INTRODUCTION TO SUPERCONDUCTING QUBITS

A. J. Leggett

Department of Physics, University of Illinois

at Urbana-Champaign

Lecture 1 (Thurs. 3 April): Quantum Computation

a) The idea of quantum computation

b) How to build a quantum computer (in principle!)

Lecture 2 (Thurs. 10 April): Superconductivity

a) Qualitative aspects and phenomenology

b) Microscopic theory

Lecture 3 (Thurs. 17 April): The Josephson effect

a) "Classical" theory

b) QM of macroscopic systems

Lecture 4 (?): Superconducting qubits

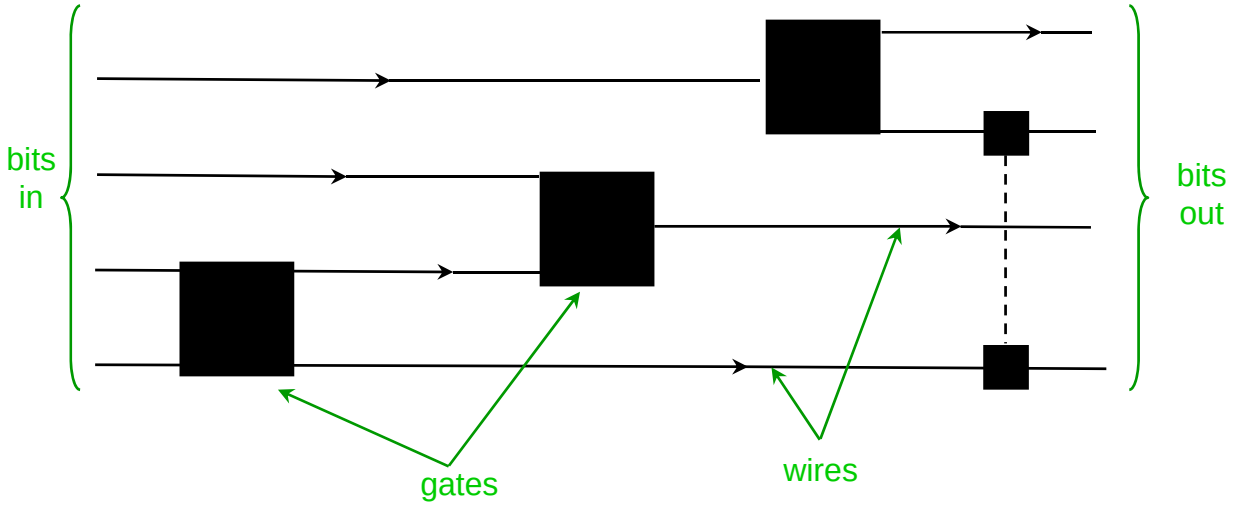
a) Types of qubit and their characteristics

b) Recent experiments and current issues

Color code: blue = main
red = emphasis
green = definitions, comments
⚠ = caution!

CLASSICAL COMPUTATION (bare bones)

Computer can be viewed as circuit composed of wires and gates which process bits.



A (classical) bit is an elementary "unit of information": physically it is a system which must be in one or other of two states, conventionally "0" or "1."

A wire simply carries a single bit from gate to gate.

A gate is a "black box" which transforms bits into other bits. In classical computation, the number of input and output bits of a gate need not be the same.

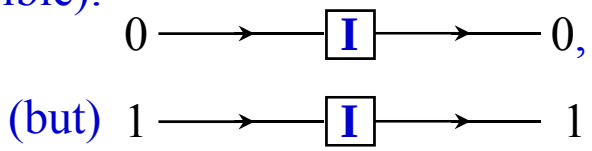
In general, classical computation is irreversible, though it is always possible to make it reversible.

In classical computation, readout is trivial.

EXAMPLES OF CLASSICAL GATES

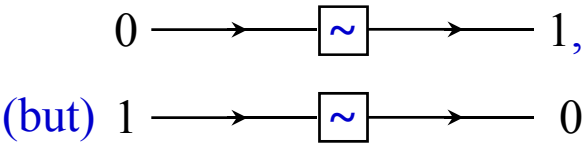
Single-bit gates (reversible):

"identity" gate (I)



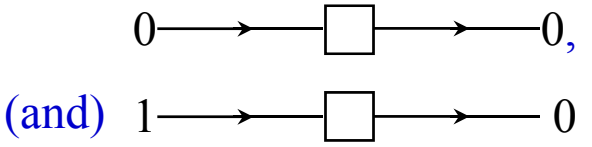
$(x \to x)$

"not" gate (~)



$(x \to x \oplus 1)$

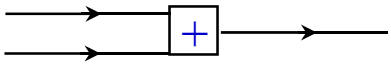
(An irreversible single-bit gate):



$(x \to 0)$

Two-bit gates:

(a) Irreversible: e.g.



"and" gate (+)

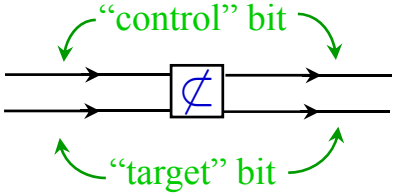
operation:

$$\begin{cases} (0,0) \to 0 \\ (0,1) \to 1 \\ (1,0) \to 1 \\ (1,1) \to 0 \end{cases}$$

$((x,y) \to x \oplus y)$

(b) Reversible, e.g.

"CNOT" gate ($\not\subset$)

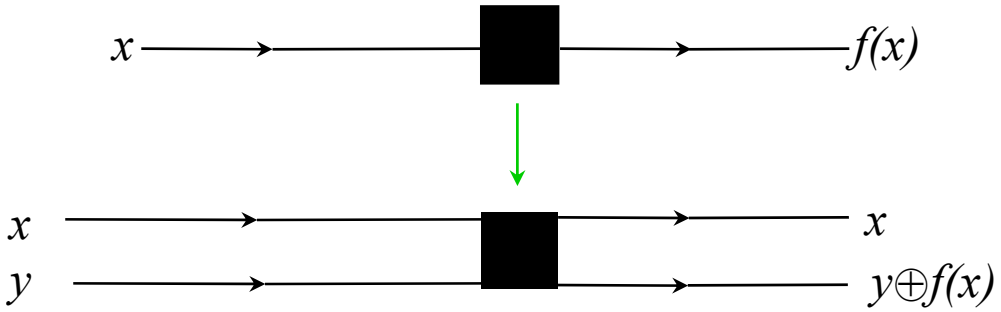


operation:

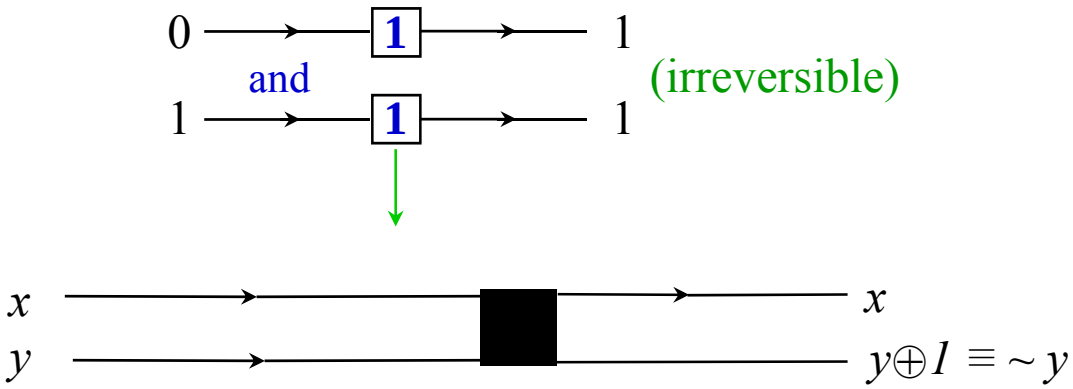
$$\begin{cases} (0,0) \to (0,0) \\ (0,1) \to (0,1) \end{cases} \text{ target unchanged}$$

$$\begin{cases} (1,0) \to (1,1) \\ (1,1) \to (1,0) \end{cases} \text{ target flipped}$$

NOTE: Any classical gate, reversible or not, can be made reversible by adding an "ancilla" bit:



Ex: the "1" gate $(f(0)=f(1)=1)$



operation:

$$\begin{cases} (0,0) \to (0,1) \\ (0,1) \to (0,0) \\ (1,0) \to (1,1) \\ (1,1) \to (1,0) \end{cases}$$

reversible!

COMPLEXITY IN (CLASSICAL) COMPUTATION

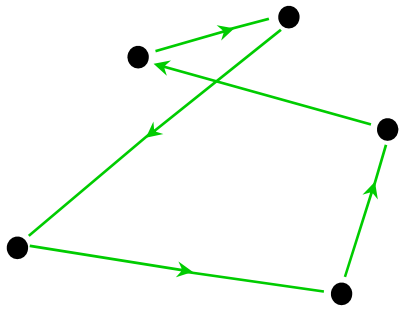
How do the "resources" needed to solve a given type of problem scale with the number of "elements" involved?

Examples:

(1) (trivial) search: If one and only one object among N is "tagged," it takes (classically) ~N trials to find it.

(2) List ordering: If N numbers are to be put in order, requires N(N–1)/2 ~N^2 pairwise comparisons.

(3) "Traveling salesman" problem: if we simply exhaust all possible trajectories, there are N! of these, so number of steps ~N! ~ exp N



(4) Factorization of large number: N~2^n where n is number of digits in binary representation. "Brute-force" approach requires us to examine possible factors up to $\sim\sqrt{N}\sim 2^{n/2}$, so number of steps ~ exp (αn) (Actually, "number sieve" method reduces this to ~ exp ($\alpha\, n^{1/3}\, ln^{2/3}\, n$), but still exponential in n).

Digression: Why is this interesting?

Answer: Cryptographic protocols!

BASIC PRINCIPLES OF QM

A. Single system

In QM, associated with a single QM system is a Hilbert space, whose dimension corresponds in an intuitive sense to the "number of different possible states" of the system. We shall mostly be interested in systems corresponding to classical "bits," so that the Hilbert space is 2-dimensional. In this case the system is isomorphic to a spin-1/2 particle, and in the context of quantum computation is called a qubit ("quantum bit"). A standard basis ("computational basis" (CB)) for the specification of the state of a qubit is the states $|0\rangle$ and $|1\rangle$ which correspond respectively to the states 0 and 1 of the classical bit. For any given physical system, usually ∃ a "natural" computational basis.

The most complete possible ("pure-state") description of the state of a qubit is given by specifying its state vector $|\Psi\rangle$ in the Hilbert space: quite generally we can write

$$|\Psi\rangle(t) = \alpha(t)\,|0\rangle + \beta(t)\,|1\rangle$$

$$(|\alpha(t)|^2 + |\beta(t)|^2 = 1 \text{ for normalization})$$

The qubit basis states are eigenstates of the Pauli matrix $\hat{\sigma}_z$ ($\equiv \hat{Z}$ in the quantum computation literature):

$$\hat{Z}\,|0\rangle = +\,|0\rangle$$

$$\hat{Z}\,|1\rangle = -\,|1\rangle$$

Single qubit, cont.

In general,

$$|\Psi\rangle(t) = \alpha(t)\,|0\rangle + \beta(t)\,|1\rangle$$

In special case $\beta(t)=0$ (i.e. $|\Psi\rangle(t)=e^{i\varphi}(t)|0\rangle$)
a measurement of $\hat{Z}\ (\equiv \hat{\sigma}_z)$ at time t gives +1.
Similarly, if $\alpha(t)=0$ (i.e. $|\Psi(t)\rangle = c^{i\chi(t)}\,|1\rangle$) a measurement of $\hat{Z}$ gives –1.

In the general case, measurement of $\hat{Z}$ at time t yields the result

$$+1 \text{ with probability } |\alpha(t)|^2$$

$$-1 \text{ with probability } |\beta(t)|^2$$

and following a measurement yielding +1(–1) the state vector becomes $|0\rangle(|1\rangle)$ ("projection postulate").

Any Hermitian operator on the qubit can be expressed in the form

$$\hat{0} = \alpha\hat{1} + \beta\hat{X} + \lambda\hat{Y} + \delta\hat{Z} \qquad (\equiv \alpha\hat{1} + \Omega\bullet\hat{\sigma})$$

unit op. $\equiv \hat{\sigma}_x$ $\equiv \hat{\sigma}_y$

To find the result of measurement of $\hat{O}$, we transform $|\Psi\rangle(t)$ into the basis of its eigenstates and apply prescription (*). E.g. if $\hat{0} = \hat{x}$, eigenstates are

$$|+\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

so (inverting)

$$|\Psi\rangle(t) = \frac{1}{\sqrt{2}}\left[\left(\alpha(t)+\beta(t)\right)|+\rangle_x + \left(\alpha(t)-\beta(t)\right)|-\rangle_x\right]$$

$$x=+1 \quad \text{with prob } \frac{1}{2}|\alpha(t)+\beta(t)|^2$$

$$x=-1 \quad \text{with prob } \frac{1}{2}|\alpha(t)-\beta(t)|^2$$

However, usually convenient to measure only in computational basis.

Single qubit, cont.

Time evolution: from time-dependent Schrödinger equation,

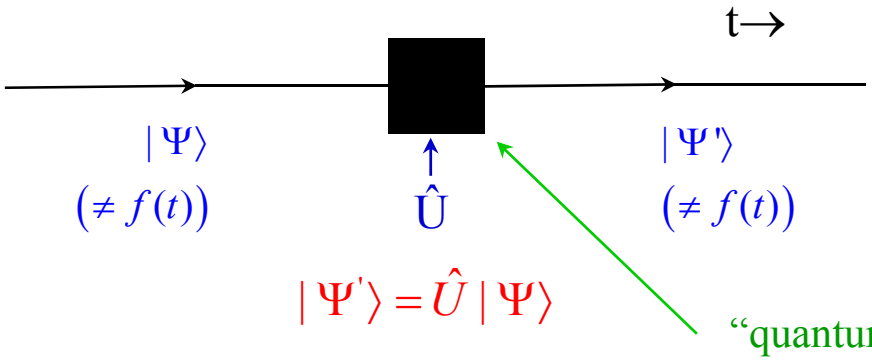
$$|\Psi\rangle t = \hat{U}(t,t')\,|\Psi\rangle(t')$$

$$\hat{U}(t,t') \equiv \exp\left(-i\int_{t}^{t'} \hat{H}(\tau)\,d\tau\right)$$

evolution operator unitary

Hamiltonian (Hermitian)

In QC, usually assume $\hat{H}(t) = 0 \left(\hat{U}(t,t') = \hat{1}\right)$ for "resting" periods ("wires"), $\hat{H}(t) \neq 0$ for "active" periods ("gates"). So for a single qubit



Note: since $\hat{U}^{-1}(t,t') \equiv \hat{U}(t',t) \equiv \exp\left(+i\int_{t}^{t'} \hat{H}(\tau)\,d\tau\right)$ quantum gates are intrinsically reversible $(|\Psi\rangle = \hat{U}^{-1}\,|\Psi'\rangle)$. Also note that Û is linear.

(Note: More general description of quantum system is by density matrix $\hat{\rho}$: crudely speaking.

"system behaves as if it were in a definite state $|\Psi_i\rangle(t)$ with probability $\rho_i(t)$ "

We will mostly not need this generalization).

BASIC PRINCIPLES OF QM, cont.

B. Coupled systems

Much more interesting! Consider 2 systems that may be mutually interacting. Associated with them is a tensor product Hilbert space $\mathcal{H}_{12} \equiv \mathcal{H}_1 \otimes \mathcal{H}_2$ of the Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ associated with each qubit separately. The dimensionality d of $\mathcal{H}_{12}$ is the product of that of $\mathcal{H}_1$ and $\mathcal{H}_2$, so for 2 qubits d = 4. In this case, computational basis is given by the 4 states

$$|0\rangle_1 |0\rangle_2, \quad |0\rangle_1 |1\rangle_2, \quad |1\rangle_1 |0\rangle_2, \quad |1\rangle_1 |1\rangle_2$$

A general pure state of the 2-qubit system is specified by an arbitrary (normalized) linear combination of these 4 states: (omitting t-dependence of coefficients)

$$|\Psi\rangle = \alpha_{00} |0\rangle_1 |0\rangle_2 + \alpha_{01} |0\rangle_1 |1\rangle_2 + \alpha_{10} |1\rangle_1 |0\rangle_2 + \alpha_{11} |2\rangle_1 |1\rangle_2$$

with

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \text{ (normalization)}$$

If we can write

$$|\Psi\rangle = |\chi\rangle_1 |\varphi\rangle_2, \qquad \left.\begin{aligned} |\chi\rangle_1 &= \alpha |0\rangle_1 + \beta |1\rangle_1 \\ |\varphi\rangle_2 &= \gamma |0\rangle_2 + \delta |1\rangle_2 \end{aligned}\right\} \qquad (\neq)$$

then the state $|\Psi\rangle$ is said to be "separable" or unentangled." But this is the exception: the vast majority of states in $\mathcal{H}_{12}$ are entangled (cannot be written in the form $(\neq)$)

Simple example of entangled state: ("EPR singlet")

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2\right) \equiv \frac{1}{\sqrt{2}}\left(\uparrow_1\downarrow_2 - \downarrow_1\uparrow_2\right)$$

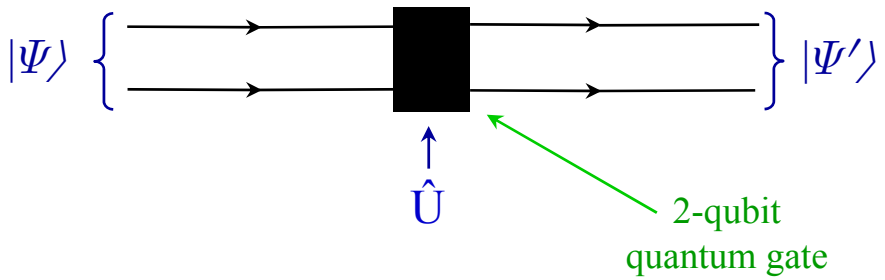
= state of 2 spin -1/2 particles with total S=0.

Coupled systems, cont.

Time evolution: just as in single-qubit case

$$|\Psi\rangle(t') = \hat{U}(t,t')\,|\Psi\rangle(t)$$

but $|\Psi\rangle$, $|\Psi'\rangle$ are now state vectors (in general entangled) in the tensor product Hilbert space $\mathcal{H}_{12}$. Thus,



Special (not very interesting) case: $\hat{H}(t) = \hat{H}_1(t) + \hat{H}_2(t)$

$$\Rightarrow \hat{U} = \hat{U}_1\hat{U}_2 \qquad \text{nonentangling}$$

More interesting:

$$\hat{H}(t) \neq \hat{H}_1(t) + \hat{H}_2(t) \Rightarrow \hat{U} \neq \hat{U}_1\hat{U}_2 \qquad \text{entangling}$$

Example:

$$\hat{H}(t) = J(t)\hat{\boldsymbol{\sigma}}_1 \cdot \hat{\boldsymbol{\sigma}}_2$$

then if $|\Psi\rangle = |\uparrow_1\downarrow_2\rangle$ unentangled

$$|\Psi'\rangle(t_0) = \frac{1}{\sqrt{2}}\left\{|\uparrow_1\downarrow_2\rangle + i\,|\downarrow_1\uparrow_2\rangle\right\} \qquad \text{entangled}$$

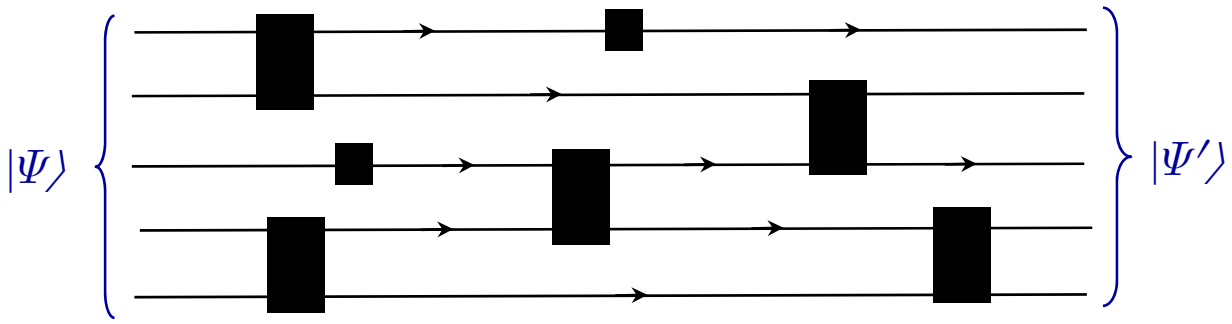
$$\left(t_0 \text{ s.t. } \int_0^{t_0} J(t)dt/\hbar = \pi/4\right)$$

Coupled systems, cont.

Generalization: for N qubits, pure state of total system described by vector in tensor product Hilbert space $\mathcal{H}_N = \mathcal{H}_1 \otimes \mathcal{H}_2 \ldots \otimes \mathcal{H}_N$, which has 2^N dimensions. Thus, 2^N independent basis states, of which only 2N are separable.

In general, for QC with N qubits, could consider all possible n-qubit gates, $n \leq N$. But it turns out that an arbitrary state in $\mathcal{H}_N$ can be generated by application only of 1- and 2-qubit gates.

Thus, possible design for a QC [quantum computer]



Benefit of QC: massively parallel processing, in principle of 2^N states!

Generic problem: Even if $|\Psi\rangle$ is an eigenstate of the computational basis (e.g. $|\Psi\rangle = |0\rangle_1 |1\rangle_2 |0\rangle_3 \ldots |1\rangle_N$), $|\Psi'\rangle$ will in general be a linear superposition of various basis states:

$$|\Psi'\rangle = \sum_{i,j,k\ldots=0,1} \alpha_{ijk\ldots N} |i\rangle_1 |j\rangle_2 |k\rangle_3 \ldots |s\rangle_N$$

Then on any one run, on measurement in the C. B., we will get just one of the C.B. states, with the appropriate probability, and lose all information on the rest.

Solution (Deutsch, Jozsa, Shor…): design clever algorithm such that, depending on answers to question, we always end up in a unique C.B. state!

SOME POSSIBLE USES OF A QUANTUM COMPUTER

(if one can be built!)

Note: First 3 applications depend only on possibility of manipulating arbitrary quantum states, not on specific circuit model described above.

1. Direct simulation of real-life QM systems (e.g. complicated spin Hamiltonians)
2. "Quantum annealing" for "classically hard" problems. Many "classically hard" (NP) problems can be cast in form of minimizing a certain function of the variables, which may then be treated as a "Hamiltonian". E.g. some problems are isomorphic to the problem of finding the groundstate of the "Ising spin glass" defined by the (classical) Hamiltonian

$$H_{SG} = -\sum_{ij} J_{ij}\sigma_i^z\sigma_j^z \qquad (J_{ij} \text{ "random"})$$

Classically, we may have to exhaust the 2^N possibilities!

Quantum annealing technique: $H_{SG} \to \hat{H}_{SG} = -\sum_{ij} J_{ij}\hat{\sigma}_i^z\hat{\sigma}_j^z$

Start with some quite different $\hat{H}$ such that $\left[\hat{H}, \hat{H}_{SG}\right] \neq 0$,

and groundstate of $\hat{H}_0$ known, e.g $\hat{H}_0 \equiv -K\sum_i \hat{\sigma}_i^x$

and initialize N-qubit system in groundstate of $\hat{H}_0$.

Now let $\alpha(0) = 1, \quad \alpha(\infty) = 0$

$$\hat{H}(t) = \alpha(t)\hat{H}_0 + (1-\alpha(t))\hat{H}_{SG}$$

If α(t) varies sufficiently slowly, system should follow adiabatically and, in absence of level crossing (△) end up in

groundstate of $\hat{H}_{SG}$!

Applications of a quantum computer (cont.)

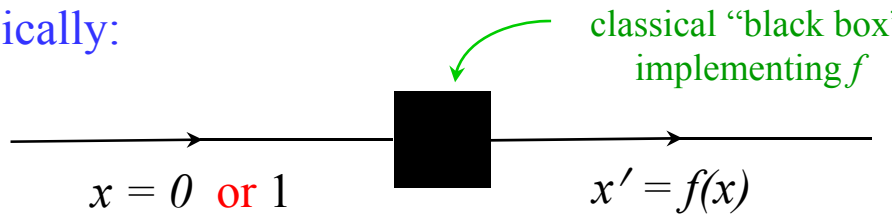
4. Speeded-up algorithms for "classically hard" problems

(Toy) example: Deutsch's problem.

Consider: $f : x \to x, \quad x = \{0,1\}$ (only 4 mappings!)

Question: Is $f(0) = f(1)$?

Classically:



Need to input first $x = 0$, then $x = 1$ (2 shots).

With a quantum computer, can we do it in one shot?

If $|0\rangle \to |f(0)\rangle$ and $|1\rangle \to |f(1)\rangle$, then (by linearity)

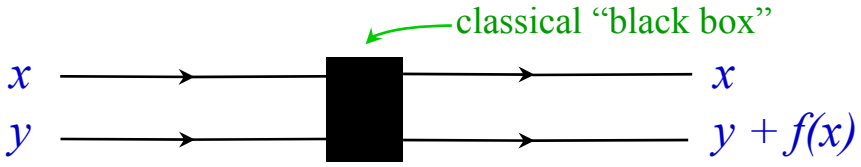
$$\alpha|0\rangle + \beta|1\rangle \to \alpha|f(0)\rangle + \beta|f(1)\rangle$$

So, tempting to try single-qubit quantum gate with input

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

Alas, if $f(0)=f(1)$ then classical gate is irreversible $\Rightarrow$ no quantum gate can be constructed!

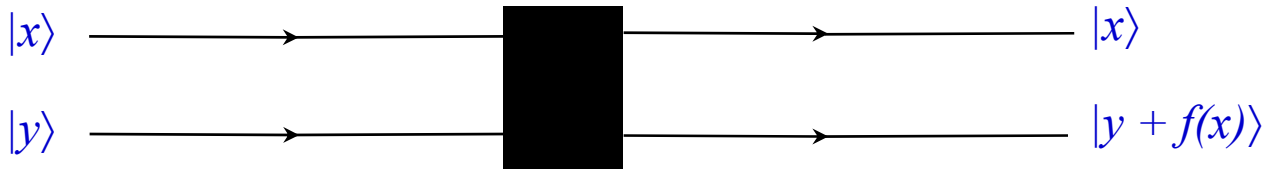
So, start from reversible classical black box (gate):



Classically, still need 2 shots (fix y, input first $x = 0$, then $x = 1$).

But, can now implement quantum version:

Quantum black box (gate for Deutsch's problem):



i.e. $\hat{U}\,|\,x_1, y_2\rangle = |\,x_1, (y + f(x_1))_2\rangle$

Digression: Is this gate entangling?

In general, yes! E.g. suppose $f(0)=0, f(1)=1$, and input

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1)\,|0\rangle_2 \qquad \text{unentangled}$$

then by linearity

$$|\Psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1\,|0\rangle_2) + |1\rangle_1\,|1\rangle_2 \qquad \text{entangled}$$

However, try $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ unentangled

i.e. $|\Psi\rangle = \frac{1}{2}(|0\rangle_1\,|0_2\rangle + |1\rangle_1\,|0\rangle_2 - |0\rangle_1\,|1\rangle_2 - |1\rangle_1\,|1\rangle_2)$

Then by linearity,

$$|\Psi'\rangle = \frac{1}{2}(|0\rangle_1\,|f(0)\rangle_2 + |1\rangle_1\,|f(1)\rangle_2 - |0\rangle_1\,|\tilde{f}(0)\rangle_2 - |1\rangle_1\,|\tilde{f}(1)\rangle_2)$$

where $\tilde{f}(0) =$ "not $f(0)$" (i.e. if $f(0)=0$ then $\tilde{f}(0)=1$, etc.)

This can be rewritten

$$|\Psi'\rangle = \frac{1}{2}(|0\rangle_1(|f(0)\rangle - |\tilde{f}(0)\rangle_2) + |1\rangle_1(|f(1)\rangle - |\tilde{f}(1)\rangle)_2)$$

If $f(1)=f(0)$ $(\text{so } \tilde{f}(1)=\tilde{f}(0))$ then

$$|\Psi'\rangle = \frac{1}{2}(|0\rangle + |1\rangle)_1 \bullet (|f(0)\rangle - |\tilde{f}(0)\rangle)_2$$

while if $f(0)\neq f(1)$ $(\text{so } \equiv \tilde{f}(1))$ then

$$|\Psi'\rangle = \frac{1}{2}(|0\rangle - |1\rangle)_1 (f(0) - \tilde{f}(0)\rangle)_2$$

Deutsch's problem (recap):

$$\text{if } f(0) = f(1), \text{ then } |\Psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_1 |x\rangle_2$$

$$\text{if } f(0) \neq f(:), \text{ then } |\Psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_1 |x\rangle_2$$

$$\text{where } |x\rangle_2 \equiv \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |\tilde{f}(0)\rangle\right)_2$$

So the output state of 2 (y′) is irrelevant, and we can measure X_1 [or perform a single-qubit rotation and measure Z_1]. If $X_1 = +1$, then $f(0)=f(1)$: if $X_1 = -1$, then $f(0) \neq f(1)$. Need only one shot!

Much more spectacular application (Shor, 1994):

recall that factorization of n-digit binary number on classical computer takes $\sim \exp\left(n^{1/3}\ell n^{2/3} n\right)$ steps.

In principle, on a quantum computer, takes $\sim n^3$ steps.

$\Rightarrow$ exponential speed-up!

RSA CRYPTOGRAPHY* ("public-key")

Two theorems:

(1) (number theory): [all numbers are positive integers]

Let p,q be primes, c any number which has no factors in common with (p-1)(q-1), and a any number. Then if

$b = a^c \pmod{pq}$

$a = b^d \pmod{pq}$, where

$d = c^{-1} \bmod (p-1)(q-1)$ (i.e. $cd = 1 + s(p-1)q-1)$

(2) (classical computer science):

a) If N=pq is a product of two primes, factoring N is hard ($\sim \exp(n'^{1/3}\ell n^{2/3} n)$ where n is number of binary digits of N)

b) However, if N is any (possibly large) number, finding the inverse of c mod N is easy ($\sim n^3$).

So:

A wishes to send B a string (key) 01001. . . . .⇒ equivalent to a (large) number a.

B selects 2 large primes p and q, and a large number c with no common factor with $(p-1)(q-1)$. He sends publicly to A:

(a) the number c

(b) the number N = pq (but not p and q individually)

A then performs the encryption: $a \rightarrow b \equiv a^c$, and sends the result publicly to B.

B alone knows p and q individually, and can therefore calculate $d=c^{-1} \bmod (p-1)(q-1)$ and decrypt: $b \rightarrow b^d \equiv a$

*based on Mermin, QCS, sections 3.2–3

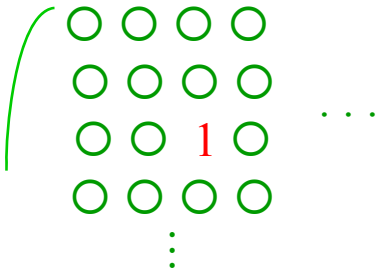
QUANTUM SEARCH ALGORITHM

(Grover: Farhi and Gutmann)

Problem: Identify one "tagged" item among N.
Classically, time taken (number of trials) ~N.
Quantum-mechanically: represent "items" by orthonormal vectors in an N-dimentional Hilbert space, and "tag" by a term in the Hamiltonian: i.e.

$$\hat{H} = \mathcal{H}\,|t\rangle\langle t|$$

$\hat{H}$=



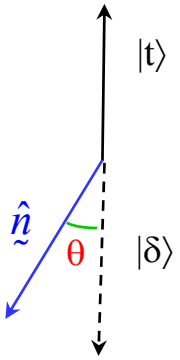
How to find |t⟩?

Solution: Create state

$$|\Psi\rangle = \frac{1}{\sqrt{N}}(1,1,1,1....1) \equiv \frac{1}{\sqrt{N}}|t\rangle + \sqrt{\frac{N}{N-1}}\,|s\rangle,\ |s\rangle \perp |t\rangle$$

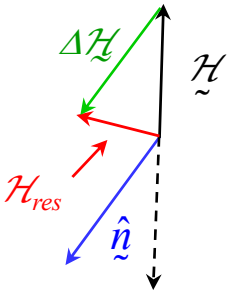
Isomorphic to state of spin ½ in 2D Hilbert space with

$|t\rangle \rightarrow |\uparrow\rangle$, $|S\rangle \rightarrow |\downarrow\rangle$



Ampl. of $|\uparrow\rangle$ (|t⟩)= $\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}}$ (not $\frac{1}{N}$!)

Now apply field || $\hat{n}$ (known vector!) of just such a magnitude (1) that resultant field (red arrow) bisects ∠ between $\hat{n}$ and t. Then



$$|\mathcal{H}_{res}| = 2\cos\left(\frac{\pi-\theta}{2}\right) = 2\sin\frac{\theta}{2} = \frac{2}{\sqrt{N}}$$

and $\mathcal{H}_{res}$ rotates $\hat{n}$ into the target (tagged) state |t⟩ in a time $T = \pi\,|\mathcal{H}_{res}$, i.e.

$$T = \frac{\pi}{2}\sqrt{N}$$

⇒ speedup over classical search