STUDIA INFORMATICA 2002
Volume 23 Number 2A (48)

Jerzy KLAMKA
Instytut Informatyki Teoretycznej i Stosowanej PAN

QUANTUM SEARCH ALGORITHM[1]

Summary. Recently, it was realized that use of the properties of quantum mechanics might speed up certain computations. It now appears that, at least theoretically, quantum computations may be much faster than classical computations for solving certain problems including for example search problems. In the present paper the fundamental Grover's search algorithm of quantum computation is discussed. Fundamental quantum operators for Grover's search algorithm are presented. Moreover, several remarks and comments concerning quantum computations are also given.

KWANTOWY ALGORYTM POSZUKIWAŃ

Streszczenie. W ostatnim czasie wykazano, że zastosowanie pewnych wybranych metod mechaniki kwantowej może znacznie przyspieszyć niektóre czasochłonne obliczenia. Teoretycznie, obliczenia kwantowe mogą być przeprowadzane znacznie szybciej niż metodami klasycznymi, czego przykładem jest problem poszukiwania. W artykule przedstawiono algorytm poszukiwań Grovera stosowany w obliczeniach kwantowych. Określono operacje kwantowe wykorzystywane w algorytmie Grovera. Ponadto przedstawiono wiele uwag i komentarzy dotyczących zgadnień obliczeń kwantowych.

[1]This work was supported by Komitet Badań Naukowych under Grant 7 T11C 017 21

1. Introduction

Recently, it was realized that use of the properties of quantum mechanics might speed up certain computations [1-10]. Interest has since been growing in the area of quantum computation. These quantum computations can be modeled formally by defining quantum Turing machine, which is able to be in the superposition of many states. It now appears that, at least theoretically, quantum computations may be much faster than classical computations for solving certain problems [4], [5], [6], [7], including for example prime factorization [7], [5]. Moreover, it should be pointed out, that the quantum computations offer powerful methods of encoding and manipulating information that are not possible within a classical framework.

Quantum computers are hypothetical machine that use principles of quantum mechanics for their basic operations. There are a number of differences between quantum and classical computers. In particular, a property of quantum systems that plays a crucial role is the so called entanglement or non-classical correlation between quantum systems [7]. In other words this means, that the quantum state cannot be written as a product of the state of two individual qubits. Another important property is the high dimensionality of quantum systems. The dimension of the joint quantum state space of n objects grows exponentially with n, whereas classically the dimension of the joint state space objects only grows linearly. The quantum computation algorithms make critical use of this extra dimensionality [7].

In the development of computer science as a scientific field there was a time period during which experimental research were based on macrosystems like relays, then electronics tubes, transistors and recently large scale and very large scale integrated systems. Research studies directed towards computer nanosystems have been initiated by focusing attention on the possibility of using atoms and molecules as coding symbols for computer programs.

Complete definition of the state of a particle requires not only a specification of its space-time coordinates but also of the direction of the spin vector, specifying the direction of spin, either up or down. The particular behavior of atomic spin called nuclear magnetic resonance is a fundamental physical phenomenon taken into account in recent research on quantum computers [7]. This phenomenon is based on resonance absorbency of electromagnetic energy taking place in some solid bodies, liquids and gases placed in constant external magnetic field and perturbed by impulsive varying magnetic field with properly chosen frequencies. In the case of atoms creating molecules the behavior of their spins depends on the neighboring atoms. It enables to create several logic quantum gates, which are used to organize quantum computation processes in quantum computers [7], [9].

Combinatorial search problems are among the most difficult computational tasks; the time required to solve them often grows exponentially with the size of the problem. Many

such problems have a great deal of structure, allowing heuristic methods to greatly reduce the rate of exponential growth. Quantum computers offer a new possibility for utilizing this structure with quantum parallelism, i.e., the ability to operate simultaneously on many classical search states, and interference among different paths through the search space.

In the present paper the fundamental Grover's search algorithm [1], [3], [4] of quantum computation is discussed. Fundamental quantum operators for Grover's search algorithm are presented. Moreover, several remarks and comments concerning quantum computations are also given.

2. Preliminaries

In a quantum computer, the logic circuits are represented by unitary matrices that act on a certain number qubits in each step.

Let $F_2=\{0,1\}$ stands for the binary field with two elements 0 and 1, and F_2^n is the n-dimensional vector space over the binary field F_2. Moreover, let $f: F_2^n \to F_2$ be the Boolean function with n independent Boolean variables $x_1,x_2,...,x_i,...,x_n$, where $x_i \in F_2$, for i=1,2,...,n and let us shortly denote $x=(x_1,x_2,...,x_i,...,x_n) \in F_2^n$.

The classical search problem can be formulated as follows: find certain solution $y \in F_2^n$ such that f(y)=1. Let $k=\{x \in F_2^n: f(x) = 1\}$ denotes the number of solutions. The Grover's quantum algorithm for finding certain solution $y \in F_2^n$ can be generally viewed as iterative amplitude amplification.

The quantum search algorithm is a sequence of unitary operations on pure quantum state, followed by a measurement operation. The three elementary unitary operations needed are the following. First is the creation of a superposition in which the amplitude of the system being in any of the basic states of the system is equal; second is the Hadamard transformation operation, and the third the selective rotation of the phases of states.

3. Quantum operators for Grover's search algorithm

As it was mentioned at the end of the previous section, in order to describe detaily the Grover's quantum search algorithm it is necessary to introduce Hadamard transformation. First of all, let us recall, that the element $x=(x_1,x_2,...,x_i,...,x_n) \in F_2^n$ has a very natural quantum representation by tensor product of n qubits $|x_i\rangle \in C^2$, i=1,2,...,n,

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_i\rangle \otimes ... \otimes |x_n\rangle = |x_1\rangle |x_2\rangle ... |x_i\rangle ... |x_n\rangle \in C^{2^n}$$

Hadamard transform H which is a linear transform acting on simple qubit $|x_i\rangle \in C^2$, can be implemented by the 2×2-dimensional so called Hadamard matrix. Therefore, Hadamard transform H is given by

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

Let $H_n=H\otimes H\otimes ...\otimes H$ (n-times) denotes tensor product of the Hadamard transform. Then, using the formula defining Hadamard transform, for $|x\rangle = |x_1\rangle|x_2\rangle...|x_i\rangle...|x_n\rangle \in C^{2^n}$ we have the following result:

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in F_2^n}(-1)^{xz}|z\rangle$$

where xz denotes the standard scalar product in the vector space C^n i.e.,

$$xz=x_1z_1+x_2z_2+...+x_iz_i+...+x_nz_n.$$

Moreover, it should be pointed out, that for any natural number n, the $2^n\times 2^n$-dimensional matrix H_n is also called a Hadamard matrix.

The other quantum operator needed for the Grover's quantum search algorithm is the so called query operator V_f, which encodes the value of the function f(x) in the sign. A query operator V_f is a linear mapping defined by

$$V_f|x\rangle|2^{-0,5}(|0\rangle-|1\rangle)\rangle = |x\rangle|2^{-0,5}(|0\rangle-|1\rangle)\oplus f(x)\rangle = (-1)^{f(x)}|x\rangle\, 2^{-0,5}(|0\rangle-|1\rangle)$$

where symbol $\oplus$ means as usually the addition modulo 2, and $2^{-0,5}(|0\rangle-|1\rangle)$ is the so called target qubit.

We will also need a quantum operator R_n, which reverses the sign of $|0\rangle$ and is defined on n qubits, which represent element $x=(x_1,x_2,...,x_i,...,x_n)\in F_2^n$ and operating as

$$R_n|0\rangle = -|0\rangle \text{ and } R_n|x\rangle = |x\rangle, \text{ if } x\neq 0.$$

It is well known, that we can easily express quantum operator R_n as $2^n\times 2^n$-dimensional matrix R_n defined as follows

$$R_n = \begin{bmatrix} -1 & 0 & 0 & K & 0 \\ 0 & 1 & 0 & K & 0 \\ 0 & 0 & 1 & K & 0 \\ M & M & M & O & M \\ 0 & 0 & 0 & K & 1 \end{bmatrix}$$

The basic quantum operator needed in the Grover's search algorithm is the quantum amplification amplitude operator

$$G_n = - H_nR_nH_nV_f$$

working on n qubits, which represent element $x=(x_1,x_2,...,x_i,...,x_n)\in F_2^n$. Linear operator $H_nR_nH_n$ can be written in quite a simple form as $2^n\times 2^n$-dimensional matrix of the following form:

$$H_nR_nH_n=\begin{bmatrix} 1-\frac{2}{2^n} & -\frac{2}{2^n} & -\frac{2}{2^n} & K & -\frac{2}{2^n} \\ -\frac{2}{2^n} & 1-\frac{2}{2^n} & -\frac{2}{2^n} & K & -\frac{2}{2^n} \\ -\frac{2}{2^n} & -\frac{2}{2^n} & 1-\frac{2}{2^n} & K & -\frac{2}{2^n} \\ M & M & M & O & M \\ -\frac{2}{2^n} & -\frac{2}{2^n} & -\frac{2}{2^n} & K & 1-\frac{2}{2^n} \end{bmatrix}$$

Quantum operator $H_nR_nH_n$ can also be expressed as

$$H_nR_nH_n = I - P_n$$

where I is $2^n\times 2^n$-dimensional identity matrix and P_n is $2^n\times 2^n$-dimensional projection matrix, whose every entry is 2^{1-n}.

In fact, it is quite an easy task to verify that linear operator P^n represents a projection into one-dimensional linear subspace generated by 2^n-dimensional vector of the following form:

$$v=\frac{1}{\sqrt{2^n}}\sum_{x\in F_2^n}|x\rangle$$

The operator $-H_nR_nH_n$ is also called inversion about average: it operates on a single amplitude by multiplying it by -1 and adding two times the average.

4. Grover's search algorithm

Quantum mechanical system can be in a superposition of computational states and hence simultaneously carry out multiple computations in the same computer. In the last few years there has been extensive research on how to use this quantum parallelism to carry out meaningful computations. In any quantum mechanical computation the system is initialized to a state that is easy to prepare and caused to evolve unitarily. The answer to the computational problem is deduced by a final measurement that projects the system onto a unique state. The amplitude (and hence the probability) of reaching a specified final state depends on the interference of all paths that take it from the initial state to the final state. Thus the quantum system is very sensitive to any magnitude of phase disturbances that affect any of the paths leading to the desired final state. Therefore, as a result, quantum mechanical algorithms are very delicate, and it is generally believed that an actual implementation would need an elaborate procedure for correcting errors [7], [8].

The Grover's quantum search algorithm can be represented as searching an image of computable Boolean function, which can only be computed forward, but whose inverse

cannot be directly computed. Problems of this type are very common. One important example, from cryptography, is searching for the key of the data encryption standard. Other examples are solutions of NP-complete problems, which include virtually all the difficult computing problems in practice. Grover's quantum search algorithm is mainly based on the following fundamental result.

Theorem. Let Boolean function $f: F_2^n \to F_2$ be such that there are k elements $x=(x_1,x_2,...,x_i,...,x_n)\in F_2^n$ satisfying f(x) = 1. Moreover, let us assume that $0<k\leq 3\cdot 2^{n-2}$, and let $\theta_0\in[0,\pi/3]$ be chosen such that $\sin^2\theta_0 = k2^{-n}\leq 0{,}75$. Then after $\text{int}[\pi/4\theta_0]$ iterations of G_n, on an initial superposition

$$v = \frac{1}{\sqrt{2^n}} \sum_{x\in F_2^n} |x\rangle$$

the probability of seeing a solution is at least 0,25.

From the general theorem stated above two corollaries follow which show the special cases of quantum search algorithm.

Corollary. If number of solution k = 1 and dimensionality n is large, then using $O(2^{0,5n})$ queries, we can find a solution $y\in F_2^n$ with nonvanishing probability, which is essentially better than any classical randomized algorithm can do.

Corollary. If $k = 2^{n-2}$, then $\sin^2\theta_0 = 0{,}25$, so $\theta_0 = \pi/6$. Therefore, the probability of seeing a solution $y\in F_2^n$ after one single iteration of linear operator G_n is

$$\sin^2(3\theta_0) = \sin^2(\pi/2) = 1$$

Thus for $k = 2^{n-2}$ we can find a solution $y\in F_2^n$ with certainty using linear operator G_n only once.

Remark. It should be stressed, that in a typical situation we, unfortunately, do not know the value of the solution k in advance. Therefore, in this case a certain simplified version of the Grover's search algorithm can be used. The main advantage of this modified version is that it enables to find the required solutions $y\in F_2^n$ even if the number of solutions k is not known.

Taking into account the theorem and corollaries given above it is possible to present step by step Grover's quantum search algorithm.

Step 1. Compute the integer number $r = \text{int}[\pi/4\theta_0]$, where the angle $\theta_0\in[0,\pi/3]$ is determined by the equality: $\sin^2\theta_0 = k2^{-n} \leq 0{,}75$.

Step 2. Prepare the initial superposition

$$v = \frac{1}{\sqrt{2^n}} \sum_{x\in F_2^n} |x\rangle$$

by using Hadamard transform H_n.

Step 3. Apply operator G_n r times.

Step 4. Observe to get some $y \in F_2^n$.

Quantum search algorithm presented above is the basic version, which has been modified in several directions (see e.g., [2], [3], [7], [10] for more details).

The importance of Grover's result stems from the fact that it proves the enhanced power of quantum computers compared to classical ones for a whole class of computational problems, for which the bound on the efficiency of classical algorithm is known.

A large number of results followed the Grover's quantum search algorithm. These include a proof that Grover's algorithm is an efficient as theoretically possible [10]. Moreover, a variety of applications in which the algorithm is used in the solution of other problems is given in the monograph [7]. Recently an experimental implementation of fast quantum searching algorithm using a nuclear magnetic resonance (NMR) techniques has been discussed in the paper [3].

Several generalizations of the Grover's original search algorithm have been recently published in many papers. For example in the monograph [7] the case of more than one marked solution of the search problem is discused.

Moreover, in the recent paper [6] it was shown that the quantum search algorithm can be also implemented by replacing the standard Hadamard transformation by almost any quantum mechanical operation. Since all quantum mechanical operations are unitary, this means that almost any quantum mechanical system can be used in quantum computations. All that is needed is a valid quantum mechanical operation and a way of selectively inverting the phase of states. Meaningful computation can hence be carried out on the basis of universal properties of quantum mechanical operations. This for example implies that the quantum search algorithm is surprisingly robust to certain kinds of perturbations. Hence, this observation leads to several new applications of quantum search algorithm where it improves the number of steps by a square root.

Moreover, it is possible to generalize the Grover's quantum search algorithm by allowing for an arbitrary complex initial amplitude distribution. The paper [2] presents an exact solution for the time evolution of the amplitudes under these general initial conditions. The case of an arbitrary initial amplitude distribution is particularly relevant in the presence of unitary errors in the gates implementing the initialization step. Such errors can result in a deviation from the uniform initial amplitude distribution, which is assumed in the usual treatment of the Grover's quantum search algorithm.

5. Conclusions

In conclusion, designing a useful quantum computer has been a rather very difficult task for at least two reasons. First, because the physics to implement this is different from what most known devices use and so it is not clear what its structure should be like. The second reason is that once such a computer is built, few applications for this are known where it will have a clear advantage over existing computers. This paper has given a general framework for the search algorithm where the quantum computer would have an advantage.

REFERENCES

1. Boyer M., Brassard G., Hoyer P., and Tapp A.: Tight bound on quantum searching. Proceedings of the Fourth Workshop on Physics and Computation, 1996, pp.36-43.
2. Biham E., Biham O., Biron D., Grassl M., Lidar D.: Grover's quantum search algorithm for an arbitrary initial amplitude distribution. Physical Review, 1999, Vol. 60, No 4, pp. 2742-2745.
3. Chuang I. L., Gershenfeld N., Kubinec M.: Experimental implementation of fast quantum searching. Physical Review Letters, 1998, Vol. 80, No 15, pp. 3408-411.
4. Grover L. K.: A fast quantum mechanical algorithm for database search. Proceedings of the 28 Annual ACM Symposium on the Theory of Computing, 1996, pp.212-219.
5. Grover L. K.: Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters, 1997, Vol. 79, No 2, pp.325-328.
6. Grover L. K.: Quantum computers can search rapidly by using almost any transformation. Physical Review Letters, 1998, Vol.80, No 19, pp.429-4332.
7. Hirvensalo M.: Quantum Computing. Springer-Verlag, Berlin 2001.
8. Hogg T.: Quantum computing and phase transitions in combinatorial search. Journal of Artificial Intelligence Research, 1996, Vol. 4, No 1, pp.91-128.
9. Węgrzyn S., Klamka J.: Kwantowe systemy informatyki. ZN Pol. Śl. Studia Informatica, Vol.21, No 1(39), Gliwice 2000.
10. Zalka C.: Grover's quantum searching algorithm is optimal. Physical Review, 1999, Vol.60, No 4, pp.2746-2751.

Recenzent: Prof. dr hab. inż. Zbigniew Czech

Wpłynęło do Redakcji 4 kwietnia 2002 r.

Streszczenie

Podstawowym zagadnieniem związanym z obliczeniami wykonywanymi za pomocą komputerów jest zaproponowanie odpowiedniego algorytmu obliczeniowego. Komputer kwantowy przeprowadza obliczenia w oparciu o specjalne algorytmy obliczeniowe nie stosowane w informatyce klasycznej. Algorytmy te dostosowane do możliwości obliczeniowych komputera kwantowego w istotny sposób wykorzystują prawa mechaniki kwantowej, a w szczególności zjawisko superpozycji stanów kwantowych.

Zasadniczym problemem klasycznej teorii algorytmów jest określenie złożoności obliczeniowej danego algorytmu. Ogólnie klasyczne algorytmy obliczeniowe dzieli się na dwie podstawowe grupy: algorytmy o wielomianowej złożoności obliczeniowej oraz algorytmy o ekspotencjalnej złożoności obliczeniowej. W przypadku algorytmów kwantowych różnica pomiędzy tymi dwoma złożonościami obliczeniowymi nie ma tak istotnego znaczenia jak w przypadku algorytmów klasycznych.

Do najważniejszych algorytmów kwantowych należą: algorytm faktoryzacji liczb naturalnych zaproponowany w 1993 roku przez Shora oraz algorytm poszukiwań opracowany przez Grovera w 1997 roku.

W 1997 roku Grover zaproponował kwantowy algorytm wyszukiwania informacji w dużych zbiorach danych. Problem polega na wyszukaniu określonego elementu $x_j=y$ w nieuporządkowanym zbiorze danych zawierającym N elementów $\{x_i, i=1,2,3,...,N\}$. Przykładowo, może to być wyszukanie w spisie telefonów danego numeru telefonu nie znając nazwiska abonenta.

Klasyczne algorytmy poszukiwań potrzebują średnio $^N/_2$ kroków na wyszukanie danej informacji w zbiorze danych zawierającym N elementów. Algorytm kwantowy poszukiwań zaproponowany przez Grovera jest w tym przypadku znacznie bardziej efektywny i potrzebuje średnio jedynie $\sqrt{N}$ kroków na wyszukanie właściwego elementu w zbiorze N elementów.

Algorytm Grovera może być uogólniony i zastosowany do jednoczesnego poszukiwania kilku wybranych elementów w nieuporządkowanym zbiorze danych oraz do wyszukiwania największego lub najmniejszego elementu w zbiorze danych.