From classical computing to quantum computing

Adina BĂRÎLĂ
"Stefan cel Mare" University of Suceava
str.Universităţii nr.13, RO-720229 Suceava
adina@eed.usv.ro

***Abstract*— Quantum computing is a new field of science which uses quantum phenomena to perform operations on data. The paper presents the basic theory of quantum computing and the recent results in quantum algorithm development.**

Keywords—quantum computing; qubit; quantum algorithm

I. INTRODUCTION

In the last years the importance of quantum computing has significantly increased due to both continuously shrinking of the size of silicon-based integrated circuits and the results in quantum algorithm development. The Moore's Law is well known today and it says that the number of transistors on integrated circuits doubles approximately every two years. But, it cannot continue forever. In 2005 Gordon Moore noted that transistors would eventually reach the limits of miniaturization at atomic levels. Quantum computing offers a path forward by taking advantage of quantum mechanical properties. So, the rapid progress of computer science led to a corresponding evolution of computation from classical computation to quantum computation.

Quantum computing is the new field of science which uses quantum phenomena to perform operations on data. The goal of quantum computing is to find algorithms that are considerably faster than classical algorithms solving the same problem.

II. HISTORY OF QUANTUM COMPUTING

The origin of quantum computing is considered to be the Richard Feynman's idea for constructing a computer to simulate the quantum systems[1]. In his paper [2], published in 1982, Feynman argued that only a quantum computer could efficiently simulate the quantum systems. His observation led to the speculation that, in general, the computations could be done more efficiently if using the quantum mechanical effects. Paul Benioff showed that quantum computation is at least as powerful as classical computation [3].

In 1985 David Deutsch introduced a model for quantum computation: a quantum version of Turing machine [4]. He showed that any physical process, in principle, could be perfectly modeled by a quantum computer. Also he demonstrated that the universal quantum computer can do things that the universal Turing machine cannot.

David Deutsch invented the first quantum algorithm which solves a computational problem in a more efficient way that classical computation. In 1989, in [5], Deutsch described a second model for quantum computation: quantum circuits. He demonstrated that quantum gates can be combined to achieve quantum computation in the same way that Boolean gates can be combined to achieve classical computation.

The Deutsch-Jozsa algorithm was designed in 1992 [1] and showed the computational advantage of quantum computing over classical computing.

In 1994, Peter Shor described a polynomial time quantum algorithm for factoring integers [6] and in 1996 Lov Grover invented the quantum database search algorithm [7].

From this year, the research in quantum computing field has accelerated, computer scientists trying to build quantum computers and find other quantum algorithms.

III. BASIC CONCEPTS

A. Qubits

The fundamental unit of quantum information is called quantum bit or qubit [8]. A qubit can exist in a state corresponding to the logical state 0 or 1 as in a classical bit. These states, written $|0\rangle$ and $|1\rangle$, are called basis states. Unlike the classical bit, the general state of a qubit is a linear combination - or a superposition- of states $|0\rangle$ and $|1\rangle$:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

The amplitudes α and β are complex numbers and they have to satisfy the relation:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

In other words, a qubit can exist as a zero, a one, or simultaneously as both 0 and 1 (when both α and β are non-zero).

A system consisting of *n* qubits has 2^n basis states, writen $|0\ 0\ ..\ 0\rangle$, …, $|1\ 1\ ..\ 1\rangle$. The general state of an n-qubit system is a superposition of all 2^n basis states:

$$|\psi\rangle = \sum_{k=0}^{2^n-1} c_k |k\rangle \tag{3}$$

where:

$$|k\rangle = |k_{n-1}\rangle \ldots |k_1\rangle |k_0\rangle \tag{4}$$

This paper was supported by the project "Sustainable performance in doctoral and post-doctoral research PERFORM - Contract no. POSDRU/159/1.5/S/138963", project co-funded from European Social Fund through Sectorial Operational Program Human Resources 2007-2013.

978-1-4799-5094-2/14/$31.00 ©2014 IEEE

with $|k_j\rangle$ representing the state of qubit j. The amplitudes must satisfy:

$$\sum_{k=0}^{2^n-1} c_k |k\rangle = 1 \quad (5)$$

Like the single-qubit system, a n-qubit register can store simultaneously all basic states.

B. Quantum gates

Evolution of a quantum system can be described by a unitary transformation U. A unitary transformation that acts on a small number of qubits is called a gate, in analogy to classical logic gates. Unlike the logic gates, a quantum gate has the same number of inputs and outputs. A one-qubit elementary gate is described by a 2x2 matrix:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (6)$$

which transforms $|0\rangle$ into $a|0\rangle+b|1\rangle$ and $|1\rangle$ into $c|0\rangle+d|1\rangle$.

One-qubit elementary gates:

- Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (7)$$

- Pauli gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (8)$$

- Phase shift gates

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad (9)$$

Two-qubit elementary gates:

Controlled-NOT (CNOT) gate is the quantum generalization of the XOR classical gate. It has two input qubits, the control and the target qubit. The target qubit is flipped only if the control qubit is set to 1.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (10)$$

Generally, if U is a one-qubit gate with matrix representation

$$U = \begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix} \quad (11)$$

then the controlled-U is a two-qubit gate with matrix representation:

$$C(U) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{pmatrix} \quad (12)$$

The first qubit is the control qubit.

The SWAP gate is the quantum generalisation of the CROSSOVER clasical gate. It swaps the quantum states of two qubits.

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (13)$$

The Cph (controlled phase) gate acts on two qubits and it has no classical equivalent.

$$U_{cph}(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(i\phi) \end{pmatrix} \quad (14)$$

C. Measurement

Measurement is the only nonreversible operation which can be applied to a quantum state. Measurement collapses a quantum state into one of the possible basis states, so measurement is a destructive operation. If a qubit is in the state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and a measure is performed, it obtains 0 with probability α^2 (the state of qubit become $|0\rangle$) and 1 with probability β^2 (the state of qubit become $|1\rangle$).

D. Quantum parallelism

Quantum parallelism arises from the fact that the qubit exists in multiple states simultaneously. Due to the superposition principle and the linearity of operations, a quantum computer is able to evaluate a function for many inputs simultaneously. The term was coined by David Deutsch [4], so as to distinguish it from classical parallel computation in standard computers. He presented an example which showed that a single quantum computation may suffice to state whether a function is constant or not. Given an unknown one-bit function f:{0,1} → {0,1}, Deutsch algorithm decides if *f* is constant or balanced in a single quantum computation. The quantum circuit looks like in Fig.1.

U_f transformation is defined by:

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle \quad (15)$$

The quantum states are:

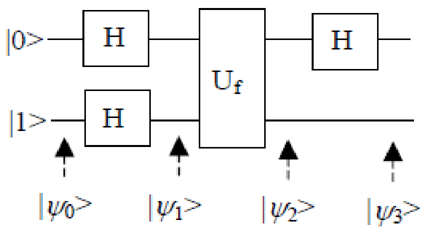

Fig. 1 - Deutsch circuit

$$|\Psi_0\rangle = |0\rangle|1\rangle \quad (16)$$

$$|\psi_1\rangle = H|0\rangle H|1\rangle$$

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

$$= \frac{1}{2}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle(|0\rangle - |1\rangle) \quad (17)$$

$$|\psi_2\rangle = U_f|\psi_1\rangle \quad (18)$$

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

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

The last qubit is ignored. The Hadamard transformation transforms the state of the first qubit into:

$$(-1)^{f(0)}|f(0) \oplus f(1)\rangle$$

f(0) ⊕ f(1) = 0 if and only if f(0)=f(1) and f(0) ⊕ f(1) if and only if f(0) ≠ f(1). So, when we measure 0, f is certainly constant and when we measure 1, f is balanced.

Deutsch showed that a quantum algorithm can evaluate f(0) ⊕ f(1) without compute f(0) and f(1).

Although a quantum computer can perform massive parallel computations, to compute a function simultaneously on many inputs, measurement collapses the superposition of all those states in one of the basis states.

IV. QUANTUM ALGORITHMS

A. Grover algorithm

In 1996 Lov Grover presented an algorithm for solving follow problem [7]: "Let a system have $N = 2^n$ states which are labelled $S_1, S_2, \ldots S_N$. These 2^n states are represented as *n* bit strings. Let there be a unique state, say S_n, that satisfies the condition $C(S_n) = 1$, whereas for all other states S, $C(S) = 0$ (assume that for any state S, the condition $C(S)$ can be evaluated in unit time). The problem is to identify the state S_n." In other words, he presented an algorithm for searching an object in an unsorted list with N objects. In classical computation, searching an unsorted database cannot be done in less than linear time. Grover's algorithm has complexity $O(N^{1/2})$.

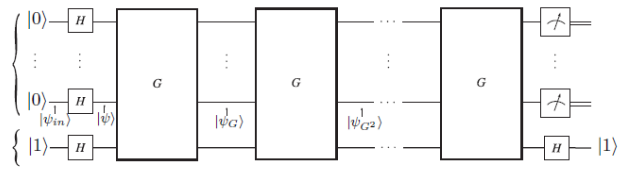

Fig. 2 - Grover circuit [9]

The circuit for implementing search has two registers: the first register has n qubits and is initialized in the state |00..00⟩, the last has one qubit initialized in the state |1⟩.

$$|\psi_1\rangle = \left(H^{\otimes n} \otimes H\right)|0\rangle_n|1\rangle$$

$$= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n\left(|0\rangle - |1\rangle\right)/\sqrt{2} = |\psi\rangle\left(|0\rangle - |1\rangle\right)/\sqrt{2} \quad (19)$$

where

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle_n \quad (20)$$

The Grover iteration (G) consists of two transformations:

- the first transformation marks the searched element

- the second transformation increases the probability amplitude of searched quantum state

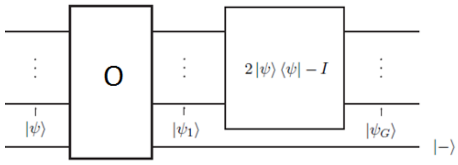

Fig. 3 - First Grover iteration [9]

The unitary transformation is called "oracle" and is defined by:

$$O|x\rangle_n|y\rangle = |x\rangle_n |y \oplus f_0(x)\rangle \qquad (21)$$

where

- $|x\rangle$ is a state of the first register ($x \in \{0, 1, \ldots, 2^n-1\}$)
- $|y\rangle$ is a state of the second register ($y\in \{0,1\}$)
- f is a boolean function, $f: \{0,1\}^n \rightarrow \{0,1\}$, $f_0(x)=1$ if $x=x_0$ is the searched element, $f_0(x)=0$, otherwise.

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle \qquad (22)$$

After O is applied the first register state is a superposition of all the basis states, but the amplitude of searched element is negative while all others are positive.

The second transformation is $2|\psi\rangle\langle\psi| - I$ and is called inversion about the mean [9] or diffusion operator. After this transformation the first register state becomes

$$|\psi_G\rangle = \frac{2^{n-2}-1}{2^{n-2}} \cdot \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} x + \frac{2}{\sqrt{2^n}}|x_0\rangle \qquad (23)$$

The amplitude of the searched element increased with $O(1/N^{1/2})$, while the amplitude of unmarked states decreased.

The Grover operator is performed round($\frac{\pi}{4}\sqrt{N}$) times and then a measurement is performed. The outcome will be the searched value with probability approaching 1

B. Shor algorithm

In 1994 Peter Shor [6] [10] invented a quantum algorithm for solving the problem: given a composite $N\in\mathbb{N}$, determine the prime factor of N. His algorithm is used for numbers which are not prime, even or power of prime numbers. For such number there are efficient classical algorithms.

The algorithm is as follows:

1.choose a random x <N

2.compute gcd(x,N)

3.if gcd(x,N) $\neq 1$ then there is a nontrivial factor of N and the algorithm ends

4.if gcd(x,N) = 1, find the order r of x (modulo N)

5.if r is even, compute gcd($x^{r/2}\pm 1$, N). Since $(x^{r/2}-1)(x^{r/2}+1) = x^r-1 \equiv 0 \pmod N$, gcd($x^{r/2}$-1,N) and gcd($x^{r/2}$-1, N) are factors of N and the algorithm ends

6.if r is odd, go to step1

The order of x modulo N is the smallest positive integer r for which $x^r \equiv 1 \bmod N$. The algorithm presented by Shor reduces the factoring problem to the order-finding problem for which there isn't an efficient classical algorithm. The quantum algorithm to compute the order has the following circuit:

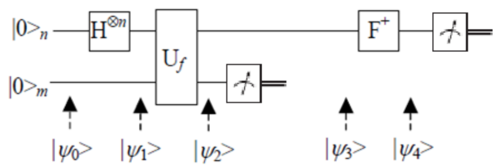

Fig. 4 - Shor circuit [10]

where U_f is the unitary operator

$$U_f\left(|j\rangle_n|k\rangle_m\right) = |j\rangle_n\left|x^j \bmod N\right\rangle_m \qquad (24)$$

The first register has n qubits ($N^2 \leq 2n < 2N^2$). If r is the power of 2 then m=n.

The states are as following:

$$|\psi_0\rangle = |0\rangle_n|0\rangle_m \qquad (25)$$

$$|\psi_1\rangle = H^{\otimes n}|0\rangle_n|0\rangle_m = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle_n|0\rangle_m \qquad (26)$$

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}U_f\left(|j\rangle_n|0\rangle_m\right)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle_n\left|x^j \bmod N\right\rangle_m \qquad (27)$$

Since $x^j \equiv x^{j+r} \bmod N$, the function $f(x,j) = x^j \bmod N$ is periodic and has the period r.

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{b=0}^{r-1} \sum_{a=0}^{2^n/r-1} |ar+b\rangle_n |x^{ar+b} \bmod N\rangle_m$$

$$= \frac{1}{\sqrt{2^n}} \sum_{b=0}^{r-1} \sum_{a=0}^{2^n/r-1} |ar+b\rangle_n |x^{b} \bmod N\rangle_m \quad (28)$$

A measurement is performed and, assuming it measures x^{b0}, the quantum state becomes:

$$|\psi_3\rangle = \sqrt{\frac{r}{2^n}} \sum_{a=0}^{2^n/r-1} |ar+b_0\rangle_n |x^{b_0} \bmod N\rangle_m \quad (29)$$

$$|\psi_4\rangle = F^+|\psi_3\rangle = \sqrt{\frac{r}{2^n}} \sum_{a=0}^{2^n/r-1} F^+|ar+b_0\rangle_n |x^{b_0} \bmod N\rangle_m$$

$$= \frac{1}{\sqrt{r}} \left[\sum_{j=0}^{2^n-1} S_j e^{-\frac{2\pi i j b_0}{2^n}} |j\rangle_n \right] |x^{b_0} \bmod N\rangle_m$$

$$|\psi_4\rangle = \frac{1}{\sqrt{r}} \left[\sum_{k=0}^{r-1} e^{-\frac{2\pi i k b_0}{r}} \left| \frac{k \cdot 2^n}{r} \right\rangle_n \right] |x^{b_0} \bmod N\rangle_m \quad (30)$$

Measuring the first register, we get the value $m=k_0 2^n/r$, where k_0 can be any value between 0 and r-1 with equal probability. If m=0, the algorithm must be run again. If m≠0, using classical algorithms, the rational value of k_0/r is obtained. The denominator if this value is the searched order of x.

V. PROGRESS IN QUANTUM ALGORITHMS

The two quantum algorithms invented by Grover and Shor have remained the most spectacular quantum algorithms. In the last years many quantum algorithms have been developed but they are generalisations and applications of the two results.

Boyer, Brassard, Høyer and Tapp [11][12] generalized Grover's algorithm for the case N isn't a power of 2. Also, they generalised the algorithm for the case when the search problem has t solutions (t known and t≠0), finding one values in $round\left(\frac{\pi}{4}\sqrt{\frac{N}{t}}\right)$ iterations. Another generalisation was done by Long, Li, Zhang şi Niu [13] who replaced Grover operators by arbitrary unitary and arbitrary phase rotation operators. Ashley Montanaro observed that in real life it is rarely necessary to search in a completely unstructured database, so he considered the problem of search when it is given an advice as to where the marked element might be located. The "advice" is a probability distribution $\mu = (p_y)$, $y \in \{1,\dots,n\}$, where p_y is the probability that f(y)=1 [14]. André J. Hoogstrate and Chris A.J. Klaassen showed that Montanaro's algorithm can speed up the search within a finite population for a single particular individual or item with rare characteristic [15]. This is very useful for optimizing security screening applications.

Brassard, Hoyer and Tapp [16] developed a quantum algorithm to solve the of counting the number of elements that satisfy some conditions instead of finding such an element. Their algorithm uses both Grover's iteration and the quantum Fourier transform.

Based on the generalized search algorithm, Dürr and Høyer [17] gave a quantum algorithm for finding the minimum in an unsorted list with $O(N^{1/2})$ complexity. Ahuja and Kappor [18] presented a quantum algorithm for finding maximum in an unsorted list.

Many applications of quantum algorithms have been developed in the graphs field. Dürr, Heiligman, Hoyer and Mhalla [19] presented some quantum algorithms for connectivity, minimum spanning tree and the single source shortest path. They showed that the algorithm for finding a minimum spanning tree has $O(n^{3/2})$ complexity in the matrix model and $O(\sqrt{nm})$ complexity in the adjacency list model. (where n is the number of vertices and m is the number of edges). The query complexity of single source shortest path algorithm is $O(n^{3/2}\log^2 n)$ in the matrix model and $O(\sqrt{nm})$ in the adjacency list model. The complexity of the connectivity algorithm is $O(n^{3/2})$ in the matrix model. In the adjacency list model, the complexity is O(n) for undirected graphs, respectively $O(\sqrt{nm})$ for directed graphs.

Magniez, Santha and Szegedy [20] presented two algorithms for finding a triangle in a n-vertex undirected graph. The first uses quantum search and gives the result in $O(n^{10/7})$ queries. The second is based on quantum walks and gives the result in $O(n^{13/10})$ queries. A. Belovs [21] designed a quantum algorithm for the triangle problem with $O(n^{35/27})$ query complexity. In 2013, Lee, Magniez and Santha [22] developed a better algorithm, with $O(n^{9/7})$ query complexity.

In 2007, Sebastian Dőrn studied the graph traversal problem on quantum computers. In his paper [23], Dőrn showed that the algorithm for Eulerian graph problem has a $O(\sqrt{n})$ query complexity in the adjacency list model and $O(n^{1.5})$ query complexity in matrix model. The quantum query complexity of Hamiltonian circuit algorithm is $O(n^{2n/(n+1)})$ in the matrix model.

The graph collision problem was studied by Magniez, Santha and Szegedy in [20]. Their algorithm has $O(n^{2/3})$ complexity. For some classes of graphs there are better algorithms. So, Jeffrey, Kothari Magniez described in [24] a quantum algorithm with $\tilde{O}(\sqrt{n}+\sqrt{m})$ query complexity, where m is the number of non-edges in the graph. Belov's algorithm has $O(n^{1/2}\alpha^{1/6})$ query complexity, where α is the size of the largest independent set of the graph [25][26]. The algorithm described by Ambainis et al. [26] has $O(n^{1/2}t^{1/6})$ query complexity, where t is the treewidth of the graph.

In 2009, Harrow, Hassidim and Lloyd produced a quantum algorithm for solving systems of linear equations in time $O(k^2 \log N)$ where k is the condition number of the system of equations [27]. In 2012, Andris Ambainis improved the running time of the algorithm of Harrow to $O(k \log^3 k \log N)$ [28]. Their algorithms are used by Dominic Berry to develop a quantum algorithm for solving linear differential equations [29].

VI. CONCLUSIONS

Quantum computing permits to perform computational operations on date much faster and efficiently by taking advantage of quantum parallelism. At the same time, by using the principle of superposition, a large amount of data could be stored.

In the last years, a lot of quantum algorithms have been developed. Many of them are generalisations and applications of the two main algorithms – Shor's factoring algorithm and Grover's search algorithm. The paper presented some of the the recent results in the quantum algorithm development focusing on the quantum search algorithm. These algorithms use the techniques of the quantum search to solve problems faster than their classical counterparts can do.

REFERENCES

[1] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists", ACM Computing Surveys 32, pages 300-335, 2000

[2] R. Feynman, "Simulating physics with computers", International Journal of Theoretical Physics, vol. 21, no. 6, pages 467–488, 1982

[3] P. Benioff, "Quantum mechanical hamiltonian models of turing machines", Journal of Statistical Physics 29 (3): 515–546, 1982

[4] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", Proceedings of the Royal Society of London A 400, pp. 97-117, 1985

[5] D. Deutsch, "Quantum computational networks", Proceedings of the Royal Society of London A 425, pp. 73-90, 1989

[6] P.W. Shor, "Algorithms for Quantum Computing: Discrete Logarithm and Factoring", Proceedings of 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994

[7] L.K.Grover, "A fast quantum mechanical algorithm for database search, Proc. 28th Annual ACM Symposium on the Theory of Computing (STOC), 1996, p. 212-219

[8] B. Schumacher, "Quantum coding", Physical Review A, Vol. 51, No. 4, April 1995

[9] C. Lavor, LRU Manssur and R. Portugal, "Grover's Algorithm: Quantum Database Search", 2003, arXiv:quant-ph/0301079

[10] C. Lavor, L.R.U. Manssur and R. Portugal, "Shor's Algorithm for Factoring Large Integers", 2003, arXiv:quant-ph/0303175

[11] M. Boyer, G. Brassard, P. Hoeyer and A. Tapp, "Tight bounds on quantum searching", Proceedings of Fourth Workshop on Physics and Computation, 1996

[12] S. Jeffery, R. Kothari and F. Magniez, "Improving quantum query complexity of boolean matrix multiplication using graph collision", Proceedings of ICALP 2012, pages 522-532

[13] G. L. Long, Y. S. Li, W. L. Zhang and L. Niu, "Phase matching in quantum searching", Phys. Lett. A, vol. 262, pp. 27-34, Oct. 1999

[14] A. Montanaro, "Quantum search with advice", Proceedings of the 5th Conference on Theory of quantum computation, communication and cryptography, 2010, pages 77-93

[15] André J. Hoogstrate and Chris A.J. Klaassen, "Information weighted sampling for detecting rare items in finite populations with a focus on security", arXiv:1310.5821v1 [math.PR], 2013

[16] G. Brassard, P. Høyer and A. Tapp, "Quantum Counting", Cambridge, U.K.: Cambridge Univ. Press, May 1998

[17] C. Dürr and P. Høyer, "A Quantum Algorithm for Finding the Minimum", Cambridge, U.K.: Cambridge Univ. Press, Jul. 1996

[18] A. Ahuja and S. Kapoor, "A Quantum Algorithm for finding the Maximum". Cambridge, U.K.: Cambridge Univ. Press, Nov. 1999

[19] C. Dürr, M. Heiligman, P. Høyer, M. Mhalla, *Quantum query complexity of some graph problems*, Proceedings of ICALP'04: pages 481-493, 2004.

[20] F. Magniez, M. Santha and M. Szegedy, "Quantum Algorithms for the Triangle Problem", SIAM Journal on Computing, Vol. 37, No. 2, pages 413-424, May 2007

[21] A. Belovs, "Span Programs for Functions with Constant-Sized 1-certificates", Proceeding STOC '12 Proceedings of the 44th symposium on Theory of Computing, pages 77-84, 2012

[22] T. Lee, F. Magniez and M. Santha, "Improved quantum query algorithms for triangle finding and associativity testing", ACM-SIAM Symposium on Discrete Algorithms, 2013

[23] S. Dőrn, "Quantum Algorithms for Graph Traversals and Related Problems", Proceedings of CIE, 2007

[24] S. Jeffery, R. Kothari and F. Magniez, "Improving quantum query complexity of boolean matrix multiplication using graph collision", Proceedings of ICALP 2012, pages 522-532

[25] A. Belovs, "Learning-graph-based uantum algorithm for k-distinctness", Proceedings of FOCS 2012, pages 207-216

[26] A. Ambainis, K. Balodis, J. Irads, R. Ozols and J. Smotrovs, "Parameterized quantum query complexity of graph collision", ICALP 2013, pages 5-16

[27] A. Harrow, A. Hassidim and S. Lloyd, "Quantum algorithm for linear systems of equations", Physical Review Letters, vol. 15, no. 103, October 2009

[28] A. Ambainis, "Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations", Proceedings of Symposium on theoretical aspects of computer science STACS 2012, pages 636-647

[29] D. W. Berry, "High-order quantum algorithm for solving linear differential equations", arXiv:1010.2745v2 [quant-ph], 2014