Quantum Computation

(Lecture 5)

Luís Soares Barbosa

Quantum Computing Course Unit

Universidade do Minho, 2021

Physics of information

Information

is encoded in the state of a physical system

Computation

is carried out on an actual physically realizable device

- the study of information and computation cannot ignore the underlying physical processes.
- ... although progress in Computer Science has been made by abstracting from the physical reality
- more precisely: by building more and more abstract models of a sort of reality, i.e. a way of understanding it
- ... and if this way changes?

A short, long way to go ...

How physics constrains our ability to use and manipulate information?

- Landauer's principle (1961): information deleting is necessarily a dissipative process.
- Charles Bennett (1973): any computation can be performed in a reversible way, and so with no dissipation.

NAND $\Longrightarrow$ Toffoli

$$(x, y) \mapsto \neg x \wedge y \qquad (x, y, z) \mapsto (x, y, z \oplus (x \wedge y))$$

with $z = 1$

A short, long way to go ...

Information is physical, and the physical reality is quantum mechanical:

How does quantum theory shed light on the nature of information?

- Quantum dynamics is truly random
- Acquiring information about a physical system disturbs its state (which is related to quantum randomness)
- Noncommuting observables cannot simultaneously have precisely defined values: the uncertainty principle
- Quantum information cannot be copied with perfect fidelity: the no-cloning theorem (Wootters, Zurek, Dieks, 1982)
- Quantum information is encoded in nonlocal correlations between the different parts of a physical system, i.e. the predictions of quantum mechanics cannot be reproduced by any local hidden variable theory (John Bell, 1967)

Quantum computing

$$\boxed{\text{The meaning of computable remains the same}}$$

A classical computer can simulate a quantum computer to arbitrarily good accuracy.

$$\boxed{\text{... but the order of complexity may change}}$$

but the simulation is computationally hard, i.e. extremely inefficient as the number of qubits increases:

- For 100 qubits the state space would require to store $2^{100} \approx 10^{30}$ complex numbers!
- And what about rotating a vector in a vector space of dimension 10^{30}?

Quantum computing

In a sense this is not the decisive argument:

Simulating the evolution of a vector in an exponentially large space can be done locally through a probabilistic classical algorithm in which each qubit has a value at each time step, and each quantum gate can act on the qubits in various possible ways, one of which is selected as determined by a (pseudo)-random number generator.

... After all, the computation provide a means of assigning probabilities to all the possible outcomes of the final measurement

Quantum computing

However, Bell's result precludes such a simulation: there is no local probabilistic algorithm that can reproduce the conclusions of quantum mechanics.

In the presence of entanglement, one can access only an exponentially small amount of information by looking at each subsystem separately.

Quantum computing as using quantum reality as a computational resource

Richard Feynman, *Simulating Physics with Computers* (1982)

The quest for efficient quantum algorithms

$$\boxed{\text{Factoring in polynomial time - } \mathcal{O}((ln\, n)^3)}$$

Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* (1994)

- Classically believed to be superpolynomial in log n, i.e. as n increases the worst case time grows faster than any power of log n.
- The best classical algorithm requires approximately

$$e^{1.9(\sqrt[3]{\ln\ n}\sqrt[3]{(\ln\ \ln\ n)^2})}$$

- From the best current estimation (the 65 digit factors of a 130 digit number can be found in around one month in a massively parallel computer network) one can extrapolate that to factor a 400 digit number will take about the age of the universe (10^{10} years)

The quest for efficient quantum algorithms

The quest

- Non exponential speedup. Not relevant for the complexity debate, but shed light on what a quantum computer can do.
  Example: Grover's search of an unsorted data base.
- Exponential speedup relative to an oracle. By feeding quantum superpositions to an oracle, one can learn what is inside it with an exponential speedup.
  Example: Simon's algorithm for finding the period of a unction.
- Exponential speedup for apparently hard problems
  Example: Shor's factoring algorithm.

The circuit model

Classical reversible circuits (which can simulate any non-reversible one with modest overhead) generalise to quantum circuits where

- logical qubits are carried along wires,
- quantum gates, corresponding to unitary transformations, act on them, and
- measurements result in a state $|i\rangle$, with probability given by the norm squared of its amplitude, $\|a_i\|^2$, together with a classical label "i" indicating which outcome was obtained.

A parenthesis: Unitary transformations

$$(\qquad \ldots$$

Unitary transformations

Gates encode transformations that

- are linear:

$$U\left(\alpha_1|v_1\rangle + \cdots + \alpha_k|v_k\rangle\right) \;=\; \alpha_1 U\,|v_1\rangle + \cdots + \alpha_2 U\,|v_k\rangle$$

- and map orthogonal subspaces to orthogonal subspaces (cf, unit length vectors map to unit length vectors)

These properties hold iff U preserves inner products:

$$\langle v|U^\dagger U|w\rangle \;=\; \langle v|w\rangle$$

which entails

$$U^\dagger U \;=\; I \qquad\qquad U \text{ is unitary}$$

Unitary transformations

- Not only unitary operators map orthonormal bases to orthonormal bases, since they preserve the inner product, but also any linear transformation with such behaviour is unitary.
- If given in matrix form, being unitary means that the set of columns of its matrix representation are orthonormal (because the ith column is the image of $U|i\rangle$). equivalently, rows are orthonormal (why?)
- Both $U_1 U_1$ and $U_1 \otimes U_2$ are unitary, if U_i are; but linear combinations of unitary operators, however, are not in general unitary.

Unitary transformations are reversible

Unitary transformations

The no-cloning theorem: well-known consequence of linearity

Let $U(|a\rangle|0\rangle) = |a\rangle|a\rangle$ and consider state $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$ for $|a\rangle$ and $|b\rangle$ orthogonal. Then

$$\begin{aligned} U(|c\rangle|0\rangle) &= \frac{1}{\sqrt{2}}(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle) \\ &\neq \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle) \\ &= |c\rangle|c\rangle \\ &= U(|c\rangle|0\rangle) \end{aligned}$$

This result, however, does not preclude the construction of a known quantum state from a known quantum state.

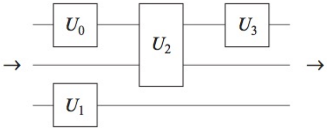
End of parenthesis

$\ldots \quad)$

Quantum gates

A gate is a transformation that acts on only a small number of qubits
Differently from the classical case, they do not necessarily correspond to physical objects

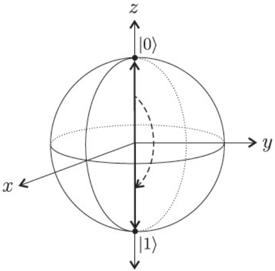
Notation



1-Gates

The action of a 1-gate U on a quantum state $|\phi\rangle$ can be thought of as a rotation of the Bloch vector for $|\phi\rangle$ to the Bloch vector for $U|\phi\rangle$, eg.

Exemple: X

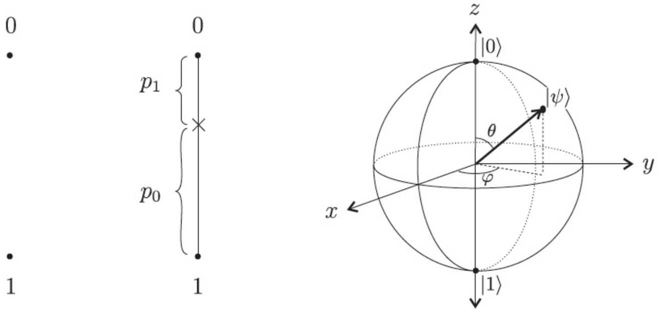


A parenthesis: Representation in the Bloch sphere

(. . .

The Bloch sphere

Deterministic, probabilistic and quantum bits



(from [Kaeys *et al*, 2007])

The Bloch sphere

The state of a quantum bit is described by a complex unit vector in a 2-dim Hilbert space, which, up to a physically irrelevant global phase factor, can be written as

$$|\psi\rangle = \underbrace{\cos\frac{\theta}{2}}_{\alpha}|0\rangle + \underbrace{e^{i\varphi}\sin\frac{\theta}{2}}_{\beta}|1\rangle$$

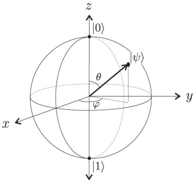
where $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$, and depicted as a point on the surface of a 3-dim Bloch sphere, defined by θ and φ.
The Bloch vector $|\psi\rangle$ has

- Spherical coordinates:
  $x = \rho\sin\theta\cos\varphi \quad y = \rho\sin\theta\sin\varphi \quad = \quad z = \rho\cos\theta$
- Measurement probabilities:

$$\|\alpha\|^2 = \left(\cos\frac{\theta}{2}\right) \quad = \quad \frac{1}{2} + \frac{1}{2}\cos\theta$$

$$\|\beta\|^2 = \left(\sin\frac{\theta}{2}\right) \quad = \quad \frac{1}{2} - \frac{1}{2}\cos\theta$$

The Bloch sphere



- The poles represent the classical bits. In general, orthogonal states correspond to antipodal points and every diameter to a basis for the single-qubit state space.
- Once measured a qubit collapses to one of the two poles. Which pole depends exactly on the arrow direction: The angle θ measures that probability: If the arrow points at the equator, there is 50-50 chance to collapse to any of the two poles.
- Rotating a vector wrt the z-axis results into a phase change (φ), and does not affect which state the arrow will collapse to, when measured.

The Bloch sphere

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

Express $|\psi\rangle$ in polar form

$$|\psi\rangle = \rho_1 e^{i\varphi_1}|0\rangle + \rho_2 e^{i\varphi_2}|1\rangle$$

and eliminate one of the four real parameters multiplying by $e^{-i\varphi_1}$

$$|\psi\rangle = \rho_1|0\rangle + \rho_2 e^{i(\varphi_2-\varphi_1)}|1\rangle = \rho_1|0\rangle + \rho_2 e^{i\varphi}|1\rangle$$

making $\varphi = \varphi_2 - \varphi_1$.

Switch back the coefficient of $|1\rangle$ to Cartesian coordinates and compute the normalization constraint

$$\|\rho_1\|^2 + \|a+ib\|^2 = \|\rho_1\|^2 + (a-ib)(a+ib) = \|\rho_1\|^2 + a^2 + b^2 = 1$$

which is the equation of a unit sphere in Real 3-dim space with Cartesian coordinates: (a, b, ρ_1).

The Bloch sphere

Back to polar,

$$\begin{aligned} x &= \rho \sin\theta \cos\varphi \\ y &= \rho \sin\theta \sin\varphi \\ z &= \rho \cos\theta \end{aligned}$$

So, recalling that $\rho = 1$,

$$\begin{aligned} |\psi\rangle &= z|0\rangle + (a + ib)|1\rangle \\ &= \cos\theta|0\rangle + \sin\theta(\cos\varphi - i\sin\varphi)|1\rangle \\ &= \cos\theta|0\rangle + e^{i\varphi}\sin\theta|1\rangle \end{aligned}$$

which, with two parameters, defines a point in the sphere's surface.

The Bloch sphere

Actually, one may just focus on the upper hemisphere ($0 \leq \theta' \leq \frac{\pi}{2}$) as opposite points in the lower one differ only by a phase factor of -1:

Let $|\psi'\rangle$ be the opposite point on the sphere with polar coordinates $(1, \pi - \theta', \varphi + \pi)$

$$\begin{aligned} |\psi'\rangle &= \cos(\pi - \theta')|0\rangle + e^{i(\varphi+\pi)} \sin(\pi - \theta')|1\rangle \\ &= -\cos\theta'|0\rangle + e^{i\varphi} e^{i\pi} \sin\theta'|1\rangle \\ &= -\cos\theta'|0\rangle + e^{i\varphi} \sin\theta'|1\rangle \\ &= -|\psi\rangle \end{aligned}$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \sin\frac{\theta}{2}|1\rangle$$

where $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$

End of parenthesis

$\ldots \qquad)$

1-Gates

The Hadamard gate

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

$$\begin{aligned} H|0\rangle &= |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Note that $HH = I$

1-Gates

The phase shift gate

$$R_\phi = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

$$\begin{aligned} R_\phi |0\rangle &= |0\rangle \\ R_\phi |1\rangle &= e^{i\phi}|1\rangle \end{aligned}$$

The T (or $\frac{\pi}{8}$) gate

$$T = R_{\frac{\pi}{4}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

which, up to global phase, is equivalent to

$$\begin{bmatrix} e^{i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix}$$

1-Gates

Pauli gates

$$
\begin{aligned}
I &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
X &= |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
Z &= |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = R_\pi \\
Y &= i(-|1\rangle\langle 0| + |0\rangle\langle 1|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}
\end{aligned}
$$

1-Gates

Rotation gates

Correspond to rotations about the three axes of the Bloch sphere, and are computed as Pauli gates squared.

$$R_e(\theta) \,\widehat{=}\, e^{\frac{-i\theta E}{2}} = \cos\left(\frac{\theta}{2}\right) I - i \sin \frac{\theta}{2} E$$

where $e \,\widehat{=}\, x, y, z$ and $E \,\widehat{=}\, X, Y, Z$.

because, for any real number r and matrix R st $R^2 = I$, which is the case for X, Y, and Z,

$$e^{irR} = cos(r) I + i \sin(r) R$$

1-Gates

Rotation gates as matrices in the computational basis

$$R_x(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$R_y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

$$R_z(\theta) = \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$$

1-Gates

Compute $R_z(\theta)|\psi\rangle$ for $|\psi\rangle = \cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i\gamma}\sin\left(\frac{\sigma}{2}\right)|1\rangle$

$$\begin{aligned}
\begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix} &= \begin{bmatrix} e^{-i\frac{\theta}{2}}\cos\left(\frac{\sigma}{2}\right) \\ e^{i\frac{\theta}{2}}e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix} \\
&= e^{-i\frac{\theta}{2}} \begin{bmatrix} \cos\left(\frac{\sigma}{2}\right) \\ e^{i\theta}e^{i\gamma}\sin\left(\frac{\sigma}{2}\right) \end{bmatrix} \\
&= e^{-i\frac{\theta}{2}} \left(\cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i(\gamma+\theta)}\sin\left(\frac{\sigma}{2}\right)|1\rangle\right)
\end{aligned}$$

As global phase is insignificant, the angle mapping $\gamma \mapsto \gamma + \theta$ is a rotation of θ around the z-axis of the Bloch sphere.

1-Gates

Theorem

Let U be a 1-gate, and v, w any two non-parallel axes of the Bloch sphere. Then there exist real numbers $\alpha, \beta\, \gamma, \delta$ st

$$U \;=\; e^{i\alpha} R_v(\beta) R_w(\gamma) R_v(\delta)$$

which means that any 1-gate can be expressed as a sequence of two rotations about an axis and one rotation about another non parallel axis, multiplied by a suitable phase factor.

proof hint: Recall U is unitary and unfold the definition of rotation gate.

2-gates: *CNOT*

Acts on the standard basis for a 2-qubit system, flipping the second bit if the first bit is 1 and leaving it unchanged otherwise.

$$\begin{aligned} CNOT &= |0\rangle\langle 0| \otimes I \; + \; |1\rangle\langle 1| \otimes X \\ &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \; + \; |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{aligned}$$

CNOT is unitary and is its own inverse, and cannot be decomposed into a tensor product of two 1-qubit transformations

2-gates: *CNOT*

The importance of *CNOT* is its ability to change the entanglement between two qubits, e.g.

$$
\begin{aligned}
CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) &= CNOT\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)
\end{aligned}
$$

Since it is its own inverse, it can take an entangled state to an unentangled one.
Note that entanglement is not a local property in the sense that transformations that act separately on two or more subsystems cannot affect the entanglement between those subsystems:

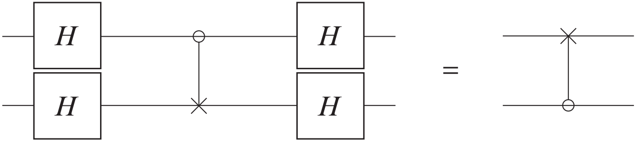
$(U \otimes V)|v\rangle$ is entangled iff $|v\rangle$ is

2-gates: *CNOT*

The notions of control/target bit in *CNOT* are arbitrary: they depend on what basis is considered. The standard behaviour is obtained in the computational basis. However, roles are interchanged in the Hadamard basis in which the effect of *CNOT* is

$$|++\rangle \mapsto |++\rangle \quad |+-\rangle \mapsto |--\rangle \quad |-+\rangle \mapsto |-+\rangle \quad |--\rangle \mapsto |+-\rangle$$

Exercise



The proof

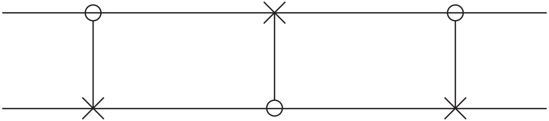
$$
\begin{aligned}
LHS &= \frac{1}{2}\begin{bmatrix} H & H \\ H & -H \end{bmatrix} \overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{CNOT} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix} H & HX \\ H & -HX \end{bmatrix} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix} I+HXH & I-HXH \\ I-HXH & I+HXH \end{bmatrix} \quad = \quad \frac{1}{2}\begin{bmatrix} I+Z & I-Z \\ I-Z & I+Z \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \\
&= I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| \quad = \quad RHS
\end{aligned}
$$

noting that

$$
H \otimes H = (I \otimes H)(H \otimes I) = \frac{1}{\sqrt{2}}\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} H & H \\ H & -H \end{bmatrix}
$$

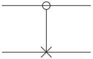
Exercise

Discuss

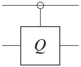


Controlled Q-gates

From



to



$$\begin{aligned} C_Q|0\rangle|\varphi\rangle &= |0\rangle|\varphi\rangle \\ C_Q|1\rangle|\varphi\rangle &= |1\rangle Q|\varphi\rangle \end{aligned}$$

$$C_Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q$$

corresponding to the following matrix in the standard basis:

$$C_Q = \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}$$

Controlled phase shift gate

$$e^{i\theta} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta}|10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$$

$$e^{i\theta} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$$

Transforming a global into a local phase

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle \quad \longrightarrow \quad \frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle$$

Actually, a unitary transformation is completely determined by its action on a basis, but not by specifying what states the states corresponding to basis states are sent to.

Example: $e^{i\theta}$ takes the four quantum states to themselves (because e.g. $|10\rangle$ and $e^{i\theta}|10\rangle$ represent the same state), but a global phase can be transformed into a local one, as above

CCNOT or Toffoli gate

A 3-bit gate corresponding to controlled *CNOT*. If the first two bits are in the state $|1\rangle$ applies X the third bit, else it does nothing:

$$|q_1 q_2 q_3\rangle \;\mapsto\; |q_1 q_2, q_3 \oplus (q_1 \wedge q_2)\rangle$$

In matrix form,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Universal set of gates?

Is there a universal set of quantum gates?

In general no: there are uncountably many quantum transformations, and a finite set of generators can only generate countably many elements. However, it is possible for finite sets of gates to generate arbitrarily close approximations to all unitary transformations.

Definitions

- The error in approximating U by V is

$$Er(U,V) \ = \ \max_{|\phi\rangle} \ \|(U-V)|\phi\rangle\|$$

- An operator U can be approximated to arbitrary accuracy if for any positive ϵ there exists another unitary transformation V st $Er(U,V) \leq \epsilon$.
- A set of gates is universal if for any integer $n \geq 1$, any n-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set.

Universal set of gates?

Some examples

- The set $\{H, T\}$ is universal for 1-gates.
- The set $\{H, T, CNOT\}$ is a universal set of gates.

How efficient is an approximation?

To approximate an unitary transformation encoding some specific computation, one would expect to use a number of gates from the universal set which is polynomial in the number of qubits and the inverse of the quality factor ϵ.

Main result: theorem of Solovay-Kitaev (1997)

Computing: A probabilistic machine

States: Given a set of possible configurations, states are vectors of probabilities in $\mathcal{R}^n$ which express indeterminacy about the exact physical configuration, e.g. $\left[p_0 \cdots p_n\right]^T$ st $\sum_i p_1 = 1$
Operator: double stochastic matrix (*must come (go) from (to) somewhere*), where $M_{i,j}$ specifies the probability of evolution from configuration j to i
Evolution: computed through matrix multiplication with a vector $|u\rangle$ of current probabilities

- $M|u\rangle$ (next state)
- $|u\rangle^T M^T$ (previous state)

Measurement: the system is always in some configuration — if found in i, the new state will be a vector $|t\rangle$ st $t_j = \delta_{j,i}$

Computing: A probabilistic machine

Composition:

$$p \otimes q \;=\; \begin{bmatrix} p_1 \\ 1 - p_1 \end{bmatrix} \otimes \begin{bmatrix} q_1 \\ 1 - q_1 \end{bmatrix} \;=\; \begin{bmatrix} p_1 q_1 \\ p_1(1 - q_1) \\ (1 - p_1) q_1 \\ (1 - p_1)(1 - q_1) \end{bmatrix}$$

- correlated states: cannot be expressed as $p \otimes q$, e.g.

$$\begin{bmatrix} 0.5 \\ 0 \\ 0 \\ 0.5 \end{bmatrix}$$

- Operators are also composed by $\otimes$ (Kronecker product):

$$M \otimes N \;=\; \begin{bmatrix} M_{1,1}N & \cdots & M_{1,n}N \\ \vdots & & \vdots \\ M_{m,1}N & \cdots & M_{m,n}N \end{bmatrix}$$

Computing: A quantum machine

States: given a set of possible configurations, states are unit vectors of (complex) amplitudes in $\mathcal{C}^n$
Operator: unitary matrix ($M^\dagger M = I$). The norm squared of a unitary matrix forms a double stochastic one.
Evolution: computed through matrix multiplication with a vector $|u\rangle$ of current amplitudes (wave function)

- $M|u\rangle$ (next state)
- $|u\rangle^T M^T$ (previous state)

Measurement: configuration i is observed with probability $\|\alpha_i\|^2$ if found in i, the new state will be a vector $|t\rangle$ st $t_j = \delta_{j,i}$
Composition: also by a tensor on the complex vector space; may exist entangled states

Computing: A quantum machine

Quantum algorithms

1. State preparation (fix initial setting)
2. Transformation
   (combination of unitary transformations)
3. Measurement
   (projection onto a basis vector associated with a measurement tool)

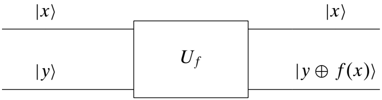
What's next?

1. Study a number of algorithmic techniques
2. and their application to the development of quantum algorithms

The Deutsch problem

Is $f : \mathbf{2} \longrightarrow \mathbf{2}$ constant, with a unique evaluation?

Oracle



where $\oplus$ stands for exclusive or, i.e. addition module 2.

- The oracle takes input $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$
- Fixing $y = 0$ the output is $|x\rangle|f(x)\rangle$

The Deutsch problem

Preparing the first qubit as $|x\rangle$ is the (quantum version of) input x:

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle|f(0)\rangle \\ |1\rangle|0\rangle &\mapsto |1\rangle|f(1)\rangle \end{aligned}$$

But in the quantum world, one can better: input a superposition of $|0\rangle$ and $|1\rangle$ to get

$$|\frac{|0\rangle + |1\rangle}{\sqrt{2}}, 0\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,|0\rangle \mapsto \cdots$$

The Deutsch problem

. . .

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2}}|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,|0\rangle\right) &= \frac{1}{\sqrt{2}}U_f|0\rangle|0\rangle + \frac{1}{\sqrt{2}}U_f|1\rangle|0\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle|0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|0 \oplus f1\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f1\rangle \end{aligned}$$

- The value of f on both possible inputs (0 and 1) was computed simultaneously in superposition
- Double evaluation — the bottleneck in a classical solution — was avoided by superposition

Is such **quantum parallelism** useful?

NO

Although both values have been computed simultaneously, only one of them is retrieved upon measurement in the computational basis: Actually, 0 or 1 will be retrieved with identical probability (why?).

YES

The Deutsch problem is not interested on the concrete values f may take, but on a global property of f: whether it is constant or not, technically on the value of

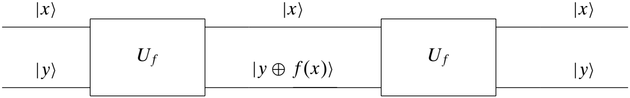
$$f(0) \oplus f(1)$$

The Deutsch algorithm explores another quantum resource — interference — to obtain that global information on f

Is the oracle a **quantum gate**?

First of all, one must prove that

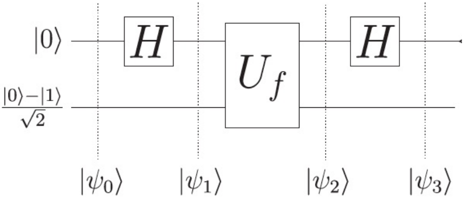
- The oracle is a unitary, i.e. reversible gate



$$|x\rangle|(y \oplus f(x)) \oplus f(x)\rangle = |x\rangle|y \oplus (f(x) \oplus f(x))\rangle = |x\rangle|y \oplus 0\rangle = |x\rangle|y\rangle$$

Deutsch algorithm

Idea: Avoid double evaluation by superposition and interference



The circuit computes:

$$|\varphi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

Deutsch algorithm

After the oracle, at φ_2, one obtains

$$|x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \Leftarrow f(x) = 0 \\ |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} & \Leftarrow f(x) = 1 \end{cases}$$

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

For $|x\rangle$ a superposition:

$$\begin{aligned} |\varphi_2\rangle &= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ &= \begin{cases} (\pm 1) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ constant} \\ (\pm 1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ not constant} \end{cases} \end{aligned}$$

Deutsch algorithm

$$\begin{aligned} |\sigma_3\rangle &= H|\sigma_2\rangle \\ &= \begin{cases} (\pm 1)\,|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ constant} \\ (\pm 1)\,|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ not constant} \end{cases} \end{aligned}$$

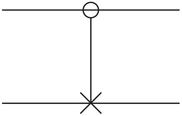
To answer the original problem is now enough to measure the first qubit: if it is in state $|0\rangle$, then f is constant.

Note

As the initial state in the second qubit can be prepared as $H|1\rangle$, the circuit is equivalent to

$$(H \otimes I)\, U_f\, (H \otimes H)(|01\rangle)$$

Recalling the *CNOT* gate



$$\overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{CNOT}$$

$$\begin{aligned} CNOT|0\rangle|\varphi\rangle &= |0\rangle I|\varphi\rangle \\ CNOT|1\rangle|\varphi\rangle &= |1\rangle X|\varphi\rangle \end{aligned}$$

Recall its effect when applied in the Hadamard basis, e.g.

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

The phase jumps, or is kicked back, from the second to the first qubit.

The phase 'kick back' technique

This happens because $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of

- X (with $\lambda = -1$) and of I (with $\lambda = 1$)
- and, thus, $X \frac{|0\rangle - |1\rangle}{\sqrt{2}} = -1 \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ and $I \frac{|0\rangle - |1\rangle}{\sqrt{2}} = 1 \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Thus,

$$\begin{aligned} CNOT\,|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= |1\rangle \left(X \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= |1\rangle \left((-1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= -|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

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

The phase ‘kick back’ technique

The phase has been kicked back to the first (control) qubit:

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

for $i \in \{0,1\}$, yielding, when the first (control) qubit is in a superposition of $|0\rangle$ and $|1\rangle$,

$$CNOT\,(\alpha|0\rangle+\beta|1\rangle)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = (\alpha|0\rangle-\beta|1\rangle)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

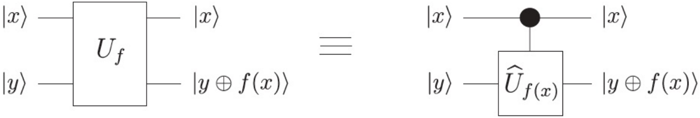
The phase ‘kick back’ technique

Input an eigenvector to the target qubit of operator $\widehat{U}_{f(x)}$, and associate the eigenvalue with the state of the control qubit

Phase ‘kick back’ in the Deutsch algorithm

Instead of *CNOT*, an oracle U_f for an arbitrary Boolean function $f : \mathbf{2} \longrightarrow \mathbf{2}$, presented as a controlled-gate, i.e. a 1-gate $\widehat{U}_{f(x)}$ acting on the second qubit and controlled by the state $|x\rangle$ of the first one, mapping

$$|y\rangle \mapsto |y \oplus f(x)\rangle$$



The critical issue is that state $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of $\widehat{U}_{f(x)}$

Phase ‘kick back’ in the Deutsch algorithm

$$
\begin{aligned}
U_f\,|x\rangle|-\rangle &= |x\rangle\,\widehat{U}_{f(x)}|-\rangle \\
&= \left(\frac{|x\rangle\,\widehat{U}_{f(x)}\,|0\rangle - |x\rangle\,\widehat{U}_{f(x)}\,|1\rangle}{\sqrt{2}}\right) \\
&= \left(\frac{|x\rangle|0\oplus f(x)\rangle - |x\rangle|1\oplus f(x)\rangle}{\sqrt{2}}\right) \\
&= |x\rangle\left(\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}\right) \\
&= |x\rangle(-1)^{f(x)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \;=\; |x\rangle(-1)^{f(x)}|-\rangle
\end{aligned}
$$

Thus, when the control qubit is in a superposition of $|0\rangle$ and $|1\rangle$,

$$
U_f\left(\alpha|0\rangle + \beta|1\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \;=\; \left((-1)^{f(0)}\alpha|0\rangle + (-1)^{f(1)}\beta|1\rangle\right)|-\rangle
$$

Generalizing Deutsch ...

Generalizing Deutsch's algorithm to functions whose domain is an

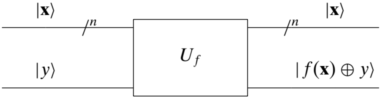
initial segment n of $\mathbb{N}$ encoded into a binary string

i.e. the set of natural numbers from 0 to $\mathbf{2}^n - 1$

The Deutsch-Jozsa problem

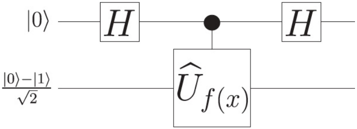
$$\boxed{\text{Assuming } f : \mathbf{2}^n \longrightarrow \mathbf{2} \text{ is either balanced or constant, determine which is the case with a unique evaluation}}$$

The oracle

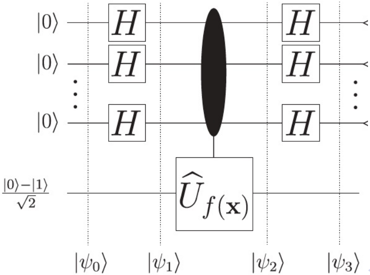


Generalizing Deutsch ...

The Deutsch circuit



The Deutsch-Joza circuit



The Deutsch-Jozsa Algorithm

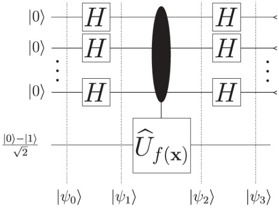
The crucial step is to compute $H^{\otimes n}$ over n qubits:

$$\begin{aligned} H^{\otimes n}|0\rangle^{\otimes n} &= \left(\frac{1}{\sqrt{2}}\right)^{n} \underbrace{(|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)}_{n} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{2}^n} |x\rangle \end{aligned}$$

Thus

$$\begin{aligned} \varphi_0 &= |0\rangle^{\otimes n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ \varphi_1 &= \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbf{2}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

The Deutsch-Jozsa Algorithm



The phase kick-back effect

$$\varphi_2 = \frac{1}{\sqrt{2^n}} U_f \left(\sum_{x \in \mathbf{2}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right)$$

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

The Deutsch-Jozsa Algorithm

Finally, we have to compute the last stage of $H^{\otimes}$ application.

$$H|x\rangle \;=\; \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x}|1\rangle) \;=\; \frac{1}{\sqrt{2}}\sum_{z\in\mathbf{2}}(-1)^{xz}|z\rangle$$

$$\begin{aligned}
H^{\otimes}|x\rangle &= H^{\otimes}(|x_1\rangle, \cdots, |x_n\rangle) \\
&= H|x_1\rangle \otimes \cdots \otimes H|x_n\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle)\;\cdots\;\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_n}|1\rangle) \\
&= \frac{1}{\sqrt{2^n}}\sum_{z_1z_2\cdots z_n\in\mathbf{2}}(-1)^{x_1z_1+x_2z_2+\cdots+x_nz_n}|z_1\rangle|z_2\rangle\cdots|z_n\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{z\in\mathbf{2}^n}(-1)^{x.z}|z\rangle
\end{aligned}$$

The Deutsch-Jozsa Algorithm

$$
\begin{aligned}
|\varphi_3\rangle &= \frac{\sum_{x\in\mathbf{2}^n}(-1)^{f(x)}\sum_{z\in\{0,1\}^n}(-1)^{z.x}|z\rangle}{2^n}\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{\sum_{x,z\in\mathbf{2}^n}(-1)^{f(x)}(-1)^{z.x}|z\rangle}{2^n}\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{\sum_{x,z\in\mathbf{2}^n}(-1)^{f(x)+z.x}|z\rangle}{2^n}\ \frac{|0\rangle-|1\rangle}{\sqrt{2}}
\end{aligned}
$$

Note that the amplitude for state $|z\rangle = |0\rangle^{\otimes}$ is

$$\frac{1}{2^n}\sum_{x\in\mathbf{2}^n}(-1)^{f(x)}$$

The Deutsch-Jozsa Algorithm

Analysis

$$\boxed{f \text{ is constant at } 1} \quad \rightsquigarrow \quad \frac{-(2^n)|0\rangle}{2^n} = -|0\rangle$$

$$\boxed{f \text{ is constant at } 0} \quad \rightsquigarrow \quad \frac{(2^n)|0\rangle}{2^n} = |0\rangle$$

As $|\varphi_3\rangle$ has unit length, all other amplitudes must be 0 and the top qubits collapse to $|0\rangle$

$$\boxed{f \text{ is balanced}} \quad \rightsquigarrow \quad \frac{0|0\rangle}{2^n} = 0|0\rangle$$

because half of the x will cancel the other half. The top qubits collapse to some other basis state, as $|0\rangle$ has zero amplitude

$$\boxed{\text{The top qubits collapse to } |0\rangle \text{ iff } f \text{ is constant}}$$

Quantum Algorithms

The Deutsch-Jozsa algorithm: Lessons learnt

- Exponential speed up: f was evaluated once rather than $2^n - 1$ times
- The quantum state encoded global properties of function f
- ... that can be extracted by exploiting cleverly such non local correlations.

Quantum Algorithms

The remaining of this course will exploe

Classes of quantum algorithm

- Based on the quantum Fourier transform: The Deutsch-Jozsa is a simple example; Phase estimation; Shor algorithm; etc.
- Based on amplitude amplification: Variants of Grover algorithm for search processes.
- Quantum simulation.

and come back to complexity in the end.
However a proper algorithmic science is still lacking
(more next year in *Quantum Logic*)