QUANTUM COMPUTING 5, 2009

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

November 5, 2013

5. SIMPLE QUANTUM ALGORITHMS

This chapter presents very basic techniques of designing quantum algorithms that are more efficient than their classical counterparts.

Quantum algorithms for the Deutsch, Deutsch-Jozsa and Simon problems are presented and analyzed.

Power of quantum parallelism, constructive and destructive interference and entanglement are illustrated.

QUANTUM PARALLELISM

If

$$f : \{0, 1, \ldots, 2^n - 1\} \Longrightarrow \{0, 1, \ldots, 2^n - 1\}$$

then the mapping

$$f' : (x, b) \Longrightarrow (x, b \oplus f(x)),$$

where $x, b \in \{0, 1, \ldots, 2^n - 1\}$ is one-to-one and therefore there is a unitary transformation U_f such that.

$$U_f(|x\rangle|0\rangle) \Longrightarrow |x\rangle|f(x)\rangle$$

Let

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$$

With a **single application** of the mapping U_f we get

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

IN A SINGLE COMPUTATIONAL STEP 2^n VALUES OF f ARE "COMPUTED"! - in some sense

INTERPRETATION of QUANTUM PARALLELISM

- Last application of the unitary transformation U_f results in a state with 2^n values of function f.
- In case of $n = 100$ that resulting state contains billion billion trillion values of function f.
- Such a massive parallelsm is an important part of the magic quantum computation exhibits.
- However, the major part of such a magic is only apparent.
- Actually one cannot say that the result of such a computation is 2^n evaluations of f.
- All one can say is that such a unitary mapping results in a state that fully specifies all values of the function f.

- There is, however, in general no way to learn from the resulting state all the values of the function f.
- There is, however, often a way to get, using such quantum parallellis, important relations between values of the function f - usually at the price of being no longer able to get values of f.

INTERPRETATION of QUANTUM PARALLELISM I

It is wrong, and deeply misleadingm to say that after an application of the unitary U_f as folllows

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

the quantum computer has evaluated the function $f(x)$ for all $0 \leq x < 2^n$.

Such assertions are based on the mistaken view that each quantum state encodes a propeety inherent in the qubits.

The state encodes only the possibilities available for the extraction of information from those qubits.

In spite of that quantum parallelism nevertheles permits a quantum computer to perform tricks that no classical computer can accomplish.

MEASUREMENT — EXAMPLE

If we "measure" second register of the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

with respect to the standard basis $\{|z\rangle \,|\, z \in \{0,1\}^n\}$, then the state $|\phi\rangle$ collapses into one of the states

$$|\phi_y\rangle = \frac{1}{\sqrt{k}} \sum_{\{x \,|\, f(x)=y\}} |x\rangle|y\rangle,$$

where

- y is in the range of the values of the function f.
- $k = |\{x \,|\, f(x) = y\}|$.

The collapse into the state $|\phi_y\rangle$ happens with the probability

$$\frac{k}{2^n}$$

and into the classical world one gets information which of y in the range of f, in the second register, has been (randomly) chosen.

This fact we usually interpret that y is the (classical) result of the measurement of the second register of the state$|\phi\rangle$, with respect to the standard basis.

REDUCTION of PROJECTIVE MEASUREMENT TO COMPUTATIONAL BASIS MEASUREMENT - I

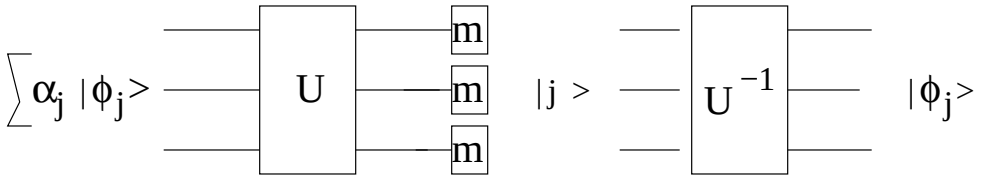


Figure 1: Transformation of any projection measurement to computational basis measurement - 1 version

The above figure shows one way how to reduce measurement with respect to any orthogonal basis $\{|\phi_j\rangle\}_j^{2^n}$ to a measurement with respect to the computational basis $\{|j\rangle_{j=1}^{2^n}\}$. After measurement the state $|j\rangle$ is obtained with probability $|\alpha_j|^2$. The state of the system after this measurement if $|j\rangle$. After inverse unitary U^{-1} is applied the resulting state will be $|\phi_j\rangle$.

At first a unitary transformation U is applied that transforms the basis $\{|\phi_j\rangle\}_j$ to the computational basis

REDUCTION of PROJECTIVE MEASUREMENT TO COMPUTATIONAL BASIS MEASUREMENT - II

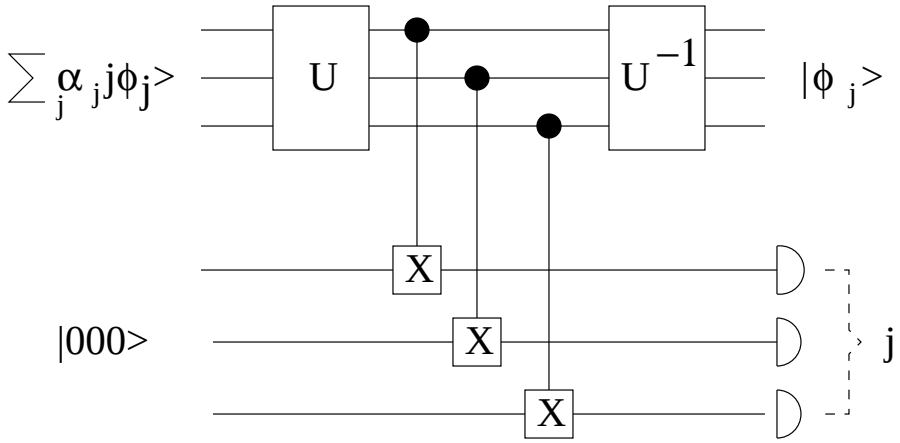


Figure 2: Transformation of any projection measurement to computational basis measurement - 2 version

Another way to implement the von Neumann measurements. At first the outcome of the transformation U is mapped into ancillary registers to create the state $\Sigma_j \alpha_j |j\rangle|j\rangle$. The inverse basis change unitary U^{-1} leaves as the outcome the state $\Sigma_j |\phi_j\rangle|j\rangle$. The following measurement of the ancillary register in the computational basis gives the outcome "j" with probability $|\alpha_j|^2$ and leaves the main register in the state $|\phi_j\rangle$.

U_f OPERATOR versus V_f OPERATOR

Another useful operator related to functions

$$f : \{0, 1, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$$

is the operator

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

where $x \in \{0, 1, 2, \ldots, 2^n - 1\}$, which can be expressed using the operator

$$U_f : |x, b\rangle \rightarrow |x, b \oplus f(x)\rangle$$

and one additional qubit, called again **ancilla**, in the state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as follows

$$\begin{aligned} U_f|x, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle &= \frac{1}{\sqrt{2}}(x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle \\ &= (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Warm-up: Show how the operator V_f can be used to implement U_f.

EXAMPLE

Mapping $V_f : \{0,1\}^2 \leftrightarrow \{0,1\}$ is realized by the unitary matrix

$$V_f = \begin{pmatrix} (-1)^{f(00)} & 0 & 0 & 0 \\ 0 & (-1)^{f(01)} & 0 & 0 \\ 0 & 0 & (-1)^{f(10)} & 0 \\ 0 & 0 & 0 & (-1)^{f(11)} \end{pmatrix}.$$

DEUTSCH PROBLEM – RANDOMIZED SOLUTION

Given a function $f : \{0,1\} \rightarrow \{0,1\}$, as a black box, the task is to determine whether f is constant or balanced.

In classical computing 2 calls of f are needed.

In quantum computing 1 call of f is sufficient.

Quantum algorithm presented below solves the problem with probability $\frac{1}{2}$ in such a way that we know whether the answer is correct. Since

$$U_f : (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle),$$

the result can be written, in the standard and dual basis, as follows:

if f is constant:

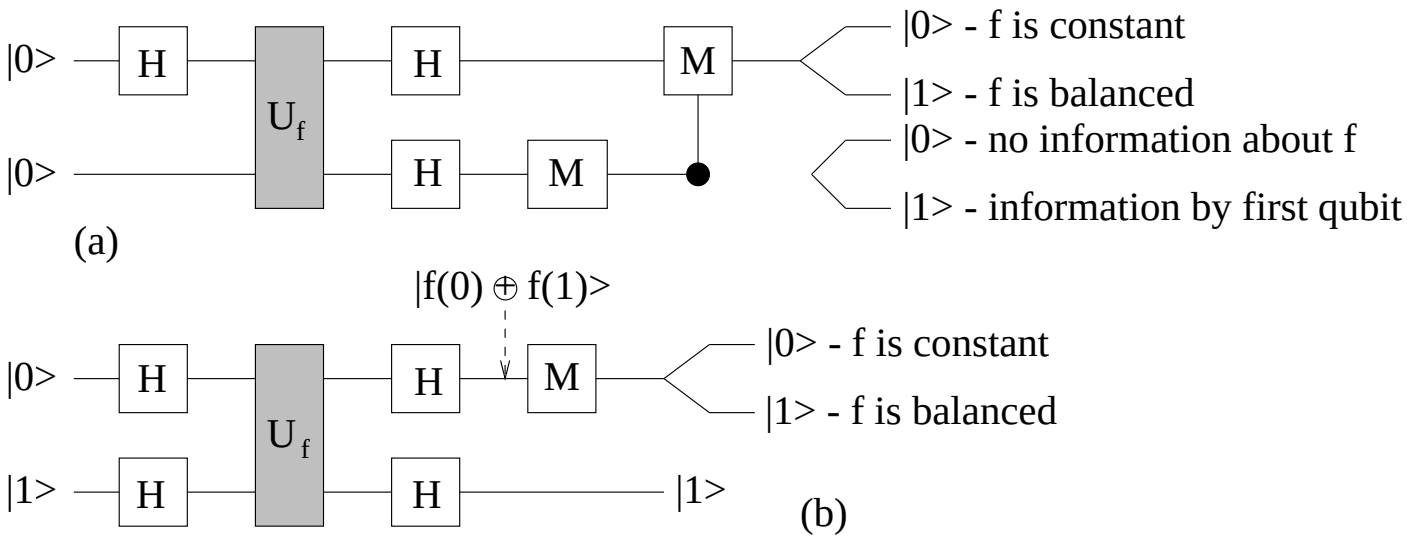
$$\frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle) = \frac{1}{\sqrt{2}}(|0', 0'\rangle + (-1)^{f(0)}|0', 1'\rangle)$$

and if f is balanced:

$$\frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle) = \frac{1}{\sqrt{2}}(|0', 0'\rangle + (-1)^{f(0)}|1', 1'\rangle).$$

If the measurement of the second qubit in the dual bases provides 0 we have lost all information about f. Otherwise the measurement of the first qubit yields the correct result.

The corresponding circuit is shown in the following Figure.


|0>
H
U_f
H
M
|0> - f is constant
|1> - f is balanced
|0>
H
M
|0> - no information about f
|1> - information by first qubit
(a)
|f(0) ⊕ f(1)>
|0>
H
H
M
|0> - f is constant
|1> - f is balanced
U_f
|1>
H
H
|1>
(b)

DEUTSCH PROBLEM – DETERMINISTIC SOLUTION

Apply first the Hadamard transform on both registers in the initial state $|0,1\rangle$ and then U_f to get

$$\begin{aligned}
|0\rangle|1\rangle &\stackrel{H_2}{\rightarrow} \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) \\
&= \frac{1}{2}(|0\rangle(|0\rangle-|1\rangle)+|1\rangle(|0\rangle-|1\rangle)) \\
&\stackrel{U_f}{\rightarrow} \frac{1}{2}(|0\rangle(|0\oplus f(0)\rangle-|1\oplus f(0)\rangle)+|1\rangle(|0\oplus f(1)\rangle-|1\oplus f(1)\rangle)) \\
&= \frac{1}{2}(\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle)(|0\rangle-|1\rangle) \\
&= \frac{1}{2}(-1)^{f(0)}(|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle-|1\rangle). \qquad (1)
\end{aligned}$$

Hence

$$|0\rangle|1\rangle \stackrel{H_2}{\rightarrow} \frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle - |1\rangle) \quad (2)$$

From the right side in (), the two possibilities for f to be constant lead to the left sides in (3) and (4) and two possibilities for f to be balanced lead to the left sides in (5) and (6):

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |0'\rangle|1'\rangle \text{ if } f(0) = 0; \quad (3)$$

$$\frac{1}{2}(|0\rangle + |1\rangle)(|1\rangle - |0\rangle) = -|0'\rangle|1'\rangle \text{ if } f(0) = 1; \quad (4)$$

$$\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) = |1'\rangle|1'\rangle \text{ if } f(0) = 0; \quad (5)$$

$$\frac{1}{2}(|0\rangle - |1\rangle)(|1\rangle - |0\rangle) = -|1'\rangle|1'\rangle \text{ if } f(0) = 1. \quad (6)$$

By measuring the first bit, with respect to the dual basis, we can immediately see whether f is constant or balanced.

EVEN-ODD PROBLEM

A function $f : \{0,1\}^2 \leftrightarrow \{0,1\}$ is called even (odd) if the range of f has even (odd) number of ones.

Classically, given such a function f as an oracle, one needs 4 calls of f to determine whether f is even or odd.

Quantumly, it holds

$$(H \otimes H)V_f(I \otimes H)V_f(H \otimes H)|00\rangle = \begin{cases} \frac{1}{\sqrt{2}}(\pm|00\rangle + |01\rangle) \text{ if f is even} \\ \frac{1}{\sqrt{2}}(\pm|10\rangle + |01\rangle) \text{ if f is odd} \end{cases}$$

and therefore using only two quantum calls of f (of V_f), the problem is transformed into the problem to distinguish two non-orthogonal quantum states.

Unfortunately, there is no projection measurement that can faithfully distinguish such non-orthogonal states. However, as discussed later, there is so called POVM measurement that either tells us whether a given function f is even or odd or the algorithm tells us "I don't know".

DEUTSCH-JOZSA PROMISE PROBLEM

Given a function $f : \{0,1\}^n \to \{0,1\}$, as a black box, that is (promised to be) balanced or constant. Decide which property f has.

Classical deterministic computers needs, in the worst case, exponential time to solve the problem. Surprisingly, there is a quantum algorithm to solve the problem by applying f only once.

Let us consider one quantum register with n qubits and apply the Hadamard transformation H_n to the first register. This yields

$$|0^{(n)}\rangle \stackrel{H_n}{\to} |\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle.$$

By applying the transformation V_f on the first register we get

$$V_f|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)}|i\rangle = |\phi_1\rangle.$$

What has been achieved by these operations? The values of f were transferred to the amplitudes.

This can be utilized, through the power of quantum superposition and a proper observable, as follows.

Let us consider the observable $\mathcal{D} = \{E_a, E_b\}$, where E_a is the one-dimensional subspace spanned by the vector

$$|\psi_a\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle,$$

and $E_b = (E_a)^{\perp}$. The projection of $|\phi_1\rangle$ into E_a and E_b has the form

$$|\phi_1\rangle = \alpha|\psi_a\rangle + \beta|\psi_b\rangle \quad \textbf{with} \quad |\alpha|^2 + |\beta|^2 = 1,$$

where $|\psi_b\rangle$ is a vector in E_b such that $|\psi_a\rangle \perp |\psi_b\rangle$. A measurement by $\mathcal{D}$ provides "the value a or b" with probability $|\alpha|^2$ or $|\beta|^2$.
It is easy to determine α in

$$|\phi_1\rangle = \alpha|\psi_a\rangle + \beta|\psi_b\rangle \quad \textbf{with} \quad |\alpha|^2 + |\beta|^2 = 1,$$

using the projection of $|\phi_1\rangle$ onto E_a by the computation

$$\alpha = \langle\psi_a|\phi_1\rangle.$$

Indeed

$$\begin{aligned}\alpha &= \langle\psi_a|\phi_1\rangle = \left(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}\langle i|\right)\left(\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}(-1)^{f(j)}|j\rangle\right)\\ &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}(-1)^{f(j)}\langle i|j\rangle = \frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(i)},\end{aligned}$$

because $\langle i|j\rangle = 1$ if and only if $i = j$ and 0 otherwise.

If f is balanced, then the sum for α contains the same number of 1s and -1s and therefore $\alpha = 0$. A measurement of $|\phi_1\rangle$, with respect to $\mathcal{D}$ therefore provides, for sure, the outcome b.

If f is constant, then either $\alpha = 1$ or $\alpha = -1$ and therefore the measurement of $|\phi_1\rangle$ with respect to $\mathcal{D}$ always gives the outcome a.

A single measurement of $|\phi_1\rangle$, with respect to $\mathcal{D}$, therefore provides the solution of the problem with probability 1.

SECOND SOLUTION

If the Hadamard transformation is applied to the state $|\phi_1\rangle$ we get the state

$$|\phi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^{u \cdot i} |u\rangle = \frac{1}{2^n} \sum_{u=0}^{2^n-1} \left(\sum_{i=0}^{2^n-1} (-1)^{u \cdot i} (-1)^{f(i)} \right) |u\rangle.$$

Case 1 f is constant. Then

$$\sum_{i=0}^{2^n-1} (-1)^{u \cdot i} = \begin{cases} 0 & \text{if } u \neq 0 \\ 2^n & \text{if } u = 0 \end{cases}$$

One measurement of the register therefore provides $u = 0$ with probability 1.

Case 2 f is balanced. In such a case

$$\sum_{i=0}^{2^n-1} (-1)^{u \cdot i} (-1)^{f(i)} = 0 \text{ if and only if } u = 0.$$

One measurement therefore shows whether f is balanced or not.

DEUTSCH-JOZSA PROBLEM - RANDOMIZED SOLUTION

It is easy to show that though deterministic algorithms to solve the Deutsch-Jozsa problem for $n = 2^k$ require $2^{k-1} + 1$ queries in the worst case, there are probabilistic algorithms to solve this problem relatively fast, if we are willing to tolerate some error.

Indeed, a randomized algorithm can solve the Deutsch-Jozsa problem with probability of error at most $\frac{1}{3}$ with only two queries.

The probability of error can be reduced to less than $\frac{1}{2^k}$ with only $k + 1$ queries.

Therefore, in spite of the fact that there is an exponential gap between deterministic classical and exact quantum query complexity, the gap between randomized classical complexity and quantum query complexity is in this case constant in the case of constant error.

SIMON's PROBLEM

Simon has discovered a simple problem with expected polynomial time quantum algorithm, but with no polynomial time randomized algorithm.

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function such that either f is one-to-one or f is two-to-one and there exists a single $0 \neq s \in \{0,1\}^n$ such that

$$\forall x \neq x'(f(x) = f(x') \Leftrightarrow x' = x \oplus s).$$

The task is to determine which of the above conditions holds for f and, in the second case, to determine also s.

To solve the problem two registers are used, both with n qubits, and the initial states $|0^{(n)}\rangle$, and (expected) $\mathcal{O}(n)$ repetitions of the following version of the so-called Hadamard-twice scheme:

1. **Apply the Hadamard transformation on the first register, with the initial value $|0^{(n)}\rangle$, to produce the superposition $\frac{1}{\sqrt{2^n}} \Sigma_{x\in\{0,1\}^n} |x, 0^{(n)}\rangle$.**
2. **Apply U_f to compute $|\psi\rangle = \frac{1}{\sqrt{2^n}} \Sigma_{x\in\{0,1\}^n} |x, f(x)\rangle$.**
3. **Apply Hadamard transformation on the first register to get**
$$\frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{x\cdot y} |y, f(x)\rangle.$$
4. **Observe the resulting state to get a pair $(y, f(x))$.**

Case 1: f is one-to-one. After performing the first three steps of the above procedure all possible states $|y, f(x)\rangle$ in the superposition are distinct and the absolute value of their amplitudes is the same, namely 2^{-n}.

$n-1$ independent applications of the scheme *Hadamard-twice* therefore produce $n-1$ pairs $(y_1, f(x_1)), \ldots, (y_{n-1}, f(x_{n-1}))$, distributed uniformly and independently over all pairs $(y, f(x))$.

Case 2: There is some $s \neq 0^{(n)}$ such that

$$\forall x \neq x'((f(x) = f(x') \Leftrightarrow x' = x \oplus s).$$

In such a case for each y and x the states $|y, f(x)\rangle$ and $|y, f(x \oplus s)\rangle$ are identical. Their total amplitude $\alpha(x, y)$ has the value

$$\alpha(x, y) = 2^{-n}((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}).$$

If $y \cdot s \equiv 0 \bmod 2$, then $x \cdot y \equiv (x \oplus s) \cdot y \bmod 2$ and therefore $|\alpha(x, y)| = 2^{-n+1}$; otherwise $\alpha(x, y) = 0$. n independent applications of the scheme *Hadamard-twice* therefore yield $n - 1$ independent pairs

$$(y_1, f(x_1)), \ldots, (y_{n-1}, f(x_{n-1})) \quad \textbf{such that} \quad y_i \cdot s \equiv 0 \pmod 2,$$

for all $1 \leq i \leq n - 1$.

In both cases, after $n - 1$ repetitions of the scheme *Hadamard-twice*, $n - 1$ vectors $y_i, 1 \leq i \leq n - 1$, are obtained.

In both cases, after $n - 1$ repetitions of the scheme *Hadamard-twice*, $n - 1$ vectors $y_i, 1 \leq i \leq n - 1$, are obtained.

If these vectors are linearly independent, then the system of $n-1$ linear equations in $\mathbf{Z}_2$,

$$y_i \cdot s \equiv 0 \pmod{n}$$

can be solved to obtain s.

In Case 2, if f is two-to-one, s obtained in such a way is the one to be found.

In Case 1, s obtained in such a way is a random string.

To distinguish these two cases, it is enough to compute $f(0)$ and $f(s)$.

If $f(0) \neq f(s)$, then f is one-to-one.

If the vectors obtained by the scheme *Hadamard-twice* are not linearly independent, then the whole process has to be repeated.

LOWER BOUND

We show that each classical algorithm needs to perform $\Omega(\sqrt{2^n})$ queries to solve Simon's problem.

Indeed, let us assume that f is a randomly chosen function satisfying requirements of the Simon's problem. If k f-queries are performed then the number of potential s is decreased at most by $\frac{k(k-1)}{2}$ possibilities.

In total there are 2^n potential s.

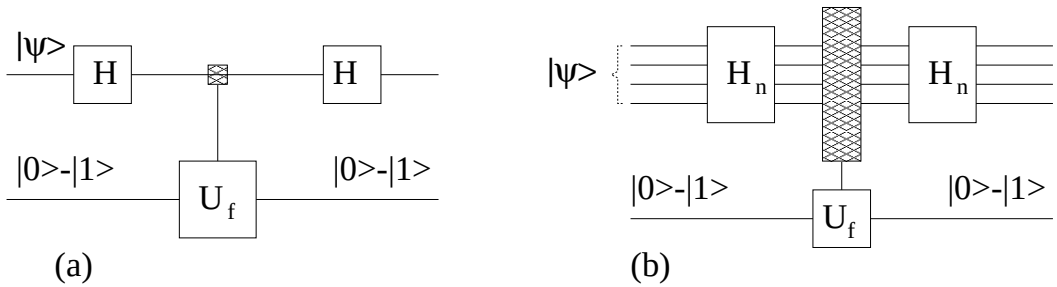
Hence at least in half of the cases any classical algorithm needs to perform $\Omega(\sqrt{2^n})$ f-queries.

HADAMARD-TWICE SCHEME

In the second algorithm for the Deutsch problem and in the algorithm for Simon's problem we have used two simple but powerful techniques which one often encounters in the design of efficient algorithms and quantum error-correcting networks:

- a change between the standard and the dual basis (for some qubits),
- the computation scheme, called **Hadamard twice** , depicted in the general form in Figure below, which uses again f-controlled NOT .

On closer examination one sees that the key point of the "Hadamard twice" scheme is again the change of the basis from standard to dual, some natural computations, and again the change of the basis back.



(Circuit for the Deutsch problem and the "Hadamard-twice scheme". The state $|0\rangle - |1\rangle$ should be normalized.)

COMPUTATIONAL POWER of ENTANGLEMENT

As illustrated in the following examples, in some cases there is a clever way to make use of quantum entanglement to compute efficiently some global properties of a function.

Let a function $f : \{1, \ldots, n\} \to \{0, 1\}$ be given as a black box.

To determine f classically, n calls of f are needed—to get the string $w_f = f(1)f(2)\ldots f(n)$.

Quantumly, this can be done, with probability greater than 0.95, using $\frac{n}{2} + \sqrt{n}$ quantum calls of f.

Indeed, on the base of equality

$$|w_f\rangle = H_n \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot w_f} |x\rangle \tag{7}$$

in order to compute $x \cdot w_f$ one needs $hw(x)$ calls of f, where $hw(x)$ is the Hamming weight of x—the number of 1' in x.

The basic trick is to compute the sum in (7) but only for x such that $hw(x) \leq k$, for a suitable k.

If F_k is such a function that for $x \in \{0,1\}^n$,

$$F_k(x) = \begin{cases} x \cdot w_f \text{ if } hw(x) \leq k \\ 0; \text{ otherwise} \end{cases}$$

then

$$V_{F_k}|x\rangle = \begin{cases} (-1)^{x \cdot w_f}|x\rangle, \text{ if } hw(x) \leq k \\ |x\rangle; \text{ otherwise} \end{cases}$$

Therefore if V_{F_k} is applied to the (initial) state

$$|\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{x \in \{0,1\}^n}^{hw(x) \leq k} |x\rangle,$$

where $M_k = \Sigma_{i=0}^{k} \binom{n}{i}$, then

$$|\psi'_k\rangle = V_{F_k}|\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{x \in \{0,1\}^n}^{hw(x) \leq k} (-1)^{x \cdot w_f}|x\rangle.$$

In order to compute $|\psi'_k\rangle$, at most k calls of f are needed. Let us now measure all n qubits of $|\psi''_k\rangle = H_n|\psi'_k\rangle$.

The probability that this way we get w_f is

$$Pr(|\psi''_k\rangle \textbf{ yields at measurement } w_f) = |\langle w_f|\psi''_k\rangle|^2 = \frac{M_k}{2^n} = \frac{1}{2^n}\sum_{i=1}^{k}\binom{n}{i}$$

and, as one can easily calculate, this probability is more than 0.95 if $k = \frac{n}{2} + \sqrt{n}$.

EXTRAS

QUANTUM FOURIER TRANSFORM

The Quantum Fourier Transform is a quantum variant of the **Discrete Fourier Transform** (DFT). It maps a discrete function to another discrete one with equally distant points as its domain. For example it maps a q-dimensional complex vector

$$\{f(0), f(1), \ldots, f(q-1)\} \text{ into } \{\bar{f}(0), \bar{f}(1), \ldots, \bar{f}(q-1)\},$$

where for $c \in \{0, \ldots, q-1\}$

$$\bar{f}(c) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{2\pi iac/q} f(a), \tag{8}$$

for $c \in \{0, \ldots, q-1\}$.

The quantum version of DFT (QFT) is the unitary transformation

$$\mathsf{QFT}_q : |a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi iac/q} |c\rangle \tag{9}$$

for $0 \leq a < q$, with the unitary matrix

$$F_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(q-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(q-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{(q-1)} & \omega^{2(q-1)} & \dots & \omega^{(q-1)^2} \end{pmatrix},$$

where $\omega = e^{2\pi i/q}$ is the q**th root of unity**.

If applied to a quantum superposition, QFT_q performs as follows;

$$\mathsf{QFT}_q : \sum_{a=0}^{q-1} f(a)|a\rangle \rightarrow \sum_{c=0}^{q-1} \bar{f}(c)|c\rangle,$$

where $\bar{f}(c)$ is defined by (8).

Observe that

$$QFT_q : |\mathbf{0}\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{i=0}^{q-1} |i\rangle,$$

GENERALIZED DEUTSCH-JOZSA PROBLEM

We say that a function $f : \mathbf{Z}_N \to \mathbf{Z}_M$ is evenly distributed if, for a fixed t,

$$\{f(x) \,|\, x \in \mathbf{Z}_N\} = \{j\mu + t \,|\, j \in \mathbf{Z}_k, M = \mu k \text{ and } k|N\},$$

and

$$|A_0| = |A_1| = |A_2| = \ldots = |A_{k-1}| = \frac{N}{k},$$

where

$$A_j = \{x \in \mathbf{Z}_N \,|\, f(x) = j\mu + t\} \text{ for any } j \in \mathbf{Z}_k.$$

In other words, f is evenly distributed if f has equally spaced k values and f is a ν-to-one function where $\nu = \frac{N}{k}$.

The generalized Deutsch-Jozsa problem is to decide, given a promise that a function f, given as an oracle, is either constant or evenly distributed, which of these two properties f has.

To solve the generalized Deutsch-Jozsa problem one application of f is again sufficient. In addition, QFT will be used.

For simplicity we assume $N = 2^n, M = 2^m$. Let

$$|\psi\rangle_\chi = QFT_{2^m}(|-\chi\rangle) = \frac{1}{\sqrt{2^m}} \sum_{z=0}^{2^m-1} e^{-2\pi i \chi z/2^m} |z\rangle$$

for a $\chi \in \mathbf{Z}_{2^m}$.

In the following algorithm to the initial state

$$|0^{(n)}\rangle \otimes |\psi\rangle_\chi$$

at first the transformation $H_n \otimes I$ is applied, then the transformation U_f, transformations $z + f(x) \to z' \to z$, and, finally, again the transformation $H_n \otimes I$. This way we get

$$|0^{(n)}\rangle \otimes |\psi\rangle_\chi \to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |\psi\rangle \tag{10}$$

$$\to \frac{1}{\sqrt{2^n 2^m}} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^m-1} e^{-2\pi i \chi z/2^m} |x\rangle |z \oplus f(x)\rangle \tag{11}$$

$$= \frac{1}{\sqrt{2^n 2^m}} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^m-1} e^{-2\pi i \chi (z-f(x))/2^m} |x\rangle |z\rangle \tag{12}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{2\pi i \chi f(x)/2^m} |x\rangle \otimes |\psi\rangle_\chi \quad (13)$$

$$\rightarrow \sum_{y=0}^{2^n-1} \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} e^{2\pi i \chi f(x)/2^m} \right) |y\rangle |\psi\rangle_\chi \quad (14)$$

Let us now denote the inner summation in the last state as

$$S_y = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} e^{2\pi i \chi f(x)/2^m},$$

It is now easy to see that

- **If f is constant then $S_y = 0$ if and only if $y \neq 0$.**
- **If f is evenly distributed, then $S_0 = 0$.**

Hence, when f is constant the final state of the first register is $|0^{(n)}\rangle$, whereas when f is evenly distributed the state is orthogonal. By one measurement of the first register we can therefore determine whether f is constant or evenly distributed.

DE-QUANTUMIZATION in CASE of DEUTSCH PROBLEM

Surprisingly, quantum algorithms for Deutsch problem can be de-quantised as follows:

For a given $f : \{0,1\} \to \{0,1\}$ we define an oraculum mapping

$$C_f(a+bi) = (-1)^{0 \oplus f(0)} a + (-1)^{1 \oplus f(1)} bi$$

For the four possible functions f we get the following four functions C_f:

$$\begin{array}{ll} C_{00}(x) = x^* & \textbf{if } f(0)=0, f(1)=0 \\ C_{01}(x) = x & \textbf{if } f(0)=0, f(1)=1 \\ C_{10}(x) = -x & \textbf{if } f(0)=1, f(1)=0 \\ C_{11}(x) = -x^* & \textbf{if } f(0)=1, f(1)=1 \end{array}$$

The Deutsch problem can now be formulated as follows: A function is chosen secretly from the set of functions $\{C_{00}, C_{01}, C_{10}, C_{11}\}$ and the task is to determine, with a single query, which type of the function it is - balanced or constant.

Algorithm **Given f, calculate $(i-1)C_f(1+i)$. If the outcome is real, then the function chosen is balanced; otherwise it is constant.**

Correctness:

$$\begin{aligned}
(i-1)C_{00}(1+i) &= (i-1)(1-i) = 2i \\
(i-1)C_{01}(1+i) &= (i-1)(1+i) = -2 \\
(i-1)C_{10}(1+i) &= (i-1)(-1-i) = 2 \\
(i-1)C_{11}(1+i) &= (i-1)(1-i) = -2i
\end{aligned}$$