Int. Journal of Engineering Research and Application *www.ijera.com*
ISSN : 2248-9622, Vol. 8, Issue 4, (Part -III) April 2018, pp.135-144

RESEARCH ARTICLE OPEN ACCESS

A Review on Quantum Computers

[1]**SHANKAR KUMAR DAS,**
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India

[2]**SUMAN MOHANTA,**
Black Diamond College of Engineering & Technology, Jharsuguda, Odisha, India

ABSTRACT
The field of quantum computing is still developing. Within the next ten years, the clock frequency of today's computer processor systems could reach roughly 40 GHz. By that time, one atom might be equal to one bit. By that point, a new model of the computer might be required because classical physics can no longer adequately represent electrons in such circumstances. One idea that might be useful in solving the difficulties at hand is the quantum computer. There are currently certain algorithms that make use of the benefit of quantum computers. For instance, while traditional factoring algorithms can factor a huge integer in exponential time, Shor's approach can do it in polynomial time. The present state of quantum computers, quantum computer systems, and quantum simulators is briefly reviewed in this study.
KeyWords Mquire large amounts of processing time.Notwithstanding,further improvements will be necessary to ensure quan-tum computers' proper performance in future, but suchimprovementsseemobtainable.
Currently,thereexistsomealgorithmsutilizingtheadvantageofquantumcomputers.Forinstance,thepolynomial-timealgorithmforfactoringalargeintegerwith $O(n^3)$ time was proposed by Peter Shor [2]. This algo-rithm performs factoring exponentially faster than classicalcomputers.Thisalgorithmcouldfactora512-bitproductin about 3.5 hours with 1 GHz clock rate [3],whereas thenumber field sieve could factor the same product in 8400MIPS years [4].(One MIPS year is the number of instruc-tions that a processor can execute in a year, at the rate ofmillions of instructions per second.) Another famous quan-tum algorithm is a database search algorithm proposed byLovGroverthatwillfindasingleitemfromanunsorted listofNelementswithO($\sqrt{N}$)time[5].

Classicalcomputers,quantumcomputers,quantumcomputersys-tems,quantumsimulators,Shor'salgorithm

I. INTRODUCTION

Howmuchcantheperformanceofacomputerbeim-proved?According to Moore's law,if the performancekeeps improving by means of technological innovations,which has occurred over the last few decades, the number oftransistors per chip may be doubled every 18 months. Fur-thermore, processor clock frequency could reach as much as40 GHz within 10 years [1].By then, one atom may repre-sent one bit [1]. One of the possible problems may be that,becauseelectronsarenotdescribedbyclassicalphysicsbutbyquantummechanics,quantummechanicalphenomenonmay cause "tunneling" to occur on a chip.In such cases,electrons could leak from circuits. Taking into account thequantum mechanical characteristics of the one-atom-per-bit level, quantum computers have been proposed as oneway to effectively deal with this predicament. In this way,quantum computers can be used to solve certain compu-tationallyintenseproblemswhereclassicalcomputersre-

In this paper we briefly survey quantum computers.First, the main characteristics of quantum computers, su-perposition states, and interference are introduced. Then,current approaches to quantum computers are reviewed.Next, research on quantum computer simulators is intro-duced.Weconcludewithafewremarks.

II. QUANTUM COMPUTER SYSTEMS

SuperpositionState

In classical computers, electrical signals such as voltagesrepresent the 0 and 1 states as one-bit information.Twobits indicate four states 00, 01, 10, and 11, and n bits canrepresent

2^n states. In the quantum computer, a quantumbit called "qubit," which is a two-state system, representsthe one-bit information.For instance, instead of an elec-trical signal in classical computers, an electron can be usedasaqubit.Thespin-upandspin-downofanelectronrepresent two states: 0 and 1, respectively.A photon canalso be used as a qubit, and the horizontal and vertical po-larizationofaphotoncanbeusedtorepresentbothstates.Using qubits, quantum computers can perform arithmeticand logical operations as does a classical computer.Theimportant difference, however, is that one qubit can alsorepresent the superposition of 0 and 1 states.When werepresent 0 and 1 states as state vectors0and1respec-tively,suchasuperpositionstateisexpressedasalinear combinationof0and1 ,$|\psi\rangle = a|0\rangle + b|1\rangle$."" is called"ket-vector" in Dirac notation, and the coefficients a and bare called probability amplitudes.$|a|^2$indicates a proba-bility that we get $|\psi\rangle = |0\rangle$ as a result of the measurement onthequbit$|\psi\rangle = a|0\rangle + b|1\rangle$ .Theyalsosatisfy$|a|^2+|b|^2=1$.

Forexample,whentheprobabilityamplitudesaandbare

exampleofastatetransitiondiagramforthePTM,and Fig. 2 derives the PTM as a computation tree. In the tree,each vertex shows a machine state and each edge showstheprobabilityoftransitionoccurrence.

equalto1/2,wecanexpress asuperpositionstateof twostatesasfollows: $|\psi\rangle = (1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$,where vectors$|0\rangle = (1,0)^Tand|1\rangle = (0,1)^T$. Inshort, whenwe

measure astateof$|\psi\rangle$,thestatewillbeobservedas$|0\rangle$ with probability$(1/\sqrt{2})^2 = 1/2$andas$|1\rangle$ withprobability $(1/\sqrt{2})^2=1/2$.
This bizarrecharacteristic in quantum computers

makesparallelcomputationpossibleintherealsense oftheterm.Because each qubit represents two states at the sametime, two qubits can represent four states simultaneously.For instance, when we use two qubits that are the super-positionof0and1statesasaninputforanoperation,we can get the result of four operations for four inputswith just one computational step, as compared to the fouroperations needed by the classical computer.Likewise,when using n qubits, we can make a superposition of 2^nstatesasaninputandprocesstheinputinjustonestepto solve a problem for which a classical computer requires2^nsteps. In this light, a quantum computer can process ninputs with only one computational step after taking thesuperpositionstateofninputs.
However, there is a crucial problem to solve before wecan use this extremely valuable characteristic of quantumcomputers.Fromtheinputofonesuperpositionstaterepresentingfourstatesandprocessinginonestepweget the superposition of four results.When we measurethe output qubits, the quantum mechanical superpositioncollapses and each qubit will be observed as either 0 or 1because a qubit is a two-state system.Consequently, weonlygetoneofthefourpossibleresults:00,01,10,or11 (for n = 2) with the same probability.Accordingly, thesuperpositionofqubitsisgovernedbyprobability,andthe

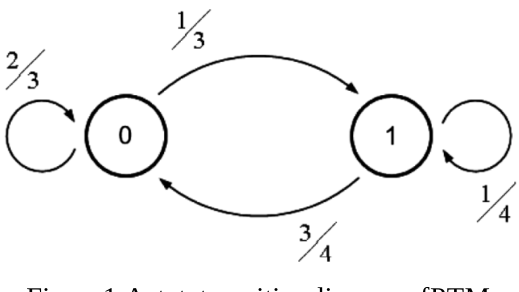

Figure1.AstatetransitiondiagramofPTM.

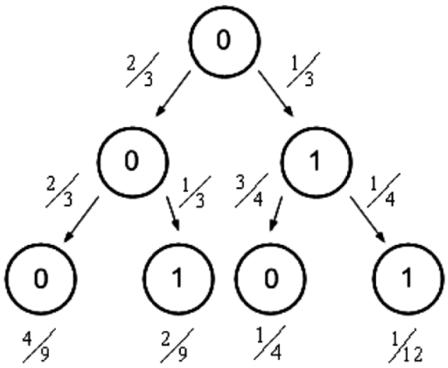

Figure2.AcomputationtreeofPTM.

Also, each level of the tree represents a computationstep and the tree's root represents the starting state.Wecan compute a probability of transition 01 after twocomputational steps, by summing the probabilities of thetwopossiblepathsfromtheroottostate1asfollows:

P(0→1)= ! 2×1 '' + ! 1×1 '' =2+1=11

measurementisnecessarytodeterminewhichoneofthe possiblestatesisrepresented.Thisdifficultyarisesfromusingthequantummechanicalsuperposition.If,however, wecanincreasetheprobabilityofgettingtheexpected

Similarly:
3 3 3 4
9 12 36

resultbydevisinganalgorithm,wemaytakeadvantage

P(0→0)= ! 2×2 '' + ! 1×3 '' =4+3=25

ofthequantummechanicalsuperpositionfeature. Inthis way,asdiscussedabove,wecanharnessthepowerof
3 3 3 4
9 12 36

quantumcomputerstosolveaproblemthattakesanexcessive amount of computational time and energy — forcertainproblemclassesonclassicalcomputers.

Interference

In this subsection, we give a simple example that illustratesthe difference between classical and quantum computation,andtheimportanceofinterference-of-statesinquantumcomputation. Clearly,anyclassicalcomputercanbesimulatedbya Turingmachine,amathematicalmodelofageneralcomputer. Before we discuss the quantum Turing machine(QTM),weintroduceacomputationtreeusingaclassical probabilisticTuringmachine(PTM)[6]. Fig.1showsan Wecaninterpretthisresultinthefollowingway.Intwosteps,startingfromstate0thePTMwilloccupystate 1withprobability11/36andstate0withprobability25/36.SimilartoPTM,we describe a computation of QTMusingthecomputationtreeshowninFig.3.EachedgeofthetreeinQTMrepresentsaprobabilityamplitude,whereasinthePTMeachedgerepresentsatransitionprobability.OnlyonestateinthesamelevelofthePTMtreeoccursatatime,butallstatesinthesameleveloftheQTMtreeoccursimultaneously!Forthisexample,theprobabilityof0 1fromtherootafteronecomputational stepis:

! 1 "2 1

−√2 = 2

1 1 1

Ψ(0→0→0)=√2×√2=2,

! " ! " 1

1 1

Ψ(0 1 0)= −√2 × √2

Ψ(0→0aftertwosteps)

=Ψ(0→0→0)+Ψ(0→1→0)

=1+ −1 =0

! "

2 2

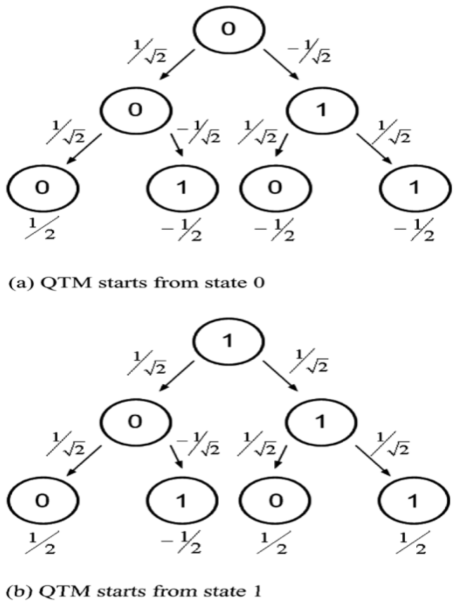

Figure3.AcomputationtreeofaQTM[7].

andtheprobabilityof0 0fromtherootafteronecom-putationalstepis:

1² 1

√2 =2 ! −"

Let us compute the probability of transition 01 aftertwosteps.First,weneedtofindtheprobabilityamplitudesofthetwopossiblepaths:Ψ(0→0→1)andΨ(0→1→1):

! "

1 1 1

Ψ(0 0 1)=√ × −√ =− 2

P(0→0aftertwosteps)=|Ψ(0→0aftertwosteps)|²

=|0|²=0

Thisisaremarkable result. After one computationalstep, the probabilities 0 1 and 0 0 were both 1/2.Butaftertwocomputationalstepsfrom the same rootthe probability 0 1 is 1 and probability 0 0 is 0.This result occurs because the probability amplitudes canhave negative values. We interpret this result as dueto the states of the QTM interfering with each other.Inshort,thecase“01aftertwosteps”had a con-structiveinterference[((1/2)) + ((1/2)) = 1] and thecase “00 after two steps” had a destructive interference[(1/2)+((1/2))=0].

In the previous subsection, we mentioned that the re-sultofacomputationinvolvingthesuperpositionofninputstates is a superposition of n-output states. For example, ifwe need to perform factorizing of an n-digit binary numberinto two prime factors, we must test 2^{n-1}numbers withEratosthenes' sieve as the worst-case scenario. Therefore,we must make a superposition of 2^{n-1}integers as inputgivingtheresultfromfactoringasthesuperposition of2^{n-1}outputs.

Ifwecandesignanoperationsuchthataconstructive interference occurs at desired outputs (e.g., prime factors)ofthesuperpositionof2^{n-1}outputsandadestructiveinterference occurs at unnecessary outputs, we can findprimefactorswithonlyonecomputationalstepascom-paredtotheclassicalcomputer,whichtakes2^{n-1}steps.Thisisan immenseimprovementincomputationtime.

$$\Psi(0\to1\to1)= -\frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} = -\frac{1}{2}$$

Weaddbothamplitudes:

Shor's algorithm performs factoring of large integers,though it is not just a single-step operation as described.Thealgorithmconsistsofbothquantumandclassicalprocessing. The quantum processing part utilizes quantuminterferenceandthesuperpositionstatetofindtheperiod

$$\Psi(0\to1\text{aftertwosteps})=\Psi(0\to0\to1)+\Psi(0\to1\to1)$$

$$= -\frac{1}{2} + -\frac{1}{2} = -1$$

rofthefunction$f_{x,n}(a)=x^a$modnwherenisanintegertobefactoredandxisanintegerchosenatrandomthatis coprimeton(i.e.,gcd(x,n)=1). Theclassicalpartmakes useofaresultfromclassicalnumbertheorytofindafactor

Thus, theprobability of transition 0 1aftertwo stepsis:

$$P(0\to1\text{aftertwosteps})=|\Psi(0\to1\text{aftertwosteps})|^2 = |(-1)|^2=1$$

Similarly,we computethe probability of transition0→0aftertwosteps:

ofnbyusingxandrfromthequantumpart.

III. CURRENT APPROACHES TO QUANTUM COMPUTERS

In this section we consider how such a quantum computercan be built. There are five experimental requirements forbuilding a quantum computer [8, 9]. The first requirementistheabilitytorepresentquantuminformationrobustly.

Because a qubit is a simple two-level system, a physicalqubitsystemwillhaveafinitesetofaccessiblestates.Some examples are the spin states of a spin 1/2 particle,the ground states and first excited states of an atom, andthe vertical and horizontal polarization of a single photon.Second,aquantumcomputerrequirestheabilitytosetafiducialinitialstate.Thisisasignificant problem formost physical quantum systems because of the imperfectisolation from their environment and the difficulty of pro-ducingdesiredinputstateswithhighfidelity.Third,a quantumcomputerrequireslongdecoherencetimes, muchlonger than the gate operation time.Decoherence is thecoupling between the qubit and its environment,whichresults in a loss of the quantum phase coherence.Afterdecoherence,thequantummechanicalpropertyassociatedwith coherence (e.g., superposition, entanglement) can nolonger be observed.The fourth requirement is the ca-pability of measuring output results from specific qubits.The outcome from a quantum algorithm is, in general, aquantum superposition.Therefore, it is necessary to readout a result from the quantum state using the classicalsystem with high fidelity.The fifth requirement concernsthe ability to construct a universal set of quantum gates.Similar to a classical computer, a quantum computer hasuniversal gates, which implement any legitimate quantumcomputation. DiVincenzo proved that just two-qubit gatesat a time are adequate to build a general quantum circuit[10].Usingtwo-qubitcontrolled-NOTgateand single-qubitgates,wecancomposeanymultiplequbitlogic gates.Moreover, once we can construct a two-qubit controlled-NOT gate,we can also build a quantum computer withcombinationsofthesegates.

Severalimplementationsforaquantumcomputerhavebeen proposed.One of the well-researched implementa-tions is a nuclear magnetic resonance (NMR) based quan-tum computer. This computer uses a vial of a liquid filledwith sample molecules as qubits.In this way, this experi-mental quantum computer solves a problem by controllingnuclear spins using NMR techniques and retrieves the re-sultsobservingtheensembledaverageofsomepropertyofthe nuclear spins in the vial.A seven-qubit NMR-basedquantum computer has been built, and the computer canperformShor'salgorithmfindingfactors of the number15[11].Thisiscurrentlythemostadvancedquantumcomputer.

An ion-trap-based quantum computer uses a string ofions confined in a linear trap [12].Each ion represents aqubit and is manipulated by laser beams.Photons fromions are observed as a result of an operation by photodetectors.A two-qubit controlled-NOT gate has alreadybeen demonstrated [13], and a quantum computer with alargenumberoftrappedionshasbeenproposed[14].

A cavity quantum electrodynamics (QED) based quan-tum computer has been proposed [15].This scheme usesphotons as qubits and implements a controlled-NOT gateusing the interaction of a linearly polarized photon as atarget bit and a circularly polarized photon as a control bitthrough cesium atoms inside an electromagnetic cavity [1].They measure a phase shift of the photon from the cavityasanoutputqubit.

In [16, 17], a linear optics quantum computer is pro-posedusingphotons. An optical mode (e.g., horizontalor vertical polarization) of a photon represents a state ofqubits.Quantum gates can be realized only with linearoptical elements. Placing beam splitters and phase shiftersbetween the paths of photons can control the states ofqubits for computations. As a two-qubit gate operation, anondeterministic controlled-NOT gate has been proposed.This gate operation requires additional ancillary photons,which are not part of the computation, and single-photondetections.

Aquantum-dot-basedquantumcomputerusesspins [18] or energy levels [19] of electrons confined in quantumdots (QDs) as qubits that are fabricated in semiconductormaterials.Because we can control states of qubitselec-trically, as we do in classical circuits, this scheme has anadvantagebecausecurrentsemiconductortechnologymaybeappliedtothefabricationofaquantumcomputer.

AsuperconductingquantumcomputerusestheJosephson-junctions in superconducting circuits as qubits[20]. Charge or energy levels in a junction represent infor-mation of qubits. A controlled-NOT gate operation on thechargedqubitswasdemonstrated,butthephaseevolutionduring the gate operation has not yet been examined [21].An implementation of the real quantum controlled-NOTgates is the next challenge in the realization of universallogicgates.

Although each proposed quantum computer has diffi-culties in its realization, a common critical problem is thatreal quantum memory registers incur errors caused by en-vironmental coupling (e.g., cosmic radiation, spontaneousemission, and decoherence).As it is extremely difficult toisolatequantumregistersperfectlyfromtheirenvironment,arealquantumcomputermustbedesignedconsideringtheeffectoferrorsonthestateofthequantumregisters.

To protect quantum states against the effects of noise,severalquantumerror-correcting(QEC)schemeshavebeenproposed [22–25].QEC codes could be developed basedupon principles similar to a classical error-correcting code.However, we need to circumvent the following three diffi-culties to design a QEC code [8]. First, we cannot pro-duce a repetition code (e.g., logical 0 and 1 is encoded as"000" and "111" respectively) by duplicating the quantumstate several times because the no-cloning theorem [26]statesthatreplicationofanarbitrary quantum state isnot possible.Second, unlike a classical bit, inspecting thestate to assess its correctness can destroy a qubit.Third,because the state of qubit depends on certain continuousparameters (e.g., a rotation angle θ), quantum errors arecontinuous. Consequently, infinite precision is required todeterminewhicherroroccurredtocorrectthem.

By implementing the QEC codes on a quantum circuit,wecanreducetheeffectofnoiseonquantumregistersandtransmissions.However, it is not sufficient for quantumcomputation because in practice gate operations (e.g., en-coding, decoding, and error correction) on the quantumcircuit are themselves prone to errors.Moreover, theseerrors are propagated and accumulated continuously untilthecomputationiscompleted. Topreventthepropagationandaccumulationoferrors on the quantum states, each procedure block in the quan-tum circuit (e.g., encoder, decoder, and error-correctingcircuit)shouldbedesignedcarefullysothatanyfailureduringtheprocedurecanonlypropagatetoasmallernum-berofqubitsthancanbecorrectedbytheQECcodes.Such procedures are called fault-tolerant procedures [8].Thedetailedtechniquesarepresentedinthetheoryoffault-tolerant quantum computation [27–33]. Accordingto the threshold theorem [8], an arbitrarily large quan-tum computation can be efficiently performed if the errorprobability per gate (EPG) is less than a certain constantthreshold.Recent research [34] indicates that the estimatesof the EPGs are as high as 3% if sufficient resources areavailable.

The first bit is called the controlled bit and the secondbit is the target bit.A unitary matrix of controlled-NOToperations for two qubits isrepresented as:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

For an n-qubits resister, a $2^n \times 2^n$ matrix is needed.We can also define the effect of errors on a qubit (i.e., a bitflip, a sign shift, both bit flip and sign shift) as the sum ofthePaulimatrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

1. QuantumComputerSimulators

Asindicatedabove,the numberof groups attemptingtorealizephysicalqubitshasincreasedoflate;however, it will take many more years before quantum gates areavailable for the computer scientist/engineer to use. Inthe meantime, we need a quantum computer simulator tofind new algorithms.Quantum computer systems can bemathematically represented by using vectors and matrices.Whenwedefine$|0\rangle = (1, 0)^T$and$|1\rangle = (0, 1)^T$,aNOToperationforonequbitcanbeexpressedwith2×2unitarymatricesas:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Wecanrepresentanoperationthataninitialcondi-tion$|1\rangle$ isconverted toasuperpositionstate$(1/\sqrt{2})|0\rangle +$

Thus,byusingthevectorsandunitarymatrices,wecansimulateatheoreticalquantumcomputermathematically.Manyquantumcomputersimulatorshavebeen pro-posedandimplemented[35,36].Someresearchershavesimulatedaquantumcomputerwithcommercial mathe-matics software packages.For example, Williams providedasimulatorasaMathematicanotebook[1]. ThissimulatorshowssomebasicoperationsonquantumcomputersandShor'salgorithm.Next,acommercialsoftware"quantumcomputersimulator"wasreleased[37].Thissoftwareal-lowsuserstosimulatemanysamplealgorithms(e.g., Shor'salgorithm,Grover'salgorithm)anduser-designedcircuits withacleavergraphicaluserinterface. Thetheoreticalquantumcomputersimulators,ingen-eral,performhighlyidealizedunitaryoperations.Inprac-

(1/√2)|1⟩ byusingamatrix:H=(1/√2)

1 1
1 1
11 0
1 1

tice,unitaryoperationsonaphysicalsystemaremore com-plicated.Therefore,anothertypeofquantumcomputersimulatorhasbeendevelopedasanemulatorofquantum computerhardware[38]. Thistypeofemulatorsimulates more realisticmodels strictlyfollowing thelawof quantum

$\mathbf{H}\cdot|1\rangle = \frac{1}{\sqrt{2}}$ −1 1

1

=√2

mechanics. MichielsensimulatesanNMR-likequantum

1 1 1 0 1 1

computer[39].Thehardwareinthesimulatorismodelled intermsofquantumspinsthatevolveintimeaccording

$= \frac{1}{\sqrt{2}}\,0 + \frac{1}{\sqrt{2}}\,1 = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

tothetime-dependentSchrödingerequation[40]. The detailedexplanationisgivenin[36]. Ageneralandsignificantproblemofquantumcom-putersimulatorsistheirinabilitytosimulatequantum computers with a large number of qubits (e.g., 500, 1000,or more bits required for RSA encryption algorithm).Torepresent a large number of qubits, an exponentially largememory is required (described earlier).Therefore, whenwe simulate a quantum computer with a large number ofqubits, we need to use a parallel computer [41]. For exam-ple, in [42] a quantum computer with up to 30 qubits wassimulatedusinganeight-processorparallelcomputer.

ThisoperationisknownasHadamardtransformation [8].

Multiple qubits are represented as a tensor product oftwo vectors 0 and 1. For example,two qubit resistersarerepresentedasfollows:

$|00\rangle = |0\rangle \otimes |0\rangle = (1000)^T$, $|01\rangle = |0\rangle \otimes |1\rangle = (0\ 1\ 0\ 0)^T$

$|10\rangle = |1\rangle \otimes |0\rangle = (0010)^T$, $|11\rangle = |1\rangle \otimes |1\rangle = (0001)^T$ Thecontrolled-NOToperationis:

$|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |11\rangle$, $|11\rangle \rightarrow |10\rangle$

IV. CONCLUSION

In this paper we have reviewed the principles, algorithms,and hardware considerations for quantum computing. Sev-eralresearchgroupsareinvestigatingqubitsandquantum logiccircuitryusingdifferentresources(i.e.,atom,ion,electron,andphoton,amongothers).Therealizationofa practical quantum computer is expected before we en-counter the limit of Moore’s law with respect to improve-ments that may be possible using the classical computermodel. A current realizable quantum computer is basedonseven-bitNMR,whichcanfactor15.Furtherresearchis needed, for example, via simulation, on quantum com-puters using classical computers. Such a simulator mustbe able to handle quantum computers that operate on apractically large number of qubits. To this end, we need toemploy large-scale parallel processing methods to acquiremoremeaningfulresultswithin a practical time frame.Byapplyingthemethods/conceptsof classicalcomput-ers such as hardware abstraction to quantum computers,the research progress may be accelerated.For example,some groups proposed quantum programming languagesthatallowustothinkofquantumcomputer operationsin an abstract manner as we do with a classical computer[43–45].

Efforts at realization for quantum computers have justbegun.Undoubtedly,weneedmoreintensiveresearchinaphysical realization of components of quantum computers[46].Computer scientists/engineers will need to considerthe various architectural solutions for quantum computersas well as the various new (practical) quantum algorithmstoadvancethestateoftheartforquantumcomputers.

REFERENCES

[1] C.P. Williams & S.H. Clearwater, Exploration in quantumcomputing(NewYork:Springer-Verlag,1997).

[2] P.W.Shor,Algorithmforquantumcomputation:Discretelogarithm and factoring, Proc. 35th IEEE Annual Symp. onFoundations of Computer Science, Santa Fe, NM, November1994,24–134.

[3] M. Oskin, F.T. Chong, & I. Chuang, A practical architecturefor reliable quantum computers, IEEE Computer, January2002,79–87.

[4] B. Preneel (Ed.), Factorization of a 512-bit RSA modules, Lec-ture Notes in Computer Science, Vol. 1807 (Berlin: Springer-Verlag,2000).

[5] L.K. Grover, A fast quantum mechanical algorithm for databasesearch,Proc.STOC,Philadelphia,1996,212–219.

[6] D.R. Simon, On the power of quantum computation, Proc. 35thAnnual Symp. on Foundations of Computer Science, Sante Fe,NM,1994,116–123.

[7] T. Nishino, Introduction to quantum computer (Tokyo: TokyoDenkiUniversityPress,1997)(inJapanese).

[8] M.A. Nielsen & I.L. Chuang, Quantum computation and quan-tuminformation(Cambridge:CambridgeUniversityPress,2000).

[9] D.P. DiVincenzo,The physical implementation of quantumcomputation,FortschrittederPhysik,48(9–11),2000,771–783.

[10] D.P.DiVincenzo,Two-bitgatesareuniversalforquantumcomputation,PhysicalReviewA,51,1995,1015–1022.

[11] IBMResearchNews,IBM'stest-tubequantumcomputermakeshistory:Firstdemonstration ofShor's historic factor-ing algorithm, http://www.research.ibm.com/resources/news/20011219_quantum.shtml.

[12] J.I.Cirac&P.Zoller,QuantumcomputationswithcoldtrappedIons,PhysicalReviewLetters,74,1995,4091.

[13] C.Monroe, D.M. Meekhof, B.E. King, W.M. Itano, &
D.J. Wineland, Demonstration of a fundamental quantum logicgate,PhysicalReviewLetters,75,1995,4714.

[14] D.Kielpinski,C.Monroe,&D.J.Wineland,Architecturefora large-scale ion-trap quantum computer, Nature, 417, 2002,709–711.

[15] Q.A.Turchette, C.J. Hood, W. Lange, H. Mabuchi, &H.J.Kimble,Measurementofconditionalphaseshiftsforquantumlogic,PhysicalReviewLetters,75,1995,4710–4713.

[16] E. Knill, R. Laflamme, & G. J. Milburn, A scheme for efficientquantum computation with linear optics, Nature, 409, 2001,46–52.

[17] T.C. Ralph, A.G. White, & G.J. Milburn, Simple scheme forefficient linear optics quantum gates, Physical Review A, 65,2002,012314-1–012314-6.

[18] D.Loss&D.P.DiVincenzo,Quantumcomputationwithquantumdots,PhysicalReviewA,57,1998,120–126.

[19] M.S. Sherwin, A. Imamoglu, & T. Montroy, Quantum com-putation with quantum dots and terahertz cavity quantumelectrodynamics,PhysicalReviewA,60,1999,3508–3514.

[20] Y. Makhlin, G. Schon, & A. Shnirman, Quantum-state engi-neering with Josephson-junction devices, Reviews of ModernPhysics,73,2001,357–400.

[21] T.Yamamoto,Y.A.Pashkin,O.Astafiev,Y.Nakamura,&J.S.Tsai,Demonstrationofconditionalgateoperationusingsuperconductingchargequbits,Nature,425,2003,941–944.

[22] P.W.Shor,Schemeforreducingdecoherenceinquantumcomputermemory,PhysicalReviewA,52,1995,R2493–R2496.

[23] A.R.Calderbank&P.W.Shor,Goodquantumerror-correctingcodesexist,PhysicalReviewA,54,1996,1098–1105.

[24] A. Ekert,& C. Macchiavello,Quantum error correction forcommunication,PhysicalReviewLett

ers,77,1996,2585–2588.
[25] A.M. Steane, Error correcting codes in quantum theory, Phys-icalReviewLetters,77,1996,793–797.
[26] W.K. Wootters& W.H. Zurek, A single quantum cannot becloned,Nature,299,1982,802–803.
[27] P.W. Shor, Fault-tolerant quantum computation, Proc. 37thIEEEAnnualSymp.onFoundations ofComputerScience,Burlington,VT,1996,56–65.
[28] J. Preskill, Reliable quantum computers, Proc. of the RoyalSocietyofLondon,A454,1998,385–410.
[29] A.M. Steane, Efficient fault-tolerant quantum computing, Na-ture,399,1999,124–126.
[30] D.Gottesman,Fault-tolerantquantumcomputationwithlocal gates,JournalofModernOptics,47,2000, 333–345.
[31] E.Knill&R.Laflamme,Concatenatedquantumcodes,quantph/9608012,1996.
[32] P.O. Boykin, C.P. Roychowdhury, T. Mor, & F. Vatan, Faulttolerant computation on ensemble quantum computers, Int.Conf. on Dependable Systems and Networks, Florence, Italy,2004,157–166.
[33] E. Knill,R. Laflamme,& W. Zurek,Accuracy threshold forquantumcomputation,quant-ph/9610011,1996.
[34] E.Knill,Quantumcomputingwithrealisticallynoisydevices,Nature,434,2005,39–44.
[35] J.Wallace,Quantumcomputersimulators,InternationalJour-nalofComputingAnticipatorySystem,10,2001,230–245.
[36] H. De Raedt& K. Michielsen,Computational methods forsimulatingquantum computers,quant-ph/0406210, 2004.
[37] World'sfirstuniversalquantumcomputationsimulator,Quantum computer simulator,SENKO Corporation,http://www.senko-corp.co.jp/qcs/index.html.
[38] H. De Raedt, A.H. Hams, K. Michielsen, & K. De Raedt, Quan-tum computer emulator, Computer Physics Communications,132(1–2),2000,1–20.
[39] K.Michielsen, H. De Raedt, & K. De Raedt, A simulatorfor quantum computer hardware, Nanotechnology, 13, 2002, 23–28.
[40] D.J.Griffiths,Introductiontoquantummechanics(EnglewoodCliffs,NJ:Prentice-Hall,1995),1–2.
[41] K.M.Obenland&A.M.Despain,Aparallel quantumcomputersimulator,HighPerformanceComputing,1998,quantph/9804039.
[42] J. Niwa, K. Matsumoto, & H. Imai, General-purpose parallelsimulatorforquantumcomputing,PhysicalReviewA,66,2002,062317-1–062317-11.
[43] J.W. Sanders & P. Zuliani, Quantum programming, Mathe-matics of program construction, Lecture Notes in ComputerScience,1837(Heidelberg:SpringerVerlag,2000),80–99.
[44] B.Ömer,Classicalconceptsinquantumprogramming,Quan-tumStructures,2002,http://arxiv.org/abs/quant-ph/0211100.
[45] P.Selinger,Towardsaquantumprogramminglanguage,Math-ematicalStructuresinComputerScience,14,2003,527.
[46] Quantum computation roadmap, http://qist.lanl.gov/qcomp_map.shtml.