International Journal of Computer Applications (0975 - 8887)
Volume 159 - No.8, February 2017

Matrix Representation of Quantum Gates

Aradhyamath Poornima
Physics Department
Vijayanagar Science College
Hosapete, Karnataka, India

Naghabhushana N. M.
Physics Department
RYM Engineering College
Ballari, Karnataka, India

Rohitha Ujjinimatad
Electronics and Communication Department
Proudhadevaraya Institute of Technology
Hosapete, Karnataka, India

ABSTRACT

The field of quantum computing is growing rapidly and there is a surprisingly large literature. Research in this area includes the design of quantum reversible circuits and developing quantum algorithms for the models of quantum computing. This paper is focused on representing quantum reversible gates in matrix form. In turn these matrices can be used to develop quantum circuits with help of K-Map. Also this paper gives the historical development of quantum algorithms and basics concepts in quantum compuation.

General Terms

Quantum Computer, Quantum Algorithms

Keywords

Quantum Computation, Quantum gates, Qubits.

1. INTRODUCTION

In 20^{th} century Quantum theory is the greatest achievement of scientists which provides a uniform frame work for the construction of various modern physical theories. After more than 50 years from its inception, quantum theory married with computer science, another great intellectual triumph of the 20^{th} century and the new subject of quantum computation was born. Todays computer both in theoretical (Turning machines) and Practical (PCs) are based on classical physics. However quantum computation tells us that the world behaves quite differently. A quantum system can be superposition of many different states at the same time and produces interference effect during its evolution. Important goals of quantum algorithms are significantly work faster than any classical algorithm solving the same problem. The potential advantage of quantum computers over classical computers has generated a significant amount of interest in quantum computation, and has resulted in a large number of quantum algorithms not only for discrete problems, such as integer factorization, but also for computational problems in science and engineering, such as multivariate integration, path integration, the solution of ordinary and partial differential equations, eigenvalues problems, and numerical linear algebra problems.
In the early 1980s, Manin (1980) and Feynman (1982) independently observed that computers built from quantum mechanical components would be ideally suited to simulating quantum mechanics. Feynman [1, 2] suggested that constructing computers based on the principles of quantum mechanics might enable the quantum systems of interest to physicists to be efficiently simulated, whereas this seemed to be very difficult with classical computers.
Also he pointed out that accurately and efficiently simulating quantum mechanical systems would be impossible on a classical computer, but that a new kind of machine, a computer itself built of quantum mechanical elements which obey quantum mechanical laws", might one day perform efficient simulations of quantum systems. Classical computers are inherently unable to simulate such a system using sub-exponential time and space complexity due to the exponential growth of the amount of data required to completely represent a quantum system. Quantum computers, on the other hand, exploit the unique, non-classical properties of the quantum systems from which they are built, allowing them to process exponentially large quantities of information in only polynomial time. Quantum computers achieve speedup over classical computation by taking advantage of interference between quantum amplitudes.
The models of quantum computation have their ancestors from the studies of connections between physics and computation. In 1973, to understand the thermodynamics of classical computation Bennet [3] noted that a logically reversible operation does not need to dissipate any energy and found that a logically reversible Turing machine is a theoretical possibility.

Benioff [4, 5, 6] defines physical systems in which the laws of quantum mechanics would lead to the simulation of classical Turning machine, but does not consider the quantum computation. He constructed a quantum mechanical model of a Turing machine. His construction is the first quantum mechanical description of computer, but it is not a real quantum computer because the machine may exist in an intrinsically quantum state between computation steps, but at the end of each computation step the tape of the machine always goes back to one of its classical states.
Another important theme in quantum computing has been the development of quantum cryptographic techniques, going back to the work of Bennett and Brassard [7] which in turn built on work, not published until several years after its conception, by Wiesner [8].
Yao [9] showed that quantum circuit model is equivalent to a quantum Turing machine in the sense that they can simulate each other in polynomial time. Since then, quantum circuits has become the most popular model of quantum computation in which most of the existing quantum algorithms are expressed. Synthesis of quantum circuits is crucial for quantum computation due to the fact that in current technologies it is very difficult to implement quantum gates acting on three or more qubits. As early as in 1995, it was shown

that any quantum gate can be (approximately) decomposed to a circuit consisting only of the CNOT gates and a small set of single qubit gates [10]. Recently, some more efficient synthesis algorithms for quantum circuits have been found; see for example [11]. Some authors initiated the studies of simplification and optimization of quantum circuits. The aim is to develop methods and techniques to reduce the number of quantum gates in a quantum circuit and the depth of a quantum circuit. Due to the difficulty of implementing large quantum circuits, this problem is even more important in quantum computation than in classical computation
In particular, Deutsch [12, 13] introduced the technique of quantum parallelism based on the superposition principle in quantum mechanics by which a quantum Turing machine can encode many inputs on the same tape and perform a calculation on all the inputs simultaneously. Furthermore, he proposed that quantum computers might be able to perform certain types of computation that classical computers can only perform very inefficiently. He investigated the possible computational power of physically realizable computers, and formulated a quantum version of the Turing machine. He defines quantum Turing machines (QTM) as the first model for general quantum computation, with the crucial property that superposition of machine states are allowed, and defines a universal QTM. He observed that quantum computers raise interesting problems for the design of programming languages, computing scientists were slow to respond to this challenge. Quantum computation offers the possibility of considerable speedup over classical computation by exploring the power of superposition of quantum states. This can be illustrated very well by the DeutschJozsa algorithm, which was designed in [14]. One of the most striking advances was made by Shor [15, 16]. By exploring the power of quantum parallelism, he discovered a polynomial-time algorithm on quantum computers for prime factorization of which the best known algorithm on classical computers is exponential. For a long time, QC research has been the luxury of just a few academic elite in the world, that is, until 1994 when Shor invented his famous prime factorization algorithm. He showed in a concrete example that a QC could do much better than a classical computer. More importantly, the difficulty in factoring a large number is the basis of the RivestShamirAdleman (RSA) public key encryption scheme that is widely used today. Through Shors algorithm, the QC has suddenly become a real possible threat, and this algorithm has sparked worldwide interests in the QC. Shors algorithm is applicable only to a specific problem. There is an interesting interplay between quantum computing and quantum cryptography, in that while Shors algorithm for integer factorization has the potential to undermine many current cryptosystems, quantum cryptographic systems can be proved secure against any form of attack, including attacks which make use of quantum computing.
Quantum search algorithms are devised by Grover [17,18,19] they are applicable to many problems. Grovers quantum search algorithm solves the problem of unsorted database searching. Finding a marked state from an unsorted database requires $N2$ searches for a classical computer. Grovers algorithm finds a marked item in only $\sqrt{N}$ steps where N is the size of the database. Grovers algorithm has many applications such as deciphering the digital encryption schyeme (DES) encryption scheme optimization. The standard Grover algorithm achieves quadratic speedup over classical searching algorithms. This algorithm suffers from one problem: the probability of finding the marked state may never be exactly 1. To overcome this difficulty, one has to generalize the standard Grover algorithm by replacing phase inversions by rotations of smaller angles so that the search step can be made smaller. The rest of the paper is organized as follows: Section 2 highlights the basic concepts in quantum computation. Section 3 represents all the basic quantum gates in matrix form. Finally section 4 gives conclusion in brief.

2. BASIC CONCEPTS IN QUANTUM COMPUTATION

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit or Qubit. Classical computer is built from an electrical circuit containing wires and logic gates where as quantum computer is built from a quantum circuit containing wires and elementary quantum gates. A classical bit is either 0 or 1. Two possible states for Qubits are $|0>$ and $|1>$. The difference between classical bits and quantum bits is that a Qubit can be in a state other than $|0>$ or $|1>$. The superposition $|\psi>$of Qubit is a linear combination of these states.

$$\psi = a_0|0> + a_1|1> \tag{1}$$

Where a_0 is the amplitude of measuring $|0>$ and a_1 is the amplitude of measuring the value $|1>$. a_0 and a_1 are the complex coefficients satisfy the normalization condition $a_0^2 + a_1^2 = 1$. The probability of observing a single possible state from the superposition is obtained by squaring the absolute value of its amplitude. The probability of the Qubit being in the state $|0>$ is a_0^2 and the probability that the Qubit will be measured as $|1>$ is a_1^2. The most common basis used in the quantum computing is called computational basis.

$$|0>= \begin{bmatrix}1\\0\end{bmatrix}, \qquad |1>= \begin{bmatrix}0\\1\end{bmatrix}$$

But any other orthonormal basis could be used. For example, the basis vector

$$|+>= \frac{|0>+|1>}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \tag{2}$$

$$|->= \frac{|0>-|1>}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} \tag{3}$$

The equivalent way of expressing of a Qubit $|\psi>= a_0|0> + a_1|1>$
The text book [20] is referred for more information on fundamentals of quantum computation and quantum algorithms.

3. QUANTUM GATES IN MATRIX FORM

The matrix representation of Quantum gate

$$\sum_i |input_i>< output_i|$$

3.1 Quantum NOT gate in the matrix form

$$\begin{aligned} &= |0><1| + |1><0| \\ &= \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} \\ &= \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} \\ &= \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \end{aligned} \tag{4}$$

3.2 Quantum Z gate in matrix form

It inverts sign of $|1>$ to give $-|1>$ and leaves $|0>$ unaltered. For $|0>$ input the ouput is $|0>$ and $|1>$ input the output is $-|1>$.

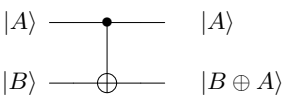
$$\begin{aligned} &= |0><0| + |1><-1| \\ &= \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & -1\end{bmatrix} \\ &= \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\0 & -1\end{bmatrix} \\ &= \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \end{aligned} \tag{5}$$

3.3 Hardmard gate in matrix form

For $|0>$ input to the Hardmard gate the output is $\frac{|0>+|1>}{\sqrt{2}}$ and for $|1>$ input the output is $\frac{|0>-|1>}{\sqrt{2}}$.

$$\begin{aligned} H &= |0>\left[\frac{|0>+|1>}{\sqrt{2}}\right] + |1>\frac{|0>-|1>}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2}}\left[|0><0| + |0><1| + |1><0| - |1><1|\right] \\ &= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}\right] \\ &= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} - \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\right] \\ &= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & -1\end{bmatrix}\right] = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \end{aligned} \tag{6}$$

3.4 Controlled NOT Gate (CNOT)



CNOT gate has two input qubits known as control qubit and target qubit respectively. The circuit representation for CNOT is shown in the figure. The top line represents the control qubit, while the bottom line represents the target qubit. The action of the gate may be described as follows. If the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped. The truth table of CNOT gate.

Input	Output
$\|00>$	$\|00>$
$\|01>$	$\|01>$
$\|10>$	$\|11>$
$\|11>$	$\|10>$

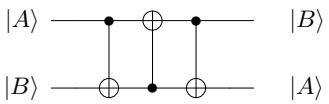
$$|00> = |0> \oplus |0> = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01> = |0> \oplus |1> = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|10> = |1> \oplus |0> = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, |11> = |1> \oplus |1> = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$\begin{aligned} C_{NOT} &= \sum_i |input_i><output_i| \\ &= |00><00| + |01><01| + |10><11| + |11><10| \end{aligned}$$

$$\begin{aligned} C_{NOT} &= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}\begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix} \\ &+ \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix} \\ &= \begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 0\end{bmatrix} \\ &= \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix} \end{aligned} \tag{7}$$

3.5 SWAP Gate in Matrix form



It swaps the states of the two qubits. The swap gate is prepared using three CNOT gates. The sequence is as follows. The inputs are $|A, B>$. The ouput of first CNOT gate is $|A, A \oplus B>$. This is fed to the second CNOT gate and oupt of the second CNOT gate is $|A \oplus (A \oplus B), A \oplus B> = |B, A \oplus B>$. The ouput of third CNOT gate is $|B, B \oplus (A \oplus B) = |B, A>$
Truth Table of Swap gate

Input	Output
$\|00>$	$\|00>$
$\|01>$	$\|10>$
$\|10>$	$\|01>$
$\|11>$	$\|11>$

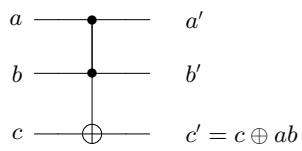
Matrix Representation of Swap gate

$$\begin{aligned} M_{swap} &= \sum_i |input_i><output_i| \\ &= |00><00| + |01><10| + |10><01| + |11><11| \end{aligned}$$

$$M_{swap} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\begin{bmatrix}1&0&0&0\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}\begin{bmatrix}0&0&1&0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix}\begin{bmatrix}0&1&0&0\end{bmatrix}$$
$$+ \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\begin{bmatrix}0&0&0&1\end{bmatrix}$$
$$= \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&1&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&1&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{bmatrix}$$
$$= \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix} \quad (8)$$

3.6 Toffoli gate in Matrix form

Any classical circuit can be replaced by equivalent circuit containing only reversible elements by making use of a reversible gate known as the Toffoli gate [21]. The Toffoli gate has three input bits and three output bits as shown in the figure. Two of the bits that are control bits that are unaffected by the action of the Toffoli gate. The third bit is a target bit that is flipped if both control bits are set to 1, otherwise is left alone.



The truth table of Toffoli gate

Input a b c	Output a' b' c'
|000 >	|000 >
|001 >	|001 >
|010 >	|010 >
|011 >	|011 >
|100 >	|100 >
|101 >	|101 >
|110 >	|111 >
|111 >	|110 >

Matrix Representation of Toffoli gate

$$M_{Toffoli} = \sum_i |input_i >< output_i|$$

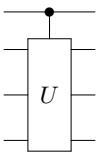
$$= |000 >< 000| + |001 >< 001| + |010 >< 010| + |011 >< 011|$$
$$+|100 >< 100| + |101 >< 101| + |110 >< 111| + |111 >< 110|$$

$$= \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}\begin{bmatrix}1&0&0&0&0&0&0&0\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix}\begin{bmatrix}0&1&0&0&0&0&0&0\end{bmatrix} + \ldots\ldots$$
$$+ \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}\begin{bmatrix}0&0&0&0&0&0&0&1\end{bmatrix} + \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix}\begin{bmatrix}0&1&0&0&0&0&1&0\end{bmatrix}$$

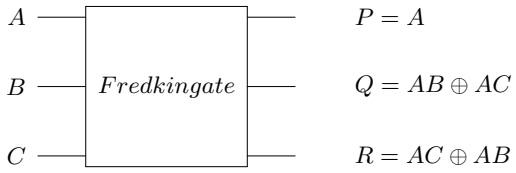
$$= \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\1&0&0&0&0&0&0&1\\1&0&0&0&0&0&1&0\end{bmatrix} \quad (9)$$

3.7 Controlled - U gate:

It is a natural extension of the controlled NOT gate. Such a gate has a single control Qubit indicated by the line with the black dot and n target Qubits indicated by the boxed U. If the control Qubit is set to 0 then nothing happens to the gate U is applied to the target Qubits.



3.8 Fredkin gate :



Truth Table of Fredkin Gate

A B C	P Q R
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 1 0
1 1 0	1 0 1
1 1 1	1 1 1

Matrix Representation of Fredkin gate

$$M_{Fredkin} = \sum_i |input_i >< output_i|$$

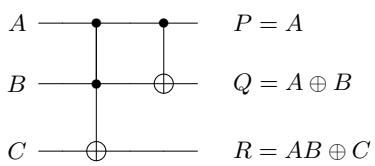
$$= |000 >< 000| + |001 >< 001| + |010 >< 010| + |011 >< 011|$$
$$+|100 >< 100| + |101 >< 110| + |110 >< 101| + |111 >< 111|$$

$$= \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix} \begin{bmatrix}1&0&0&0&0&0&0&0\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{bmatrix} \begin{bmatrix}0&1&0&0&0&0&0&0\end{bmatrix} + \ldots\ldots$$

$$+ \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix} \begin{bmatrix}0&0&0&0&0&1&0&0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix} \begin{bmatrix}0&1&0&0&0&0&0&1\end{bmatrix}$$

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

3.9 Peres Gate in Matrix form:



Truth table of Peres gate:

A B C	P Q R
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 1 0
1 0 1	1 1 1
1 1 0	1 0 1
1 1 1	1 0 0

Matrix Representation of Peres gate:

$$M_{Peres} = \sum_i |input_i >< output_i|$$

$$= |000 >< 000|+|001 >< 001|+|010 >< 010|+|011 >< 011|$$
$$+|100 >< 110|+|101 >< 111|+|110 >< 101|+|111 >< 100|$$

$$= \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\\1&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0\end{bmatrix} \quad (11)$$

4. CONCLUSION

In this paper we studied the pre-history of quantum computation and challenges in the quantum field. Also we have given the basic concepts in the quantum computation. All quantum gates are studied thoroughly and represented them in the matrix form. These matrices are useful in generating quantum circuits. We strongly feel that this paper will be helpful for the beginners who are doing research in the models of quantum computation.

5. REFERENCES

[1] R. P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, vol. 21, no. 6/7, pp. 467- 488, 1982.

[2] R. P. Feynman, Quantum mechanical computers, *Foundation of Physics*, Vol. 16, pp. 507 - 531(1986). (Originally appeared in optics news, February 1985).

[3] C. H. Bennet, Logical reversibility of computation, *IBM Journal of Research and Development* 17 (1973) 525532.

[4] Benioff . P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turning machines. *Journal of Statistical Physics* 22(5):563-591.

[5] Benioff. P. quantum mechanical Hamiltonian model of Turning machines *Journal of Statistical Physics* Vol 29, pp. 515-546 (1982)

[6] Benioff . P. quantum mechanical Hamiltonian model of Turning machines that dissipate no energy, *Physics Review letters* Vol. 48, pp. 1581 - 1585 (1982)

[7] C. H. Bennett and G. Brassard, *in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, Bangalore, India (1984), pp. 175179.

[8] S. Wiesner, " Conjugate coding, " written circa 1970 and belatedly published *in Siact News* 15(1), pp. 78-88, 1983

[9] A.C. Yao, Quantum circuit complexity, in: Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science, 1993, pp. 352361.

[10] A. Barenco, C. Bennet, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, Elementary gates for quantum computation, Physical Review A 52 (1995) 34573467.

[11] V. V. Shende, A.S. Bullock, I. L. Markov, Synthesis of quantum-logic circuits, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 25 (2006) 10001010.

[12] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer, *Proceedings of the Royal Society of London* A400:97117.

[13] Deutsch D. Quantum computational networks, *Proceedings of the Royal Society of London*, Vol. A425, 7390, 1989.

[14] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, *Proceedings of the Royal Society of London* A 439 (1992) 553.

[15] Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring, *In Proceedings of the* 35^th *Annual IEEE Symposium on Foundations of Computer Science*, pages 124134. IEEE Press.

[16] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, http://arxiv.org/abs/quant-ph/9508027v2

[17] Grover L. K. A fast quantum mechanical algorithm for database search, *In Proceedings of the* 28^th *Annual ACM Symposium on the Theory of Computation*, pages 212219. ACM Press. Also arXiv:quant-ph/9605043.

[18] Grover L. K. Quantum mechanics helps in searching for a needle in a haystack, *Physical Review letters* 79(2), pp. 325-328, 1997.

[19] L. K. Grover, Quantum telecomputation, arXiv:quant-ph/9704012.

[20] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.

[21] T. Toffoli, Reversible computing , *Tech. Memo MIT/LCS/TM-151, MIT Lab. For Com. Sci.* 1980.