Quantum Computers

Hemant rana, Deepti Agarwal, Akshay singh

student, Teerthankar mahaveer university,

[*]Assistant professor CCSIT Teethankar mahaveer university

Akshay singh, Teerthankar mahaveer university,

hkr110085@gmail.com

deepti.computers@tmu.ac.in

thakurakshay333@gmail.com

Abstract- **A promising technology is the “quantum computers,” and this paperp provides the general summary about the Quantum computers. Quantum Computation is a new and is the new way intersection of mathematics, computer science and physics. It focuses on the usage of quantum mechanics to provide the better efficiency of computation. Here we gives a smooth introduction to some of the aspects in quantum computing. The paper starts with motivating the core ideas of quantum mechanics and quantum computation with easy toy models. From there we move ahead to a formal presentation of the small segment of (unite dimensional) quantum mechanics that we will need for basic quantum computation. Central notions of quantum architecture (qubits and quantum gates) are explained. The paper ends with presentations of one of the easiest quantum algorithms: Deutsch’s algorithm. Our presentation demands neither advanced mathematics nor advanced physics.**

Keywords— **include at least 4 keywords or phrases**

I. INTRODUCTION

A promising innovation is the "quantum PCs." An ever increasing number of researchers are occupied with it on the grounds that of the exhibitions' improvement it could bring to the present registering world.

Quantum PCs require quantum rationale, which is in a general sense distinctive to traditional Boolean rationale.

This distinction prompts a more noteworthy effectiveness of quan-tum calculation over its traditional partner.

Be that as it may, numerous articles about quantum computers are still somewhat hard to comprehend for the "absolute tenderfoot." Thus, the primary point of this paper is to give a basic outline, without coming into specialized subtle elements, of quantum registering, constructing chiefly with respect to.

II. . Prerequisites

Here we give some vital prerequisite about quantum computers and quantum computing.

A. Dirac’s Notation

Dirac imagined the "bra-ket-ket" documentation. It is exceptionally useful in quantum mechanics. The documentation depicts the "ket" vector, meant by ψi, hφ| being its conjugate transpose (likewise called Hermitian conjugate: the "bra-ket-ket"). The "bra-ketcket" is then signified by hφ|ψi. [14] The inward item is direct, and defined by

$$\langle \phi | \psi \rangle = c, \quad (1)$$

c is a number. [10] If c = hφ|ψi the intricate conjugate is

c∗ = hφ|ψi∗ = hψ|φi. (2)

The state of a physical framework is identified with a beam in a complex separable1 Hilbert space, spoke to by H, or comparably, by a point in the projective Hilbert spaces of the frameworks. [14] Each vector in the beam is known as a "ket." Evidently, in the ket ψi, ψ can be supplanted by any sort of images, letters, numbers, or even words. The ket can be viewed as a segment vector and (given a reason for the Hilbert space) said out in parts,

|ψi = ^ (c0,c1,•••)(3),

when the thought Hilbert space is finite dimensional. In endless dimensional space there are endless numerous parts and the ket might be composed in complex capacity documentation, by prepending it with a bra-ket. Dirac's documentation's presentation is frequently discarded.

B. Qubit

Definition 1 (Qubit). A qubit is a quantum framework in which the Boolean states 0 and 1 are spoken to by a recommended match of standardized and commonly orthogonal quantum states marked as {|0i,|1i}. The |0i is called "ground express;" the |1i is the "energized state." As the most broad electronic state is a 1 Remind that a topological space is distinguishable on the off chance that it countains a countable thick subset. 2 More by and large, a general standardized vector can be extended in an orthonormal reason for the space of measurement 2N, N being the quantity of qubits. superposition of the two fundamental states, we at that point have

$$|\Psi_1\rangle = a|0\rangle + b|1\rangle, \quad (4)$$

that is, a normalized2 vector, with a,b ∈ C. The two states shape a "computational premise" and some other (unadulterated) condition of the qubit can be composed as a superposition α|0i + β|1i for α and β, for example, |α|2 + |β|2 = 1. Habitually, a qubit is a tiny framework, for example, a molecule, an atomic turn, or an energized photon.

C. Quantum Register

A gathering of n qubits is known as a quantum enlist of size n.

Illustration 1. For instance, a quantum enroll of size 4 can store singular numbers, for example,

$$|1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \equiv |1101\rangle \equiv |13\rangle,$$

where ⊗ indicates the tensor item. It can likewise store both of them all the while.

2.4 Quantum Logic Gates

For this, and for different controls on qubits, unitary activities must be performed. Normally, the definitions of quantum rationale door and quantum organize take after. Random yield with rise to probabilities of the yield being equivalent to 0 or 1. However two such doors connected successively deliver a yield that is the reverse of the info, and therefore carry on similarly as the an established NOT entryway. We at that point have

$$|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (10)$$

$$|1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (11)$$

In this way, a contribution of |0i prompts an equivalent and inverse adequacy of the yield being |0i or |1i. A contribution of |1i prompts an equivalent sufficiency of the yield of the door being |0i and |1i.

the ax’s being in C, satisfyingPx |ax|2 = 1.3 We shall see the definition of the universality of a gate in sub subsection Universality

Definition 4 (Universality of doors). Entryways are called widespread in the event that they can be utilized to make any rationale circuit, similar to the NAND (the conjunctive foreswearing) door in traditional boolean-based circuits.

A to a great degree helpful consequence of this all inclusiveness is that any quantum calculation should be possible as far as a C-NOT entryway and a solitary qubit door (which shifts), in spite of the fact that, obviously, it may here and there be more advantageous to utilize different doors too. Also, a basic link of the Toffoli entryway and the C-NOT door gives a simplified quantum snake, which is a decent beginning stage for development of full adders, multipliers, and more detailed systems. If a stage door is defined as an a contribution of |0i prompts an equivalent and inverse sufficiency of the yield being |0i or |1i. A contribution of |1i prompts an equivalent sufficiency of the yield of the entryway being |0i and |1i. [8], entryway that flips the period of the upper condition of the objective qubit just if the control qubit is in the upper state the Hadamard and stage doors are sufficient to build any unitary activity on a solitary qubit. 4 truth be told, the difficulty of building a quantum entryway extraordinarily ascends with the quantity of contributions to door.

III. *. Quantum Reversibility*

Consider the Boolean AND entryway. There is no chance to get of totally deriving the contributions of an AND entryway from the yields, and accordingly the AND door shows up not to be reversible, on account of its reality table. An entryway of AND type produces squander warm when working (i.e. offering yields to its sources of info). The "lost" data about the sources of info are contained in this waste warmth. In quantum PCs, we can't enable this circumstance to happen. The radiation of the warmth would rely upon the condition of the contributions to the quantum door. In this manner, in effect, the radiation of the warmth would be an estimation on the information sources and decoherence would result. The universes would be so far separated as to be not able meddle with each and the outcome, which relies on the impedance of these universes, would be invalid. Hence, quantum entryways must be reversible. Reversible entryways must, by their extremely definition, have an equivalent number of information sources and yields. [8] More formally, a n-bit reversible door is a bijective mapping f from the set {0,1}n of n-bit information to itself. Reversible doors are likewise helpful as they would be the main potential approach to enhance the vitality efficiency of PCs past the crucial von Neumann-Landauer point of confinement of

$$kT \ln 2$$

vitality scattered per irreversible piece activity, where k is Boltzmann's steady of 1.38•10−23 J/K, and T is the temperature of nature into which undesirable entropy will be ousted.

IV. Quantum Entanglements

We say that an unadulterated condition of two qubits is trapped on the off chance that it can't be composed as a result of the individual conditions of the two qubits (in this manner, with a tensor item, for example, |v1i⊗|v2i. For instance, the EPR (Einstein-Podolski-Rosen) state isn't decomposable into an immediate result of any frame, and is accordingly caught:

$$|\Psi_{\mathrm{EPR}}\rangle = \frac{(|01\rangle + |10\rangle)}{\sqrt{2}}, \qquad (16)$$

as two qubits in this state show a level of relationship inconceivable in established material science and thus disregard the Bell disparity which is satisfied by all neighborhood (i.e. established) states. At the opposite, for two qubits (n = 2), the state α|00i+ β|01i = |0i⊗(α|0i+ β|1i) (17) is separable: |Ψ1i = |0i and |Ψ2i = α|0i+ β|1i. The exploitation of a number of entangled qubits can lead to a considerable computational speed-up in a quantum computer over its classical counterpart. [13] This leads us to the interest of using quantum computers.

V. . Quantum Interest

A. Finding Prime Factors

Assume we wish to find prime components of N. It is identical to finding the littlest r with the end goal that ar ≡ 1 mod N, where gcd(a,N) = 1. At the end of the day, we need to decide the time of the capacity

$$a^r \bmod N.$$

There is no known efficient traditional calculation to factorize N. The season of calculation is corresponding to the quantity of divisions we need to perform, and this is √N = 2 l 2 . [9] Put essentially, there are two particular stages in this calculation. At first, two registers are at the contribution to the quantum PC. At that point, the first enlist is prepared5 in a superposition of back to back characteristic numbers, while leaving the second enlist in 0 state to acquire |ψi = M−1 X n=0 |ni|0i, where M = 2m is some sufficiently expansive number. In the second enroll, the capacity ai mod N is figured. This can be accomplished unitarily and the outcome is |ψ1i = M−1 X n=1 |ni|an mod N. [9] Then, the period r is separated from the first enroll. [9] However, the Shor's calculation is probabilistic: it doesn't generally give the right answer.

Anyway, it 5 By setting we up, need to state that N qubits are placed in a standard starting state, for example, |0i|0i•••|0i, or |x = 0i.

isn't a genuine issue, as the appropriate responses' legitimacy can be checked effortlessly: the components are increased and should level with N. In the event that it doesn't equivalent N, the calculation circles until the point that the factorization is right. [9] indeed, calculating is a case of recalcitrant issue with the properties [9]:

1. The arrangement can be effectively verified, once discovered, 2. In any case, the arrangement is difficult to find.

That is, it can't be comprehended in a period limited by a polynomial in the measure of the contribution, for this situation logn. [9] The best known considering calculation (called "the number field strainer") requires a period comparably equivalent to exp c(lnn)1 3 (ln(lnn)) 2 3 , (18) where c = (64/9) 1 3 ' 1.9. The present best in class is that the 65 digits elements of a 130 digit number can be found in the request of one month (!) by a system of several work stations. Shor demonstrated that a PC can factor in polynomial time, e.g. in time Oln(n)3 . It would bring about a major difference, as appeared in the following passage. On the off chance that we had a quantum PC that could factor a 130 digit number in one month, running Shor's calculation could factor 400 digit numbers in under 3 years, where it would take around 1010 years for a traditional PC. It has likewise viable significance, as the difficulty of calculating is the premise of plans for open key cryptography, for example, RSA. If quantum PCs could break current RSA calculations, it would be valuable (and objective!) to utilize quantum cryptography. There are likewise some advanced mark plots that are as of now accepted to be secure against quantum PCs. For instance, Lamport marks regularly utilize crypto hash capacities. Lamentably each Lamport key must be utilized to sign a solitary message. Be that as it may, joined with hash trees, a solitary key could be utilized for some, messages, making this a reasonably efficient advanced mark plot. Put along these lines, quantum figuring would have preferable exhibitions to time proportion's over established processing. Different cases are reproduction of quantum physical procedures, from science and solide state material science, estimation of Jones polynomials, and tackling Pell's equation6. [17] Anyway, it isn't generally as straightforward, as quantum calculation is exceptionally delicate. [9] The justification of this delicacy is given in the accompanying segment.

VI. . Quantum Problem

This segment originates from [9]. A major quantum framework can't be impeccably confined from its condition. To play out a perplexing quantum calculation, a fragile superposition of conditions of a generally substantial quantum framework must be readied. As this sytem can't be splendidly segregated from its condition, this superposition rots quickly. Subsequently, contact between the PC and the earth (decoherence) cause blunders that debase the quantum data. Decoherence isn't the main issue. To enhance execution, the bits, after each entryway, could be cooled. By along these lines, little blunders that could be made would end up, warming the earth as opposed to bargaining the gadget's execution. Shockingly, a quantum PC can't be cooled along these lines: contact with the earth would demolish encoded quantum data. A traditional mistake redressing code is a redundancy code: a bit we wish te secure is then supplanted by, say, three duplicates of this bit. Utilizing it, regardless of whether a bit flips, the bit can even now be decoded effectively, by greater part voting. Obviously, it is workable for in excess of one piece to flip. It can be enhanced utilizing longer codes. Drawing nearer a Gaussian, the lion's share vote is said to fall flat (for expansive N) at Perror ' e−Ne2. 6 Recall that Pell's condition is any Diophantine condition of the shapex 2 − ny2 = 1

where n is a nonsquare whole number, and x,y ∈ Z. Numerous arrangements of this condition exist, and they yield great reasonable approximations of the shape x y to the square foundation of n. 7 It was in 1995, and, later, a more broad hypothesis of quantum mistake revision was produced.. This advancement has proceeded and has prompted a torrential slide of different codes that were improved in different regards and adjusted to exceptional circumstances. The harsh thought is to entrap our data conveying qubit with some helper qubits to such an extent that we can circulate the data about the data qubit over numerous assistant qubits.

Anyway, it isn't as easy to utilize this procedure with quantum PCs: regardless of whether Shor has discovered7 a blunder revising code, there can in any case be stage mistakes, which are not kidding, as they make the state 1 √2 [|0i+|1i] (20) fliping to the orthogonal state 1 √2 [|0i−|1i]. (21) As σz = 0 1 0 = 1 2 1 −1 • 0 1 0 • 1 −1 , (22) on the off chance that we think about a stage blunder (σz administrator) in a pivoted premise, it at that point shows up as an adequacy mistake, and the other way around. This new premise we get from the {|0i,|1i} by utilizing a Hadamard change is given by |e 0i = (|0i+|1i) √2 and |e 1i = (|0i−|1i) √2 . In this new premise, a stage blunder has the effect of an abundancy mistake, and has hence the effect σz|e 0i = |e 1i, σz|e 1i = |0i.Therefore, rather than encoding the state α|0i+ β|1i,we encode it as α|0i+ β|1i→ α|e 0e 0i+ β|e 1e 1i. Furthermore, estimating the qubits to recognize blunders would irritate the quantum data they encode. Repeating qubits is likewise difficult, as replicating quantum data can't be duplicated with consummate fidelity.

VII. . Quantum Programming

This area originates from. Utilizing quantum programming, one can permit the declaration of quantum calculations utilizing abnormal state develops [18]. Its point is to give a device to scientists to see better how quantum calculation functions and how to formally reason about quantum calculations.

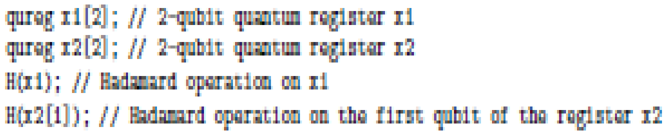
A. Imperative Quantum Programming Languages

Quantum Pseudocode Firstly, a quantum pseudocode was proposed by E. Knill. It was the first formalized dialect for portrayal of quantum calculations.

Quantum Computer Language After it, a Quantum Computer Language (QCL) was proposed. It is one of the first actualized quantum programming dialects. Its sentence structure looks like linguistic structure of the C programming dialect and traditional information composes are like information writes in C. The fundamental implicit quantum information write in QCL is the qureg (quantum enlist). It can be deciphered as a variety of qubits (quantum bits). A case of such a code would take after the accompanying model.

qureg x1[2];/2-qubit quantum enroll x1 qureg x2[2];/2-qubit quantum enlist x2 H(x1);/Hadamard activity on x1 H(x2[1]);/Hadamard task on the principal qubit of the enlist x2

As the qcl translator utilizes qlib reenactment libra-ketry, it is conceivable to watch the inner condition of the quantum machine amid execution of the quantum program:



```
qureg x1[2]; // 2-qubit quantum register x1
qureg x2[2]; // 2-qubit quantum register x2
H(x1); // Hadamard operation on x1
H(x2[1]); // Hadamard operation on the first qubit of the register x2
```

Luckily, the landfill activity is different from estimation, since it doesn't influence the condition of the quantum machine and can be acknowledged just utilizing a test system. Mostly, the QCL standard libra-ketry gives standard quantum administrators utilized as a part of quantum calculations, for example, 1. controlled-not with numerous objective qubits, 2. Hadamard task on numerous qubits, 3. parse and controlled stage.

The most critical element of QCL gives off an impression of being the help for client defined administrators and capacities. Like in present day programming dialects, it is conceivable to define new activities which can be utilized to control quantum information. Q Language Q Language is the second executed basic quantum programming dialect. It was actualized as an expansion of C++ programming dialect. It gives classes to fundamental quantum activities like QFourier, QHadamard, QNot, and QSwap, which are gotten from the base class Qop . New administrators can be defined utilizing C++ class system. Quantum memory is spoken to by class Qreg. Here is a case of Q code.

Qreg x1();/1-qubit quantum enlist with beginning worth 0 Qreg x2(2,0);/2-qubit quantum enlist with starting quality 0

Calculation process is executed utilizing given test system. Boisterous condition can be mimicked utilizing parameters of the test system.

qGCL Quantum Guarded Command Language (qGCL) was defined by P. Zuliani in his PhD proposition. It depends on Guarded Command Language made by Edsger Dijkstra. It can be depicted as a dialect of quantum programs specification.

7.2 Functional Quantum Programming Languages

Amid the most recent couple of years numerous quantum programming dialects in view of the utilitarian programming worldview were proposed. Practical programming dialects are appropriate for thinking about projects.

QFC, QPL QFC and QPL are two firmly related quantum programming dialects defined by Peter Selinger. They differ just in their linguistic structure: QFC utilizes a flow diagram grammar, though QPL utilizes a printed language structure. These dialects have traditional control flow, however can work on quantum or established information. Selinger gives a denotational semantics for these dialects in a class of superoperators.

QML is a Haskell-like quantum programming dialect by Altenkirch and Grattage. Not at all like Selinger's QPL, this dialect takes duplication, instead of disposing of, of quantum data as a crude activity. Duplication in this setting is comprehended to be the activity that maps |φi to |φi⊗|φi.

Quantum Lambda Calculi Quantum lambda calculi are expansions of the lambda math, presented by Alonzo Church and Stephen Cole Kleene in the 1930s. The motivation behind quantum lambda calculi is to expand quantum programming dialects with a hypothesis of higher-arrange functions8. The first endeavor to define a quantum lambda math was made by Philip Maymin in 1996. His lambda-q math is sufficiently effective to express any quantum calculation. This dialect can efficiently tackle NP-finish issues, and in this manner has all the earmarks of being entirely more grounded than the standard quantum computational models, (for example, the quantum Turing machine9 or the quantum circuit model10). In 2003, Andr'e van Tonder defined an augmentation of the lambda math appropriate for demonstrating accuracy of quantum programs. He likewise gave a usage in the Scheme programming dialect. In 2004, Selinger and Valiron defined a specifically lambda math for quantum calculation with a sort framework in view of direct rationale.

VIII. . The Future

A. Overview of Research

As said in [3], examine in quantum calculation and in its every conceivable variety has turned out to be enthusiastically dynamic and any exhaustive survey of the field must be out of date when it is composed. The accompanying content originates.

B. Practical View of Realizing a Quantum Computer

To understand a quantum PC (or to be sure some other PC) we need to have a physical medium in which to store and control data. It is here that quantum data turns out to be exceptionally delicate and things being what they are the undertaking of its stockpiling and control requires a great deal of test inventiveness. 8 Remind that high-arrange capacities are capacities which can take at least one capacities as an info, and yield a capacity. 9 As in established PCs, a Turing machine is a dynamic machine which means to display the effect of a PC. Here, the PC is a quantum PC. The Turing machine hence gives an exceptionally straightforward model which catches the majority of the energy of quantum calculation. Any quantum calculation can be communicated formally as a specific quantum Turing machine; hence, quantum Turing machines have a similar connection to quantum calculation that ordinary Turing machines need to established calculation. Quantum Turing machines can be identified with traditional and probabilistic Turing machines in a structure in light of change (stochastic) networks, as appeared by Lance Fortnow 10 This last is regularlyprefered to quantum Turing machines. Here, a calculation is a grouping of reversible changes on a quantum mechanical simple of a n bit enlist. This practically equivalent to structure is alluded to as a n-qubit enroll.

An extremely excellent proposition for a particle trap quantum PC was made by Cirac and Zoller. Hence, other reasonable recommendations, for example, quantum calculation in light of atomic attractive reverberation techniques have been made. In spite of the fact that these new recommendations are extremely fascinating, we confine ourselves here to the condensed portrayal of the straight particle trap usage of Cirac and Zoller.

Straight Ion Trap The direct particle trap is one of the additionally encouraging recommendations for a physically feasible quantum PC. Here, data is put away into electronic conditions of particles, which are thus confined to a straight trap and cooled to their ground condition of movement. Laser light is then used to control data as different electronic advances. In any case, the wild connections of particles with their condition initiate different blunders known as decoherence, (for example, e.g. unconstrained discharge in particles) and subsequently extremely constrain the energy of calculation. There is a technique to battle decoherence amid calculation known under the name of quantum blunder adjustment. This at that point prompts the idea of faulttolerant quantum calculation, which is a strategy for performing solid quantum calculation utilizing untrustworthy essential segments (e.g. entryways) giving that the blunder rate in this segments is beneath a specific permitted constrain. Much hypothetical work has been embraced around there right now and there is presently a decent comprehension of its forces and restrictions. The primary errand is currently with the experimentalists to attempt to construct the first completely useful quantum PC, in spite of the fact that it ought to be noticed that none of the present usage seem to permit long or expansive scale quantum calculations and a leap forward in innovation may be required. Notwithstanding the way that at show substantial computational errands appear to lie in the remote future, there is a great deal of fascinating and basic material science that should be possible very quickly with the present innovation. Various down to earth data exchange conventions utilize strategies for quantum calculation. Be that as it may, actualizing extensive quantities of quantum entryways on numerous qubits isn't simple since clamor from all sort of sources will bother the quantum PC. Obviously, likewise an established PC experiences the association with an uproarious situation and by the by works exceptionally well. The benefit of a traditional PC is, in any case, that it is an established gadget as in one piece of data is spoken to by the nearness or nonattendance of countless. In this way a little fluctuation in the quantity of electrons does not bother the PC by any means. Despite what might be expected, in a quantum PC, the qubit is put away in the electronic level of flexibility of a solitary molecule. Far more terrible than that, a quantum PC vitally relies upon the survival of quantum mechanical superposition states which are famously touchy to decoherence and dissemination. This makes a quantum PC to a great degree touchy to little bothers from the earth. It has been demonstrated that even uncommon unconstrained emanations from a metastable state discount long figurings unless new thoughts are produced. We trust that quantum factorization and other expansive and essential quantum calculations will be acknowledged in the long run. Luckily, there is a tremendous measure of effort and resourcefulness being connected to these issues, and the future probability of a completely working quantum PC still stays especially alive.

References

[1] Berkeley University, The Mathematical Formalism of Quantum Mechanics, (2006). Physics 221A, University ofCalifornia,Berkeley;http://bohr.physics.berkeley.edu/classes/221/0708/notes/hilbert.pdf.

[2] Dowek, Gilles and Arrighi, Pablo, Linear-algebra-ketic Lambda-calculus: higher-order, encodings and confluence, Quantum Physics, (2006). http://arxiv.org/abs/quant-ph/0612199

[3] Ekert, Artur, Hayden, Patrick and Inamori, Hitoshi, Basic concepts in quantum computation, (2001).

[4] Fortnow, Lance, One complexity theorist's view of quantum computing, (2002). http:// www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V1G-44M2G3W-4&_user=10&_rdoc=1&_ fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_ version=1&_urlVersion=0&_userid=10& md5=60761b323b55062ac8cd2ea22abb88b0.

[5] Grattage, J, QML: A Functional Quantum Programming Language, 2009. http://sneezy.cs.nott.ac.uk/ qml/.

[6] Iriyama, Satoshi and Ohya, Masanori, On generalized quantum Turing machine and its language classes, (2007). http://wseas.us./e-libraketry/conferences/2007dallas/papers/567-277.pdf.

[7] Lenstra, H.W. Jr., Solving the Pell Equation, American Mathematical Society, (2002). http://www.ams.org/ notices/200202/fea-lenstra.pdf.

[8] Marshall, Jonathan, Simulating Quantum Circuits, 2009

[9] Preskill, John, Quantum Information and Computation, 1998.

[10] Saffman, M., Dirac Notation and rules of Quantum Mechanics, (2006). Atomic and Quantum Physics; http:// hexagon.physics.wisc.edu/teaching/2007f_ph448/diracnotation.pdf.

[11] Selinger, Peter, Towards a Quantum Programming Language, (2003). http://www.mathstat.dal.ca/ ~selinger/papers/qpl.pdf.

[12] van Tonder, Andr, A Lambda Calculus for Quantum Computation, SIAM Journal on Computing, (2004). http://scitation.aip.org/getabs/servlet/GetabsServlet?prog=normal& id=SMJCAT000033000005001109000001&idtype=cvips&gifs=yes; http://www.het.brown.edu/people/andre/ qlambda/.

[13] Vedral, Vlatko and Plenio, Martin B., Basics of Quantum Computation, (2002).

[14] Wikipedia, Bra-ket-ket notation - Wikipedia, the free encyclopedia, 2009.

[15] Fredkin gate - Wikipedia, the free encyclopedia, 2009.

[16] Pell's equation - Wikipedia, the free encyclopedia, 2009.

[17] Quantum computer - Wikipedia, the free encyclopedia, 2009.

[18] Quantum programming - Wikipedia, the free encyclopedia, 2009.

[19] Quantum Turing machine - Wikipedia, the free encyclopedia, 2009.

[20] Reversible computing - Wikipedia, the free encyclopedia, 2009.

[21] Tooli gate - Wikipedia, the free encyclopedia, 2009. links) are classed by date of browsing.