
Natural Computing **1:** 135–155, 2002.

Quantum computing – Facts and folklore

MIKA HIRVENSALO
TUCS – Turku Centre for Computer Science and, Department of Mathematics, University of Turku, FIN-20014 Turku, Finland (E-mail: mikhirve@utu.fi)

Abstract. We represent and analyze two important quantum algorithms – Finding the hidden subgroup and Grover search. As the analysis goes on, we mention some pieces of "Fact" and "Folklore" associated to quantum computing.

Key words: computation, computational complexity, Fourier transform, quantum physics

1. Introduction

This article is written in an introductory manner – no previous knowledge on quantum computing is required. Instead, some knowledge on linear algebra and group theory will ease the understanding.

We will use widely-spread notations: $\mathbb{Z}$ stands for the set of integers, $\mathbb{C}$ for the set of complex numbers, $|A|$ stands for the cardinality of set A, etc.

But what is meant by the word "computation"? Here we will mainly concentrate on the notion of "algorithmic computation", which, loosely speaking, means computation guided by a finite number of rules. However, it is not so straightforward to give any definite description of "computation", so let us first rewind the time backwards for more than 60 years.

In 1930's Alan Turing studied deeply the notion of a "finitary method" and finally arrived at a concept which later became known as *Turing Machine*.

Nowadays it seems that the notion of a "finitary method" studied by Turing involves the idea that the "processor" which makes use of the method is indeed a human being: firstly, Turing argued that the "method" must be based on manipulating *symbols*. Secondly, Turing emphasized that the number of different symbols to be handled must be finite (due to the limited capacity of a human being for distinguishing reliably the symbols). Thirdly, Turing noted that the action on symbols must take place only *locally* (since a human being cannot handle arbitrarily large amount of symbols at the same time).

Nowadays we cannot find anyone to claim that the notion of a Turing Machine does not correspond to the notion of an "intuitive algorithm". The contrary is not so clear, but Turing's argumentation was quite convincing;

so convincing that for more than 60 years the notion of *algorithmic computability* has been used synonymously to *Turing Machine computability*. The hypothesis that the notion of a Turing Machine indeed captures the full power of "algorithmic computability" is known as *Church-Turing Thesis*.

Another significant but not so often mentioned achievement by Turing was the construction of a *universal Turing Machine*. A *universal Turing Machine* is a Turing machine, which is capable of simulating any other Turing machine. Turing showed that those universal machines indeed exist, and that result established the notion of a *programmable computer*.

The notion of a Turing Machine is indeed clever: it provides an opportunity to give a good definition for the *time of computation*, as well as for the *space needed by the computation*. For example, we can define the computational time as the number of the computational steps the machine takes from initial configuration to a final one.

On the other hand, anyone could argue that the notion of a Turing Machine is clumsy: even to program any simplest algorithm on a Turing Machine requires a long and rather non-intuitive list of machine's transition rules. For an example, we invite the reader to describe a Turing Machine which multiplies the given input (in a decimal notation) by two.

2. Entering the quantum era

2.1 *What is physics indeed?*

Let us first agree on a couple of notational affairs: a very first attempt to explain the notion of *physics* could be something like that physics is the branch of science which tries to find an explanation for all the possible experimental phenomena in the world we live in. It is not the purpose of the present article to create any new characterization for *physics*, but rather, I am satisfied with mentioning some of its features. I wish that a physical theory eventually has at least the four following characteristic features:

- The theory should *describe* the observed phenomena. The description can be given, for instance, in a mathematical form, cf. Kepler's laws on how the planets orbit around the sun.
- The theory should *explain* the observed phenomena in some, hopefully a deep sense. For an example, consider Newton's gravitation law which explains why the planets orbit elliptically around the sun.
- The theory should have *reliable predictions*. By this I mean that for example, the current theory of the planet movements can reliably predict the future eclipses very precisely.

- The theory must have all the three features mentioned above, but also the *support of experience*. By this I mean that a physical theory should be regarded valid only if it agrees with the experiments.

A modern view of local astronomy (only consisting of the solar system of ours) seems to be rather well-explained by using the gravity theory of Newton: even the exceptions (e.g. the motion of the perihelion of planet mercury, which rather supports Einstein's theory of gravitation), are rather small when the time scale is suitable for a human being.

I would like to point out a difference between physics and some other human activities. It is true that the theories we now have about our solar system can explain almost any local event (read: an event in the solar system) but they are not *reproducible*. Yes, I restrict the study of "physics" for the events which satisfy the conditions above, but such that the events could be reproduced.

The above characteristic features obviously exclude many human scientific activities, like biology, history, linguistics, etc. Notice also that *physics*, as I it characterized, cannot be the same as *mathematics*, even though the language of mathematics is quite often used to describe the phenomena in the physical world. The obvious reason for making this difference is due to the fact that mathematics is not an empirical science: within mathematics, the truths or untruths are obtained by logical deduction.

It is however true that one can ask e.g., which is the difference between chemistry and physics or which is the difference between geography and physics, etc. To these questions I am not offering any answers, I just wish to refer to the criteria mentioned above. Instead, I am closing *that* discussion by merely saying that any deeper analysis of these questions is not the purpose of the present article. I will hereafter assume that the reader can understand the notion "physics" mostly by intuition, which hopefully quite well coincides with that one of my own.

2.2 *Mechanics – Classical and quantum*

Physics itself can be divided into many different subareas: traditionally thermodynamics, mechanics, and electromagnetism are some of them, just to mention. In what follows, we will concentrate on electromagnetism and mechanics.

For centuries, the physicists have discussed about the nature of *light*. It has been argued that we should regard light as particle flow, but on the other hand, some characteristic features of light (such as interference phenomena) have given a good reason to explain light as some kind of wave movement.

Then which explanation is good? Just by considering the progress up to the middle of 19th century, we could say that the theory of electromagnetism nowadays mainly inherited to Maxwell was able to describe the behaviour of light by explaining that light is indeed an undulatory phenomenon in electromagnetic field. But this theory was not good enough: it was unable to explain the radiation spectrum of a *black body*.

A black body is an ideal object which can emit, as well as absorb, electromagnetic radiation in all possible wavelengths. In real life, black bodies do not exist, but it turns out that a small hole in a cavity is a pretty good approximation of a black body. The theory predicted that in a fixed temperature, a black body should radiate in all wavelengths, but not equally. Some wavelengths should be present more intensively than the others, but any of the theories based on that one of Maxwell was not able to describe the intensity curve.

In his famous article, Planck established a *quantum hypothesis*, which essentially says that all the radiation could be emitted or absorbed only in discrete packets. Using this hypothesis, he was finally able to describe the intensity curve in a way which agreed with the measurements. Recall that the description was based on an idea that the radiation can be emitted and absorbed only in discrete packets. In some sense, that description contained the idea that electromagnetic radiation should be considered as a particle flow.

Many phenomena observed later supported the idea that microscopic physical systems indeed have a strange duality: some of their properties are very well explained by assuming the corpuscular nature of the objects, but some must be accounted to the wave theory.

It is quite reasonable to state, that *quantum mechanics* was eventually created to describe objects which have both undulatory and corpuscular characteristics.

3. Information represented in quantum systems

Again we choose not to enter very deeply into the mazes of the word *information*, but we will merely give some of its descriptive features.

The basic unit of information we choose to use is a *binary digit, bit for short*: A bit can have two potential values 0 and 1, and hence a bit can be presented by using any physical system capable of being in two distinguishable states. Hereafter such a system will be called a *two-level* system. If a system representing a bit is a quantum mechanical system, we will call such a system a *quantum bit* or *qubit*, for short.

A general *state* of a qubit is described by using two complex numbers c_0 and c_1 which satisfy $|c_0|^2 + |c_1|^2 = 1$. Following the notations of P. Dirac, the state of the qubit is denoted by

$$c_0 \,|0\rangle + c_1 \,|1\rangle, \tag{1}$$

and the numbers c_0 and c_1 are called the *amplitudes* of $|0\rangle$ and $|1\rangle$, respectively. The interpretation of a (1) is the following: when the qubit (1) is observed, we get '0' with a probability of $|c_0|^2$, and '1' with a probability of $|c_1|^2$. A combination (1) is called a *superposition* of $|0\rangle$ and $|1\rangle$.

Folklore: When a qubit in state (1) is observed, and 0 (1) is seen as outcome, then the state (1) "collapses" into the state $|0\rangle$ ($|1\rangle$)

Fact: The above "Folklore" is known as the *projection postulate*. The projection postulate can be regarded as an ad-hoc -explanation for the measurement procedure, but it is not consistent with the unitary time evolution of quantum systems (described later). Most interpretations of the modern quantum physics cannot explain the measurement procedure in a consistent way. This problem is often referred as to the *measurement paradox of quantum physics*. It is also true that all the significant quantum algorithms can be reformulated to avoid any reference to the projection postulate.

The above description and interpretation resembles very closely to the notion of *random bit*: we do not know the value of the bit for sure, but we know that it takes value 0 with a probability of $|c_0|^2$ and value 1 with a probability of $|c_1|^2$. Then, what makes the description of a quantum bit so different from that one of a random bit? We will explain that quite soon, but first we will concentrate on the mathematical nature of representation (1).

Evidently we can regard (1) as a vector in a two-dimensional vector space over complex numbers, having $\{|0\rangle, |1\rangle\}$ as an orthonormal basis. The condition $|c_0|^2 + |c_1|^2 = 1$ would then mean that vector (1) has norm equal to one. In fact, this is the structure that the quantum mechanical description will be based on: a state of an n-level quantum system will be described by using a unit-length vector in an n-dimensional vector space over complex numbers. Such a vector space is called n-dimensional *Hilbert space* and denoted by H_n. It is clear that H_n is isomorphic to the Cartesian product $\mathbb{C}^n$.

To choose an orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ for H_n is to choose n perfectly distinguishable physical properties which the system can have. Any unit-length vector

$$c_0 \,|0\rangle + c_1 \,|1\rangle + \ldots + c_{n-1} \,|n-1\rangle \tag{2}$$

is called a *superposition* of vectors $|0\rangle, \ldots, |n-1\rangle$ describes a potential state of the system, and (2) is interpreted analogously to (1): when the system in state (2) is observed, value $k \in \{0, 1, \ldots, n-1\}$ will be seen with a probability of $|c_k|^2$.

Fact: The representation of quantum states as unit-length vectors in Hilbert spaces is not very precise: if $\psi \in H_n$ represents a state of a quantum system, then $e^{i\theta}\psi$ for each $\theta \in \mathbb{R}$ represents the same state. Thus it is rather difficult to speak about the *construction* of superpositions: $|\,1\rangle$ and $-\,|\,1\rangle$ describe the same qubit state, but $\frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle)$ and $\frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle)$ for instance do not.

A better representation of the states of quantum systems can be obtained by replacing any unit-length vector with the projection onto the one-dimensional subspace it generates. In this extended formalism, the one-dimensional projections are called *pure states*, and the other states, which generally are self-adjoint positive mappings having a unit trace, are called *mixed states*.

So far we have only discussed about the *representation* of quantum information. We also should know which *transformations* we can apply to quantum systems. In physical terms, we should know how the system whose state is described in (2) evolves in time, i.e., we should know the *equations of the motion*.

Rather simple premises (see Hirvensalo 2001) imply that there exists *unitary* mappings $U(t) : H_n \to H_n$ which govern the time evolution in the following way: if

$$\psi(0) = c_0\,|0\rangle + c_1\,|1\rangle + \ldots + c_{n-1}\,|n-1\rangle$$

is the state of the system at time $t = 0$, then the state at time t is given by

$$\psi(t) = U(t)\psi(0). \tag{3}$$

Moreover, the unitary mappings $U(t)$ satisfy $U(t_1 + t_2) = U(t_1)U(t_2)$. If we further assume that the mapping $t \mapsto U(t)$ is continuous, it follows that there exists a *self-adjoint mapping* $H : H_n \to H_n$ such that $U(t) = e^{-itH}$. Such a mapping H is called the *Hamiltonian operator* of the system and is of course determined by the physical conditions. A componentwise differentiation of (3) implies that

$$i\frac{\mathrm{d}}{\mathrm{d}t}\psi(t) = H\psi(t). \tag{4}$$

Equation (4) is called *Schrödinger's equation of motion*. Here we will be mainly interested in the system states at discrete time steps $t_0, t_1, t_2, \ldots$, which

naturally leads to the following formalism: If ψ_k stands for the system state at time t_k, then there is a unitary mapping U_k such that

$$\psi_{k+1} = U_k \psi_k.$$

Folklore: The time evolution in quantum systems is always unitary and therefore also reversible.

Fact: In the case that the time evolution does not preserve pure states pure, the evolution can be non-unitary and irreversible as well. It is however true that in that case, the time evolution can be interpreted as a unitary evolution in a larger quantum system, see Hirvensalo (2001).

EXAMPLE 1. *By denoting* $|0\rangle = (1,0)^T$ *and* $|1\rangle = (0,1)^T$ *we can define a unitary mapping* W_2 *by its matrix representation in basis* $(1,0)^T$, $(0,1)^T$*:*

$$W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It is plain to verify that W_2 *is indeed unitary, and that*

$$W_2 |0\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle, \tag{5}$$

$$W_2 |1\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle. \tag{6}$$

Now it must be emphasized that an observation of state (5), as well as an observation of state (6) will give 0 *or* 1*, both with a probability of* $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$*. Hence we can regard the operation* W_2 *as an unbiased "quantum coin flip": applying* W_2 *to either* $|0\rangle$ *or* $|1\rangle$ *will give us* 0 *or* 1 *with a probability of* $\frac{1}{2}$*. But when applying the operation* W_2 twice*, we will see a peculiar feature which can never appear in traditional computation: assume, for instance that we begin with a quantum bit at state* $|0\rangle$*. Now, the first application of* W_2 *will result a qubit in state*

$$\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle. \tag{7}$$

Another application of W_2 *on state (7) will result in state*

$$\begin{aligned} &\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right) \\ = \; &\frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle + \frac{1}{2} |0\rangle - \frac{1}{2} |1\rangle = |0\rangle, \end{aligned} \tag{8}$$

which can be observed to give 0 *with certainty. A classical analogue of this procedure would be something like this: beginning a coin with the head on, flipping but not observing the outcome, and flipping it again. In the classical case it is clear that after the second flip, we are able to observe both head and tail with a probability of* $\frac{1}{2}$.

Let us reconsider the "quantum coin flipping". After the first flip (operation W_2*), both basis vectors* $|0\rangle$ *and* $|1\rangle$ *occur with an amplitude of* $\frac{1}{\sqrt{2}}$*, which means that if the state would be observed, we would get* 0 *and* 1*, both with a probability of* $\frac{1}{2}$*. The second flip in turn divides* $|0\rangle$ *into* $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ *and* $|1\rangle$ *into* $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ *and, after rearranging the terms we have* $|0\rangle$ *with amplitude* $\frac{1}{2} + \frac{1}{2} = 1$ *and* $|1\rangle$ *with amplitude* $\frac{1}{2} - \frac{1}{2} = 0$*. We say that the coefficients of* $|0\rangle$ *have* interfered constructively *and that the coefficients of* $|1\rangle$ *have* interfered destructively. *Later we will see that the interference will be an important computational resource.*

4. Fourier transforms

4.1 *Discrete fourier transform*

The Fourier analysis is one of the most important techniques in mathematics, physics and engineering. Loosely speaking, the most elementary starting point for Fourier analysis is to represent a function as a linear combination of some suitably chosen *basis functions* and then considering the coefficients of the representation as another function, the *Fourier transform* of the original function. Here we will consider the following case:

Let G be a finite abelian group (we use additive notation here), and consider functions $f : G \to \mathbb{C}$. Such functions clearly form a vector space V_G over complex numbers, when the addition and scalar the multiplication are both defined pointwise. This vector space clearly has dimension $|G|$, and we can introduce an inner product by

$$\langle f_1 \mid f_2 \rangle = \sum_{g \in G} f_1(g)^* f_2(g).$$

It is a well-known fact that there are $|G|$ *characters* (see Hirvensalo 2001 for details) of group G, and that the characters $\{\chi_g \mid g \in G\}$ form an orthogonal basis of V_G. Moreover, by scaling the characters to the unit length we obtain

$$\left\{ \frac{1}{\sqrt{|G|}} \chi_g \mid g \in G \right\},$$

an orthonormal basis of V_G. Hence each function $f \in V_G$ can be uniquely represented as

$$f = \sum_{g \in G} c_g \frac{1}{\sqrt{|G|}} \chi_g. \tag{9}$$

We denote $c_g = \widehat{f}(g)$ and say that the function $\widehat{f} : G \to \mathbb{C}$ induced in this way is the (discrete) *Fourier transform* of f. By using the orthonormality of functions $\frac{1}{\sqrt{|G|}}\chi_g$ it is easy to find the values $\widehat{f}(g)$:

$$\widehat{f}(g) = \langle \frac{1}{\sqrt{|G|}} \chi_g \mid f \rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi_g(h)^* f(h).$$

An important relation between function f and its Fourier transform is the *Parseval's identity*

$$\langle f \mid f \rangle = \langle \widehat{f} \mid \widehat{f} \rangle,$$

which is easy to verify, see Hirvensalo (2001).

EXAMPLE 2. *Let $\mathbb{Z}_2 = \{0, 1\}$ denote the ring of two elements and $\mathbb{Z}_2^n$ the n-fold Cartesian product of $\mathbb{Z}_2$. By defining the addition componentwise, we see that $\mathbb{Z}_2^n$ becomes an abelian group of cardinality 2^n. It is easy to see that all the characters (see Hirvensalo 2001) of $\mathbb{Z}_2^n$ are of form*

$$\chi_{\boldsymbol{y}}(\boldsymbol{x}) = (-1)^{\boldsymbol{x} \cdot \boldsymbol{y}},$$

where $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \ldots + x_n y_n$ (all the products and sums are computed in $\mathbb{Z}_2$), and $(-1)^b$ for $b \in \mathbb{Z}_2$ is interpreted in the most obvious way. Thus the so-called Walsh functions

$$W_{\boldsymbol{y}}(\boldsymbol{x}) = \frac{1}{\sqrt{2^n}} (-1)^{\boldsymbol{x} \cdot \boldsymbol{y}}$$

form an orthonormal basis of function space $V_{\mathbb{Z}_2^n}$, and hence each function $f : \mathbb{Z}_2^n \to \mathbb{C}$ can be uniquely represented as

$$f = \sum_{\boldsymbol{y} \in \mathbb{Z}_2^n} \widehat{f}(\boldsymbol{y}) W_{\boldsymbol{y}}. \tag{10}$$

The Fourier transform has now form

$$\widehat{f}(\boldsymbol{y}) = \sum_{\boldsymbol{x}} W_{\boldsymbol{y}}(\boldsymbol{x}) f(\boldsymbol{x}) = \sum_{\boldsymbol{x}} f(\boldsymbol{x}) W_{\boldsymbol{x}}(\boldsymbol{y}), \tag{11}$$

since $W_{\boldsymbol{y}}(\boldsymbol{x}) = W_{\boldsymbol{x}}(\boldsymbol{y})$. Formulae (10) and (11) show that in $\mathbb{Z}_2^n$ the symmetry between the function and its Fourier transform is perfect: it follows that $\widehat{\widehat{f}} = f$.

4.2 *Quantum fourier transform*

Let G again denote a finite abelian group. Recall that the representation of a $|G|$-level quantum system is based on a Hilbert space $H_{|G|}$. We enumerate an orthonormal basis of $H_{|G|}$ by using the elements of G, and choose notation

$$\{|\, g\rangle \mid g \in G\}$$

to stand for such a basis. A quantum system like this is called *a quantum representation* of group G (more precisely: of the underlying set of G). A general state of the quantum system can be represented as

$$\sum_{g\in G} f(g)\, |\, g\rangle, \tag{12}$$

where

$$\sum_{g\in G} |f(g)|^2 = 1.$$

The *quantum Fourier transform* (QFT for short) of state (12) is defined to be the state

$$\sum_{g\in G} \widehat{f}(g)\, |\, g\rangle, \tag{13}$$

where $\widehat{f}$ is the ordinary (discrete) Fourier transform of f. Notice that also

$$\sum_{g\in G} \left|\widehat{f}(g)\right|^2 = 1$$

by the Parseval's identity, so (13) represents a state as well. Later we well see that QFT is an important computational primitive, but first we will see how to *implement* QFT, i.e., how to find a unitary transform which carries (12) into (13).

EXAMPLE 3. *Let G be a cyclic group of order n. As a prototype for G we can choose $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, where addition is defined modulo n. The characters of $\mathbb{Z}_n$ are well-known: For each $k \in \mathbb{Z}_n$ function*

$$\chi_k(l) = e^{\frac{2\pi i \cdot kl}{n}} \tag{14}$$

is a character of $\mathbb{Z}_n$, and all the characters of $\mathbb{Z}_n$ are of form (14). Now the Fourier transform of $f : \mathbb{Z}_n \to \mathbb{C}$ can be written as

$$\widehat{f}(k) = \frac{1}{\sqrt{n}} \sum_{l \in \mathbb{Z}_n} e^{-\frac{2\pi i \cdot kl}{n}} f(l).$$

Hence if H_n with orthonormal basis $\{|\,0\rangle, |\,1\rangle, \ldots, |\,n-1\rangle\}$ is a quantum representation of group $\mathbb{Z}_n$, then the QFT of $\mathbb{Z}_n$ is the operation

$$|\,l\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{-\frac{2\pi i \cdot kl}{n}} |\,k\rangle, \tag{15}$$

whose matrix on basis $|\,0\rangle = (1, 0, \ldots, 0)^T$, $|\,1\rangle = (0, 1, \ldots, 0)^T$, $\ldots$, $|\,n-1\rangle = (0, 0, \ldots, 1)^T$ can be directly read from (15). Notice that by the linearity, it suffices to define QFT only for basis vectors.

In case $n = 2$ we simply have $\mathbb{Z}_2$, the group of two elements, which can be represented by using a single quantum bit. Then the operation (15) becomes merely

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

whose matrix is simply W_2 of Example 1. For short, we can write

$$W_2\,|\,l\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{l \cdot k}\,|\,k\rangle \tag{16}$$

for $l \in \{0, 1\}$.

EXAMPLE 4. *A* compound system *of n qubits is represented by using a 2^n-dimensional Hilbert space H_{2^n} having orthonormal basis $\{|\,\boldsymbol{x}\rangle \mid \boldsymbol{x} \in \{0,1\}^n\}$. This means that the "labels" of the basis vectors are the bit strings of length n. A general state of the system of n qubits is simply represented by a vector*

$$\sum_{\boldsymbol{x} \in \{0,1\}^n} c_{\boldsymbol{x}}\,|\,\boldsymbol{x}\rangle,$$

where $\sum_{\boldsymbol{x} \in \{0,1\}^n} |c_{\boldsymbol{x}}|^2 = 1$. Notice that a similar system can be obtaining as an n-fold tensor product *(see Hirvensalo 2001) of H_2: in that tensor product, the basis vectors would be of form*

$$|\,x_1\rangle \otimes |\,x_2\rangle \otimes \ldots \otimes |\,x_n\rangle, \tag{17}$$

where $x_i \in \{0, 1\}$. But abbreviating (17) into $|x_1\rangle\,|x_2\rangle \ldots |x_n\rangle$ and even into $|x_1x_2 \ldots x_n\rangle$ we end up again in the same system we defined here. Thus it is clear that $H_2 \otimes \ldots \otimes H_2$ (n times) is isomorphic to H_{2^n}. In fact, this tensor product construction is indeed the general principle for treating compound quantum systems.

Space H_{2^n} with basis $\{|\boldsymbol{x}\rangle \mid \boldsymbol{x} \in \{0, 1\}^n\}$ forms a natural quantum representation for group $\mathbb{Z}_2^n$. By considering the tensor product representation of H_{2^n} we see that this representation of $\mathbb{Z}_2^n$ is also pretty well consistent with the algebraic decomposition

$$\mathbb{Z}_2^n = \mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2.$$

We have already learned how to implement the Fourier transform in the case $n = 1$. For the general case, there exists a nice decomposition result: in order to compute the Fourier transform in $G_1 \oplus G_2$, it is sufficient to know how the corresponding transforms in G_1 and G_2 are computed (see Hirvensalo 2001).

We use the tensor decomposition $|x_1x_2 \ldots x_n\rangle = |x_1\rangle\,|x_2\rangle \ldots |x_n\rangle$ to find out how the QFT in $\mathbb{Z}_2^n$ is performed. We define an unitary operation $W_2 \otimes \ldots \otimes W_2$ on H_{2^n} as an operation of W_2 on each qubit:

$$\begin{aligned}
&(W_2 \otimes W_2 \otimes \ldots \otimes W_2)\,|x_1\rangle\,|x_2\rangle \ldots |x_n\rangle \\
&= \frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} (-1)^{x_1 \cdot y_1}\,|y_1\rangle \frac{1}{\sqrt{2}} \sum_{y_2=0}^{1} (-1)^{x_2 \cdot y_2}\,|y_2\rangle \ldots \frac{1}{\sqrt{2}} \sum_{y_n=0}^{1} (-1)^{x_n \cdot y_n}\,|y_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_1 y_2 \ldots y_n \in \{0,1\}^n} (-1)^{x_1 \cdot y_1 + x_2 \cdot y_2 + \ldots + x_n \cdot y_n}\,|y_1\rangle\,|y_2\rangle \ldots |y_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{y} \in \mathbb{Z}_2} (-1)^{\boldsymbol{x} \cdot \boldsymbol{y}}\,|\boldsymbol{y}\rangle.
\end{aligned}$$

Hence the unitary operation $W_2 \otimes \ldots \otimes W_2$ on $H_2 \otimes \ldots \otimes H_2$ indeed implements the QFT

$$|\boldsymbol{x}\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{y} \in \mathbb{Z}_2^n} (-1)^{\boldsymbol{x} \cdot \boldsymbol{y}}\,|\boldsymbol{y}\rangle$$

on $\mathbb{Z}_2^n$.

Fact: QFT's on other groups than $\mathbb{Z}_2^n$ can also be devised, and the "quantum complexity" of QFT depends on the structure of the particular group. For instance, QFT in $\mathbb{Z}_{2^n}$ can be performed by using n^2 quantum operations, each accessing only on at most two qubits Hirvensalo (2001).

4.3 *The complexity of computing QFT*

Let us first think about the complexity of computing the Fourier transform of $f : \mathbb{Z}_2^n \to \mathbb{C}$ in the classical case. We assume that 2^n function values $(f(\boldsymbol{x}))_{\boldsymbol{x}\in\mathbb{Z}_2^n}$ are given as input, and the task is to output vector $(\widehat{f}(\boldsymbol{y}))_{\boldsymbol{y}\in\mathbb{Z}_2^n}$.

The elementary method to compute each $\widehat{f}(\boldsymbol{y})$ individually by using formula

$$\widehat{f}(\boldsymbol{y}) = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x}\in\mathbb{Z}_2^n} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}} f(\boldsymbol{x}) \tag{18}$$

would result into a complexity of $\Theta(2^n \cdot 2^n) = \Theta(2^{2n})$ operations to reach the output. However, a faster method is obtained by denoting $\boldsymbol{x} = x_1\boldsymbol{x}'$, $\boldsymbol{y} = y_1\boldsymbol{y}'$ and representing (18) as

$$\widehat{f}(\boldsymbol{y}) = \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x}'\in\mathbb{Z}_2^{n-1}} (-1)^{\boldsymbol{x}'\cdot\boldsymbol{y}'} f(0\boldsymbol{x}') + (-1)^{y_1} \sum_{\boldsymbol{x}'\in\mathbb{Z}_2^{n-1}} (-1)^{\boldsymbol{x}'\cdot\boldsymbol{y}'} f(1\boldsymbol{x}') \tag{19}$$

Decomposition (19) reveals the fact that the Fourier transform in $\mathbb{Z}_2^n$ can be computed by first computing two Fourier transforms in $\mathbb{Z}_2^{n-1}$ and then combining the results. By recursively applying the decomposition (19) we eventually reach into the complexity of $O(n2^n)$ operations to discover the outcome. This recursive method for computing Fourier transform is called the *fast Fourier transform* (FFT).

On the other hand, the case of QFT is different: we are given a state

$$\sum_{\boldsymbol{x}\in\mathbb{Z}_2^n} f(\boldsymbol{x}) \,|\boldsymbol{x}\rangle \tag{20}$$

as an input and we should output a state

$$\sum_{\boldsymbol{y}\in\mathbb{Z}_2^n} \widehat{f}(\boldsymbol{y}) \,|\boldsymbol{y}\rangle. \tag{21}$$

We have already seen that (21) can be obtained by applying operation W_2 on each individual qubit of the system in state (20). It is therefore reasonable to say that *n quantum operations* are sufficient to implement the QFT in $\mathbb{Z}_2^n$, and this is a huge improvement over $O(n2^n)$ operations in the classical case of FFT.

Folklore: QFT is a special case of FFT.

Fact: It is worth emphasizing that the nature of QFT is quite different from that one of the classical Fourier transform. First, the size of the input in the classical case is $\Omega(2^n)$, and even though the description of (20) requires 2^n complex numbers, the *physical size* of a system representing $\mathbb{Z}_2^n$ is only n qubits. Secondly, each $\widehat{f}(\boldsymbol{y})$ can be read out in the classical case, whereas in quantum case we only have a state (21) with *amplitudes* $\widehat{f}(\boldsymbol{y})$. The observation of (21) will give only some $\boldsymbol{y}$ as the output – any such with a probability of $\left|\widehat{f}(\boldsymbol{y})\right|^2$, thus no direct information about the numbers $\widehat{f}(\boldsymbol{y})$ is available.

However, as we will see, the ability of computing QFT by using only a few quantum operations is enough to create fast methods for solving problems which seem to be intractable in classical computation.

5. Hidden subgroups

5.1 *Simon's problem*

In a general form, *Simon's subgroup problem* can be stated as follows: The input is a finite commutative group G and a function $\rho : G \to R$ (R is a finite set) which satisfies the *promise* that there exists a nontrivial subgroup $H \leq G$ such that ρ is constant and distinct on each coset of H. The task is to find a generating set of H.

The task is trivially solvable: Since H itself is the only coset containing the neutral element, we can use function ρ to find *all* elements of H, as well as a generating set. But if G is a very large group, an exhaustive search for H will be hopelessly slow. At the same time, the *representation size* of the elements of G can be small – it suffices to use $O(\log_2 |G|)$ bits to represent the elements of G, and if there are only a few generators, then G can have a very small representation size.

We will now concentrate on the case $G = \mathbb{Z}_2^n$. Let H be the subgroup of the promise, and

$$H^{\perp} = \{\boldsymbol{y} \in \mathbb{Z}_2^n \mid \boldsymbol{y} \cdot \boldsymbol{h} = 0 \text{ for each } \boldsymbol{h} \in H\}$$

the *orthogonal complement* of H. Notice that $\mathbb{Z}_2$ can be also be regarded as $\mathbb{F}_2$, the finite field of two elements, and that $\mathbb{Z}_2^n$ can be regarded as an n-dimensional vector space over $\mathbb{F}_2$. Therefore, notions such as the dimension and the basis are available. The following statement is easy to prove Hirvensalo (2001): for any $\boldsymbol{y} \in \mathbb{Z}_2^n$,

$$\sum_{\boldsymbol{h} \in H} (-1)^{\boldsymbol{h} \cdot \boldsymbol{y}} = \begin{cases} |H|, & \text{if } \boldsymbol{y} \in H^{\perp}, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

Let us now assume that there exists a unitary operator U_ρ which is capable of computing function ρ in the following sense:

$$U_\rho \, |\boldsymbol{x}\rangle \, |\mathbf{0}\rangle = |\boldsymbol{x}\rangle \, |\rho(\boldsymbol{x})\rangle,$$

where $\boldsymbol{x} \in \mathbb{Z}_2^n$, and the second factor of the product is a basis vector of a system capable of representing set R.

Fact: If $f : \{0, 1\}^n \to \{0, 1\}^m$ is a function such that value $f(\boldsymbol{x})$ is computable with a Boolean circuit with T elementary gates (and, or, not -gates), then there exists a unitary mapping U_f which performs an operation

$$U_f \, |\boldsymbol{x}\rangle \, |\mathbf{0}\rangle \, |\mathbf{0}\rangle = |\boldsymbol{x}\rangle \, |f(\boldsymbol{x})\rangle \, |\mathbf{0}\rangle. \tag{23}$$

In (23), $|\boldsymbol{x}\rangle$ contains n qubits which represent an element of $\mathbb{Z}_2^n$, the first $|\mathbf{0}\rangle$ consists of m qubits which represent an element of $\mathbb{Z}_2^m$, and the last $|\mathbf{0}\rangle$ consists of $k = O(T)$ *ancilla* qubits which are needed for reversible computing. The unitary mapping U_f can be implemented by using $O(T)$ consecutive simple quantum operations (chosen from a finite set) which operate on at most 3 qubits each (see Hirvensalo (2001), for instance). Such simple quantum operations are called *quantum gates*. Usually, the ancilla qubits are not written down explicitly, but we merely write operation of U_f as

$$U_f \, |\boldsymbol{x}\rangle \, |\mathbf{0}\rangle = |\boldsymbol{x}\rangle \, |f(\boldsymbol{x})\rangle.$$

Now we begin with state

$$|\mathbf{0}\rangle \, |\mathbf{0}\rangle, \tag{24}$$

where the first factor represents $\mathbf{0} \in \mathbb{Z}_2^n$, and the second one an element $\mathbf{0} \in R$. Computing the QFT in $\mathbb{Z}_2^n$ by using operation W_2 on n first qubits of the first factor results into a state

$$\frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} |\boldsymbol{x}\rangle \, |\mathbf{0}\rangle. \tag{25}$$

After this, we operate with U_ρ on (25) getting

$$\frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} |\boldsymbol{x}\rangle \, |\rho(\boldsymbol{x})\rangle. \tag{26}$$

Choosing a set T which contains exactly one element of each coset of H and using the promise that ρ is constant on each coset of H we can rewrite (26) as

$$\frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{t}\in T} \sum_{\boldsymbol{x}\in H} |\boldsymbol{t}+\boldsymbol{x}\rangle \, |\rho(\boldsymbol{t})\rangle. \tag{27}$$

A QFT on the first n qubits of (27) results into

$$\begin{aligned} &\frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{t}\in T} \sum_{\boldsymbol{x}\in H} \frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{y}\in\mathbb{Z}_2^n} (-1)^{(\boldsymbol{t}+\boldsymbol{x})\cdot\boldsymbol{y}} \, |\boldsymbol{y}\rangle \, |\rho(\boldsymbol{t})\rangle \\ = \; &\frac{1}{2^n} \sum_{\boldsymbol{t}\in T} \sum_{\boldsymbol{y}\in\mathbb{Z}_2^n} (-1)^{\boldsymbol{t}\cdot\boldsymbol{y}} \sum_{\boldsymbol{x}\in H} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}} \, |\boldsymbol{y}\rangle \, |\rho(\boldsymbol{t})\rangle. \end{aligned} \tag{28}$$

By (22), the superposition (28) can be written as

$$\frac{|H|}{2^n} \sum_{\boldsymbol{t}\in T} \sum_{\boldsymbol{y}\in H^\perp} (-1)^{\boldsymbol{t}\cdot\boldsymbol{y}} \, |\boldsymbol{y}\rangle \, |\rho(\boldsymbol{t})\rangle. \tag{29}$$

An observation of the first n qubits (29) will hence give an element of $H^\perp$, any such with a probability of

$$\sum_{\boldsymbol{t}\in T} \left(\frac{|H|}{2^n}(-1)^{\boldsymbol{t}\cdot\boldsymbol{y}}\right)^2 = \frac{1}{\left|H^\perp\right|},$$

see Hirvensalo (2001) for details.

By collecting all the facts above together we find out that the above method will produce an element of $H^\perp$, any such with a probability of $\frac{1}{|H^\perp|}$. All this can be done by using $2n$ quantum operations W_2 together with one application of U_ρ.

How does the ability of choosing uniformly an element of $H^\perp$ help us to find a basis of H? First is easy to see that once we have a basis of $H^\perp$, the *Gauss-Jordan* elimination method (see Hirvensalo 2001) allows us to rapidly find a basis of H, too. Hence it is sufficient to find a basis for $H^\perp$. But it can be shown (see Hirvensalo 2001), that if we draw elements $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_k$ of $H^\perp$ uniformly, then the probability that $\boldsymbol{y_1}, \ldots, \boldsymbol{y}_k$ form a basis of $H^\perp$ is

$$\begin{cases} 0, & \text{if } k > \dim(H^\perp), \\ \geq \frac{1}{4}, & \text{if } k \leq \dim(H^\perp). \end{cases}$$

Moreover, the question whether $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_k$ are indeed linearly independent, can be quickly resolved by using the Gauss-Jordan elimination method (see

Hirvensalo 2001). Therefore, by uniformly choosing an element $\boldsymbol{y} \in H^{\perp}$ by using the quantum computational method described above, we can eventually find a basis of $H^{\perp}$. The expected number of computational steps to find such a basis can easily be seen to be $O(\left|H^{\perp}\right| n) = O(n)$, if H is considered as a fixed subgroup, and U_{ρ} as an operation which can be computed in constant time.

Let us now reconsider the whole procedure: we first prepared an equally weighted superposition (25) by using QFT. After this, the computation of function ρ resulted into (27), and finally another QFT resulted in state (28), where we were able to exactly compute the *effects of the interference* in order to get (29). It turned out that vectors $|\boldsymbol{y}\rangle$ where $\boldsymbol{y} \in H^{\perp}$, interfered with each other constructively, whereas the remaining ones interfered destructively. However, it could be stated that the operational step in moving the information about subgroup H into the whole superposition was carried out by operator U_{ρ}.

5.2 *An application of the hidden subgroup problem*

Fact: If n is an odd composite integer having at least two distinct prime factors, and $a \in \{1, \ldots, n\}$ is a uniformly chosen number such that $\gcd(a, n) = 1$. Then the knowledge about $r = \mathrm{ord}_n(a)$ (the least positive number such that $a^r \equiv 1 \pmod{n}$) can be used to reveals a nontrivial factor of n in polynomial time with a probability of at least $\frac{9}{16}$ (see Hirvensalo (2001) and the references therein).

Fact: In the additive group $\mathbb{Z}$ the hidden subgroup associated to the function $\rho(x) = a^x + n\mathbb{Z}$ is $r\mathbb{Z}$, where $r = \mathrm{ord}_n(a)$, see Hirvensalo (2001).

The above two facts suggest that in order to factorize n, we should uniformly pick a number $a \in \{1, \ldots, n\}$ and then find $r = \mathrm{ord}_n(a)$ by using a quantum computer. But now the group $\mathbb{Z}$, as well as the hidden subgroup $r\mathbb{Z}$ is infinite, and QFT for finding the generators of the hidden subgroup were described only for finite groups.

Fact: Choose $l = \lfloor 2 \log_2 n \rfloor$ and use $\mathbb{Z}_{2^l}$ instead of $\mathbb{Z}$ in the QFT method for finding the hidden subgroup $r\mathbb{Z}$ of function $\rho(x) = a^x + r\mathbb{Z}$. Then the QFT method augmented with a method for computing continued fractions is enough to reveal a generator $r\mathbb{Z}$ (see Hirvensalo (2001) and the references therein).

The above three facts form the very core of famous Shor's fast quantum algorithm for factorizing integers (Shor 1994). For further details, see Hirvensalo (2001).

6. Grover search

As an example of a *search problem* we will here consider the following: there is a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$, and we wish to find any element $\boldsymbol{x} \in \mathbb{Z}_2^n$ such that $f(\boldsymbol{x}) = 1$ (if there is any). Such an $\boldsymbol{x}$ will be called a *solution*.

If there is no knowledge about how to compute function f, but f is given as an *oracle function*, it is clear that in order to solve the problem requires 2^n calls to function f in the worst case.

Notice that a quick solution to the above search problem would yield also a rapid solution to all problems in class **NP**.

Consider a quantum superposition

$$\frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} |\boldsymbol{x}\rangle \, |0\rangle \tag{30}$$

and a potential unitary mapping U_f capable of computing f in the sense that $U_f \, |\boldsymbol{x}\rangle \, |0\rangle = |\boldsymbol{x}\rangle \, |f(\boldsymbol{x})\rangle$. This operator U_f would transform (30) into

$$\frac{1}{\sqrt{2^n}} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} |\boldsymbol{x}\rangle \, |f(\boldsymbol{x})\rangle, \tag{31}$$

which means that all the values of $f(\boldsymbol{x})$, $\boldsymbol{x} \in \mathbb{Z}_2^n$ are computed by the cost of a *single* application of U_f (this phenomenon is referred as to *quantum parallelism*).

On the other hand, the observation of the rightmost qubit of (31) will yield 1 with a probability of $\frac{T}{2^n}$ and 0 with a probability of $\frac{2^n - T}{2^n}$, where $T = |\{\boldsymbol{x} \mid f(\boldsymbol{x}) = 1\}|$ is the number of solutions. Thus if T is very small, the direct application of quantum parallelism does not offer us any good opportunity for finding a solution $\boldsymbol{x} \in \mathbb{Z}_2^n \; f(\boldsymbol{x}) = 1$ (or making a decision that no solution exists).

A natural question arising now is that does there exist some opportunity of using quantum operations cleverly in such a way, that the probability of seeing a solution (if there is any such) could be increased more rapidly, with a fewer number of calls to function f, that is, with a fewer number of applications of operator U_f.

Lov Grover has invented a method of "amplitude amplification" (Grover 1996), which we will now briefly describe.

First, it is easy to see that by using U_f we can construct a mapping V_f operating as

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

(see Hirvensalo 2001). The construction of mapping $R_{2^n} : H_{2^n} \to H_{2^n}$ defined by conditions $R_{2^n} \mid \mathbf{0}\rangle = - \mid \mathbf{0}\rangle$ and $R_{2^n} \mid \boldsymbol{x}\rangle = \mid \boldsymbol{x}\rangle$ for $\boldsymbol{x} \neq \mathbf{0}$ is not a difficult task, either. We will still need the QFT on $\mathbb{Z}_2^n$, but we have seen that it can be implemented by using operation $W_2 \otimes \ldots \otimes W_2$. We will abbreviate this operator as $W_{2^n} = W_2 \otimes \ldots \otimes W_2$.

The reader can verify or find the verification in Hirvensalo (2001) that

$$-W_{2^n} R_{2^n} W_{2^n} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} c_{\boldsymbol{x}} \mid \boldsymbol{x}\rangle = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (2A - c_{\boldsymbol{x}}) \mid \boldsymbol{x}\rangle, \tag{32}$$

where

$$A = \frac{1}{2^n} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} c_{\boldsymbol{x}}$$

is the average of the amplitudes. The operation of the unitary mapping $-W_{2^n} R_{2^n} W_{2^n}$ is called the *inversion about the average*, since it operates on a single amplitude $c_{\boldsymbol{x}}$ by reversing its sign and then adding two times the average amplitude: notice that $(2A - c_{\boldsymbol{x}}) - A = A - c_{\boldsymbol{x}}$.

The inversion about the average, together with V_f form the *Grover's iteration mapping* G_n:

$$G_n = -W_{2^n} R_{2^n} W_{2^n} V_f,$$

which can be used to amplify the amplitudes of the solutions.

Fact: Assume that a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ has $k \leq \frac{3}{4} \cdot 2^n$ solutions and $r = \lfloor \frac{\pi}{4\theta_0} \rfloor$, where $\theta_0 \in [0, \pi/3]$ satisfies $\sin^2 \theta_0 = \frac{k}{2^n}$. Then the probability that the observation of superposition

$$(G_n)^r W_{2^n} \mid \mathbf{0}\rangle. \tag{33}$$

will give a solution is at least $\frac{1}{4}$ (see Hirvensalo 2001).

In order to estimate r, the number of Grover iterations to be used, assume that k, the number of solutions is very small. Then $\frac{k}{2^n}$ is close to zero, and estimation $\sin \frac{k}{2^n} \approx \frac{k}{2^n}$ is quite precise. Therefore, $\theta_0 \approx \sqrt{\frac{k}{2^k}}$ and approximately after $\frac{\pi}{4}\sqrt{\frac{2^n}{k}}$ iterations of G_n we can find a solution with a probability of at least $\frac{1}{4}$.

Now if k, the number of solutions is a known fixed number, a solution can be found by making $O(\sqrt{2^n})$ calls to function f, which clearly outperforms

any classical method. On the other hand, if the number of solutions is not known in advance, the previous method does not give us any clue on how many times we should use the operator G_n. However, the previous methods can be combined with some methods of classical computation in order to get the following fact:

Fact: Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be any function. By using the Grover's amplitude amplification method together with a classical probabilistic algorithm, it can be decided whether a solution to f exists by using $O(\sqrt{2^n})$ queries to f. Moreover, if solutions exists, one such can be found by using $O(\sqrt{2^n})$ queries to f.

Of course a natural question after the previous fact is that does there exist any faster quantum method to decide whether a solution exists.

Fact: Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a *black-box function*, i.e., it is not known how to compute f but its values are received just as an oracle call. Then, any quantum algorithm with decides (with nonvanishing correctness probability) whether there exists an element $\boldsymbol{x} \in \mathbb{Z}_2^n$ such that $f(\boldsymbol{x}) = 1$, requires $\Omega(\sqrt{2^n})$ calls to function f (Beals et al. 1998; Bennett et al 1997; Hirvensalo 2001).

Folklore: The above fact implies that quantum computers cannot solve **NP**-complete problems in polynomial time.

Fact: The above fact does not imply the above "folklore", it only gives a strong reason to believe on that. Recall that it is not known even whether the ordinary computers can solve **NP**-problems in polynomial time! The above fact talks merely about solving whether a *black-box* -function f has a solution or not – it does not refer to any computable function. In fact, it is not known how much the (known) algorithm for computing f can ease the decision "is there a solution for f or not" over the exhaustive searching.

Acknowledgement

Supported by the Academy of Finland under grant 44087.

References

Beals R, Buhrman H, Cleve R, Mosca M and de Wolf R (1998) Quantum lower bounds by polynomials. Proceedings of the 39th IEEE Conference on Foundations of Computer Science, pp. 352–361

Bennett CH, Bernstein E, Brassard G and Vazirani UV (1997) Strengths and weaknesses of quantum computation. SIAM Journal of Computing 26(5): 1510–1523

Grover LK (1996) A fast quantum mechanical algorithm for database search. Proceedings of STOC, pp. 212–219

Hirvensalo M (2001) Quantum Computing. Springer

Shor PW (1994) Algorithms for quantum computation: Discrete log and factoring. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 20–22