

FoCM 2002

Quantum Computation
without
Entanglement

Eli Biham

Gilles Brassard

Dan Kenigsberg danken@cs.technion.ac.il

Tal Mor

What is Quantum Mechanics?

A framework with 3 rules:

1. Statics: the state of an isolated physical system lies in a vector space.
2. Dynamics: the state evolves unitarily.
3. Measurement: The specific rule of how information about the system can be extracted, is discussed later.

The rest of quantum mechanics is special cases.

Qubit: The Most Special Special Case

A qubit is a two-dimensional quantum system. Possible implementations are:

- Electron spin (parallel/antiparallel to external magnetic field).
- Photon polarization (vertical/horizontal).
- Nuclear spin- $\frac{1}{2}$.
- other ideas...

The two states are called $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Their *superpositions* are also possible states.

Qubit, cont'd

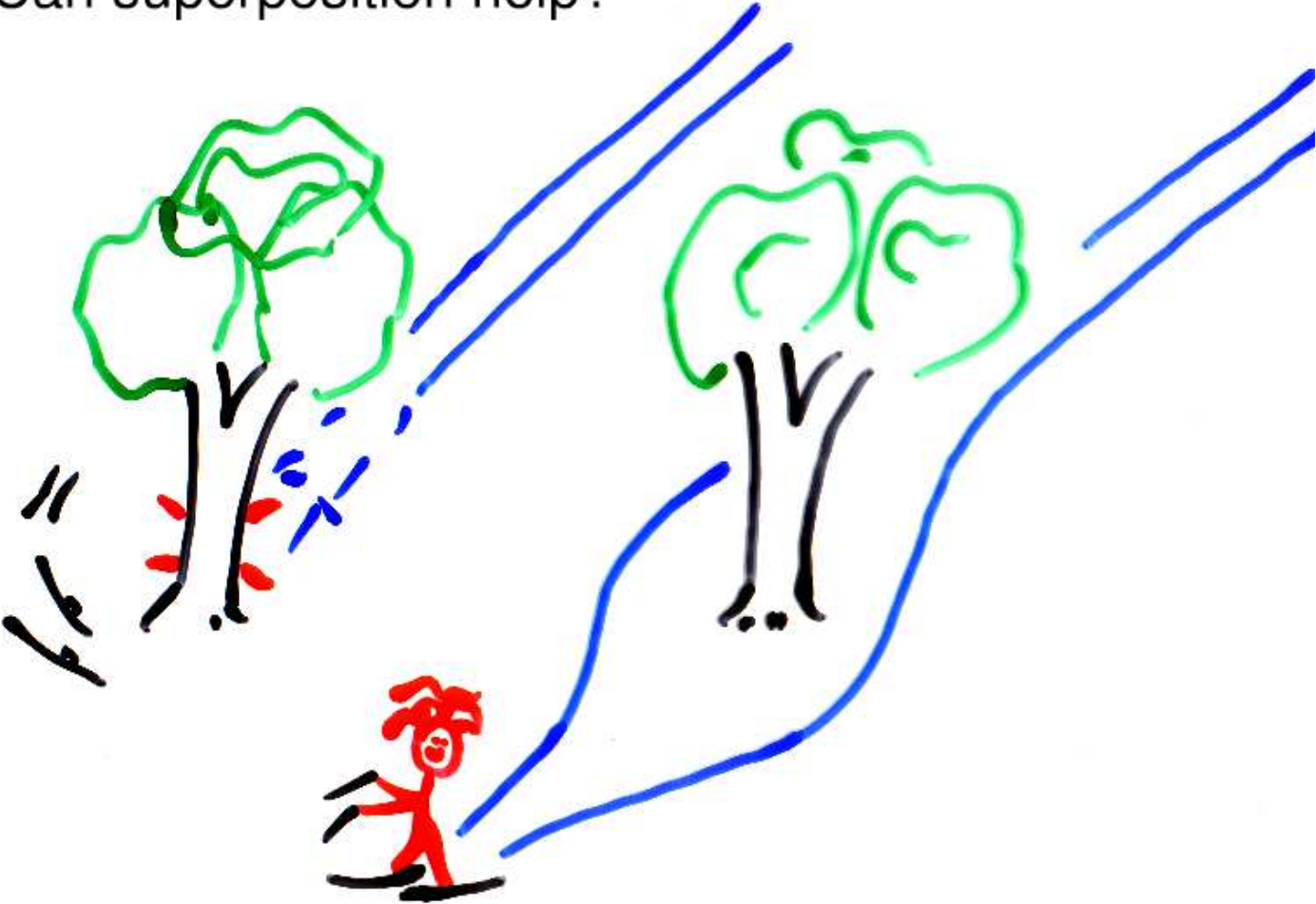
1. State: $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha_0|0\rangle + \alpha_1|1\rangle$

where $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

2. Dynamics: $|\psi\rangle$ evolves into $|\chi\rangle = U|\psi\rangle$, where U is unitary, that is, $U^\dagger U = I$.

3. Measurement: Outputs $|0\rangle$ with probability $|\alpha_0|^2$, $|1\rangle$ with probability $|\alpha_1|^2$.

Can superposition help?



More About bra-ket

$$\langle\psi| = \begin{pmatrix} \alpha_0^* & \alpha_1^* \end{pmatrix} \quad |\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Density Matrix Formalism

1. State: The bilinear form $\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* \\ \alpha_0^*\alpha_1 & |\alpha_1|^2 \end{pmatrix}$
2. Evolution: $|\psi\rangle\langle\psi| \xrightarrow{U} U|\psi\rangle\langle\psi|U^\dagger$
3. Measurement: Outputs $|i\rangle\langle i|$ with probability $\rho_{ii} = \langle i|\rho|i\rangle$.

Density matrix can capture the concept of probabilistic state, and would come up pretty handy later on.

Mixed States

Concise means to express partial knowledge about the state

$$\begin{aligned} \begin{pmatrix} \frac{1}{2} & \\ & \frac{1}{2} \end{pmatrix} &= \begin{cases} |0\rangle\langle 0| & \text{with } p_0 = \frac{1}{2} \\ |1\rangle\langle 1| & \text{with } p_1 = \frac{1}{2} \end{cases} \\ &= \begin{cases} |+\rangle\langle +| & \text{with } p_+ = \frac{1}{2} \\ |-\rangle\langle -| & \text{with } p_- = \frac{1}{2} \end{cases}, \\ \begin{pmatrix} \cos^2 \theta & \\ & \sin^2 \theta \end{pmatrix} &= \begin{cases} |0\rangle\langle 0| & \text{with } p_0 = \cos^2 \theta \\ |1\rangle\langle 1| & \text{with } p_1 = \sin^2 \theta \end{cases} \\ &= \begin{cases} \cos \theta |0\rangle + \sin \theta |1\rangle & \text{with } p_+ = \frac{1}{2} \\ \cos \theta |0\rangle - \sin \theta |1\rangle & \text{with } p_- = \frac{1}{2} \end{cases} \end{aligned}$$

In General: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

Some Unitary Operations (=Quantum Gates)

$$\text{Identity: } I_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ Hadamard: } H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\text{Not} = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

$$H_1|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Pair of Qubits

1. State space: Tensor product of the two spaces, spanned by

$$|0\rangle \otimes |0\rangle = |00\rangle = |0\rangle,$$

$$|0\rangle \otimes |1\rangle = |01\rangle = |1\rangle,$$

$$|1\rangle \otimes |0\rangle = |10\rangle = |2\rangle \text{ and}$$

$$|1\rangle \otimes |1\rangle = |11\rangle = |3\rangle. \text{ (the Computation Basis)}$$

2. Operations: $H_2 = H_1 \otimes H_1$,

$$\text{C-Not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Universal sets are known (such as C-Not + 1-qubit-rotation).

Entangled States

Cannot be factorized, that is, broken into a state of qubit A and a state of qubit B .

Claim: the state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ is entangled.

Proof: unentangled pure state can be written as

$$\begin{aligned} & (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ = & \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle, \end{aligned}$$

and no choice of $\alpha_0, \alpha_1, \beta_0, \beta_1$ can induce $\alpha_0\beta_0 = \alpha_1\beta_1 = \frac{1}{\sqrt{2}}$ and $\alpha_0\beta_1 = \alpha_1\beta_0 = 0$.

Separable Mixed States

A mixture of entangled states may be unentangled.

Example: Both

$$\rho_{\pm} = \frac{(|01\rangle \pm |10\rangle)(\langle 01| \pm \langle 10|)}{2} = \frac{1}{2} \begin{pmatrix} 0 & & & \\ & 1 & \pm 1 & \\ & \pm 1 & 1 & \\ & & & 0 \end{pmatrix}$$

are entangled, yet their mixture

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

is not.

Bell's Inequality

Let $\alpha, \alpha', \beta, \beta'$ be random variables, distributed arbitrarily above $\{\pm 1\}$. Bell's inequality states that:

$$b_{\alpha, \alpha', \beta, \beta'} = E(\alpha\beta) - E(\alpha'\beta) + E(\alpha'\beta') + E(\alpha\beta') \leq 2.$$

Proof:

$$\begin{aligned} b_{\alpha, \alpha', \beta, \beta'} &= E(\alpha\beta - \alpha'\beta + \alpha'\beta' + \alpha\beta') \\ &= E(\beta(\alpha - \alpha') + \beta'(\alpha + \alpha')) \\ &= E(\pm 2) \leq 2. \end{aligned}$$

Bell's Inequality—Violated

However, given systems in the entangled state $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ of two qubits, A and B. We may apply $R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ to B, and:

- either measure A assign the outcome to a , or apply H to it beforehand and assign the outcome to a' .
- then, either measure B and assign the outcome to b , or apply H to it before-hence and assign the outcome to b'
- define $\alpha = (-1)^a$, $\alpha' = (-1)^{a'}$, $\beta = (-1)^b$, $\beta' = (-1)^{b'}$.

One may confirm that $E(\alpha\beta) = E(\alpha'\beta') = -\cos 2\theta$,
 $E(\alpha\beta') = -\sin 2\theta$, $E(\alpha'\beta) = \sin 2\theta$.

Amazingly, for $\theta = \frac{5\pi}{8} = 112^\circ$, $b_{\alpha,\alpha',\beta,\beta'} = 2\sqrt{2}$.

Quantum Register

A quantum register is a $N = 2^n$ -dimensional system, made of n qubits,.

1. State space: Tensor product of individual spaces, spanned by $\{|i\rangle\}_{i=0}^{N-1}$, the Computation Basis.

Sometimes better written in binary.

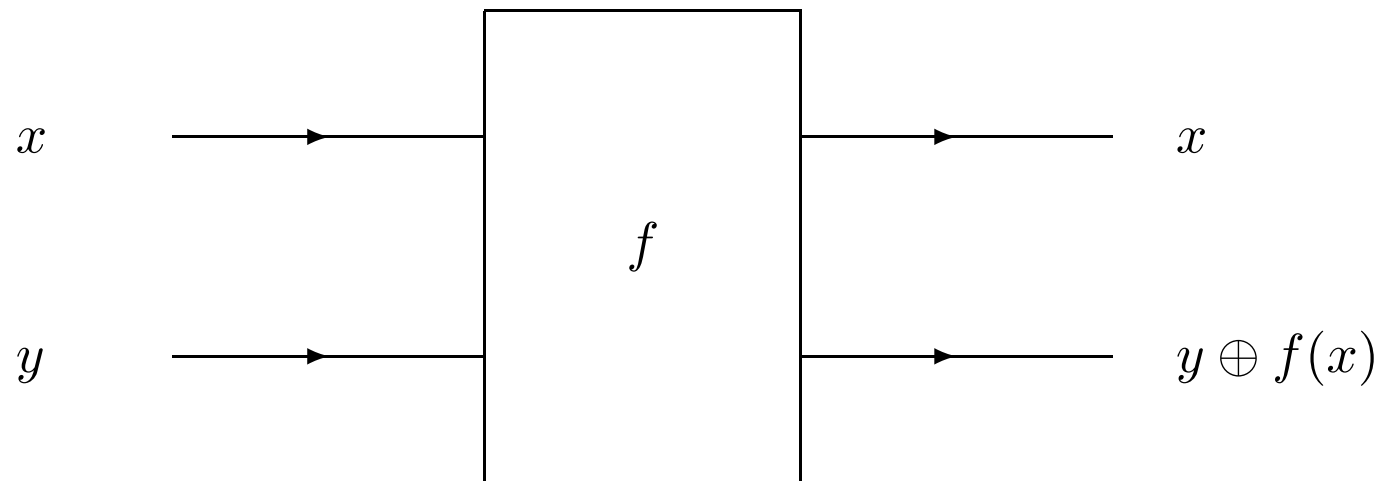
2. Any $N \times N$ unitary operation, such as $H_{n+1} = H_n \otimes H_1$

$$|0\rangle \xrightarrow{H_n} \frac{1}{\sqrt{N}} \sum_i |i\rangle \xrightarrow{H_n} |0\rangle$$

3. When $|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ is measured, $|i\rangle$ is obtained with probability $|\alpha_i|^2$.

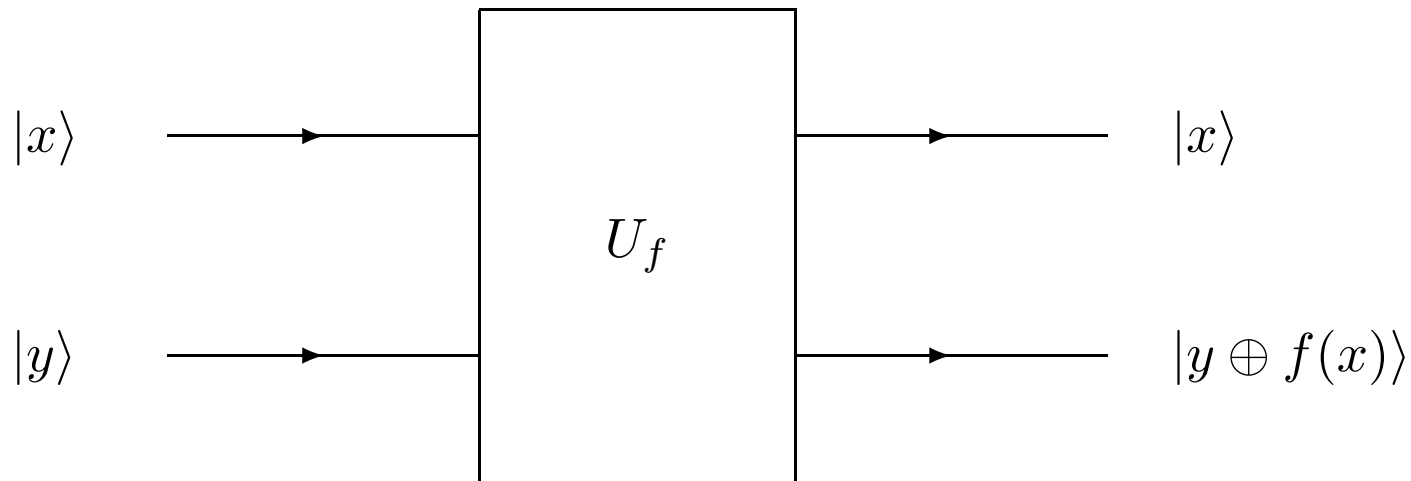
Classical (Reversible) Computation

A classical computation of a function f may be viewed as the gate:



Quantum Computation

A quantum computation of the same function f is very similar:



However, exponentially many values can be computed simultaneously if we start with a superposition:

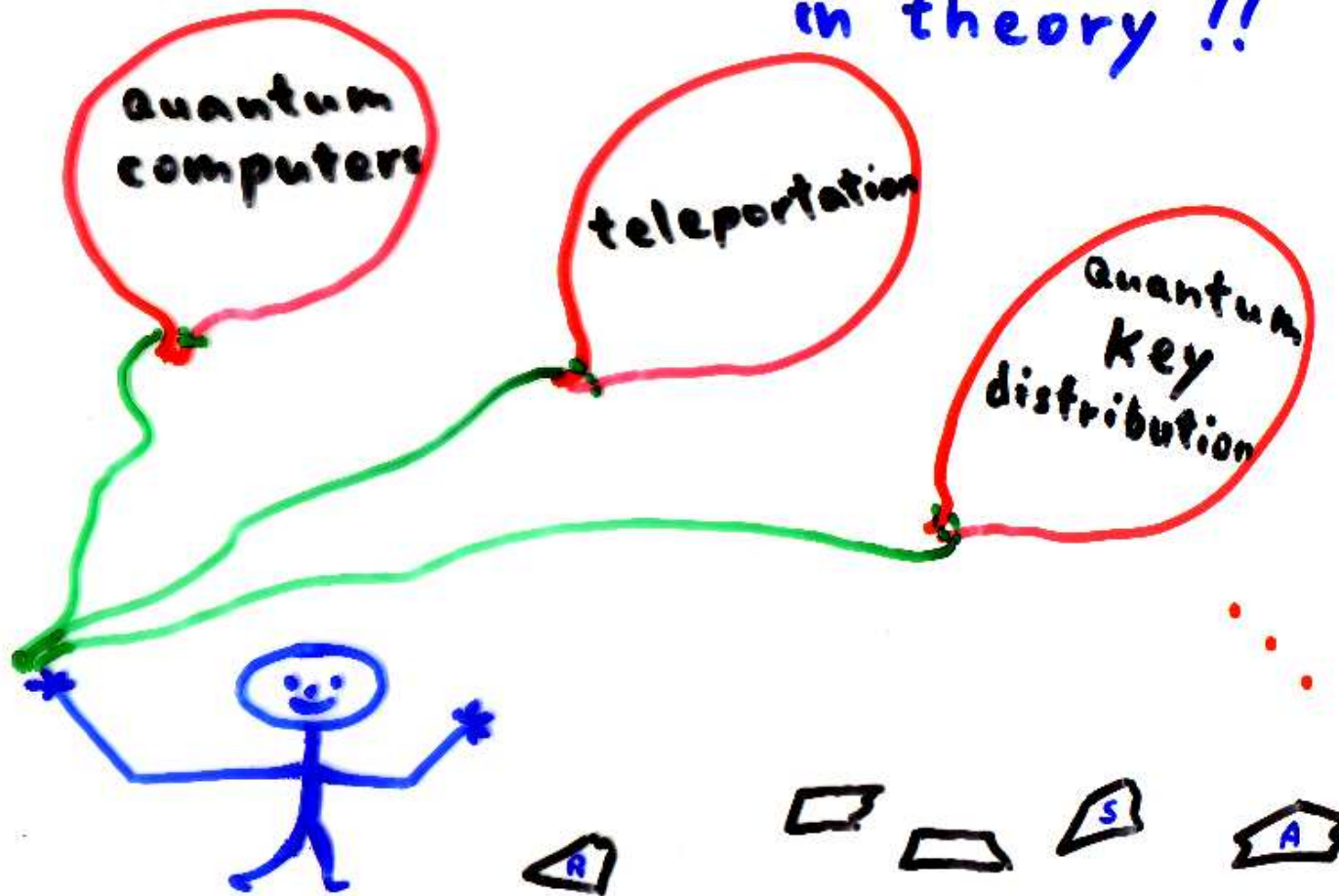
$$U_f \sum_{i=1}^{2^n} \alpha_i |x_i\rangle |y\rangle = \sum_{i=1}^{2^n} \alpha_i |x_i\rangle |y \oplus f(x_i)\rangle$$

(It means that quantum computation could be more powerful.)

Current State of Affairs — Software

- Algorithms that probably give exponential speedup. (Shor's algorithms break RSA and DH cryptosystems)
- Algorithms that give proven polynomial speedup, and seem useful. (Grover's search algorithm finds one of a million in only one thousand iterations)
- And many more...

Quantum Info. Processing in theory !!



Current State of Affairs — Hardware

Strongest quantum computers to date: Laflamme et al. (LANL),
Chuang et al. (IBM)

- Architecture: Liquid NMR
- RAM Size: 7 qubits

Accomplishments:

- Pseudo-pure “cat state”: $\frac{|0000000\rangle + |1111111\rangle}{\sqrt{2}}$.
- Factorization of 15.

in practice ???



The Deutsch-Jozsa Problem

The function $f : \{0 \dots N - 1\} \rightarrow \{0, 1\}$ is either *constant* or *balanced*.
DJ's problem: given an *oracle* of the function, decide which of the two kinds is f .

- Classical exact solution: $N/2$ queries—exponential in the input size.
- Classical exponentially good solution: $O(n) = O(\log N)$ queries.
- Quantum exact solution: 1 query.

$$|0\rangle \xrightarrow{H_n} \frac{1}{\sqrt{N}} \sum_i |i\rangle \xrightarrow{f} \frac{1}{\sqrt{N}} \sum_i (-1)^{f(i)} |i\rangle \xrightarrow{H} \frac{1}{N} \sum_{i,j} (-1)^{f(i)+j \cdot i} |j\rangle$$

The coefficient of $|0\rangle$ is $\begin{cases} 0 & \text{if } f \text{ is balanced,} \\ \pm 1 & \text{if } f \text{ is constant.} \end{cases}$

× The Simon Problem

The function $f : \{0 \dots N - 1\} \rightarrow \{0, N - 1\}$ is a 2 - 1 function. There is a single s where for all x , $f(x) = f(x \oplus s)$. Simons's problem: find s .

- Classical solution: $O(\sqrt{N})$ queries (find a colliding pair).
- Quantum exact solution: $O(n)$ queries.

Pseudo-Pure States

A mixed state where all basis states are with equal probability $\frac{1-\epsilon}{N}$, and some $|\psi\rangle$ is with probability ϵ .

$$\rho = \frac{1-\epsilon}{N} I_n + \epsilon |\psi\rangle\langle\psi|$$

Mixed states appear in nature, whether we want it or not.

Pseudo-pure states are important since they may be very mixed, but still “behave” like a pure state:

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

(Pseudo-purity is conserved by unitary operations.)

Furthermore, they are created in NMR.

Factorizing Pseudo-Pure States

Some mixed states can be written as a mixture of unentangled states.

- Braunstein, Caves, Jozsa, Linden, Popescu and Schack's Lower Bound: In any dimension and for any $|\psi\rangle$, the pseudo-pure state

$$\frac{1 - \epsilon}{N} I_n + \epsilon |\psi\rangle\langle\psi|$$

is unentangled if $\epsilon < \frac{2}{N^2}$.

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.
- “... state entanglement ... is not necessary for quantum computation: entanglement in unitary operators can be use[d] as well.”, Laflamme, <http://quickreviews.org/qc>, 1998
- “Whether or not entanglement is a necessary condition for quantum computation is a question of fundamental importance”, Linden & Popescu, PRL 87(4)047901, 2001.

The Debate Goes On...

- “... for $N > 2$... the control register be coupled to [is entangled with] the remaining qubits. Thus meaningful test of the Deutsch-Jozsa algorithm occur if and only if $N > 2$. Collins, Kim & Holton, PRA 58(3)1633R, 1998.
- “... one should not conclude that entanglement is required for quantum-over-classical complexity reduction.”, Meyer, quant-ph/0007070 (and similarly in Science).
- “Can this [using small ϵ s] provide a computational benefit (over classical computations) in the total absence of entanglement?”, Jozsa & Linden, quant-ph/0201143.

Information Gained by q Queries

Fixing the number of queries, we ask how much information about the system can be gained, in the following 3 cases:

- Classical,
- Quantum,
- Quantum, but without entanglement.

If we obtained more information in the third case than in the first one, we would demonstrate quantum computation without entanglement!

DJ—Information Gained by One Query

Assume we know that f is balanced with probability $\frac{1}{2}$ and constant with probability $\frac{1}{2}$. The amount of information* we lack about its *kind* is exactly one bit.

How much of this information can be gained by one query, in the aforementioned cases?

*The exact definition uses entropy.

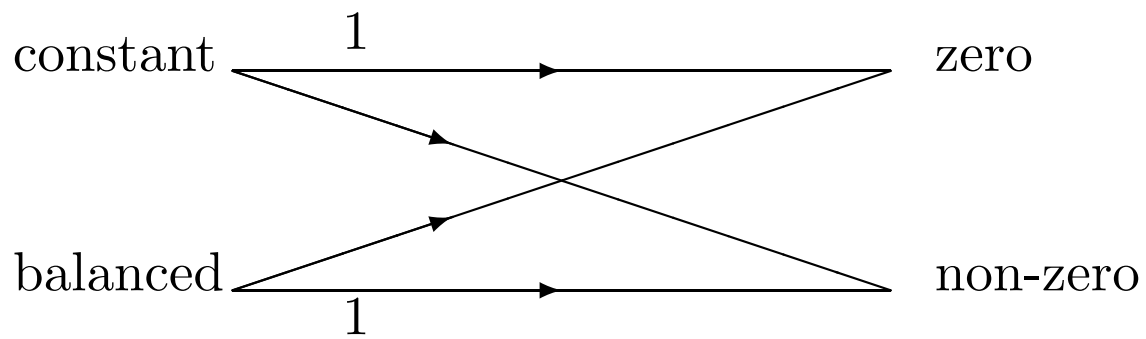
• Classical Computation

Nothing is gained. $I = 0$.

- Whatever x we choose, a single value of $f(x)$ has nothing to do with the kind f .
- Either 0 or 1 has the same probability of stemming from a constant or a balanced function

- Quantum Computation

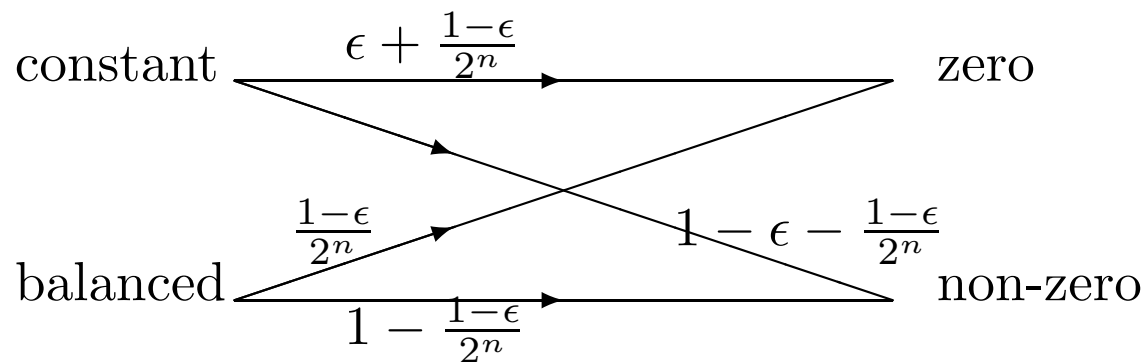
All knowledge is gained using one query. $I = 1$.



- **Quantum Computation, Without Entanglement**

If we apply the well-known DJ algorithm on a pseudo-pure state, instead of the pure state $|0\rangle$, we would obtain *some* information.

$I > 0$.



Even if ϵ is below Braunstein et al.'s bound.

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

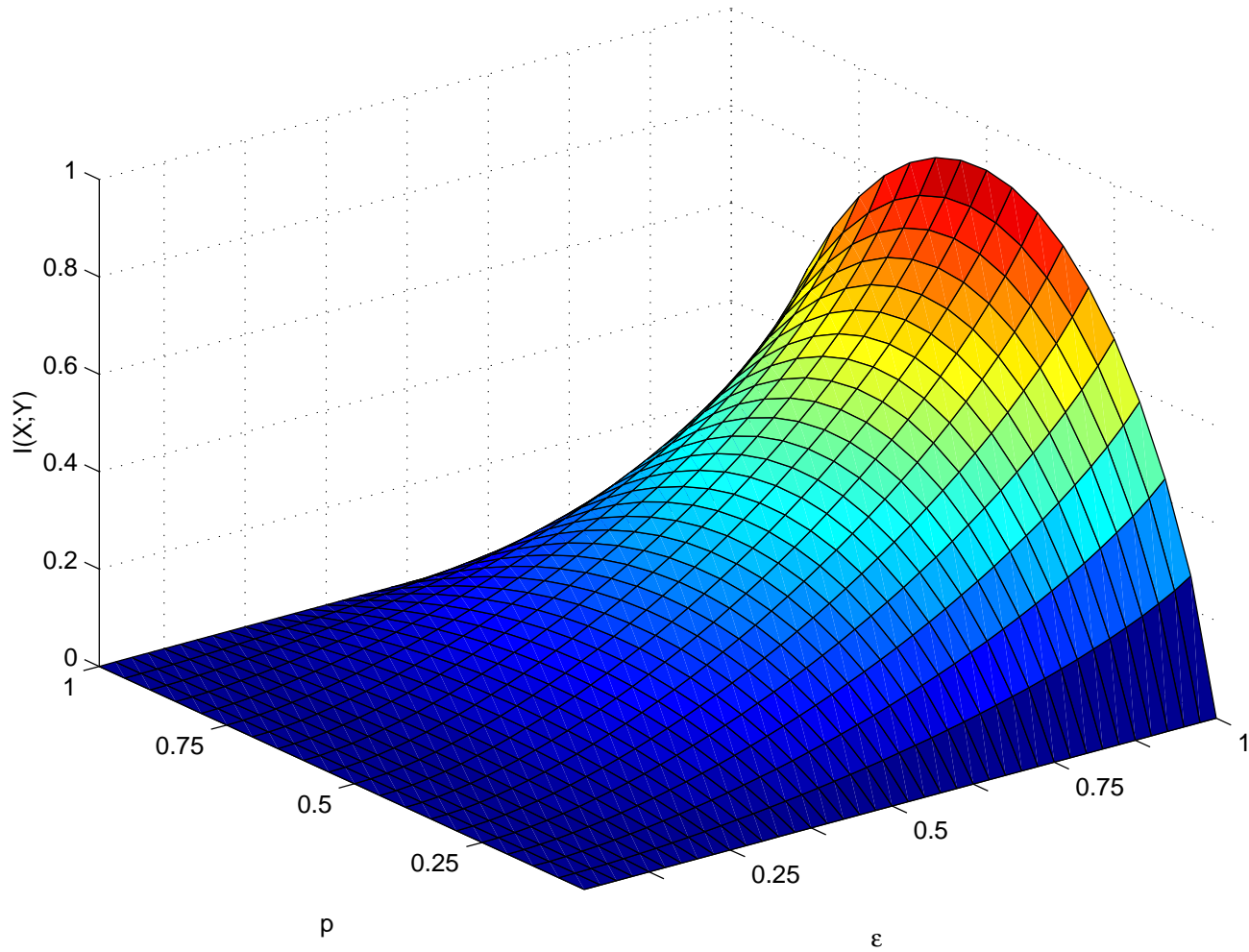
where

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

and

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

DJ — Information Gained by One Query



Simon—Information Gained by First Query

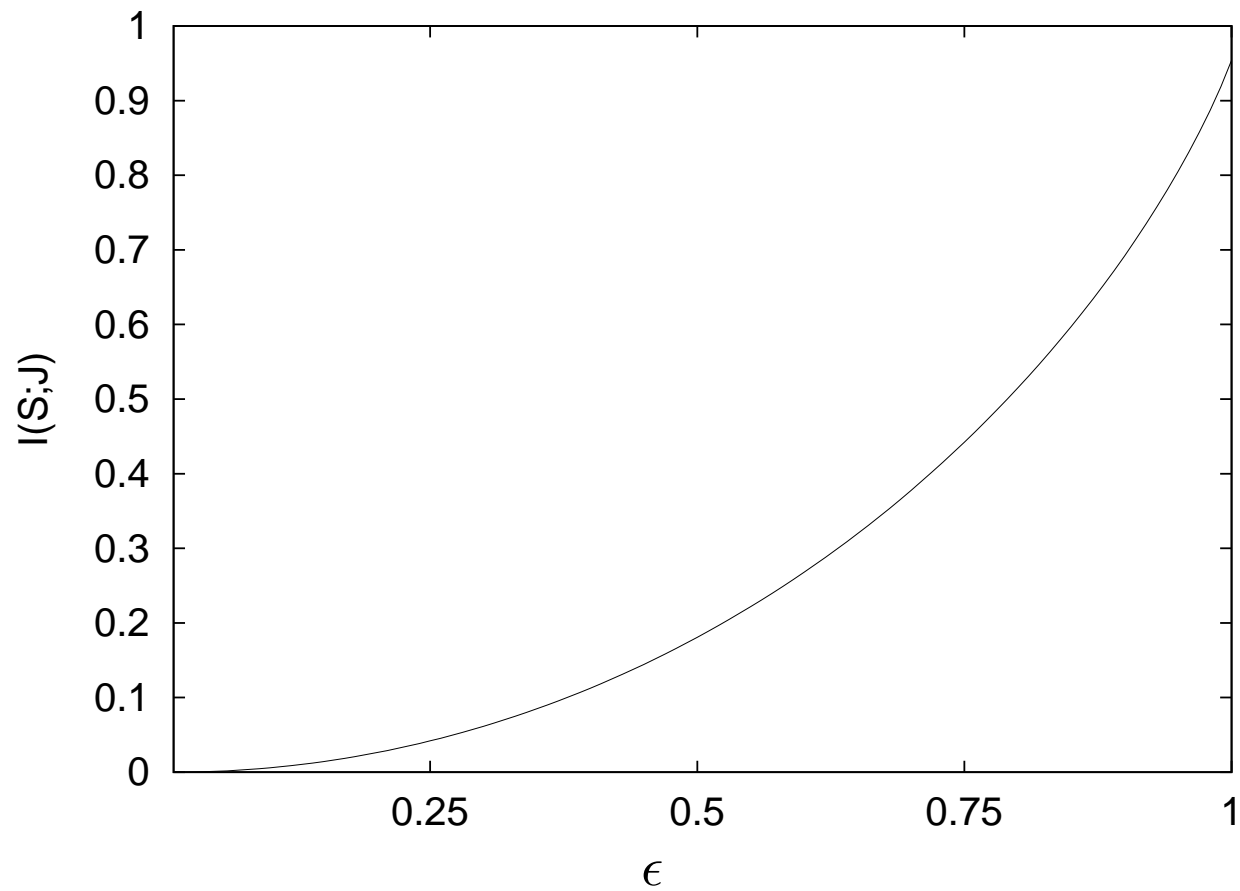
Assume s is selected uniformly from $\{1 \dots 2^n - 1\}$. The amount of information we lack about its value is $\log(2^n - 1) \approx n - O(2^{-n})$.

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

$$\begin{aligned} & - \left(1 - \frac{1 + \epsilon}{2^n}\right) \log \frac{1 - \frac{1 + \epsilon}{2^n}}{2^n - 1} \\ & + (2^{n-1} - 1) \frac{1 + \epsilon}{2^n} \log \frac{1 + \epsilon}{2^n} \\ & + \frac{1 - \epsilon}{2} \log \left(\frac{1 - \epsilon}{2^n}\right) > 0 \end{aligned}$$

× Simon — Information Gained by The First Query



Conclusions

- Entanglement is not a strictly unavoidable requirement for quantum computation
- Similar results to these of DJ are found for Simon's problem.
- Promising evidence that bound entanglement is “enough” for Grover (using more than one query).

Limits

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

FIN

Other Bases

Many different bases are conceivable (and useful), such as:

$$\{|+\rangle, |-\rangle\} = \left\{ \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

Note that $|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt{2}}$, $|1\rangle = \frac{|+\rangle-|-\rangle}{\sqrt{2}}$.

This basis in density matrix formalism:

$$\left\{ |+\rangle\langle+| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, |-\rangle\langle-| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right\}.$$

Bell's Violation - cont'd

Let's take $\alpha'\beta$ for example:

$$\frac{|10\rangle - |01\rangle}{\sqrt{2}} \xrightarrow{H_{\text{left}}} \frac{|00\rangle - |10\rangle - |01\rangle - |11\rangle}{2}.$$

When a' is measured, 1 is obtained with probability $\frac{1}{2}$ and the right qubit's state collapses into $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$.

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{R_{\text{right}}} \frac{(\cos \theta - \sin \theta)|0\rangle + (\cos \theta + \sin \theta)|1\rangle}{\sqrt{2}}.$$

$$\Rightarrow P(a' = 1, b = 0) = \frac{(\cos \theta - \sin \theta)^2}{4}, \quad P(a' = 1, b = 1) = \frac{(\cos \theta + \sin \theta)^2}{4}.$$

Similarly, $P(a' = 0, b = 0) = \frac{(\cos \theta + \sin \theta)^2}{4}$ and

$$P(a' = 0, b = 1) = \frac{(\cos \theta - \sin \theta)^2}{4}.$$

Therefore $P(\alpha'\beta = 1) = \frac{(\cos \theta - \sin \theta)^2}{2}$ and

$P(\alpha'\beta = -1) = \frac{(\cos \theta + \sin \theta)^2}{2}$, which induces

$$E(\alpha'\beta) = 2 \cos \theta \sin \theta = \sin 2\theta$$

What Has Happened Here?

- Assume that the same arbitrary operation is applied to each of the qubits of the state $|01\rangle - |10\rangle$. When measured, the results of the two qubits are always opposite. How could that happen if the two are far apart?
- Could it be that each qubit “knows” what would be its result (for each basis of measurement), just like in the **socks** problem?
- If it did, the values of $\alpha, \alpha', \beta, \beta'$ would have been defined, and Bell’s inequality should have hold.
- However, this is not what is predicted by quantum mechanics.
- Therefore, no hidden variables are allowed by quantum mechanics.

Why Not Exponential Speedup (Yet?)

Hard to say since $P \subseteq BQP \subseteq PSPACE$.

