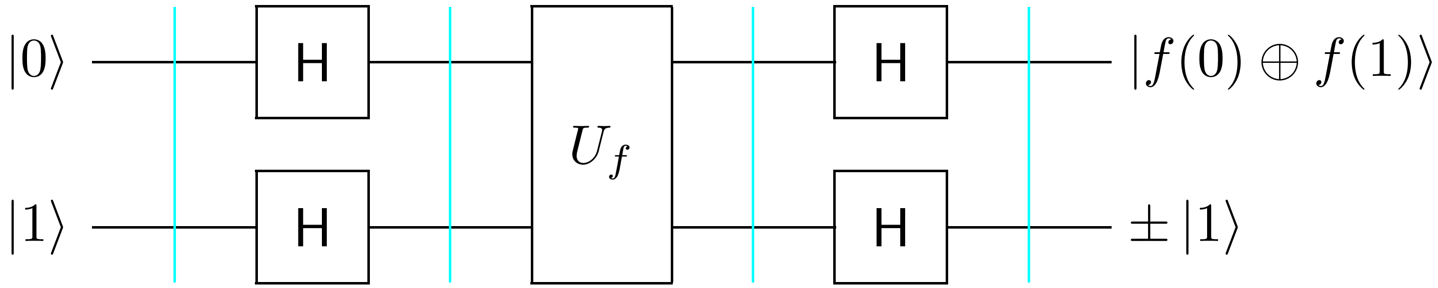


No entanglement here.

No entanglement anywhere!

Deutsch's Algorithm

Consider function $f : \{0,1\} \to \{0,1\}$.
We want to know whether or not $f(0) = f(1)$.

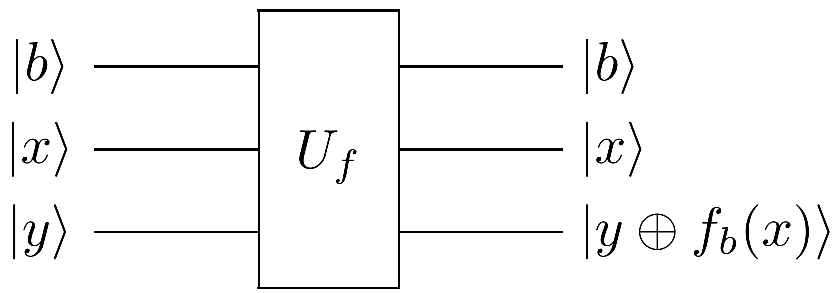


No entanglement anywhere!

Really?

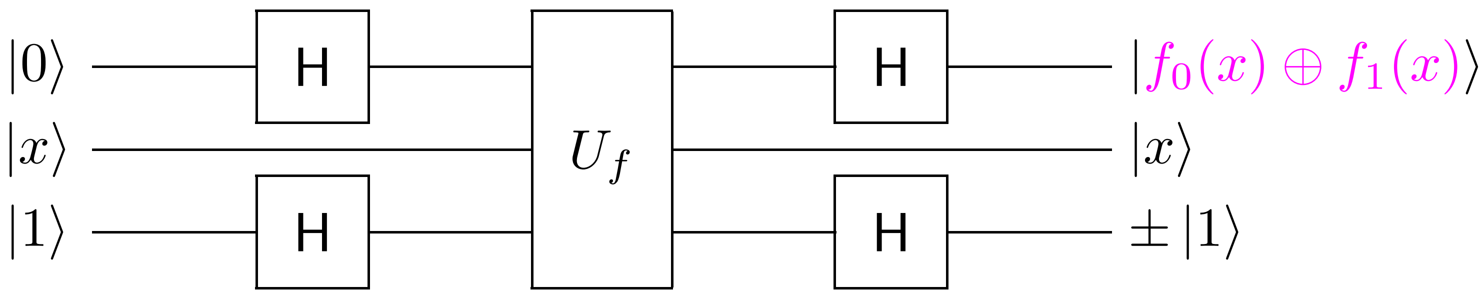
Deutsch's Algorithm

Consider functions $f_0 : \{0,1\}^n \rightarrow \{0,1\}$ and $f_1 : \{0,1\}^n \rightarrow \{0,1\}$.
We want to know whether or not $f_0(x) = f_1(x)$ for given x.



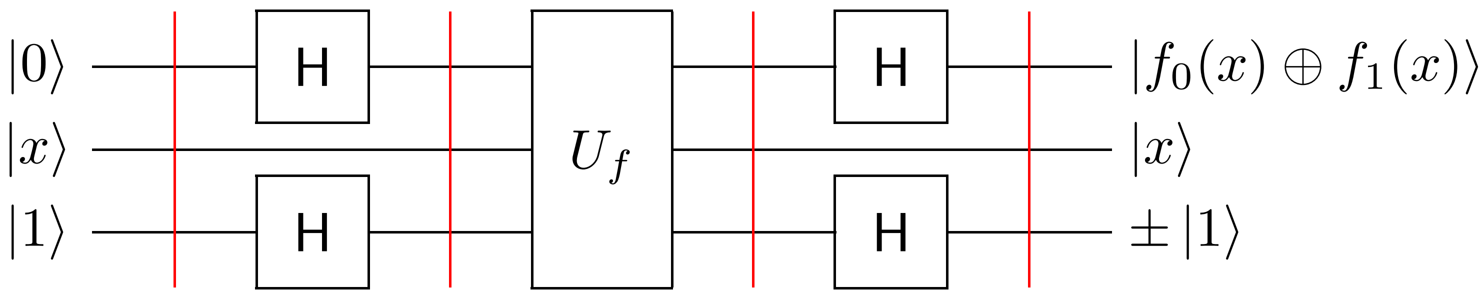
Deutsch's Algorithm

Consider functions $f_0 : \{0,1\}^n \rightarrow \{0,1\}$ and $f_1 : \{0,1\}^n \rightarrow \{0,1\}$.
We want to know whether or not $f_0(x) = f_1(x)$ for given x.



Deutsch's Algorithm

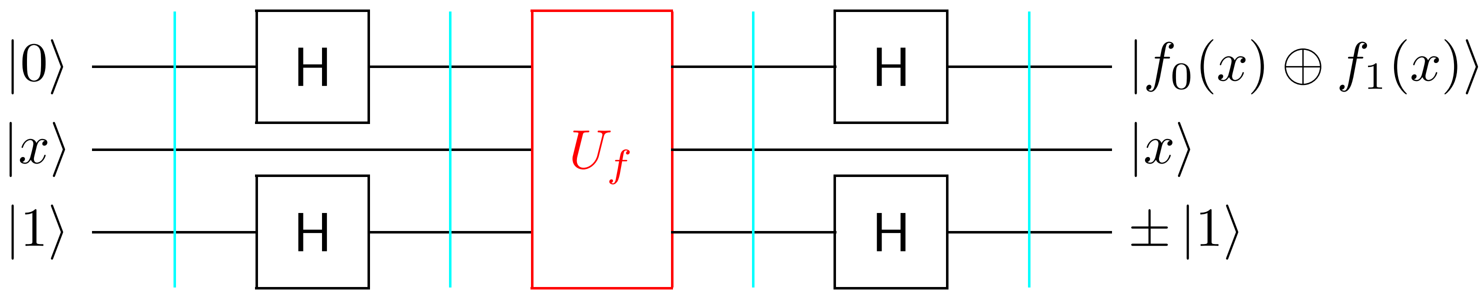
Consider functions $f_0 : \{0,1\}^n \to \{0,1\}$ and $f_1 : \{0,1\}^n \to \{0,1\}$.
We want to know whether or not $f_0(x) = f_1(x)$ for given x.



No entanglement here

Deutsch's Algorithm

Consider functions $f_0 : \{0,1\}^n \to \{0,1\}$ and $f_1 : \{0,1\}^n \to \{0,1\}$.
We want to know whether or not $f_0(x) = f_1(x)$ for given x.



No entanglement here

Lots of entanglement there!

Mixed States

Definition: A mixed state ρ is *separable* if it can be written as

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$$

where each $|\psi_i\rangle = |\psi_i\rangle_A \otimes |\psi_i\rangle_B$ is separable.

Mixed States

Definition: A mixed state ρ is *separable* if it can be written as

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$$

where each $|\psi_i\rangle = |\psi_i\rangle_A \otimes |\psi_i\rangle_B$ is separable.

Such states can be prepared by local operations at A and B given classical communication *and the power of forgetting*:

- ◇ A chooses some i with probability p_i and tells B the choice of i;
- ◇ A prepares $|\psi_i\rangle_A$ and B prepares $|\psi_i\rangle_B$; now they share $|\psi_i\rangle$;
- ◇ Both A and B *forget* the choice of i ; now they share ρ.

Mixed States

Definition: A mixed state ρ is *separable* if it can be written as

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$$

where each $|\psi_i\rangle = |\psi_i\rangle_A \otimes |\psi_i\rangle_B$ is separable.

Such states can be prepared by local operations at A and B given classical communication *and the power of forgetting*:

- ◇ A chooses some i with probability p_i and tells B the choice of i;
- ◇ A prepares $|\psi_i\rangle_A$ and B prepares $|\psi_i\rangle_B$; now they share $|\psi_i\rangle$;
- ◇ Both A and B *forget* the choice of i ; now they share ρ.

This is very different from requiring that $\rho = \rho_A \otimes \rho_B$.

Example of Separable Mixed State

A mixture of entangled states may be separable.

Example of Separable Mixed State

A mixture of entangled states may be separable.

Example: Consider $|\Psi^{\pm}\rangle = \dfrac{|01\rangle \pm |10\rangle}{\sqrt{2}}$ and $\rho_{\pm} = |\Psi^{\pm}\rangle\langle\Psi^{\pm}|$.

Both

$$\rho_{\pm} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

are entangled.

Example of Separable Mixed State

A mixture of entangled states may be separable.

Example: Consider $|\Psi^\pm\rangle = \dfrac{|01\rangle \pm |10\rangle}{\sqrt{2}}$ and $\rho_\pm = |\Psi^\pm\rangle\langle\Psi^\pm|$.

Both

$$\rho_\pm \;=\; \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

are entangled, yet their equal mixture

$$\frac{1}{2}\rho_+ + \frac{1}{2}\rho_- \;=\; \frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|$$

is separable.

Pseudo-Pure States

Consider some pure state $|\psi\rangle$ in $\mathcal{H}_N$ and probability $\varepsilon > 0$.

Pseudo-Pure States

Consider some pure state $|\psi\rangle$ in $\mathcal{H}_N$ and probability $\varepsilon > 0$.

Pseudo-pure states are mixed states in which $|\psi\rangle$ occurs with probability ε and all basis states appear with remaining equal probability $\frac{1-\varepsilon}{N}$.

$$\rho \;=\; \varepsilon|\psi\rangle\langle\psi| + \frac{1-\varepsilon}{N} I_N$$

Pseudo-Pure States

Consider some pure state $|\psi\rangle$ in $\mathcal{H}_N$ and probability $\varepsilon > 0$.

Pseudo-pure states are mixed states in which $|\psi\rangle$ occurs with probability ε and all basis states appear with remaining equal probability $\frac{1-\varepsilon}{N}$.

$$\rho \ = \ \varepsilon|\psi\rangle\langle\psi| + \frac{1-\varepsilon}{N} I_N$$

Pseudo-pure states "behave" like pure states no matter how mixed:

$$U\rho U^\dagger \ = \ \varepsilon U|\psi\rangle\langle\psi|U^\dagger + \frac{1-\varepsilon}{N} I_N$$

Pseudo-Pure States

Consider some pure state $|\psi\rangle$ in $\mathcal{H}_N$ and probability $\varepsilon > 0$.

Pseudo-pure states are mixed states in which $|\psi\rangle$ occurs with probability ε and all basis states appear with remaining equal probability $\frac{1-\varepsilon}{N}$.

$$\rho \;=\; \varepsilon|\psi\rangle\langle\psi| + \frac{1-\varepsilon}{N} I_N$$

Pseudo-pure states "behave" like pure states no matter how mixed:

$$U\rho U^\dagger \;=\; \varepsilon U|\psi\rangle\langle\psi|U^\dagger + \frac{1-\varepsilon}{N} I_N$$

Pseudo-purity ε is conserved by unitary operations.

Separable Pseudo-Pure States

Braunstein, Caves, Jozsa, Linden, Popescu and Schack's Bound

In any dimension N and for any $|\psi\rangle$, the pseudo-pure state

$$\varepsilon|\psi\rangle\langle\psi| + \frac{1-\varepsilon}{N} I_N$$

is separable whenever $\varepsilon < \frac{2}{N^2}$.

Separable Pseudo-Pure States

Braunstein, Caves, Jozsa, Linden, Popescu and Schack's Bound

In any dimension N and for any $|\psi\rangle$, the pseudo-pure state

$$\varepsilon|\psi\rangle\langle\psi| + \frac{1-\varepsilon}{N} I_N$$

is separable whenever $\varepsilon < \frac{2}{N^2}$.

These pseudo-pure states appear naturally in NMR experiments.

Is Entanglement Necessary?

◇ "... this Letter suggest[s] that current NMR experiments are not true quantum computations, since no entanglement appears in the physical states at any stage.", Braunstein, Caves, Jozsa, Linden, Popescu & Schack, PRL 83(5)1054, 1999.

Is Entanglement Necessary?

- "... this Letter suggest[s] that current NMR experiments are not true quantum computations, since no entanglement appears in the physical states at any stage.", Braunstein, Caves, Jozsa, Linden, Popescu & Schack, PRL 83(5)1054, 1999.
- "Whether or not entanglement is a necessary condition for quantum computation is a question of fundamental importance", Linden & Popescu, PRL 87(4)047901, 2001.

Is Entanglement Necessary?

- "… this Letter suggest[s] that current NMR experiments are not true quantum computations, since no entanglement appears in the physical states at any stage.", Braunstein, Caves, Jozsa, Linden, Popescu & Schack, PRL 83(5)1054, 1999.
- "Whether or not entanglement is a necessary condition for quantum computation is a question of fundamental importance", Linden & Popescu, PRL 87(4)047901, 2001.
- "Can this [using small ε] provide a computational benefit (over classical computations) in the total absence of entanglement?", Jozsa & Linden, quant-ph/0201143, 2002.

The Deutsch-Jozsa Problem

Function $f : \{0,1\}^n \to \{0,1\}$ is promised to be *constant* or *balanced*.

DJ's problem: Decide which is the case.

The Deutsch-Jozsa Problem

Function $f:\{0,1\}^n \rightarrow \{0,1\}$ is promised to be *constant* or *balanced*.

DJ's problem: Decide which is the case. *Errors are not tolerated.*

The Deutsch-Jozsa Problem

Function $f : \{0,1\}^n \to \{0,1\}$ is promised to be *constant* or *balanced*.

DJ's problem: Decide which is the case. *Errors are not tolerated.*

- Classical exact solution: $2^{n-1} + 1$ queries are required.

The Deutsch-Jozsa Problem

Function $f : \{0,1\}^n \to \{0,1\}$ is promised to be *constant* or *balanced*.

DJ's problem: Decide which is the case. *Errors are not tolerated.*

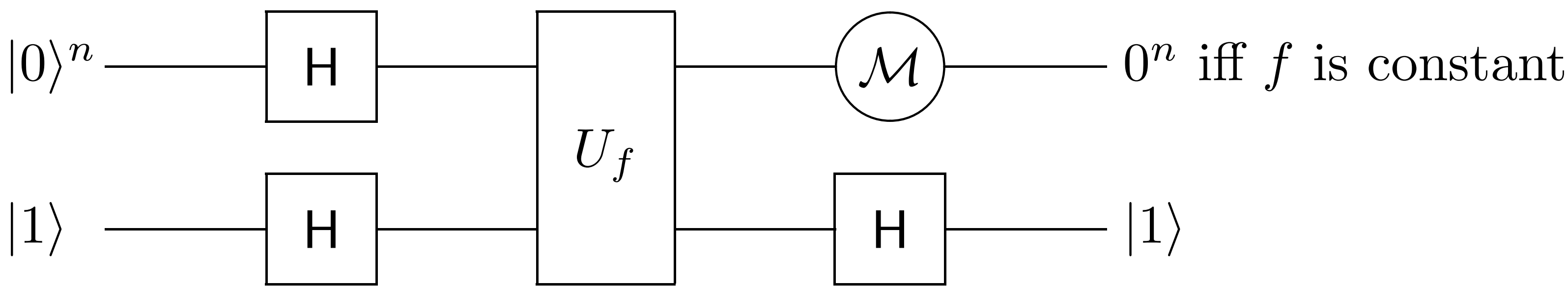
- ⋄ Classical exact solution: $2^{n-1} + 1$ queries are required.
- ⋄ Quantum exact solution: 1 query suffices.

The Deutsch-Jozsa Problem

Function $f : \{0,1\}^n \to \{0,1\}$ is promised to be *constant* or *balanced.*

DJ's problem: Decide which is the case. *Errors are not tolerated.*

- Classical exact solution: $2^{n-1}+1$ queries are required.
- Quantum exact solution: 1 query suffices.



Information Gained by q Queries

Fixing the number of function evaluations, we investigate how much information can be gained about the system.

Information Gained by q Queries

Fixing the number of function evaluations, we investigate how much information can be gained about the system.

We consider the following three cases.

- ◇ Classical computation;
- ◇ Quantum computation;
- ◇ Quantum computation, but without entanglement.

Information Gained by q Queries

Fixing the number of function evaluations, we investigate how much information can be gained about the system.

We consider the following three cases.

- ◇ Classical computation;
- ◇ Quantum computation;
- ◇ Quantum computation, but without entanglement.

We demonstrate the power of quantum computation without entanglement by showing cases in which more information can be obtained in the third case than in the first.

DJ — Information Gained by One Query

Assume *a priori* that f is balanced with probability $\frac{1}{2}$ and constant with probability $\frac{1}{2}$. The amount of information we *lack* about which is the case is exactly one bit.

DJ — Information Gained by One Query

Assume *a priori* that f is balanced with probability $\frac{1}{2}$ and constant with probability $\frac{1}{2}$. The amount of information we *lack* about which is the case is exactly one bit.

How much of this information I can be gained by a single function evaluation?

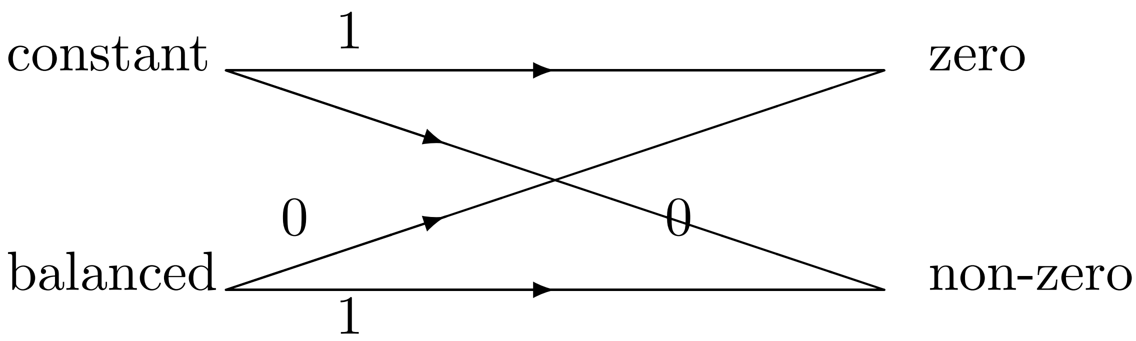
Classical Computation

Nothing is gained. $I = 0$.

Whatever x we choose, a single value of $f(x)$ tells us nothing about whether the function is balanced or constant.

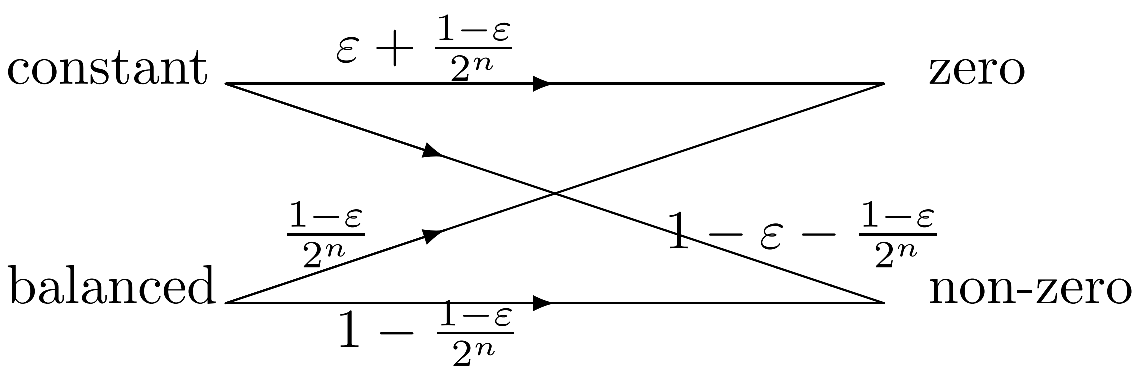
Pure Quantum Computation

Complete knowledge is obtained after a single query. $I = 1$.



Quantum Computation Without Entanglement

If we apply the Deutsch-Jozsa algorithm on a pseudo-pure state, instead of the pure state $|0\rangle^n|1\rangle$, we do obtain *some* information.



Even if $\varepsilon < \frac{2}{N^2}$ is below the Braunstein, Caves, Jozsa, Linden, Popescu and Schack bound.

$$I = h(p) - p_0 h\left(\frac{p}{p_0}\left(\varepsilon + \frac{1-\varepsilon}{2^n}\right)\right) + (1-p_0)h\left(\frac{p(1-\varepsilon)}{1-p_0}\left(1 - \frac{1}{2^n}\right)\right) > 0$$

where

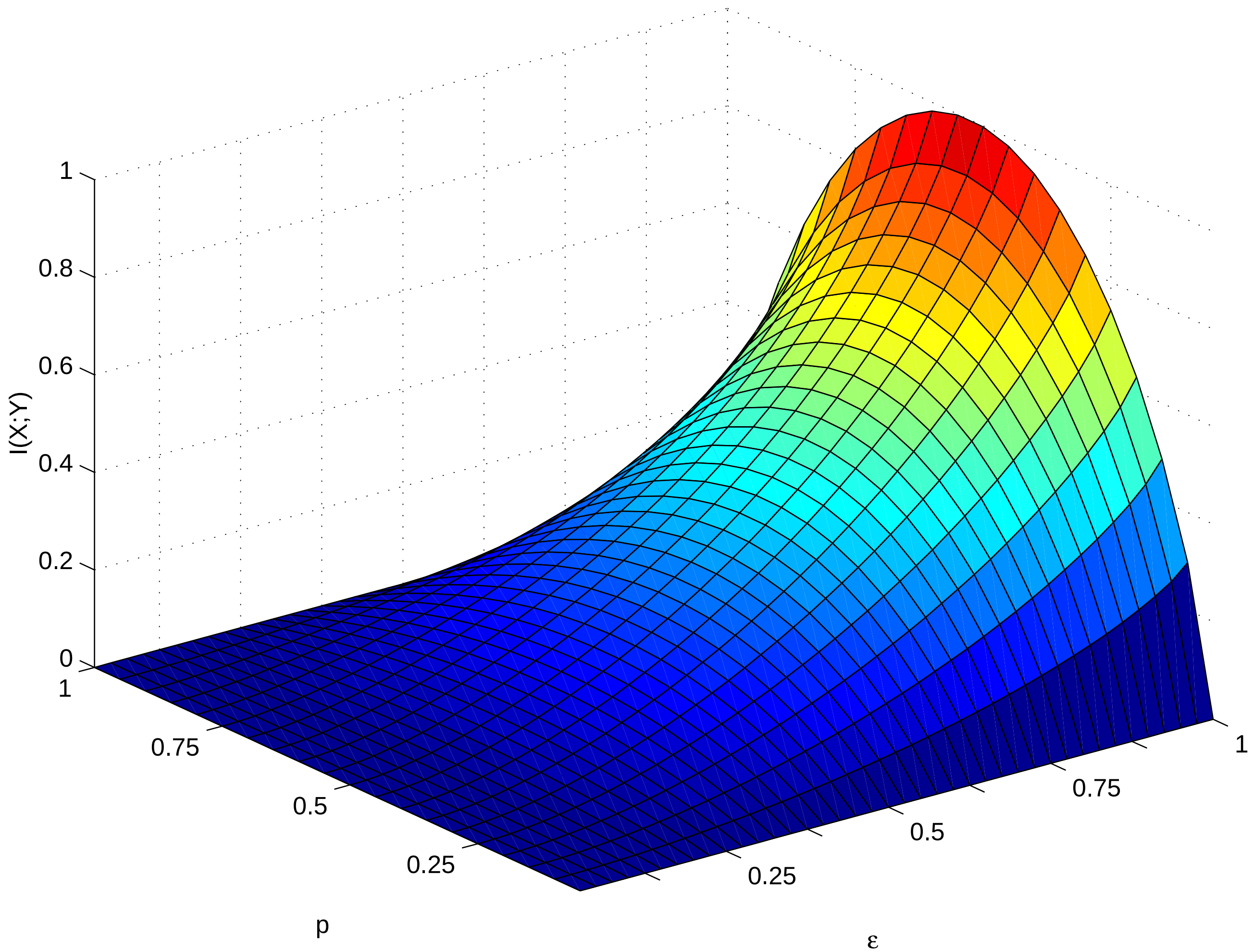
$$p_0 = \frac{1-\varepsilon}{2^n} + \varepsilon p$$

and

$$h(q) \equiv -q\log_2 q - (1-q)\log_2(1-q)$$

is the Shannon binary entropy function.

DJ — Information Gained by One Query



Simon's Problem

Consider two-to-one function $f : \{0,1\}^n \to \{0,1\}^{n-1}$.
There is a single nonzero s such that $f(x) = f(x \oplus s)$ for all x.
Simon's problem: find s.

- ◇ Classical solution: $\Theta(2^{n/2})$ queries are necessary and sufficient (by the birthday "paradox").
- ◇ Quantum solution: $\Theta(n)$ queries in the expected sense with Simon's original algorithm.
- ◇ Exact quantum solution: $\Theta(n)$ queries in the worst case [BH97].

Simon — Information Gained by One Query

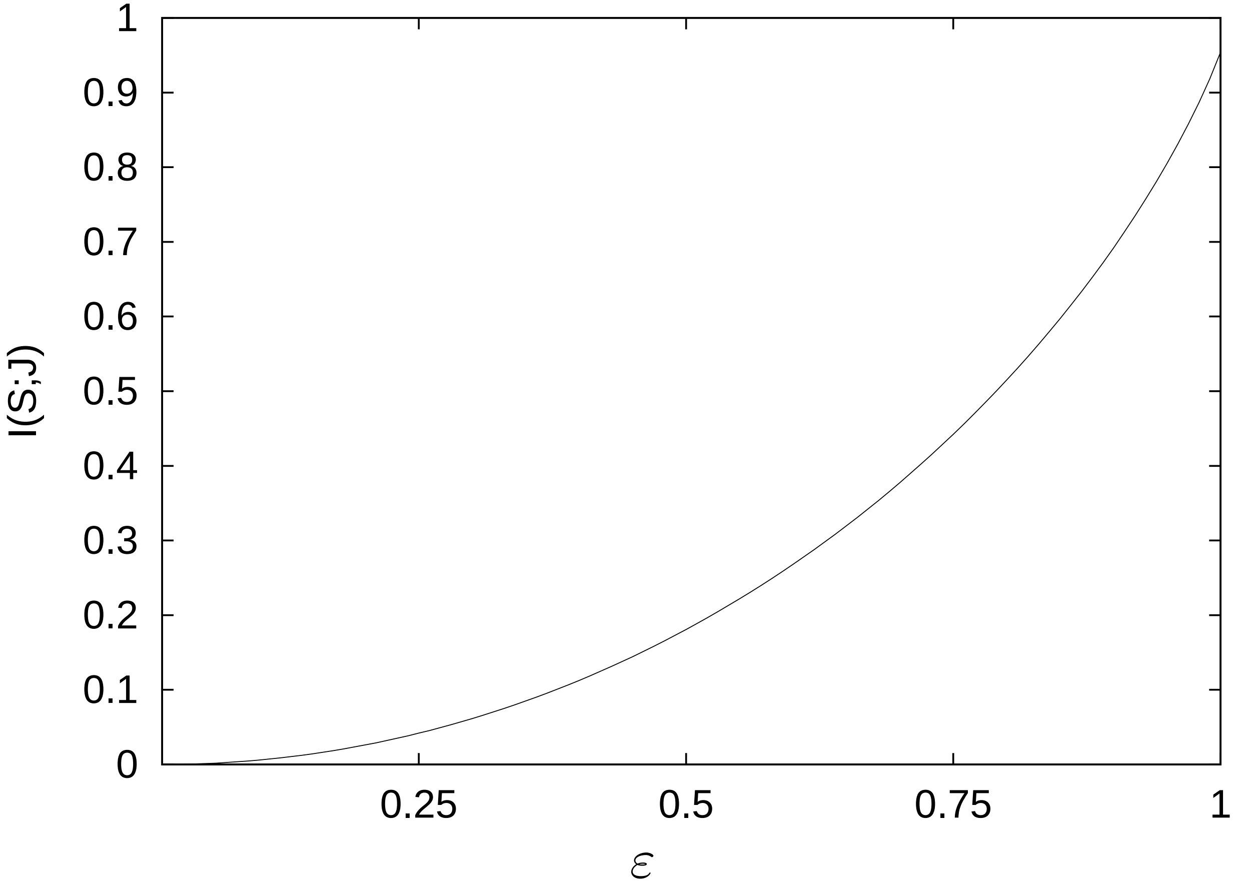
Assume s is selected uniformly from $\{1...2^n - 1\}$. The amount of information we lack about its value is $\log(2^n - 1) \approx n - O(2^{-n})$.

How much of this information can be obtained using one query?

- If it's classical query—nothing.
- If it's the first *quantum* query of Simon's algorithm—almost one bit.
- And with pseudo-pure state, it is

$$\left(2^{n-1} - 1\right) \frac{1+\varepsilon}{2^n} \log \frac{1+\varepsilon}{2^n}$$
$$- \left(1 - \frac{1+\varepsilon}{2^n}\right) \log \frac{1 - \frac{1+\varepsilon}{2^n}}{2^n - 1}$$
$$+ \frac{1-\varepsilon}{2} \log \left(\frac{1-\varepsilon}{2^n}\right) > 0$$

Simon — Information Gained by One Query



Conclusions

- Quantum computing without entanglement *is* possible.
- There is potential evidence that *bound entanglement* is sufficient for making Grover search better than classical (using more than one query).

Limits

- The advantage we found is tiny—exponentially small.
- Entanglement is still required for all practical purposes!
  (so far)

Open Questions

◇ Find cases for which quantum computing without entanglement provides a non-negligible advantage over classical computation.

◇ Find examples in which the Quantum Computation Without Entanglement advantage persists for more than one query.

◇ What does this *really* tell us about why quantum computers (may) have a computational advantage over classical computers?

◇ What does this *really* tell us about how separability is a richer notion for mixed states compared to pure states?

FIN