Quantum Computation

(Lecture 1)

Luís Soares Barbosa

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

UNITED NATIONS UNIVERSITY UNU-EGOV

Quantum Computing Course Unit

Universidade do Minho, 2020

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

$$\Big(\qquad \ldots$$

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.

$\boxed{\text{Unitary transformations are reversible}}$

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.

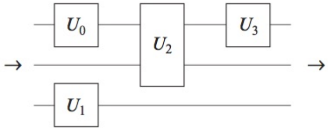
End of parenthesis

$\ldots$ $)$

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

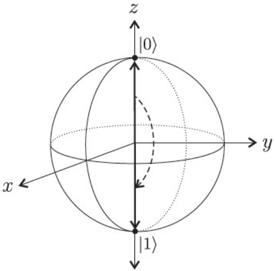
Notation



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

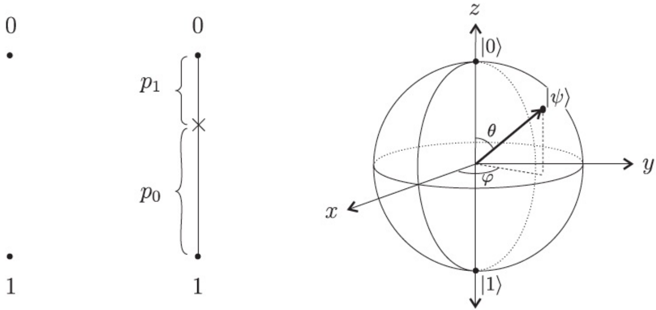


A parenthesis: Representation in the Bloch sphere

$$(\quad \dots$$

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

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

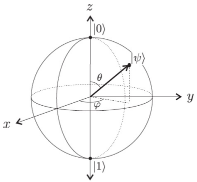
where $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$, and depicted as a point on the surface of a 3-dim Bloch sphere, defined by θ and φ.
The Bloch vector $|\psi\rangle$ has

- 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

$\ldots \quad)$

1-Gates

The Hadamard gate

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

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

Note that $HH = I$

1-Gates

The phase shift gate

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

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

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.

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

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

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:

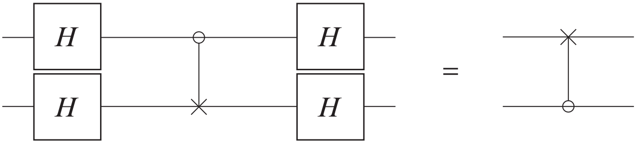
$$(U \otimes V)\,|v\rangle \quad \text{is entangled} \quad \text{iff} \quad |v\rangle \text{ is}$$

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

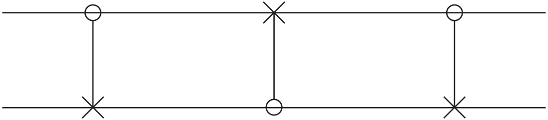
$$
\begin{aligned}
\textit{LHS} &= \frac{1}{2}\begin{bmatrix} H & H \\ H & -H \end{bmatrix} \overbrace{\begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}}^{CNOT} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} \\
&= \frac{1}{2}\begin{bmatrix} H & HX \\ H & -HX \end{bmatrix} \begin{bmatrix} H & H \\ H & -H \end{bmatrix}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

noting that

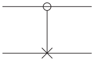
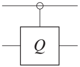
$$
H \otimes H = (I \otimes H)(H \otimes I) = \frac{1}{\sqrt{2}}\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}\begin{bmatrix} I & I \\ I & -I \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} H & H \\ H & -H \end{bmatrix}
$$

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

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

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

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 $t_j = \delta_{j,i}$

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):

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

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

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 phase 'push up' technique

Recall the role swap between control and target qubits when a $CNOT$ is applied in the Hadamard basis, e.g.

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

This happens because $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of X (with $\lambda = -1$) and of I (with $\lambda = 1$). Thus,

$$\begin{aligned} CNOT\,|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= |1\rangle\left(NOT\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= |1\rangle\left((-1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\ &= -|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

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 'push up' technique

The phase has been pushed up to the 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 control qubit is in a superposition of $|0\rangle$ and $|1\rangle$,

$$CNOT\,(a_0|0\rangle + a_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \;=\; (a_0|0\rangle - a_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

The phase 'push up' technique

Now, replace *CNOT* by an oracle (reversible implementation) U_f for an arbitrary Boolean function $f : \mathbf{2} \longrightarrow \mathbf{2}$:

$$U_f \, |xy\rangle \; = \; |x\rangle |y \oplus f(x)\rangle$$

The phase 'push up' technique

Fix the target as $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and an arbitrary basis state as the control,

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

Clearly,

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

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

$$U_f\,(a_0|0\rangle + a_1|1\rangle)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left((-1)^{f(0)}a_0|0\rangle + (-1)^{f(1)}a_1|1\rangle\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

The phase 'push up' technique

U_f can be regarded as 1-gate $\hat{U}_{f(x)}$ acting on the second qubit and controlled by the state $|x\rangle$ of first one, mapping

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

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

Note that the state $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ of the target is an eigenvector of $\hat{U}_{f(x)}$

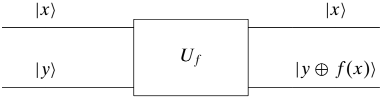
The phase 'push up' technique

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

My first quantum program

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

Oracle



where $\oplus$ stands for exclusive disjunction.

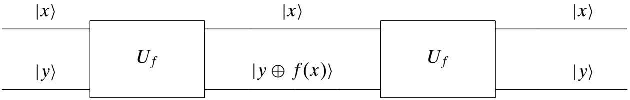
- The oracle takes input $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$
- for $y = 0$ the output is $|x, f(x)\rangle$

My first quantum program

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

Oracle

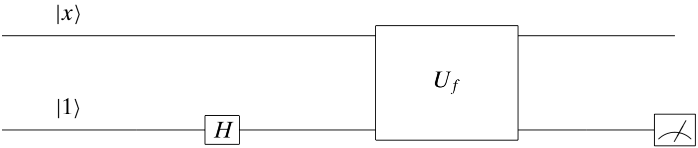
- The oracle is a unitary, i.e. reversible gate



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

My first quantum program

Idea: Avoid double evaluation by superposition

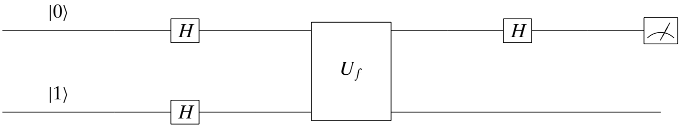


The circuit computes:

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

My first quantum program

Idea: Avoid double evaluation by superposition



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

Input in superposition

$$|\sigma_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\, \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

My first quantum program

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

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

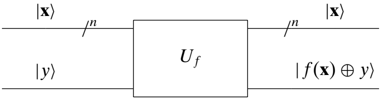
To answer the original problem is now enough to measure the first qubit: if it is in state $|0\rangle$, then f is constant.

The Deutsch-Jozsa Algorithm

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 $\mathbf{2}^n - 1$).

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

Oracle



Using $H^{\otimes n}$ to put n qubits superposed

Computing $H^{\otimes n}$

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

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

Using $H^{\otimes n}$ to put n qubits superposed

Computing $H^{\otimes n}$

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

$$= \frac{1}{2} \begin{bmatrix} (-1)^{\langle 00,00\rangle} & (-1)^{\langle 00,01\rangle} & (-1)^{\langle 01,00\rangle} & (-1)^{\langle 01,01\rangle} \\ (-1)^{\langle 00,10\rangle} & (-1)^{\langle 00,11\rangle} & (-1)^{\langle 01,10\rangle} & (-1)^{\langle 01,11\rangle} \\ (-1)^{\langle 10,00\rangle} & (-1)^{\langle 10,01\rangle} & (-1)^{\langle 11,00\rangle} & (-1)^{\langle 11,01\rangle} \\ (-1)^{\langle 10,10\rangle} & (-1)^{\langle 10,11\rangle} & (-1)^{\langle 11,10\rangle} & (-1)^{\langle 11,11\rangle} \end{bmatrix}$$

where $\langle x, y\rangle = (x_0 \wedge y_0) \oplus (x_1 \wedge y_1) \oplus \cdots \oplus (x_n \wedge y_n)$
Note that

$$(-1)^{a\wedge b} \otimes (-1)^{a'\wedge b'} = (-1)^{a\wedge a' \oplus b\wedge b'} = (-1)^{\langle aa', bb'\rangle}$$

Using $H^{\otimes n}$ to put n qubits superposed

Computing $H^{\otimes n}$

In general, the value of $H^{\otimes n}$ at coordinates $\text{ß}i, \text{ß}j$ (row and column numbers as binary strings) is given by

$$H^{\otimes n}_{\text{ß}i,\text{ß}j} \;=\; \frac{1}{\sqrt{2^n}}(-1)^{\langle \text{ß}i,\text{ß}j\rangle}$$

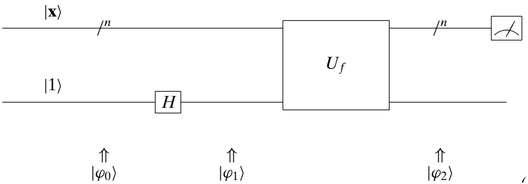
Applying $H^{\otimes n}$ to an arbitrary basic state $|\text{ß}i\rangle$ (which is a column vector with 1 in line $\text{ß}i$ and 0 everywhere else), extracts the $\text{ß}i$-column of $H^{\otimes n}$:

$$H^{\otimes n}|\text{ß}i\rangle \;=\; \frac{1}{\sqrt{2^n}} \sum_{\text{ß}x\in\{0,1\}^n} (-1)^{\langle \text{ß}x,\text{ß}i\rangle}|\text{ß}x\rangle$$

e.g.

$$H^{\otimes 2}|\text{ß}0\rangle \;=\; \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \;=\; \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \;=\; \frac{1}{2}\sum_{\text{ß}x\in\{0,1\}^n} |\text{ß}x\rangle$$

First move: $U_f(I \otimes H)|\text{ß}x, 1\rangle$

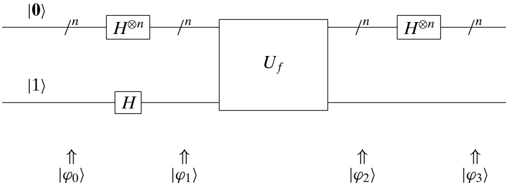


$$|\varphi_1\rangle = |\text{ß}x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|\text{ß}x, 0\rangle - |\text{ß}x1\rangle}{\sqrt{2}}$$

$$|\varphi_2\rangle = |\text{ß}x\rangle \frac{|f(\text{ß}x) \oplus 0\rangle - |f(\text{ß}x) \oplus 1\rangle}{\sqrt{2}} = (-1)^{f(\text{ß}x)}|\text{ß}x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Second move: $(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes H)|\text{ß}0, 1\rangle$

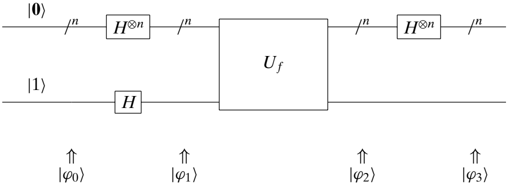
Put input $|\text{ß}x\rangle$ into a superposition in which all 2^n possible strings have equal probability: $H^{\otimes n}|\text{ß}0\rangle$.



$$|\varphi_1\rangle = \frac{\sum_{\text{ß}x\in\{0,1\}^n} |\text{ß}x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|\varphi_2\rangle = \frac{\sum_{\text{ß}x\in\{0,1\}^n} (-1)^{f(\text{ß}x)}|\text{ß}x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Second move: $(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes H)|\text{ß}0, 1\rangle$



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

Finally: observe!

When do the top qubits of $|\varphi_3\rangle$ collapse to $|\text{ß}0\rangle$?

Making $|\text{ß}z\rangle = |\text{ß}0\rangle$ (and thus $\langle \text{ß}z, \text{ß}x\rangle = 0$ for all $\text{ß}x$) leads to

$$|\varphi_3\rangle \;=\; \frac{\sum_{\text{ß}x\in\{0,1\}^n} (-1)^{f(\text{ß}x)}|\text{ß}0\rangle}{\sqrt{2^n}}\;\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

i.e.

$\boxed{\text{the probability of collapsing to } |\text{ß}0\rangle \text{ depends only on } f(\text{ß}x)}$

Finally: observe!

Analyse the top qubits

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

$\boxed{f \text{ is constant at } 0} \quad \rightsquigarrow \quad \frac{\sum_{\text{ß}x\in\{0,1\}^n} 1|\text{ß}0\rangle}{\sqrt{2^n}} = \frac{(2^n)|\text{ß}0\rangle}{2^n} = |\text{ß}0\rangle$

$\boxed{f \text{ is balanced}} \quad \rightsquigarrow \quad \frac{\sum_{\text{ß}x\in\{0,1\}^n} (-1)^{f(\text{ß}x)}|\text{ß}0\rangle}{\sqrt{2^n}} = \frac{0|\text{ß}0\rangle}{2^n} = 0|\text{ß}0\rangle$

because half of the ßx will cancel the other half

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

Exponential speed up: f was evaluated once rather than $2^n - 1$ times