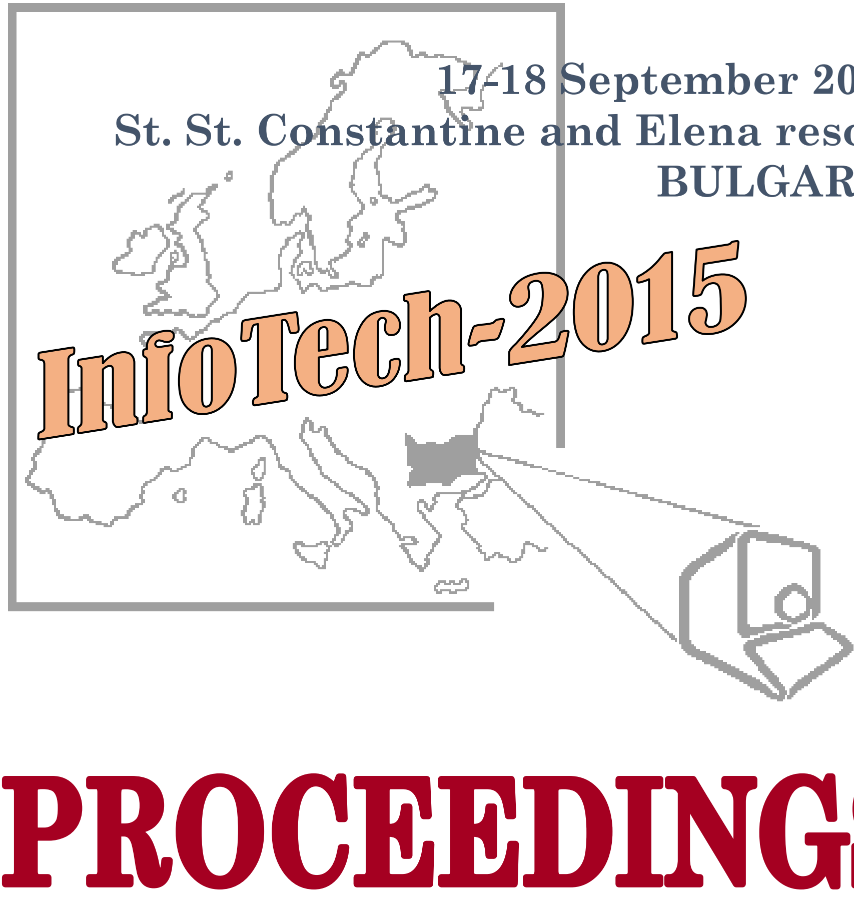
XXIX International Conference on Information Technologies

17-18 September 2015
St. St. Constantine and Elena resort
BULGARIA



PROCEEDINGS

International Conference on Information Technologies is organized with the support of:

Technical University – Sofia

RILA Solutions Ltd.

Institute of Electrical and Electronics Engineers, Inc., Section Bulgaria

Union of Scientists in Bulgaria

Union of Electronics, Electrical Engineering and Communications

InfoTech-2015

29^{th} International Conference on Information Technologies (InfoTech-2015)

17^{th} – 18^{th} September 2015
Varna – St. St. Constantine and Elena resort, Bulgaria

The forum is organized in the frame of
"Days of the Science of Technical University-Sofia, 2015"

PROCEEDINGS

Edited by Prof. Radi Romansky, D.Sc.

Sofia, 2015

InfoTech-2015 Organizers

Technical University of Sofia
Web site: http://www.tu-sofia.bg/

Union of Electronics, Electrical Engineering and Communications
Web site: http://ceec.fnts-bg.org

Union of Scientists in Bulgaria
Web site: http://www.usb-bg.org

ISSN: 1314-1023

Publishing House of Technical University – Sofia

InfoTech-2015 is organized with the financial support of:

Technical University of Sofia
Scientific and Research Sector
Web site: http://www.tu-sofia.bg/

RILA Solutions Ltd.
Web site: http://www.rila.bg

Institute of Electrical and Electronics Engineers, Section Bulgaria
Web site: http://www.ieee.bg

Union of Scientists in Bulgaria
Web site: http://www.usb-bg.org

International Program Committee

Prof. Luís BARROSO	(Portugal)
Prof. Dencho BATANOV, Ph.D.	(Cyprus)
Prof. Francesco BERGADANO	(Italy)
Prof. Dumitru Dan BURDESCU, Ph.D.	(Romania)
Prof. Pino CABALLERO-GIL, Ph.D.	(Spain)
Prof. Ed F. DEPRETTERE	(The Netherlands)
Assoc. Prof. Vassil FOURNADJIEV, Ph.D.	(Bulgaria)
Prof. Georgi GAYDADJIEV, Ph.D.	(Sweden)
Victor GAYOSO MARTÍNEZ, Ph.D.	(Spain)
Prof. Iliya GEORGIEV	(USA)
Prof. Luis HERNÁNDEZ ENCINAS	(Spain)
Prof. Atanas ILIEV, Ph.D.	(Macedonia)
Assoc. Prof. Ivan JELINEK, Ph.D.	(Czech Republic)
Assoc. Prof. Karl O. JONES	(UK)
Prof. Nikola KASABOV, Ph.D.	(New Zealand)
Assoc. Prof. Todor KOBUROV, Ph.D.	(Bulgaria)
Prof. Karol MATIAŠKO	(Slovakia)
Assoc. Prof. Irina NONINSKA, Ph.D.	(Bulgaria)
Assoc. Prof. Angel POPOV, Ph.D.	(Bulgaria)
Prof. Radi ROMANSKY, D.Sc.	(Bulgaria) – ***Chairman***
Assoc. Prof. Giancarlo RUFFO, Ph.D.	(Italy)
Prof. Heather RUSKIN, Ph.D.	(Ireland)
Prof. Radomir STANKOVIĆ, Ph.D.	(Serbia)
Anastassios TAGARIS, Ph.D.	(Greece)
Prof. Ivan TASHEV	(USA)
Assoc. Prof. Dimitar TSANEV, Ph.D.	(Bulgaria)
Prof. Philip TSANG, Ph.D.	(China)
Prof. Michael VRAHATIS, Ph.D.	(Greece)
Prof. Larissa ZAITSEVA, D.Sc.	(Latvia)

National Organizing Committee

Chairman: Radi ROMANSKY

Members: Angel POPOV, Dimitar TZANEV, Irina NONINSKA, Todor KOBUROV, Elena PARVANOVA, Dela STOYANOVA

Web site: **http://infotech-bg.com**

Contents

All indexed reports could be finding in the enclosed CD ROM (ePROCEEDINGS)

Section 'C': Intelligent Systems and Applications

Intelligent and Agent Systems

Section 'D': Technologies for System Design

Computer Architectures and Automation of System Design and Research

Section 'E': Technological Aspects of e-Governance and Data Protection

Technological Aspects of e-Governance

e-Learning and Educational Aspects

Conference Proceedings Publishing and Dissemination

The PROCEEDINGS (ISSN 1314-1023) includes conference papers accepted after reviewing by members of *InfoTech* International Program Committee and will be deposited* in the libraries listed below:

Bulgaria	♦ National Library "St. St. Cyril and Methodius", *Sofia* ♦ NACID – Central Research and Technical Library, *Sofia* ♦ Library of Technical University of Sofia, *Sofia* ♦ Library of International Business School, *Botevgrad*
Germany	♦ Technische Informationsbibliothek und Universitatsbibliothek, *Hanover* ♦ Universitatsbibliotthek, *Stuttgart* ♦ Universitatsbibliotthek, *Kaiserslautern*
India	♦ The Institution of Electronics and Telecommunication Engineers, *New Delhi*
Japan	♦ National Diet Library, *Tokyo*
Republic of Moldova	♦ Biblioteca Stiintifica Centrala a Academiei de Stiinte, *Chisinau*
Russia	♦ Государственная публичная НТ библиотека (ГПНТБ), *Moscow* ♦ Всерусийский институт НТ информации (ВИНИТИ), *Moscow* ♦ Библиотека Росийской АН (РАН), *Sanct Petersburg* ♦ ГПНТБ Сибирскоко отделения РАН, *Novosibirsk*
Spain	♦ Centro de Informacion y Documentacion Cientifica (CINDOC), *Madrid*
USA	♦ The Library of Congress, *Washington DC*

* *with the support of National Centre for Information and Documentation (NACID) – Central Research and Technical Library*, ***Bulgaria***
(http://mail.nacid.bg/newdesign/en/index.php)

InfoTech papers Indexing & Abstracting

Conference Program Overview

Thursday, 17th September 2015

10:30 – 12:00	On-Site Registration and Conference Materials (*Conf. Office*)
13:30 – 14:00	**Official Opening Session** (*Hall 5*) Conference Opening Invited Keynote
14:00 – 15:00	**Report Session** (*Hall 5*) Section "A"
15:00 – 15:40	**Coffee Discussion** in the IHS Foyer
15:40 – 18:00	**Report Session** (*Hall 5*) Sections "B" & "C" & "D"
20:00 – 23:00	**Official Conference Dinner** (Cocktail)

Friday, 18th September 2015

09:00 – 11:20	**Report Session** (*Hall 5*) Sections "A" & "E"
11:20 – 12:00	**Poster Session & Coffee Discussion** (*Foyer*) All Sections
12:00	**Conference InfoTech-2015 Closing** (*Foyer*)

- The PROCEEDINGS of the International Conference on Information Technologies (InfoTech) is indexed by ***EBSCO Publishing Inc.***, Ipswich, MA, USA (http://www.ebsco.com).
- Electronic version of the Conference PROCEEDINGS will be included in two specialized scientific databases of ***EBSCO Publishing Inc.***, Ipswich, MA, USA (http://www.ebscohost.com/title-lists)
  - ***Academic Search Complete (Other Sources)***
    http://www.ebscohost.com/titleLists/a9h-other.pdf - *see page 10*
  - ***Academic Search Elite (Other Sources)***
    http://www.ebscohost.com/titleLists/afh-other.pdf - *see page 12*
  - ***Computers & Applied Sciences Complete (Database Coverage List)***
    http://www.ebscohost.com/titleLists/iih-coverage.pdf - *see page 28*

Proceedings of the International Conference on
Information Technologies (InfoTech-2015)
17-18 September 2015, Bulgaria

QUANTUM CIRCUITS FOR QUANTUM WALKS ON THE HYPERCUBE[1]

Adina BĂRÎLĂ

„Ștefan cel Mare" University of Suceava
e-mail: adina@eed.usv.ro
Romania

Abstract: The field of quantum computing investigates the computational power of computers based on quantum mechanical principles. In the last years new quantum algorithms have appeared: algorithms based on quantum walks model and on adiabatic model. The paper presents some fundamental concepts of quantum walks and proposes a quantum circuit for quantum walks on the hypercube. Also, a QCL implementation of quantum walk algorithm is presented. QCL (Quantum Computation Language) is the most advanced implemented quantum computer simulator and was conceived by Bernhard Ömer.

Key words: quantum computing, quantum gate, quantum walk.

1. INTRODUCTION

Quantum computing is a field of science which investigates the computational power of computers based on quantum mechanical principles. It was introduced in the early 1980's and recent research has proved the potential of quantum computing systems to solve problems that are considered unsolvable due to the necessary computing effort.

The first quantum algorithm which solves a computational problem in a more efficient way than classical computation was invented by David Deutsch. He presented an example which showed that a single quantum computation may suffice to decide whether a given one-bit function is constant or balanced. Other notable algorithms were developed by Simon and Vazirani.

[1] ACKNOWLEDGMENT 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

But, two important discoveries have led to shaping this area of quantum computing [1]: the Shor's and the Grover's algorithms. In 1994, Peter Shor described a polynomial time quantum algorithm for factoring large integers [2] and in 1996 Lov Grover invented the quantum database search algorithm which achieved quadratic speedup for the classic problem of database search [3]. Since then, each of the two algorithms has been analyzed and generalized. Shor's algorithm has been generalized to solve the problem of finding hidden subgroup and Grover's algorithm has been generalized to solve problems like approximate counting and collision-finding.

In the last years new quantum algorithms have appeared: algorithms based on quantum walks model and on adiabatic model. Quantum walks are quantum generalizations of classical random walks. Adiabatic computation is a physics-based paradigm for quantum algorithms [1].

Section 2 presents some basic concepts in quantum computing. Section 3 considers some fundamental concepts of quantum walks. Section 4 proposes a quantum circuit for the quantum walk on the hypercube and a QCL implementation of quantum walk algorithm. Section 5 draws the conclusion.

2. BASIC CONCEPTS IN QUANTUM COMPUTING

2.1.Qubits

The quantum analogous of the classical bit is called quantum bit or qubit [4]. A qubit is a quantum system whose general state is a linear combination (or a *superposition*) of two basis states, conventionally written $|0\rangle$ and $|1\rangle$. The quantum bit is describe by a unit vector $|\psi\rangle$ in a Hilbert space $H = C^2$ which computational basis is $\{|0\rangle, |1\rangle\}$. So

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

where

$$|0\rangle = (1\ 0)^T \quad |1\rangle = (0\ 1)^T \tag{2}$$

and the amplitudes α and β are complex numbers such that:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

In other words, a qubit can exist in a state $|0\rangle$, or $|1\rangle$ or simultaneously in $|0\rangle$ and $|1\rangle$ (when both α and β are nonzero).

When measuring a qubit it obtaines 0 with probability α^2 (and the qubit's state becomes $|0\rangle$) or 1 with probability β^2 (and the qubit's state becomes $|1\rangle$). Measurement collapses a quantum state into one of the possible basis states, so measurement is a destructive operation.

A system consisting of n qubits has 2^n basis states and its general state is a superposition of all basis states:

$$|\psi\rangle = \sum_{k=0}^{2^n-1} c_k |k\rangle \tag{4}$$

where:

$$|k\rangle = |k_{n-1} \ldots k_1 k_0\rangle \tag{5}$$

with $|k_j\rangle$ represents the state of qubit j and $|k_{n-1} \ldots k_1 k_0\rangle$ (or $|k_{n-1}\rangle \ldots |k_1\rangle |k_0\rangle$ or $|k_{n-1}, \ldots, k_1, k_0\rangle$) represents the tensor product $|k_{n-1}\rangle \otimes \ldots \otimes |k_1\rangle \otimes |k_0\rangle$. The amplitudes c_k are complex numbers such that:

$$\sum_{k=0}^{2^n-1} |c_k|^2 = 1 \tag{6}$$

Like the single-qubit system, a n-qubit register can store simultaneously all the basis states. A state of a n-qubit register is an element in the space $H^{\otimes n} = H \otimes H \otimes . . . \otimes H$ (tensor product).

2.2.Quantum gates

A quantum gate is a unitary transformation that acts on a small number of qubits. Every operation applied to a quantum state must be reversible so a quantum gate has the same number of inputs and outputs. A one-qubit elementary gate is described by a 2x2 matrix:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{7}$$

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

The Hadamard (H) and the Pauli (X,Y,Z) gates are examples of quantum gates that act on a single qubit:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{8}$$

The most important two-qubit gate is the CNOT (controlled-not gate). It has two input qubits, the control and the target qubit. The target qubit is flipped if and only if the control qubit is set to 1. The matrix form of this gate is given in eqn. 9 and the circuit representation is shown in fig.1.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{9}$$

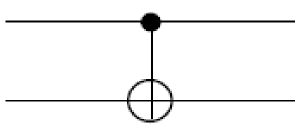


Fig. 1 The CNOT gate

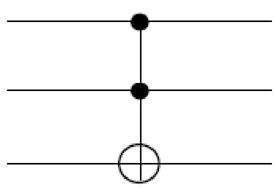


Fig. 2 The CCNOT gate

An important three-qubit gate is the Toffoli gate, also known as CCNOT (controlled-controlled-not) gate. It has two control qubits and a target qubit. The target qubit is flipped only if and only if the control qubits are set to 1. The matrix form of CCNOT gate is given in eqn. 9 and the circuit representation is shown in fig.2.

3. QUANTUM WALKS

Quantum walk can be regarded as quantum equivalent of the classical random walk. Like in the classical case, there are two quantum walk models: discrete time quantum walk and continuous time quantum walk. In this paper the discrete time quantum walks will be considered.

3.1.Discrete time quantum walk on the line

A discrete time quantum walk on the line is defined in analogy with the classical random walk on the line.[5] In the classical case, a walker is placed at the origin of a line numbered from –N to N. The walker tosses an unbiased coin and moves either left or right by one position depending on outcome. If the random walk is performed a large enough number of times, one gets a binomial distribution of the walker final position centered about the origin.

In the quantum case, the position of the walker is a vector in a Hilbert space H_P with the following computational basis

$$\{ |n\rangle : n \in Z \} \tag{10}$$

The evolution of the walk depends on a quantum "coin". If one obtains "head" after tossing, the walker "moves" from the position described by the vector $|n\rangle$ to the position described by $|n+1\rangle$. If one obtains "tail" the walker "moves" from $|n\rangle$ to the position described by $|n\text{-}1\rangle$. The coin is a vector in a Hilbert space H_C with computational basis $\{|0\rangle, |1\rangle\}$. The Hilbert space of the quantum system is $H = H_P \otimes H_C$. Since quantum operations must be reversible , „toss" must be performed by a unitary operator called *coin operator*.[6]

The most used coin [7] for unidimensional quantum walks is the Hadamard operator:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{11}$$

This operator/which acts on basis states as follow:

$$H|0,n\rangle = \frac{1}{\sqrt{2}}(|0,n\rangle+|1,n\rangle) \tag{12}$$

$$H|1,n\rangle = \frac{1}{\sqrt{2}}(|0,n\rangle-|1,n\rangle) \tag{13}$$

The shift from $|n\rangle$ to $|n+1\rangle$ or $|n\text{-}1\rangle$ is described by a unitary operator, called *shift operator* S [6]. This acts as follows:

$$S|0\rangle|n\rangle = |0\rangle|n+1\rangle \tag{14}$$

$$S|1\rangle|n\rangle = |1\rangle|n-1\rangle \tag{15}$$

The quantum walk consists in applying the unitary operator [8]

$$U = S\,(C \otimes I) \tag{16}$$

a number of times without intermediate measurements, where C is the coin operator and I is the indentity operator on the Hilbert space H_P.

So, the algorithm which implements the quantum walk can be implemented as follows

1.initialize the system

2.for every iteration

  toss the coin

  shift the position

3.perform measurement

After *t* steps, the final state before measurement is given by

$$|\Psi_t\rangle = U^t|\Psi_0\rangle \tag{17}$$

where $|\Psi_0\rangle$ represents the initial state.

For example, if the initial position of the walker is $|x{=}0\rangle$ and the coin state is $|0\rangle$, then the initial quantum state is

$$|\psi_0\rangle = |0\rangle\,|0\rangle \tag{18}$$

If Hadamard operator is the coin operator, after "tossing" and shifting the quantum state becomes

$$|0\rangle\otimes|0\rangle \xrightarrow{H\otimes I} \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|0\rangle \xrightarrow{S} \frac{1}{\sqrt{2}}\big(|0\rangle\otimes|1\rangle+|1\rangle\otimes|-1\rangle\big) \tag{19}$$

The result is a superposition of the walker both in position 1 and -1. In the classical random walk, the walker can only go in one direction at a time. In contrast, in quantum walk he can go in both directions until the measuring operation is performed. So, the quantum state at the moment t=1 is

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\big(|1\rangle|-1\rangle+|0\rangle|1\rangle\big) \tag{20}$$

The next step can be computed by $|\psi_2\rangle = U|\psi_1\rangle$.

$$\begin{aligned}|\psi(2)\rangle &= U|\psi(1)\rangle = S(H\otimes I)\frac{1}{\sqrt{2}}\big(|1\rangle|-1\rangle+|0\rangle|1\rangle\big) = S\,\frac{1}{\sqrt{2}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|-1\rangle+\frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle\right)= \\ &= \frac{1}{2}S\big(|0\rangle|-1\rangle-|1\rangle|-1\rangle+|0\rangle|1\rangle+|1\rangle|1\rangle\big)=\frac{1}{2}\big(|0\rangle|0\rangle-|1\rangle|-2\rangle+|0\rangle|2\rangle+|1\rangle|0\rangle\big)= \\ &= \frac{1}{2}\big(-|1\rangle|-2\rangle+\big(|0\rangle+|1\rangle\big)|0\rangle+|0\rangle|2\rangle\big)\end{aligned} \tag{21}$$

Quantum walk has different behaviour compared to its classical counterpart: spreading at a rate proportional to *t*, quadratically faster than the classical random walk.[9] Unlike the classical case, probability distribution is not always symmetric. The distribution of the walk is dependent on the initial state. When the initial position of the walker is $|0\rangle$ and the initial coin state is $|0\rangle$, the distribution is 'skewed' to the right (the thick line in Fig.3) because of Hadamard coin. If the initial state is $|1\rangle|0\rangle$ the distribution is 'skewed' to the left (the thin line in Fig.3) .

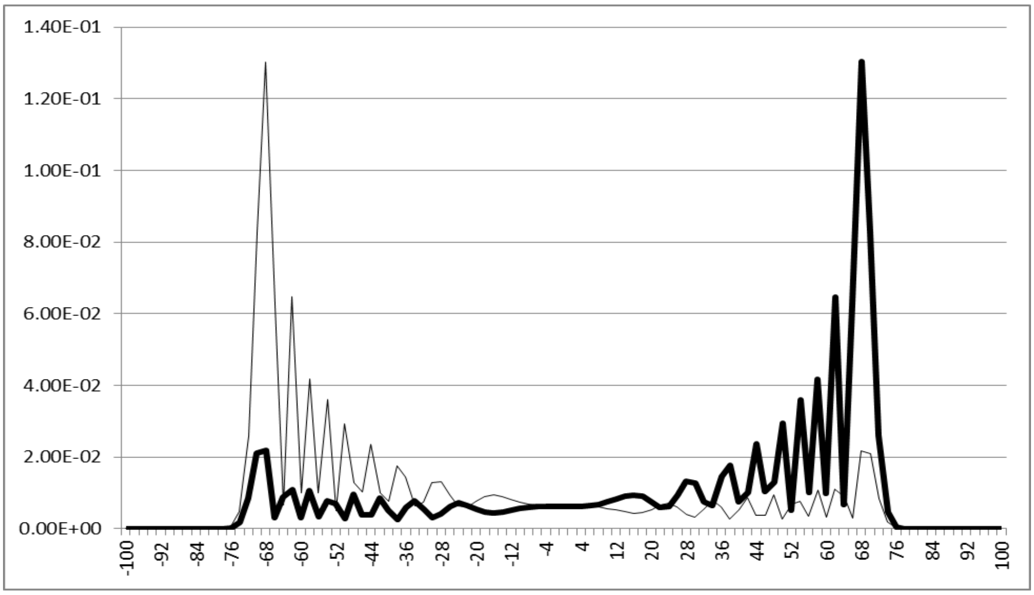


Fig. 3 Probability distribution after 100 steps of a quantum walk on the line with the Hadamard coin and initial state |0〉|0〉 (the thick line) and 1〉|0〉 (the thin line), respectively.

An initial state that leads to a symmetrical distribution is [6]

$$|\psi(0)\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}|n=0\rangle \qquad (22)$$

3.2.Discrete time quantum walk on a regular graph

The difference between the quantum walk on a regular graph and the quantum walk on the line is the Hilbert space of the quantum system.

Let G = (V,E) be a regular undirected graph, where V = {1,2,…N} is the set of vertices and E is the set of edges. The Hilbert space of the quantum system is

$$H = H_C \otimes H_v \qquad (23)$$

where H_v is the vertices space which has the following computational basis

$$H_v = \{\ |v\rangle: v \in Z_N\} \qquad (24)$$

where N is the number of vertices, and H_C is the coin space and has the computational basis

$$H_C = \{|k\rangle: k \in Z_d\ \} \qquad (25)$$

where d is the degree of every vertex.

G is a regular graph, so for every vertex there exists a set of d edges $\{ e_v^j \in E \mid j = 1,2,\dots, d\}$ so that e_v^j is the j-th edge which connects the vertices v and v_j. The walker can move in any of d directions. The shift operator S maps the state $|k,v\rangle$ into $|k,v_j\rangle$.

Often used coin operators are the Hadamard, the Grover and the DFT (Discrete Fourier Transform) operators. The Grover and DFT operators are given by

$$G^{(d)} = \begin{pmatrix} \frac{2}{d} & \cdots & \frac{2}{d} \\ \vdots & \ddots & \vdots \\ \frac{2}{d} & \cdots & \frac{2}{d} \end{pmatrix} - I_d \qquad DFT^{(d)} = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & \cdots & \omega^{(d-1)(d-1)} \end{pmatrix} \qquad (26)$$

where d is the vertex degree, I_d is the identity operator and where $w = \exp(2\pi i/d)$.

3.3.Discrete time quantum walk on the hypercube

The hypercube of dimension n is a regular graph with $N = 2^n$ vertices. The every vertex degree is n. Vertices are labeled by n-bit strings and two vertices are adjacent if and only if their labels differ only by one bit. The edges are also labeled. If two vertices differ by the j-th bit, the label of the edge connecting these vertices is j. [6] The Hilbert space associated with a quantum walk on the hypercube is $H = H^n \otimes H^{2^n}$.

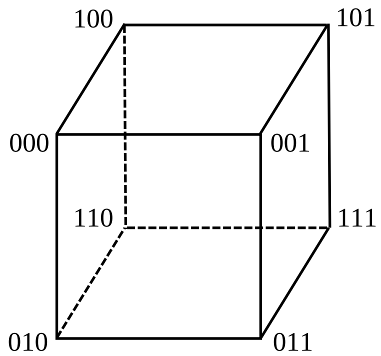


Fig. 4 Hypercube of dimension 3

4.QUANTUM CIRCUITS FOR QUANTUM WALKS ON THE HYPERCUBE

On a hypercube, the shift operator maps the state $|k,v\rangle$ into $|k,v_j\rangle$, where the n-bit strings v and v_j differ by the j-th bit. So, the shift operator S can be represented as follows:

$$S|1\rangle|p_1,p_2,\ldots,p_n\rangle = |1\rangle|p_1\oplus 1, p_2,\ldots,p_n\rangle \qquad (27)$$

$$S|2\rangle|p_1,p_2,\ldots,p_n\rangle = |2\rangle|p_1, p_2\oplus 1,\ldots,p_n\rangle \qquad (28)$$

. . .

$$S|n\rangle|p_1,p_2,\ldots,p_n\rangle = |n\rangle|p_1, p_2,\ldots, p_n \oplus 1\rangle \qquad (29)$$

where $\oplus$ denotes addition modulo two.

If n is a power of two, the action of this operator can be reproduced by $(\text{Controlled})^m$-NOT quantum gates as shown in figure 5.

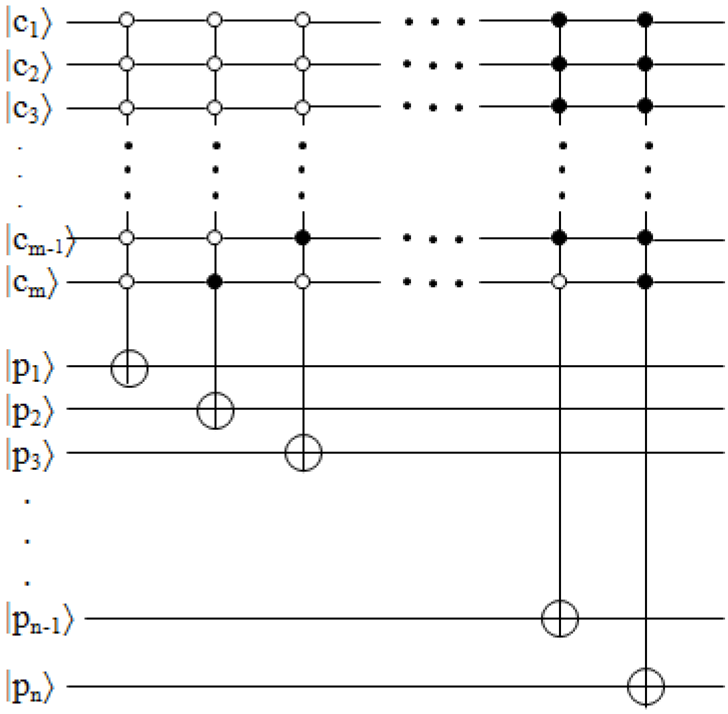


Fig. 5 Quantum circuit for the shift operator

where $|c_1\rangle|c_2\rangle\ldots|c_m\rangle$ is the coin state and $|p_1\rangle|p_2\rangle\ldots|p_n\rangle$ is the position state (vertex state). For example, the shift operator for the quantum walk on the hipercube of dimension 4 is shown in figure 6.

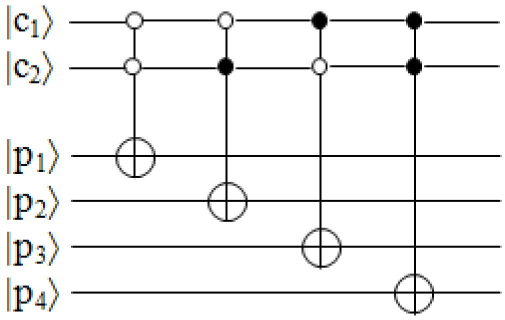
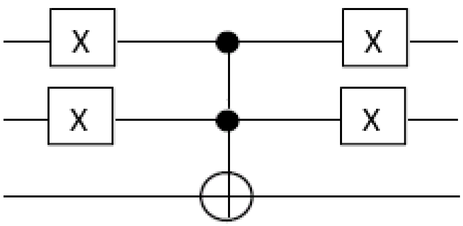


Fig. 6 The quantum circuit for the shift operator in the case n=4

The first gate flips the target qubit if and only if the control qubits are set to 0. It can be represented using CCNOT and X gates as follow



Also, the second and the third gates can be represented using CCNOT and X gates.

The QCL implementation of the quantum walk algorithm on the hypercube of dimension 4 with Hadamard coin and initial state $|00\rangle|0000\rangle$ is presented below:

```
procedure walk4(int steps) {
  qureg c[2]; //coin register
  //vertices register
  qureg v[4];
  int i;
  int m1;
  int m2;
  for i=1 to steps {
    //Hadamard coin
    H(c);
    //the first gate
    Not(c);
    CCNot(c[0],c[1],v[3]);
    Not(c);
    //the second gate
    Not(c[1]);
    CCNot(c[0],c[1],v[2]);
    Not(c[1]);
    //the third gate
    Not(c[0]);
    CCNot(c[0],c[1],v[1]);
    Not(c[0]);
    //the last CCNOT gate
    CCNot(c[0],c[1],v[0]);
  }
  measure c,m1;
  measure v,m2;
  print "m1 = ",m1, " m2= ",
m2;
}
```

In the case of $n>4$, the quantum circuit for the shift operator uses $(\text{Controlled})^m$-NOT gates. Such gates can be implemented using $2(m-1)$ CCNOT gates and $(m-1)$ ancilla qubits as follows

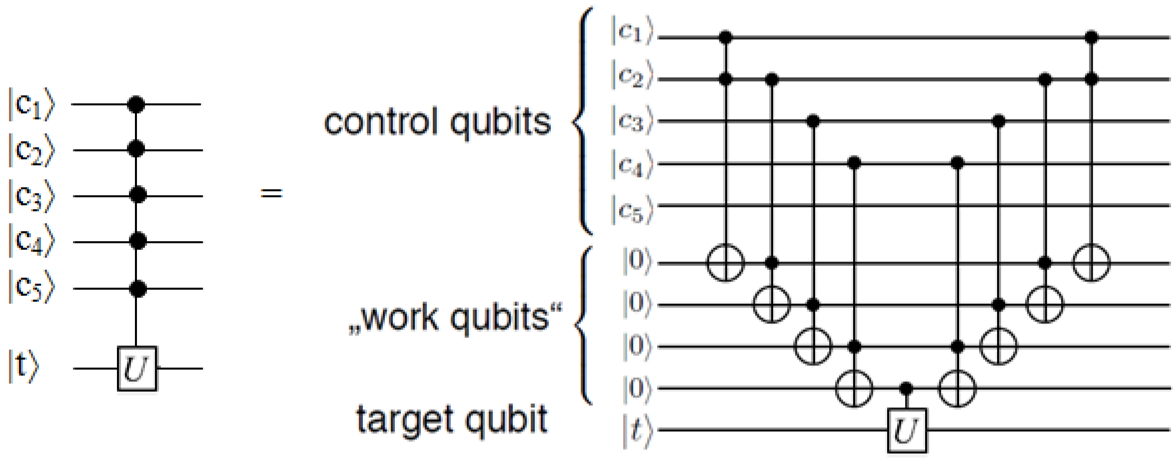


Fig. 7(Controlled)^m-U gate [10]

A QCL implementation of the $(\text{Controlled})^m$-NOT gate is proposed below:

```
operator CmNOT(int m, qureg x, qureg y) {
  qureg a[m-1]; //ancilla qubits
  int i;
  CCNot(x[m-1], x[m-2], a[m-2]);
  for i=3 to m-1 {
    CCNot(x[m-i],a[m-i+1],a[m-i]);}
  for i=3 to m-1 step -1 {
    CCNot(x[m-i],a[m-i+1],a[m-i]);}
  CCNot(x[m-1], x[m-2], a[m-2]);
}
```

5. CONCLUSION

Quantum computing promises to find algorithms which can run faster than their classical counterparts. In the last years new model of quantum algorithms have apperead: the quantum walk based algorithms. The research have shown that quantum walks present different behaviour than classical random walks. This paper presented a brief overview of quantum walks and a quantum circuit for the shift operator of a quantum walk on the hypercube. Also, a proposal for QCL implementation of the quantum walk algorithm on the hypercube was presented. In absence of quantum devices, quantum computing simulators helps programmers to understand the constraints imposed by these devices. In this paper, the QCL quantum language [11] was used in order to simulate the quantum walk algorithm.

REFERENCES

[1] Ambainis A. (**2010**). New developments in quantum algorithms. *Proceedings of the 35th International Conference on Mathematical foundations of Computer Science MFCS'10,* 23-27 August 2010, Czech Republic

[2] Shor P.W. (**1994**). Algorithms for Quantum Computing: Discrete Logarithm and Factoring. *Proceedings of 35th Annual Symposium on Foundations of Computer Science,* Los Alamitos, CA, USA, pp. 124-134

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

[4] Schumacher B. (**1995**). Quantum coding. *Physical Review A*, Vol. 51, No. 4, April

[5] Lovett N.B., Cooper S., Everitt M., Trevers M., Kendon V. (**2010**) Universal quantum computation using the discrete time quantum walk. *Physical Review. A.* 81, 042330, April

[6] Portugal R. (**2013**).Quantum Walks and Search Algorithms. Springer-Verlag New York Inc, ISBN 9781461463351

[7] Venegas-Andraca S.E. (**2012**). Quantum walks: a comprehensive review. *Quantum Information Processing* vol. 11(5), pp. 1015-1106

[8] Kempe J., (**2003**). Quantum random walks - an introductory overview. *Contemporary Physics*, vol. 44 (4), p.307-327

[9] Lovett N.B., (**2011**). Application of quantum walks on graph structures to quantum computing. *PhD Thesis*, University of Leeds

[10] Verdenhalven E., (**2008**). Universal Quantum Gates. Berlin

[11] Ömer B., (**2003**). Strucured Quantum Programming in QCL, *PhD Thesis*, Technical University of Vienna, Austria