QUANTUM COMPUTING

A **qubit** is the quantum state of a two-level system, e.g. a spin-$\frac{1}{2}$ particle. If we choose an orthonormal basis $|0\rangle$, $|1\rangle$ in the (2-dim.) state space, we can write a general qubit as

$$\phi = a_0|0\rangle + a_1|1\rangle,$$

where we can normalise ϕ so that $|a_0|^2 + |a_1|^2 = 1$. More generally, an n-qubit state is the state of an ensemble of n two-level systems, i.e. a vector in a given 2^n-dimensional Hilbert space. It can be written analogously in the form

$$\phi = \sum_{i_1,\ldots,i_n=0,1} a_{i_1,\ldots,i_n}|i_1,\ldots,i_n\rangle = \sum_{x\in\{0,1\}^n} a_x\,|x\rangle.$$

Basic Postulate: *A* **quantum computation** *is the controlled (unitary) evolution of an originally prepared n-qubit state and its subsequent measurement.*

ENTANGLEMENT

An n-qubit state with $n > 1$ is said to be **entangled** if it is *not* a tensor product of single qubits, i.e. it cannot be written in the form $\phi = \phi_1 \otimes \ldots \otimes \phi_n$, where each ϕ_i is a qubit.

Exercise 1. Prove that the 2-qubit $\phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled.

A measurement of the z-component of the spin of the first qubit in this state corresponds to the operator $S^z \otimes \mathbf{1}$. The two eigenvalues $\pm\frac{1}{2}\hbar$ are degenerate and the corresponding eigenprojections are

$$P_+ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbf{1} \text{ and } P_- = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \mathbf{1}.$$

Now, $P_+\phi = \frac{1}{\sqrt{2}}|00\rangle$ and $P_-\phi = \frac{1}{\sqrt{2}}|11\rangle$, if we identify $|0\rangle$ with the eigenstate with eigenvalue $+\frac{1}{2}\hbar$ and $|1\rangle$ with that with eigenvalue $-\frac{1}{2}\hbar$. It follows that if we next measure the z-component of the spin of the second qubit the result is the same as that for the first qubit with probability 1! This is called the Einstein-Podolski-Rosen experiment. Notice that the two spins can be arbitrarily far removed from one another.

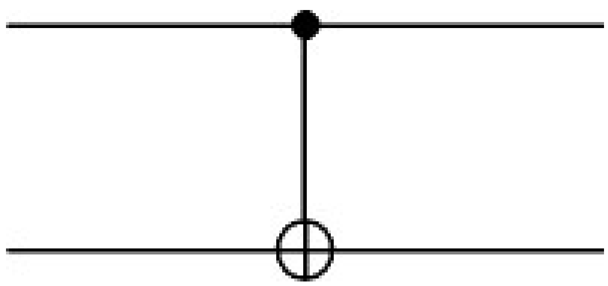
QUANTUM GATES

Definition. *A* **quantum gate** *with n inputs and outputs is specified by a unitary operator on an 2^n-dimensional Hilbert space.*

There is no quantum analogue of the classical AND gate, i.e. there is no unitary 4×4-matrix U such that $U|00\rangle = |00\rangle$, $U|01\rangle = |00\rangle$, $U|10\rangle = |10\rangle$ and $U|11\rangle = |11\rangle$. However, the XOR gate does generalise. It is usually called the **controlled-NOT** gate, and is defined by

$$
\begin{aligned}
U_{\mathrm{CN}}|00\rangle &= |00\rangle, \quad & U_{\mathrm{CN}}|01\rangle &= |01\rangle, \\
U_{\mathrm{CN}}|10\rangle &= |11\rangle, \quad & U_{\mathrm{CN}}|11\rangle &= |10\rangle.
\end{aligned}
$$

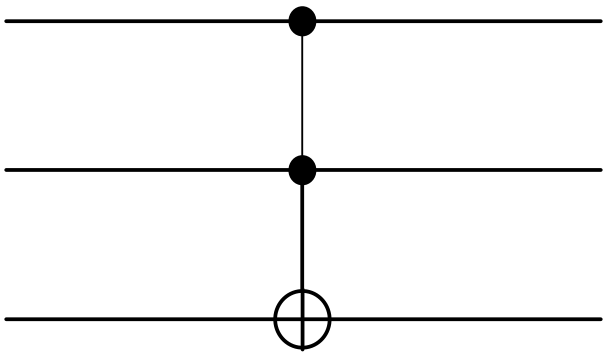
Instead of the electronic component symbol we use the simpler



The NOT gate has an obvious quantum analogue, which is a 1-qubit gate. To complete the Boolean algebra, we complement this with the so-called **Toffoli gate** on 3 qubits:

$$
\begin{aligned}
U_{\mathrm{Tof}}|000\rangle &= |000\rangle, \quad & U_{\mathrm{Tof}}|001\rangle &= |001\rangle, \\
U_{\mathrm{Tof}}|010\rangle &= |010\rangle, \quad & U_{\mathrm{Tof}}|011\rangle &= |011\rangle, \\
U_{\mathrm{Tof}}|100\rangle &= |100\rangle, \quad & U_{\mathrm{Tof}}|101\rangle &= |101\rangle, \\
U_{\mathrm{Tof}}|110\rangle &= |111\rangle, \quad & U_{\mathrm{Tof}}|111\rangle &= |110\rangle.
\end{aligned}
$$

The symbol for a Toffoli gate is as follows:



These gates suffice for generating all Boolean gates, i.e. permutations of basis elements. However, we would like to decompose every quantum gate into elementary gates.

Definition. *A* **quantum circuit** *on n qubits is a collection of quantum gates acting sequentially, each on a subset of the qubits.*

For example, a quantum circuit on 4 qubits is $(\mathbf{1}_2 \otimes U_{\mathrm{Tof}})(U_{\mathrm{CN}} \otimes U_{\mathrm{CN}})(\mathbf{1}_2 \otimes U_{\mathrm{CN}} \otimes \mathbf{1}_2)$. ($\mathbf{1}_2$ is the 2×2 identity matrix.)

Exercise 2. Argue that the **Hadamard gate** defined by the matrix

$$U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

is unitary, but cannot be represented as a quantum circuit of NOT gates, CNOT gates, and Toffoli gates. We define $U_H^{(n)} = U_H \otimes \ldots \otimes U_H$ (n factors). Show that for the basis states $|x\rangle$ with $x \in \{0,1\}^n$,

$$U_H^{(n)}|x\rangle = 2^{-n/2} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle,$$

where $x \cdot y$ is the scalar product modulo 2.

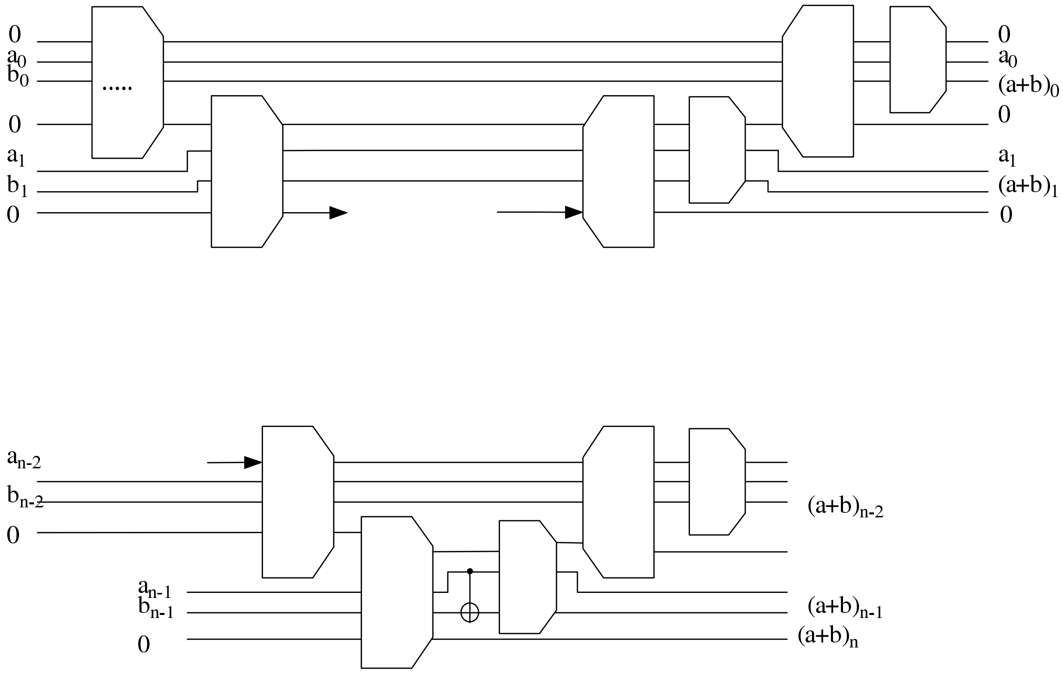
Exercise 3. Write an 8×8 matrix representation of the CNOT gate operating on the first and third qubits of a 3-qubit state.

Exercise 4. Design quantum circuits consisting of Hadamard and CNOT gates to generate the *cat states* $\frac{1}{\sqrt{2}}(|0^{(l)}\rangle + |1^{(l)}\rangle)$ with input state given by $|0^{(l)}\rangle$ for arbitrary l.

As in the classical case, one can build circuits to do logical operations. For example, one can construct an ADDER from an elementary CARRY gate and a SUM gate. The CARRY gate has operates on 4 qubits c (the previous carry), a, b (the actual qubits), and and auxiliary qubit d. The first two qubits are unchanged: $c' = c$ and $a' = a$, whereas $b' = a \oplus b$ and $d' = |0\rangle$ if $a = b = d$ or $a \neq b$ and $c = d$; $d' = |1\rangle$ otherwise. The SUM gate operates on three qubits c, a and b with $c' = c$, $a' = a$ and $b' = a \otimes b \otimes c$.

Exercise 5. Construct these gates as circuits of CNOT and Toffoli gates.

A full adder can now be constructed as follows:



Quantum Adder

MEASUREMENT

A measurement in quantum mechanics is commonly associated with a set of projection operators corresponding to the eigenvalues of a hermitian operator. This is called a *projective measurement.* In fact, in many practical situations, this is not general enough. A more general type of **measurement** is given by a collection $\{M_m\}$ of *measurement operators.* The index m refers to the possible outcomes of the measurement, and if the state of the system before the measurement is ψ, then the probability that the measurement results in the value m is given by

$$\mathbb{P}(m) = \langle \psi \,|\, M_m^* \, M_m \, \psi \rangle.$$

The normalised state of the system after the measurement is

$$\mathbb{P}(m)^{-1/2} M_m \psi.$$

For consistency, the operators M_m must satisfy the completeness relation

$$\sum_m M_m^* M_m = \mathbf{1}.$$

Clearly, projective measurements are special cases in which the operators M_m are orthogonal projections P_m.

Exercise 6. Consider again the imperfect measurement of which hole the particle passed through in the two-slit experiment discussed in the section on Quantum Mechanics, and show that it is a measurement of the above kind described by measurement operators M_1 and M_2 given by $M_1 = aP_1 + bP_2$ and $M_2 = bP_1 + aP_2$.

In fact, a general measurement can always be implemented by a projective measurement on an enlarged system consisting of the original system $\mathcal{S}$ together with an auxiliary system $\mathcal{A}$ with an orthogonal basis labelled by the possible measurement outcomes m. To prove this, define an operator on $\mathcal{H}_{\mathcal{S}} \otimes \mathcal{H}_{\mathcal{A}}$ as follows. Choose an arbitrary fixed state $\phi_0 \in \mathcal{H}_{\mathcal{A}}$ as initial state of the auxiliary system and put

$$U(\psi \otimes \phi_0) = \sum_m M_m \psi \otimes |m\rangle.$$

It is easily seen that

$$\langle \psi_1 \otimes \phi_0 \,|\, U^* U \,|\psi_2 \otimes \phi_0\rangle = \langle \psi_1 \,|\, \psi_2 \rangle.$$

Exercise 7. Show that U can be extended to a unitary operator on $\mathcal{H}_{\mathcal{S}} \otimes \mathcal{H}_{\mathcal{A}}$.

Now define the projection operators $P_m = \mathbf{1}_{\mathcal{S}} \otimes |m\rangle\langle m|$. Then a projective measurement on the combined system with these projection operators results in the outcome m with probability

$$\mathbb{P}(m) = \langle \psi \otimes \phi_0 | \, U^* P_m U \, | \psi \otimes \phi_0 \rangle = \langle \psi | \, M_m^* M_m \, \psi \rangle.$$

Moreover, the resulting state of the combined system is

$$\mathbb{P}(m)^{-1/2} M_m \psi \otimes |m\rangle.$$

Note that in a quantum computation we are usually only interested in the outcome of the measurement, and have no further use for the resulting state. In such situations, one only needs the operators $E_m = M_m^* M_m$. A system of positive definite operators E_m such that $\sum_m E_m = \mathbf{1}$ is called a *positive operator-valued measure*, or POVM.

UNIVERSALITY

We would like to prove a quantum analogue of the classical theorem that every binary function can be constructed from a limited number of elementary gates (AND, OR and NOT). However, there is a continuously infinite number of unitary matrices, so we can only hope to *approximate* these by circuits consisting of elementary gates.

Definition. A matrix M is called an **ϵ-approximation** to a unitary matrix U for a given $\epsilon > 0$, if $||M - U|| \leq \epsilon$, where the **norm** of a matrix is defined by $||M|| = \sup_{\phi:\,||\phi||\leq 1} ||M\phi||$.

Exercise 8. Show that, if a matrix M is ϵ-approximation of a unitary matrix U, then the rows M_i of M satisfy:
(a) $1 - \epsilon \leq ||M_i|| \leq 1 + \epsilon$; and
(b) $|\langle M_i \mid M_j \rangle| \leq 2\epsilon + \epsilon^2$ if $i \neq j$.

Definition. A set $\{U_1, \ldots, U_n\}$ of quantum gates is called **universal** if any unitary gate U operating on an n-qubit register with arbitrarily large n can be approximated with arbitrary precision $\epsilon > 0$ by a circuit $C_{U,\epsilon}$ consisting of gates from that set.

Exercise 9. Show that any single-qubit gate U can be written in the form

$$U = \Phi(\delta) PS(\alpha) R(\theta) PS(\beta)$$

for real numbers α, β, θ and δ, where $\Phi(\delta) = e^{i\delta}\mathbf{1}$, and

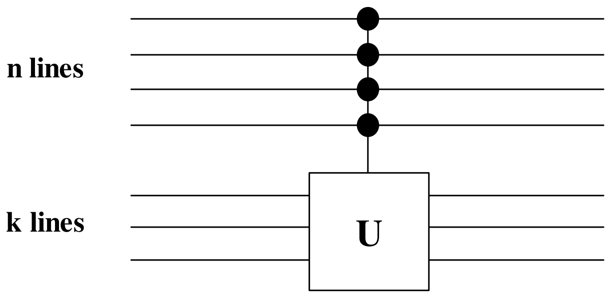
$$PS(\alpha) = \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix},$$

and

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Exercise 10. Show that $R(\theta)$ and $PS(\alpha)$ can be implemented to arbitrary precision by a single $R(\theta_0)$ and $PS(\alpha_0)$ where θ_0 and α_0 are irrational multiples of π.

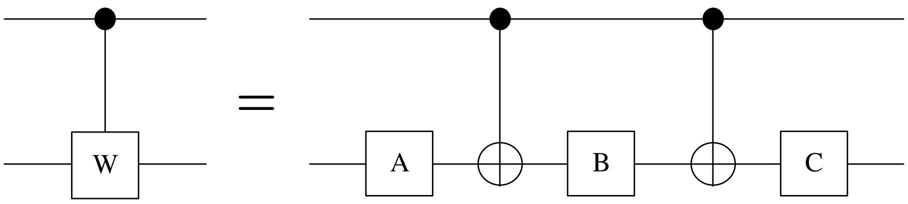
In the following we use the notation $\Lambda_n(U)$ for the gate defined as follows. Let U be an arbitrary k-qubit gate. Then $\Lambda_n(U)$ is a $2^{n+k} \times 2^{n+k}$ block-diagonal matrix with the first block being a $(2^n-1)2^k$-dimensional identity matrix and the second block the matrix U. This means that the gate operates on the last k qubits if the first n qubits are 1, and otherwise it is the identity. The symbol for this gate is as follows:



Theorem. *If* δ_0, α_0 *and* θ_0 *are irrational multiples of* π, *then* $\Phi(\delta_0)$, $PS(\alpha_0)$ *and* $R(\theta_0)$ *together with the CNOT gate are universal.*

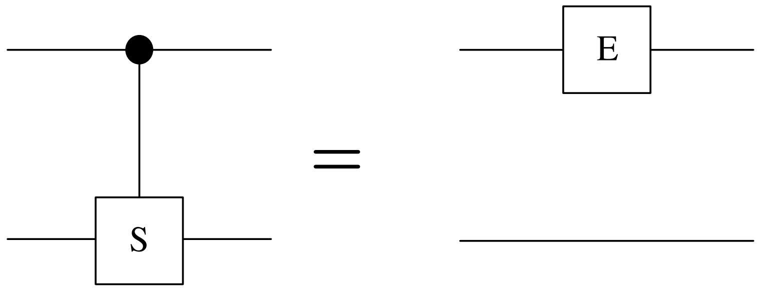
We shall prove this theorem by means of a sequence of lemmas. First we remark that any single qubit gate can be obtained through Exercises 8 and 9. Next consider a $\Lambda_1(U)$ gate:

Lemma 1. Given a unitary 2×2-matrix W, the $\Lambda_1(W)$ gate can be implemented as follows:



provided W has determinant 1.

Lemma 2. For any δ, and $S = \Phi(\delta)$, the matrix $\Lambda_1(S)$ can be realised as follows

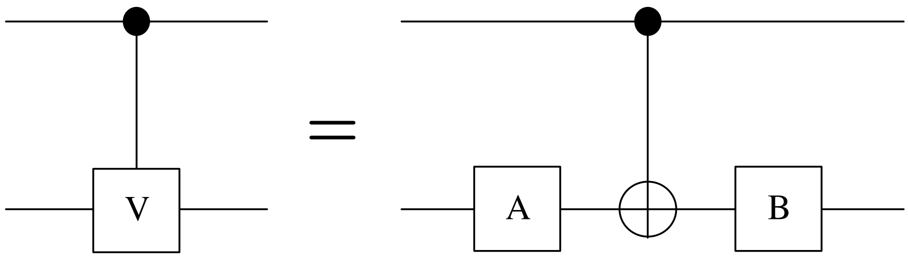


where E is a unitary 2×2-matrix.

Exercise 11. Show that for matrices V of the form

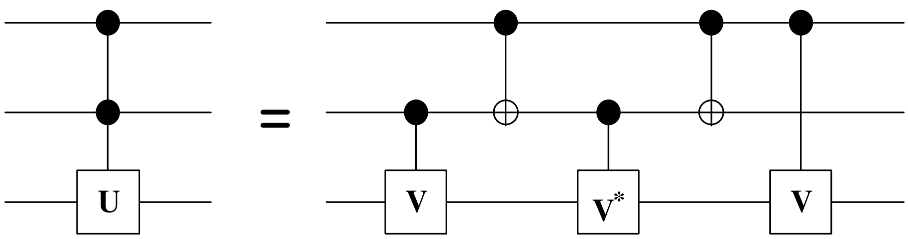
$$V = \begin{pmatrix} \sin\theta & e^{i\alpha}\cos\theta \\ e^{-i\alpha}\cos\theta & -\sin\theta \end{pmatrix}$$

the $\Lambda_1(V)$ gate can be simulated more efficiently as follows:



where A and B are unitary matrices.

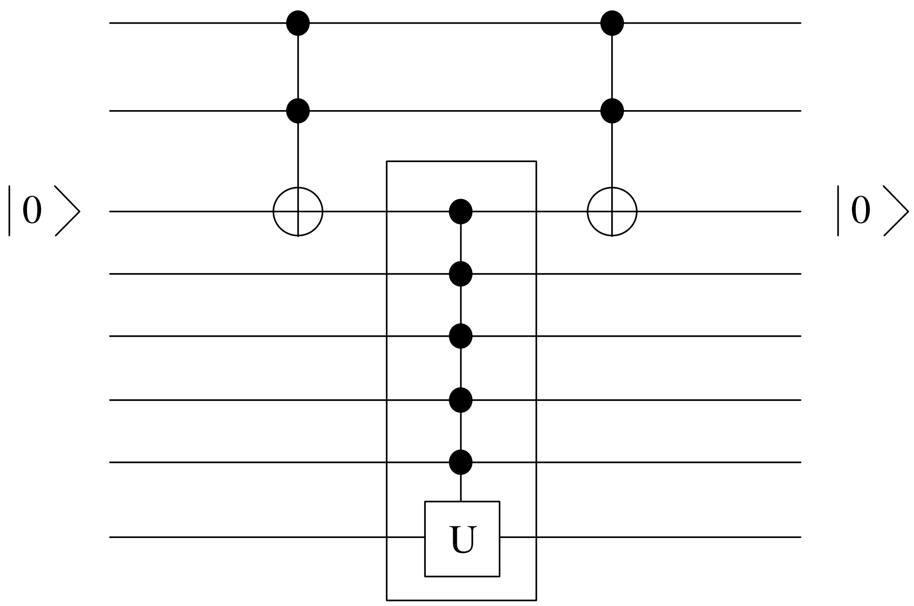
Lemma 3. For any 2×2-matrix U, the $\Lambda_2(U)$ gate can be implemented by the circuit



where V is a unitary matrix such that $V^2 = U$.

Exercise 12. Give an explicit implementation of the Toffoli gate using the CNOT gate and single-qubit gates.

We now show by induction that any gate of the form $\Lambda_n(U)$ where U is a single-qubit gate can be implemented. This has already been proved for $n = 1, 2$ above. Now suppose it is true for $n - 1$. Then we can implement $\Lambda_n(U)$ as follows:



To construct a general $n \times n$ unitary gate U, we diagonalise it in the form

$$U = \sum_{x \in \{0,1\}^n} e^{i\sigma(x)} P_{\psi_x},$$

where $e^{i\sigma(x)}$ are the eigenvalues of U, and P_{ψ_x} are one-dimensional projections onto an orthonormal system of eigenvectors ψ_x. Given any normalised vector ψ, let S_{ψ_x} be a unitary matrix such that $S_{\psi_x}\psi_x = |11\ldots1\rangle$. Then we can write U as follows:

$$U = \prod_{x \in \{0,1\}} S_{\psi_x}^{-1} X_{\sigma(x)} S_{\psi_x},$$

where $X_{\sigma(x)} = \Lambda_{n-1}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\sigma(x)} \end{pmatrix}$.

It remains to construct S_ψ for any ψ. By induction, it suffices to show that we can construct for every n a unitary S_n mapping a vector $\psi^{(n)} \in \mathcal{H}^{\otimes n}$ to $\psi^{(n-1)} \otimes |1\rangle$ with $\psi^{(n-1)} \in \mathcal{H}^{\otimes(n-1)}$. This follows again by induction on n.

For $n = 1$ it is clear. For $n > 1$ we write

$$\psi = \sum_{x \in \{0,1\}^{n-1}} |x\rangle \otimes \psi_x$$

with $\psi_x \in \mathcal{H}$, and apply successively the operators

$$(NOT_A)\Lambda_{n-1}(S_{\psi_{0_A,1_{A^c}}})(NOT_A)$$

for all subsets $A \subset \{1, \dots, n-1\}$.

Exercise 13. Show that $U = \frac{1}{\sqrt{2}}(\sigma_x \otimes \sigma_x + \sigma_z \otimes \mathbf{1})$ is a unitary matrix. Compute the eigenvalues and corresponding eigenvectors. Construct a circuit consisting of single-qubit gates and CNOT gates to implement S_ψ for one of these eigenvectors.

ALGORITHMS

Given a binary function $f : \{0,1\}^m \to \{0,1\}^n$ we define the f-controlled NOT by

$$U_f \, |x, b\rangle = |x, b \oplus f(x)\rangle.$$

If $n = 1$ we also define V_f on $\mathcal{H}^{\otimes n}$ by

$$V_f \, |x\rangle = (-1)^{f(x)} |x\rangle.$$

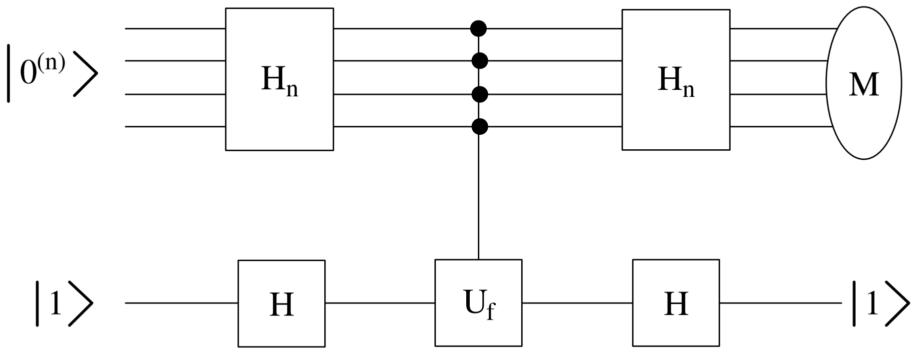
The Deutsch-Jozsa promise problem

Let it be given that the function $f : \{0,1\}^m \to \{0,1\}$ is either constant or *balanced*, i.e.

$$\#\{x : \, f(x) = 0\} = \#\{x : \, f(x) = 1\}.$$

Decide which of these cases applies.

Solution:



Exercise 14. Show that the Deutsch-Jozsa problem can be solved in polynomial time with a classical algorithm with arbitrarily small error probability.

Simon's XOR Problem

Suppose it is given that the function $f : \{0,1\}^n \to \{0,1\}^n$ is *either* one-to-one *or* there exists $s \in \{0,1\}^n$, $s \neq 0$ such that $f(x') = f(x) \iff x' = x$ or $x' = x \oplus s$. Determine which is the case, and in the second case, what is s.

Solution:
Use two n-qubit registers, both initialised to $|0^{(n)}\rangle$ and apply the following algorithm:

1. Apply H_n to the first register;
2. Apply U_f;
3. Apply H_n to the first register again;
4. Observe the resulting state in the standard basis.

If f is one-to-one, the amplitude of all possible states $|y, z\rangle$ is the same (up to a sign), so $n-1$ repetitions of the algorithm produces $n-1$ pairs (y, z) with uniform distribution. On the other hand, if the second case applies, then $n-1$ applications of the algorithm yield vectors $y_1, \ldots, y_{n-1}$ with $y_i \cdot s = 0$. If these are independent, this determines s uniquely. To check that this s satisfies the condition, we simply compute $f(0)$ and $f(s)$.

Lemma. If $u \in \{0, 1\}^n$ is a non-zero binary vector then $n-1$ randomly chosen $y \in \{0, 1\}^n$ such that $y \cdot u = 0$ are linearly independent with probability at least $\frac{1}{4}$.

Grover's Search Algorithm

Given a binary function $f : \{0,1\}^n \to \{0,1\}$ such that there is a unique $x_0 \in \{0,1\}^n$ for which $f(x_0) = 1$, determine x_0.

Grover's quantum algorithm for this problem is as follows:
1. Apply H_n to $|0^{(n)}\rangle$ to get $2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle$.
2. Apply V_f.
3. Apply the *inversion about the average* operator defined by

$$D_n \left(\sum_{x \in \{0,1\}^n} a_x |x\rangle \right) = \sum_{x \in \{0,1\}^n} (2M - a_x)|x\rangle,$$

where $M = 2^{-n} \sum_{x \in \{0,1\}^n} a_x$.
4. Repeat steps 2 and 3 $\lfloor \pi 2^{n/2-2} \rfloor$ times.
5. Measure x. If $f(x) \neq 1$, goto step 1, else $x_0 = x$.

Exercise 15. Show that D_n is unitary.

Basic idea of the algorithm: V_f changes the sign of the amplitude of $|x_0\rangle$, and D_n reflects all amplitudes about the average. As long as $|a_{x_0}|$ remains of the same order as the other amplitudes, then the average is close to the other the other amplitudes, and a_{x_0} is almost doubled. If a_k is the amplitude of $|x_0\rangle$, and b_k that of the states $|x\rangle$ with $x \neq x_0$ after k iterations of steps 2. and 3., then $a_0 = b_0 = \frac{1}{\sqrt{2^n}}$ and

$$\begin{pmatrix} a_k \\ b_k \end{pmatrix} = \begin{pmatrix} 1 - 2^{-n+1} & 2 - 2^{-n+1} \\ -2^{-n+1} & 1 - 2^{-n+1} \end{pmatrix} \begin{pmatrix} a_{k-1} \\ b_{k-1} \end{pmatrix}.$$

Eigenvalues:

$$\lambda_\pm = 1 - 2^{-n+1} \pm i\delta,$$

writing

$$\delta = 2^{-\frac{n}{2}+1}\sqrt{1 - 2^{-n}}$$

. Notice that $|\lambda_\pm| = 1$.

We can write $\begin{pmatrix} a_k \\ b_k \end{pmatrix}$ in terms of eigenvectors:

$$\begin{pmatrix} a_k \\ b_k \end{pmatrix} = \frac{1}{2} z_k \begin{pmatrix} 1 \\ \frac{i\delta}{2(1-2^{-n})} \end{pmatrix} + \frac{1}{2} \bar{z}_k \begin{pmatrix} 1 \\ -\frac{i\delta}{2(1-2^{-n})} \end{pmatrix}.$$

In particular,

$$z_0 = 2^{-\frac{n}{2}+1} \left(\frac{1}{2} - (1-2^{-n})\delta^{-1} i \right)$$

and $|z_0| = 1$. For large n, $z_0 \approx -i$. But $z_k = \lambda_+^k z_0$ and λ_+ rotates z over an angle θ given by

$$\tan\theta = \frac{\delta}{1-2^{-n+1}} \approx 2^{-\frac{n}{2}+1}.$$

To make $a_k \approx 1$ we therefore need to rotate $\lfloor \frac{\pi}{2} 2^{n/2-1} \rfloor$ times.

Shor's Algorithm.

Lemma 1. If there is a polynomial-time algorithm to find a n on-trivial solution of $x^2 \equiv 1 \pmod{n}$ then there is also a polynomial-time algorithm to factorise integers.

Define $f_{n,x}(k) = x^k \operatorname{mod} n$. The period of $f_{n,x}$ is called the **order** of x, i.e. the smallest r such that $x^r \equiv 1 \pmod{n}$.

Algorithm.

1. Choose $x \in \{2, \ldots, n-1\}$ randomly.
2. Check that $\gcd(x, n) = 1$. If not, then we have a factor of n.
3. Find the period r of $x^k \bmod n$.
4. If r is odd, or $x^{r/2} \equiv \pm 1 \pmod{n}$ then goto 1., otherwise STOP.

If this algorithm stops then $x^{r/2}$ is a nontrivial solution of $x^2 \equiv 1 \pmod{n}$.

Lemma 2. If $x \in \{2, \ldots, n-1\}$ is selected randomly such that $\gcd(x, n) = 1$, and n is odd and not a prime, then

$$\text{Prob}\left\{r = \text{ord}(x) \text{ is even, and } x^{r/2} \not\equiv \pm 1\right\} \geq \frac{1}{4}.$$

Corollary. If there is a polynomial-time (random) algorithm to compute the period of the function $f_{n,x}$ then there is a polynomial-time (random) algorithm to find non-trivial solutions of $x^2 \equiv 1 \pmod{n}$.

To compute the period of $f_{n,x}(k)$, Shor proposed to use the **quantum Fourier transform** defined by

$$QFT_q : |a\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a c/q} |c\rangle.$$

His algorithm has three stages:

(I) Create a state with the period we need to determine.

(II) Apply the QFT.

(III) Extract the period by measurement and a classical computation.

To explain how this algorithm works, we consider the simple example $n = 35$ and $x = 11$. The steps are as follows:

(I) Start with two registers, each of length $l = \lceil \log n \rceil = 6$, initialised to 0, and apply a Hadamard transform to the first. This yields with $q = 2^l = 64$,

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle.$$

Then applying $U_{f_{n,x}}$ we obtain the state

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a, x^a\ (\mathrm{mod}\, n)\rangle$$

$$= \frac{1}{8}\sum_{j=0}^{20}(|3j+1, 11\rangle + |3j+2, 16\rangle)$$

$$+ \frac{1}{8}\sum_{j=0}^{21}|3j, 1\rangle.$$

(II) Applying the QFT we get

$$\frac{1}{64}\sum_{c=0}^{63}\left[\sum_{j=0}^{20} e^{3\pi icj/32}[e^{\pi ic/32}|c, 11\rangle + e^{\pi ic/16}|c, 16\rangle]\right.$$

$$\left. + \sum_{j=0}^{21} e^{3\pi icj/32}|c, 1\rangle\right].$$

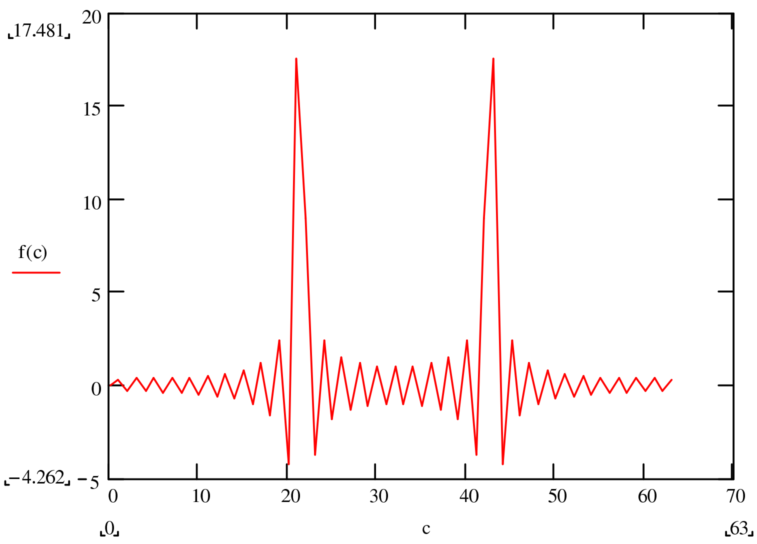
(III) Summing over j we get the functions

$$f(c)=\sum_{j=0}^{20} e^{3\pi icj/32}=\frac{\sin\left(\frac{63}{64}\pi c\right)}{\sin\left(\frac{3/}{64}\pi c\right)}$$

and

$$g(c)=\sum_{j=0}^{21} e^{3\pi icj/32}=\frac{\sin\left(\frac{33}{32}\pi c\right)}{\sin\left(\frac{3/}{64}\pi c\right)}.$$

These attain maxima at $c=32\pm 11$:



A measurement there of c therefore leads with high probability to $c = 21$ or $c = 43$, irrespective of what value the second register has. One now determines the period by expanding c/q as a partial fraction:

$$\frac{21}{64} = \frac{1}{3 + \frac{1}{21}}$$

and

$$\frac{43}{64} = \frac{1}{1 + \frac{1}{2 + \frac{1}{21}}}.$$

Now ignore the large denominator 21 in these expressions, to get $\frac{1}{3}$ and $\frac{2}{3}$. The denominator 3 is the period r. One can prove that in general for large n the probability is strongly concentrated near values of c which are very close to multiples of $1/r$.