CSI Elections 2015-2016/2017

As authorised by the Constitution section 5.7 and section 5.8, we present herewith the results of the elections conducted for the year 2015-2016/2017. The closing date for the receipt of the ballots was January 16, 2015. The results of the elections are given below:

The following are declared elected:

For the Term 2015-2016 (April 1, 2015 - March 31, 2016)

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President cum President Elect (2015-16)</td>
<td>Dr. Anirban Basu</td>
</tr>
<tr>
<td>Nomination Committee (2015-16)</td>
<td>Prof. (Dr.) Anil K Saini</td>
</tr>
<tr>
<td></td>
<td>Mr. Rajeev Kumar Singh</td>
</tr>
<tr>
<td></td>
<td>Prof. (Dr.) U K Singh</td>
</tr>
<tr>
<td>Hon. Treasurer (2015-17)</td>
<td>Mr. R K Vyas</td>
</tr>
<tr>
<td>Regional Vice President (Region I - 2015-17)</td>
<td>Mr. Shiv Kumar</td>
</tr>
<tr>
<td>Regional Vice President (Region III - 2015-17)</td>
<td>Dr. Vinip Tyagi</td>
</tr>
<tr>
<td>Regional Vice President (Region V - 2015-17)</td>
<td>Mr. Raju L Kanchibhotla</td>
</tr>
<tr>
<td>Regional Vice President (Region VII - 2015-17)</td>
<td>Mr. K Govinda</td>
</tr>
<tr>
<td>Divisional Chair Person - Div. I (2015-17)</td>
<td>Prof. M N Hoda</td>
</tr>
<tr>
<td>Divisional Chair Person - Div. III (2015-17)</td>
<td>Mr. Ravikiran Manikkar</td>
</tr>
<tr>
<td>Divisional Chair Person - Div. V (2015-17)</td>
<td>Mr. Suresh Chandra Satapathy</td>
</tr>
</tbody>
</table>

For the Term 2015-2017 (April 1, 2015 - March 31, 2017)

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President cum President Elect (2015-16)</td>
<td>Dr. Anirban Basu</td>
</tr>
<tr>
<td>Nomination Committee (2015-16)</td>
<td>Prof. (Dr.) Anil K Saini</td>
</tr>
<tr>
<td></td>
<td>Mr. Rajeev Kumar Singh</td>
</tr>
<tr>
<td></td>
<td>Prof. (Dr.) U K Singh</td>
</tr>
<tr>
<td>Hon. Treasurer (2015-17)</td>
<td>Mr. R K Vyas</td>
</tr>
<tr>
<td>Regional Vice President (Region I - 2015-17)</td>
<td>Mr. Shiv Kumar</td>
</tr>
<tr>
<td>Regional Vice President (Region III - 2015-17)</td>
<td>Dr. Vinip Tyagi</td>
</tr>
<tr>
<td>Regional Vice President (Region V - 2015-17)</td>
<td>Mr. Raju L Kanchibhotla</td>
</tr>
<tr>
<td>Regional Vice President (Region VII - 2015-17)</td>
<td>Mr. K Govinda</td>
</tr>
<tr>
<td>Divisional Chair Person - Div. I (2015-17)</td>
<td>Prof. M N Hoda</td>
</tr>
<tr>
<td>Divisional Chair Person - Div. III (2015-17)</td>
<td>Mr. Ravikiran Manikkar</td>
</tr>
<tr>
<td>Divisional Chair Person - Div. V (2015-17)</td>
<td>Mr. Suresh Chandra Satapathy</td>
</tr>
</tbody>
</table>

CSI Chapters Elections

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treasurer (Bangalore Chapter) (2015-17)</td>
<td>Mr. Satish B G</td>
</tr>
<tr>
<td>Management Committee (Bangalore Chapter) (2015-16)</td>
<td>Dr. Prahlad Rao</td>
</tr>
<tr>
<td></td>
<td>Dr. Manju Nanda</td>
</tr>
<tr>
<td></td>
<td>Dr. Arindam Sen</td>
</tr>
<tr>
<td></td>
<td>Mr. Ravi K S</td>
</tr>
<tr>
<td></td>
<td>Mr. Mohan Ramanathan</td>
</tr>
<tr>
<td></td>
<td>Dr. K Satyanarayan Reddy</td>
</tr>
<tr>
<td></td>
<td>Dr. C K B Nair</td>
</tr>
<tr>
<td></td>
<td>Mr. Anbunathan R</td>
</tr>
<tr>
<td>Treasurer (Kolkata Chapter) (2015-17)</td>
<td>Dr Ambar Dutta</td>
</tr>
<tr>
<td>Management Committee (Kolkata Chapter) (2015-16)</td>
<td>Prof. Paramartha Dutta</td>
</tr>
<tr>
<td></td>
<td>Dr. Tanushyam Chattopadhyay</td>
</tr>
<tr>
<td></td>
<td>Dr. Ajanta Das</td>
</tr>
<tr>
<td></td>
<td>Ms. Sharmila Ghosh</td>
</tr>
<tr>
<td></td>
<td>Dr. Abhik Mukherjee</td>
</tr>
<tr>
<td></td>
<td>Prof. Subho Chaudhuri</td>
</tr>
<tr>
<td></td>
<td>Ms. Madhumita Sengupta</td>
</tr>
<tr>
<td></td>
<td>Dr. Sanjoy Kumar Saha</td>
</tr>
</tbody>
</table>

Following two amendments were also put to vote and the results are in favour, as detailed below,

1) Under CSI Constitution and Byelaws:
   a) Addition Under Section 4.3.3 (b) Finance Committee of CSI Constitution and Byelaws which reads as:
      v) in prescribing the manner of maintaining centralised accounts as required for consolidation on a monthly/annual basis for complying with statutory requirements.
   b) “Section 3.5 Student Branches” to be replaced by “section 3.5 Accredited Student Branches”.

2) Under CSI Chapter Byelaws:
   a) Section 4.2.6 of Chapter Byelaws which reads as follows:
      “The MC shall approve a Scheduled bank to deposit the funds received by the Chapter. It shall also designate the Officers (s) authorised to operate thereon.”
      It shall read
      “The ExecCom shall approve a Scheduled bank to deposit the funds received by the Chapter. ExecCom shall also designate the Officers (s) authorised to operate thereon.”
   b) “Section 3.1 of Chapter Byelaws “Student Branches” to be replaced by “Section 3.1 Accredited Student Branches”

CSI 2015-16/17 Highlights/ Statistics

Total eligible votes: 14,903
Total no. of votes casted: 3,696
Total % of voting: 24.80%

Votes secured by individuals candidates can be viewed at http://www.csi-india.org/results-2014 and follow the link Please click here to see no. of ballots against each candidate.
## Contents

**Volume No. 38 • Issue No. 11 • February 2015**

### Editorial Board
- **Chief Editor**
  - Dr. R M Sonar
- **Editors**
  - Dr. Debasish Jana
  - Dr. Achuthsankar Nair
- **Resident Editor**
  - Mrs. Jayshree Dhere

### Published by
- **Executive Secretary**
  - Mr. Suchit Gogwekar
  - For Computer Society of India

### Design, Print and Dispatch by
- CyberMedia Services Limited

### Cover Story
- **Quantum Information and Computation Systems**
  - Vishal Sahni and Dayal Pyari Srivastava

### Technical Trends
- **Study of Quantum Computing with Significance of Machine Learning**
  - Hardik A Gohel and Priyanka Sharma

### Research Front
- **Frontiers of Research in Harnessing the Quantum World**
  - Martin Laforest

### Practitioner Workbench
- **Software Engineering Tips**
  - A New Software Engineering
  - Ivar Jacobson and Ed Seidewitz

### Security Corner
- **Case Studies in IT Governance, IT Risk and Information Security**
  - A Case Study of Niti Aayog of the State of Surashtra
  - Dr. Vishnu Kanhere

### Plus
<table>
<thead>
<tr>
<th>Topic</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brain Teaser</td>
<td>44</td>
</tr>
<tr>
<td>Dr. Debasish Jana</td>
<td></td>
</tr>
<tr>
<td>Happenings@ICT</td>
<td>45</td>
</tr>
<tr>
<td>H R Mohan</td>
<td></td>
</tr>
<tr>
<td>CSI Reports</td>
<td>46</td>
</tr>
<tr>
<td>CSI News</td>
<td>47</td>
</tr>
</tbody>
</table>

---

Please note:
CSI Communications is published by Computer Society of India, a non-profit organization. Views and opinions expressed in the CSI Communications are those of individual authors, contributors and advertisers and they may differ from policies and official statements of CSI. Those should not be construed as legal or professional advice. The CSI, the publisher, the editors and the contributors are not responsible for any decisions taken by readers on the basis of these views and opinions.

Although every care is being taken to ensure genuineness of the writings in this publication, CSI Communications does not attest to the originality of the respective authors’ content. © 2012 CSI. All rights reserved.

Instructors are permitted to photocopy isolated articles for non-commercial classroom use without fee. For any other copying, reprint or republication, permission must be obtained in writing from the Society. Copying for other than personal use or internal reference, or of articles or columns not owned by the Society without explicit permission of the Society or the copyright owner is strictly prohibited.

Published by Suchit Gogwekar for Computer Society of India at Unit No. 3, 4th Floor, Samruddhi Venture Park, MIDC, Andheri (E), Mumbai-400 093.
Tel.: 022-2926 1700 • Fax.: 022-2830 2133 • Email: hq@csi-india.org Printed at GP Offset Pvt. Ltd., Mumbai 400 059.
Important links on CSI website

For queries, correspondence regarding Membership, contact helpdesk@csi-india.org
Dear Members

Let me, on behalf of CSI family, excom and my own self congratulate Dr. Vijay P Bhaktar for being awarded Padma Bhushan, the third highest civilian award. CSI along with the entire Scientific Community is proud of his contributions in high performance computing (including the development of Paraview, the Indian supercomputer), Indian language computing, education to home and integrative education and building institutions like CDAC, ER&DCC and I2IT. CSI also congratulates Prof. Bimal K. Roy, Director of the Indian Statistical Institute and a well-known Statistician and Cryptologist who has been a supporter of CSI in many events for being awarded Padma Shri award.

The Annual Students Convention (ASC) on the theme “Campus to Corporate and Beyond” was hosted by the Guru Nanak Institutions (GNI) at their campus on 3rd and 4th Jan 2015 was well attended with about 1000 student members of which over 450 came from outside Hyderabad. Shri E.S.L. Narasimhan, Governor of Andhra Pradesh & Telengana inaugurated the ASC and in his address highlighted the need for innovation, creativity and the changes in the current educational system to nurture the talents and use for the nation building. Prof. S.V. Raghavan, Past President of CSI and Dr. S.S. Mantha, Former Chairman of AICTE delivered motivational talks. The ASC comprised panel discussions on topics such as “Campus to Corporate”, “Career Opportunities”, “Entrepreneurship”, “Employment Opportunities in Public Sector” and “Technology Enablement in Education” with panelists drawn from CSI family, industry and academia had several other technical events/competitions including paper presentations which benefited the participants and were completed fully during the two days of the convention. On behalf of CSI, I congratulate and thank Dr. H.S. Saini, Managing Director of GNI, Fellow of CSI and the Convention Chair ably supported by the dedicated contributions of Dr. D.D. Sarma, Fellow of CSI, Mr. Raju, RVP-S, Mr. Gautam Mohapatra, Chair of CSI Hyderabad and Mr. Chandrasekhar, RSC, the entire staff of GNI and a team of CSI Hyderabad for the successful conduct of the ASC even though it had to be postponed and run in a short lead time after the CSI-2014. Our sincere thanks to the management of GNI for their direct involvement and extending full hearted support and hosting the convention in style providing all facilities including accommodation tooustation participants. It was heartening to note that a group of over 50 student members along with all staff came the way from Kanyakumari, the tip of India to attend the ASC.

I had the honour and privilege of inaugurating a new CSI Chapter at Mylavaram, an interior town near Vijayawada in Andhra Pradesh, Prof. P. Thrimurthy, CSI Fellow was instrumental in promoting this chapter. The efficient follow-up of Mr. Y. Kathiresan, Senior Manager (Promotions) at CSI ED and the initiative of Dr. E.V. Prasad, Prasad, of CSE and Director at Lakreddy Bali Reddy College of Engineering and the support of the college management facilitated the chapter formation in a record time. Mr. Raju, RVP-S Mr. A.V. Praveen Krishna, SB Counselor of CSI KL Univ. SB and Y. Kathiresan from CSI ED joined me at the inauguration of the Chapter and highlighted about the CSI activities and how it can help professional, academic and student community. The first Management Committee of the Mylavaram chapter was formed with Dr. Prasad as its first and founding chairman who in his address highlighting the plans of the chapter informed that the membership will be increased to over 100 within a year and also proposed to organize two to three conferences in this year itself. The chapter is the youngest one and has desire to grow. Let us support for its growth in all possible ways.

I wish to inform that the members of the CSI Nominations Committee for the year 2014-15 had conducted the CSI elections for the period 2015-2016 as per guidelines and announced the results in time. It is encouraging to note an increase in voting from 15.6% last year to 24.8%. However, there had been some concerns from members during the election period and after the announcement of results. These are being addressed.

As informed in my earlier message that in the Think Tank Meeting held during the CSI-2014, our Fellows deliberated on the Past, Present and Future of the CSI and shared their wish list. The compiled list is available at: http://goo.gl/Uwx9Ii and it will be updated regularly while excom will discuss and prioritize the items to be taken up for implementation.

I would like to take this opportunity in renewing my request for your contributions for the CSI HISTORY compilation. I am sorry to inform that the response to our request sent by email in multiple times during the last year and few inserts in CSI Communications has not been significant. May I once again request you to provide us whatever material you could share with us to compile the CSI HISTORY to present the same at least at the CSI-2015 to be held at Delhi in Oct 2015. Capturing information spread over about 50 years is a difficult task and without your help it is near impossible. I earnestly request all of you to do the needful and help us in documenting the CSI HISTORY. While physical items can be sent to CSI ED, material in electronic form may be sent to us by email at csi.history@gmail.com

Our activity year is nearing end and we have just two more months to go. While a number of CSI Chapters have celebrated and are planning to celebrate CSI@50 - the Golden Jubilee celebrations at their chapters involving people who had contributed to the growth of CSI. I urge other chapters to take initiative to conduct CSI@50 event at their chapters and also utilize the financial support being extended from CSI HQ. While doing so, I request all the divisions, chapters, student branches to update their other events and activities carried out during the year in the google form at http://goo.gl/nL1akS One can see the updated list at http://goo.gl/IBQaK3 It may please be noted that the activities included in this list will be taken as a record for CSI awards to chapters and SBs and also for compiling our annual report.

In an endeavor to build a reference library at CSI ED, we have been requesting the various Organizational Units of CSI organizing the conferences to provide a copy of the proceedings to CSI ED. While some have complied with our request, we note that we are not receiving all the proceedings. It will be great if we can build this reference library which will be very useful to our student members and members at large. In this context, I also request our members to donate books and other reference materials for adding in the library at CSI ED. Their contributions will be suitably acknowledged. A partial list of additions in the CSI ED may be seen at http://goo.gl/5aNCLD

An update from the CSI ED. Conducted a two days BOSS MOOL Workshop with the support of CDAC & IIT Madras at KPR College of Engineering, Coimbatore; Organised the first Research Symposium which provided the platform for the young researchers to present and deliberate their findings with the peer group and increase their confidence level; Participated in the MSME exhibition at Chennai and promoted the CSI activities among the small scale industries; Organising the first Research Conclave with the patronage of DeitY at CUSAT in Feb 2015 to propagate the Visvesvaraya Ph.D. Assistance Scheme of the Government of India and help the academicians and the aspiring researchers to identify research areas and to explore possibilities of support under the Scheme.

Consistent with realizing the enhanced and ambitious vision of “IT for Masses,” CSI has launched an initiative that extends its services to schools through Institutional Membership (IM) to schools. The IM scheme is aimed at helping schools in computer education and use. As can be seen from the brochure at http://goo.gl/aXY625 the IM provides significant, long lasting benefits of value to the school - its management, teachers and students. The website at http://goo.gl/ZeEQ7k provides the details on how a school can become an Institutional Member. We request our members to promote the IM in CSI among the schools.

I am sure that members would have noted the extension of the 15% Golden Jubilee discount to enroll as Life Members in CSI till March 2015. Please encourage your colleagues and contacts to avail this limited time offer and become members and strengthen CSI.

Due to space constraints, let me close my message now and include few more interesting items in the next month.

With best regards
H.R. Mohan
President
Computer Society of India
This article presents the fundamental concepts in quantum computation and information and some of the startling speedups obtained with quantum algorithms. The future outlook of quantum computing is also presented along with interesting ideas about quantum computing in microtubules in the brain.

**Introduction to Quantum Computing**

Calculations like searching the Internet, modeling the national economy, forecasting the weather, strain the capacities of even the fastest and most powerful computers. The difficulty is not so much that microprocessors are too slow; it is that computers are inherently inefficient. The reason, in large part, is that the logic built into microprocessors is inherently serial. A truly parallel computer, in contrast, would have simultaneity built into its very nature. It would be able to carry out many operations at once, to search instantly through a long list of possibilities and point out the one that solves a problem.

Such computers do exist and are called quantum computers - not so much because they are inherently small, but because they operate according to the bizarre rules of quantum mechanics, which do indeed govern the world of the very small: the waves and particles of subatomic physics. One quantum rule in particular creates an enormous incentive to apply quantum mechanics to computing: the startling discovery by twentieth-century physicists that elementary particles such as protons, neutrons and electrons can persist in two or more states at once. That makes it possible, at least in principle, for them to be harnessed as processing units in a machine more efficient than any conventionally designed “classical” computer could ever be.

**A Historical Note**

In the 1970s and early 1980s physicists and computer scientists began to investigate how the properties of quantum superpositions might be applied to computing. Early workers in the field - including the physicists Charles H. Bennett of the IBM Thomas J. Watson Research Center in Yorktown Heights, New York, Paul A. Benioff of Argonne National Laboratory in Illinois, David Deutsch of the University of Oxford and the late Richard P. Feynman - showed that particles in superposed states can function as quantum bits, or qubits, and can undergo operations analogous to the NOT, OR and AND operations of classical computing. But that is not all. Quantum computers, if they can be built, could achieve results that would seem almost magical - and quite different from anything a classical system has to offer.

**Quantum computers, if they can be built, could achieve results that would seem almost magical and quite different from anything a classical system has to offer**

In principle, for 500 particles, we could create a quantum system that is a superposition of as many as $2^{500}$ states. Each state would be a single list of 500 1's and 0's. Any quantum operation on that system - a particular pulse of radio waves, for instance, whose action was, say, to execute a controlled-NOT operation on the 175th and 176th qubits - would simultaneously operate on all $2^{500}$ states. Hence with one machine cycle, one tick of the computer clock, a quantum operation could compute not just on one machine state, as serial computers do, but on $2^{500}$ machine states at once! That number, which is approximately equal to a 1 followed by 150 zeros, is far larger than the number of atoms in the known universe. Eventually, of course, observing the system would cause it to collapse into a single quantum state corresponding to a single answer. A single list of 500 1's and 0's - but that answer would have been derived from the massive parallelism of quantum computing.

The consequence is that for some purposes quantum computers would be so much faster than classical computers that they could solve problems the classical computers cannot touch. If functioning quantum computers can be built, harnessing their potential will be just a matter of creating algorithms that carry out the right operations in the right order.

Quantum information has arisen in response to a variety of converging scientific challenges. One goal is to probe the foundations of the theory of computation. What limits are imposed on computation by the fundamental laws of physics, and how can computational power be enhanced by exploiting the structure of these laws? Another goal is to extend the theory of communication. What are the ultimate physical limits on the performance of a communication channel, and how might quantum phenomena be harnessed by new communication protocols? Yet another challenge is to understand and overcome the quantum effects that constrain how accurately we can monitor and manipulate physical systems. What new strategies can be devised to push back the frontier of quantum-limited measurements, or to control the behavior of intricate quantum systems?

What makes this quest intellectually compelling is that the results are so surprising. At first glance, quantum effects seem to compromise our efforts to store, transmit, and process information, because quantum states are highly unstable and cannot be observed without being disturbed. Indeed, as the components of integrated circuits continue to shrink toward the atomic scale, quantum phenomena will pose increasingly serious limitations on the performance of information processing hardware, and one important task of quantum information science will be to illuminate whether and how such obstacles can be overcome. But the great surprise is that the news about quantum effects is not all bad — far from it! The fragility of quantum information becomes a very positive feature when it is recognized that eavesdropping on a quantum communication channel necessarily leaves a detectable imprint, so that communicating with qubits provides better privacy than communicating with classical bits. Far more astonishing,
the intrinsic complexity of quantum information ensures that quantum systems of modest size are endowed with truly vast computational power, so that a quantum computer acting on just hundreds of qubits is capable in principle of performing tasks that could never be performed by conventional digital computers.

Moore's Law Limits

The question that arises is that how long can Moore's law (Fig. 1) continue to hold since he formulated it in 1965. What are the ultimate limits, if any, to computing technology? How will the technology need to change in order to improve as much as possible? What will happen to our civilization if the Moore Law will stop to work? While quantum computers will perform computations at the atomic scale, we might ask at this point how close conventional computations are to this scale already? Figure 2 shows Moore's law in a different way as the size of transistors reduces on silicon real-estate, i.e. the number of dopant impurities in the bases of bipolar transistors used for digital logic against the year. This plot may be thought of as showing the number of electrons required to store a single bit of information. An extrapolation of the plot suggests that we might be within reach of the atomic-scale computations within a decade. This plot is perhaps even more relevant for the development of quantum computation. Conventional computers have been improving in speed and miniaturization at an exponential rate since their earliest days. Clearly there is a bound to our ability to miniaturize conventional electronics and we will likely be touching that limit within the next ten to twenty years. The question is raised, can we continue to expect to see an exponential improvement in performance twenty and more years from now? As we approach some of the physical limits to conventional computational construction we may begin to see a slow-down of this exponential rate. A detailed study of quantum computation may help us understand the fundamental physical limitations upon computation, conventional or otherwise.

Providing a complete history of ideas relevant to quantum computing is a formidable task. Our subject brings together what are arguably two of the greatest revolutions in twentieth-century science, namely quantum mechanics and information science (including computer science). Figure 3 attempts to give a relationship between these two giants. The well-established theory of classical information and computation is actually a subset of a much larger topic, the emerging theory of quantum information and computation (Fig. 4).

From Bits to Qubits (Quantum Bits) to Quantum Dits (Qdits)

Boiled down to its essentials, any computer must meet two requirements: it must be able to store information as strings of 1’s and 0’s, or bits, and it must have a way of altering the bits in accordance with instructions. A computer transforms its bits by means of gates, or devices designed to carry out simple operations in logic. For example, a NOT gate converts any input bit into its opposite (0 becomes 1, and 1 becomes 0). An OR gate, by contrast, converts two input bits into a single bit whose value is the higher of the two (0 OR 0 yields 0; any other combination gives 1). And an AND gate yields a 1 only if both input bits are 1’s; otherwise, its output is a 0. Everything a computer does - whether synthesizing speech, calculating the billionth digit of pi or beating Garry Kasparov at chess - ultimately comes about through the transformation of bits by gates.

Every electron acts as if it were a little magnet, spinning about an axis, whose magnetic moment can point in only one of two directions, up or down

Could subatomic particles store bits? Could they form gates? Consider the electron. Every electron acts as if it were a little magnet, spinning about an axis, whose magnetic moment can point in only one of two directions, up or down. Thus the spin of the electron is quantized: it has just two possible states, which can readily be identified with the 0’s and 1’s of an ordinary computer processor. And we can flip the bit - that is, change a down, or 0, to an up, or 1, by adding just a smidgen of energy.
Suppose, however, we give it less energy than that - say, half a smidgen. Once again, when we observe the electron’s spin state, we will find that the spin is quantized: it points either up or down. But now there is an important, though subtle, difference. According to the rules of quantum mechanics, the probability of observing the spin in one or the other state will change. That change arises from a qualitatively new state, with no analogue in the ordinary, nonquantum, laws of physics, called a superposition of the two spin states: a combined, in-between condition that can be, say, 60 percent up and 40 percent down, or 22 percent up and 78 percent down.

We can generalize quantum information processing further to quantum dits or qudits that are d-level systems as an extension of qubits that could speed up computing tasks even further. A qubit is then a special case of a qudit with d = 2. In comparison to the qubit system, d-dimensional quantum states will be more efficient in quantum applications. With larger state space, the qudit algorithms may improve channel capacity and quantum gates implementation, increase security and explore quantum features. The qudit systems have also been experimentally realized. The high-dimensional quantum system maybe provide different quantum correlations and efficient information processing.

With larger state space, the qudit algorithms may improve channel capacity and quantum gates implementation, increase security and explore quantum features.

Suppose we want to look up a phone number in a telephone directory that has 10^24 entries. An optimal classical search algorithm will take on the order of 10^24 steps to find the phone number. That’s a lot of work! But suppose there is a quantum computer that can search through the phone book in about 10^10 steps. How does that compare? In 1996, Grover discovered a quantum search algorithm that can search an unsorted database in O(n) steps. That’s an exponential speedup over any classical algorithm.

### Table 1: An interesting comparison between classical and quantum computers in factorizing a 300 digit number

<table>
<thead>
<tr>
<th>Algorithm Type</th>
<th>Order</th>
<th>Steps</th>
<th>Execution Time on a Terahertz (THz) Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Classical Algorithm</td>
<td>O(2^n/3 log(n)^(1/3))</td>
<td>10^24</td>
<td>150,000 years (Classical THz computer)</td>
</tr>
<tr>
<td>Shor’s Quantum algorithm</td>
<td>O(n^3)</td>
<td>10^10</td>
<td>&lt; 1 second (Quantum THz computer)</td>
</tr>
</tbody>
</table>

Another startling result is Grover’s contribution to quantum computation as an efficient quantum mechanical algorithm for searching unsorted databases. That algorithm, discovered in 1996, is faster than any classical algorithm can ever be. More than that, it has been shown that no other quantum mechanical algorithm can ever beat it either, i.e. it is optimal.

Suppose we want to look up a phone number in a telephone directory that has
A quantum computer could do much better, thanks to its ability to carry out many operations at the same time.

A million entries. Suppose, too, that we have forgotten the person’s name; all the information to search with is an address. In that case, our only recourse is trial and error. On average, we will read the names of 500,000 strangers before we find the one we want; on a very bad day, we might have to look at 999,999 of them. A computer could search much faster, but algorithmically it would be in the same boat: in general, a list of N items takes, on average, $N/2$ steps to search.

A quantum computer could do much better, thanks to its ability to carry out many operations at the same time. quantum superposition, the computation takes place on all states simultaneously. Table 2 illustrates some “quantum” type algorithms giving a startling speedup over classical algorithms.

<table>
<thead>
<tr>
<th>Year</th>
<th>Algorithm</th>
<th>Speedup obtained</th>
</tr>
</thead>
<tbody>
<tr>
<td>1985</td>
<td>Deutsch’s algorithm</td>
<td>Demonstrates tasks quantum computers can perform in one shot that classical takes two shots</td>
</tr>
<tr>
<td>1992</td>
<td>Deutsch-Jozsa algorithm</td>
<td>Demonstrates an exponential separation between classical deterministic and quantum algorithms</td>
</tr>
<tr>
<td>1993</td>
<td>Bernstein-Vazirani algorithm</td>
<td>Demonstrates a superpolynomial separation between probabilistic and quantum algorithms</td>
</tr>
<tr>
<td>1994</td>
<td>Simon’s algorithm</td>
<td>Demonstrates an exponential separation between probabilistic and quantum algorithms</td>
</tr>
<tr>
<td>1994</td>
<td>Shor’s algorithm</td>
<td>Demonstrates that quantum computers can efficiently factor numbers</td>
</tr>
<tr>
<td>1996</td>
<td>Grover’s Algorithm</td>
<td>Demonstrates quantum search has polynomial speedup over classical search</td>
</tr>
</tbody>
</table>

Table 2: Some Quantum Algorithms with Startling Speedup
The field of quantum information processing has made numerous promising advancements since its conception, including the building of two- and three-qubit quantum computers capable of some simple arithmetic and data sorting by scientists and researchers in the fields of Quantum and Nano Computing like Dr. Charles Bennett, Dr. Lov Grover, Prof. Stuart Hameroff, Prof. Vlatko Vedral, Prof. Gilles Brassard, Prof. Richard Jozsa, Prof. Lajos Diosi, Prof. Artur Ekert, Prof. Leonard Modinow, Sir Roger Penrose, Prof. Stuart Hameroff, Prof. Mani Lal Bhaukim and Nobel Laureates Prof. Douglas Osheroff and Prof. Robert Richardson (Physics, 1996) among others. You can refer to ‘http://www.dei.ac.in/dei/quantumNano/’ for further details.

Obstacles and Research

The field of quantum information processing has made numerous promising advancements since its conception, including the building of two- and three-qubit quantum computers capable of some simple arithmetic and data sorting. However, a few potentially large obstacles still remain that prevent us from “just building one,” or more precisely, building a quantum computer that can rival today’s modern digital computer. Among these difficulties, error correction, decoherence, and hardware architecture are probably the most formidable. Error correction is rather self explanatory, but what are errors need correction? The answer is primarily those errors that arise as a direct result of decoherence, or the tendency of a quantum computer to decay from a given quantum state into an incoherent state as it interacts, or entangles, with the state of the environment. These interactions between the environment and qubits are unavoidable, and induce the breakdown of information stored in the quantum computer, and thus errors in computation. Before any quantum computer will be capable of solving hard problems, research must devise a way to maintain decoherence and other potential sources of error at an acceptable level. Thanks to the theory (and now reality) of quantum error correction, first proposed in 1995 and continually developed since, small scale quantum computers have been built and the prospects of large quantum computers are looking up. Probably the most important idea in this field is the application of error correction in phase coherence as a means to extract information and reduce error in a quantum system without actually measuring that system.

At this point, only a few of the benefits of quantum computation and quantum computers are readily obvious, but before more possibilities are uncovered theory must be put to the test. In order to do this, devices capable of quantum computation must be constructed. Quantum computing hardware is, however, still in its infancy. As a result of several significant experiments, nuclear magnetic resonance (NMR) has become the most popular component in quantum hardware architecture. Groups from Los Alamos National Laboratory and MIT constructed the first experimental demonstrations of a quantum computer using nuclear magnetic resonance (NMR) technology. Currently, research is underway to discover methods for battling the destructive effects of decoherence, to develop an optimal hardware architecture for designing and building a quantum computer, and to further uncover quantum algorithms to utilize the immense computing power available in these devices. Naturally this pursuit is intimately related to quantum error correction codes and quantum algorithms, so a number of groups are doing simultaneous research in a number of these fields. To date, designs have involved ion traps, cavity quantum electrodynamics (QED), and NMR. Though these devices have had mild success in performing interesting experiments, the technologies each have severe limitations. Ion trap computers are limited in speed by the vibration frequency of the modes in the trap. NMR devices have an exponential attenuation of signal to noise as the number of qubits in
A system increases. Cavity QED is slightly more promising; however, it still has only been demonstrated with a few qubits. All-silicon quantum computers are also in the vogue nowadays.

In principle, a large scale quantum computer can be built using a controllable quantum system, provided the physical system meets the following requirements, called as the DiVincenzo criteria (DiVincenzo, 2000):

1. A scalable physical system with well-characterized qubits.
2. The ability to initialize the state of the qubits to a simple fiducial state.
3. Long (relative) decoherence times, much longer than the gate-operation time.
5. A qubit-specific measurement capability.
6. The ability to interconvert stationary and flying qubits.
7. The ability to faithfully transmit flying qubits between specified locations.

The general problems to be solved for physical realization of Quantum Information Processing or Quantum Computation are in particular:

- Identification of the best suitable physical system which allows for scalability, coherence and fast implementation of Quantum Information Processing
- Engineering and control of quantum mechanical systems far beyond anything achieved so far, in particular concerning reliability, fault tolerance and using error correction.
- Development of a computer architecture taking into account quantum mechanical features.
- Development of interfacing and networking techniques for quantum computers.
- Investigation and development of quantum algorithms and protocols.
- Transfer of academic knowledge about the control and measurement of quantum systems to industry and thus, acquisition of industrial support and interest for developing and providing quantum systems.

In conclusion, the future of quantum computer hardware architecture is likely to be very different from what we know today; however, the current research has helped to provide insight as to what obstacles the future will hold for these devices.

Acknowledgements

The authors are extremely grateful to Revered Prof. P S Satsangi, Chairman, Advisory Committee on Education, Dayalbagh Educational Institutions for motivation and support. They also thank Dr. Dayal Pyari Srivastava for providing encouragement and guidance.

References

Can Quantum Computing Provide Exponential Speedup?

Some New Developments
A recent development in quantum computing is the assembling of a team of twenty researchers by Google to build quantum computing devices. University of California Santa Barbara physicist John Martinis will lead the team. Work will be based in part on previous research with machines built by D-Wave, a Canadian company. D-Wave claimed to have created “the world’s first commercially available quantum computer” in 2011.

Quantum computing has been a theoretical and even speculative field. It is based on the notion of qubits (pronounced “Q-bits”), whose values may be 0, 1, or a probability distribution over that set. Qubits are fragile in that tiny perturbations in a system may destroy them. Researchers have been able to extend their lives from nanoseconds, decades ago, to minutes, today. Martinis reports a 10,000-fold rise in the lifetimes of qubits that can be regularly maintained, up to 50 to 100 microseconds.

The progress of quantum computing to recognition by significant forces in industry and academia is striking. Twenty years ago, an expert noted that capabilities “permit only the most rudimentary implementations of quantum computing”\(^1\). Has this changed?

The progress of quantum computing to recognition by significant forces in industry and academia is striking

Also in 2014, a test of the $10 million D-Wave computer, posted online at Science magazine in June, produced results that some researchers described as not supporting claims of exponential speedup\(^1\). The machine used from 8 to 512 qubits. The summer 2014 testing was done by a team that included Martinis, as well as Matthias Troyer of the Swiss Federal Institute in Zurich. The co-founder of D-Wave has been quoted disparaging the test in a communication to Wired magazine.

The test team, which included researchers from the University of Southern California, University of California Santa Barbara, Google, and Microsoft, defined quantum speedup, \(S(n)\), for a problem with input of size \(n\), as \(C(n) / Q(n)\), where \(C(n)\) is the time required by a classical device and \(Q(n)\) is the time required by a quantum one.

The D-Wave machine is not a universal programmable computer, like classical devices, but rather what is called a quantum annealer. It solves certain problems by having a two-dimensional array of qubits interact to reach a “ground state.” Annealing, a metaphor for which is used in some artificial-intelligence algorithms, is a physical process of “cooling down” or lowering energy level or disorder in a system.

A Fast Quantum Algorithm for Factoring
Independent of claims for the performance of particular machines, an efficient quantum-computing algorithm for finding the factors of large integers has been published and studied since the mid-1990s\(^4\). Peter Shor’s algorithm executes in time that is a polynomial function of the size of the input, but is not guaranteed always to provide the correct answer to the factoring problem. However, the answer it provides may be easily checked in polynomial time\(^7\). No known algorithm for classical computer architectures factors numbers in polynomial time. Hence Shor’s algorithm provides exponential speedup for this task. But we find no indication that it has been used on a D-Wave or other quantum device.

The prospect that quantum computing might enable exponential speedup was explored by David Deutsch in the 1980s\(^6\). Research in the 1990s identified problems that quantum computers can theoretically solve quickly and exactly, that classical devices cannot. It induced discussion about a possible quantum-computing challenge to the principle, known as the quantitative Church’s Thesis, that any physical computing device can be simulated by a Turing machine in a number of steps that is polynomial in the resources used by the computing device.

According to Alan Turing and Alonzo Church, can simulate any algorithmic computation. Turing and Church were logicians working in the 1930s.

Shor wrote, however, that “quantum computers will likely not become widely useful unless they can solve NP-complete problems.... There are some weak indications that quantum computers are not powerful enough to solve NP-complete problems”\(^14\). Moreover, the only practical application of the quantum algorithm described by Shor appears to be in breaking public-key cryptography.

Satisfiability and Other Hard Problems
Many practical problems faced and solved by life forms require exponentially large amounts of time to solve perfectly. These include planning, because threats and opportunities explode exponentially as we look farther into the future to weigh them. They also include resolving ambiguities in communication, since alternative possibilities also explode with the length of utterances. A large set of such problems exists, called NP-complete (NPC), none of which has a known polynomial-time solution but all of which would have such solutions if any one of them did. We don’t solve them exactly; rather we obtain satisfactory approximate solutions.

Let us consider a case where the exponential speed-up, claimed by some for quantum computing, would open up entirely new practical computing horizons, if it were applicable to general-purpose computing. A classical NPC problem is the satisfiability problem (SAT) in propositional logic.

We may approach satisfiability by starting with the easier problem of evaluation of logic formulas. Suppose we are offered a formula, such as \((p \lor q)\)
A different problem, about formulas alone, is to tell whether some set of variable assignments exists that makes the formula true. One way to solve this is to write a truth table and see if any row makes the formula true. For the formula \( \neg p \lor (q \land r) \), the truth table is as follows:

<table>
<thead>
<tr>
<th>( q )</th>
<th>( r )</th>
<th>( p \lor q )</th>
<th>( \neg (p \lor q) )</th>
<th>( \neg r )</th>
<th>( (p \lor q) \land \neg r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The formula is satisfiable because it evaluates to true in at least one case: the third row of the truth table (T, T, F). Unlike the evaluation problem in propositional logic, the satisfiability problem is believed to be very time consuming. This is because the size of a truth table with \( n \) variables is \( 2^n \), and no faster method of solving SAT in the general case is known, other than checking every row of such a truth table. If \( n \) is 200, then the truth table will fill the universe.

A 2006 paper by S. Bravyi describes a quantum algorithm for quantum 2-SAT, a version of the satisfiability problem that replaces propositional-logic formulas with two variables by 2-qubit states, and replaces the assertion that a set of variable assignments satisfies a formula with the quantum \( n \)-qubit state. Bravyi describes BQP, the set of problems that a quantum computer can solve in polynomial time with a bounded probability of error. Similarly, QMA is a set of problems whose solutions may be verified efficiently on a quantum computer, given a possible solution, analogous to the problem set \( \text{NP} \) in classical computing.

On the other hand, a 2010 paper by researchers at Princeton and the Max Planck Institute indicates pessimistic prospects for quantum solutions to the SAT problem. For problems like satisfiability or other NP-complete problems, “the quantum benefits appear to be inherently more restricted” than for factoring.

**Quantum Theory and Computing**

Classical computing, with microprocessors, bits, and random-access memory, could not have become practical without quantum theory, which made possible the invention of the transistor. The transistor replaced the slow, unreliable relay and vacuum tube. A 2006 paper by S. Bravyi describes a quantum algorithm for quantum 2-SAT, a version of the satisfiability problem that replaces propositional-logic formulas with two variables by 2-qubit states, and replaces the assertion that a set of variable assignments satisfies a formula with the quantum \( n \)-qubit state. Bravyi describes BQP, the set of problems that a quantum computer can solve in polynomial time with a bounded probability of error. Similarly, QMA is a set of problems whose solutions may be verified efficiently on a quantum computer, given a possible solution, analogous to the problem set \( \text{NP} \) in classical computing.

On the other hand, a 2010 paper by researchers at Princeton and the Max Planck Institute indicates pessimistic prospects for quantum solutions to the SAT problem. For problems like satisfiability or other NP-complete problems, “the quantum benefits appear to be inherently more restricted” than for factoring.

**Quantum Theory and Computing**

Classical computing, with microprocessors, bits, and random-access memory, could not have become practical without quantum theory, which made possible the invention of the transistor. The transistor replaced the slow, unreliable relay and vacuum tube. A 2006 paper by S. Bravyi describes a quantum algorithm for quantum 2-SAT, a version of the satisfiability problem that replaces propositional-logic formulas with two variables by 2-qubit states, and replaces the assertion that a set of variable assignments satisfies a formula with the quantum \( n \)-qubit state. Bravyi describes BQP, the set of problems that a quantum computer can solve in polynomial time with a bounded probability of error. Similarly, QMA is a set of problems whose solutions may be verified efficiently on a quantum computer, given a possible solution, analogous to the problem set \( \text{NP} \) in classical computing.

On the other hand, a 2010 paper by researchers at Princeton and the Max Planck Institute indicates pessimistic prospects for quantum solutions to the SAT problem. For problems like satisfiability or other NP-complete problems, “the quantum benefits appear to be inherently more restricted” than for factoring.

**Quantum Theory and Computing**

Classical computing, with microprocessors, bits, and random-access memory, could not have become practical without quantum theory, which made possible the invention of the transistor. The transistor replaced the slow, unreliable relay and vacuum tube. A 2006 paper by S. Bravyi describes a quantum algorithm for quantum 2-SAT, a version of the satisfiability problem that replaces propositional-logic formulas with two variables by 2-qubit states, and replaces the assertion that a set of variable assignments satisfies a formula with the quantum \( n \)-qubit state. Bravyi describes BQP, the set of problems that a quantum computer can solve in polynomial time with a bounded probability of error. Similarly, QMA is a set of problems whose solutions may be verified efficiently on a quantum computer, given a possible solution, analogous to the problem set \( \text{NP} \) in classical computing.

On the other hand, a 2010 paper by researchers at Princeton and the Max Planck Institute indicates pessimistic prospects for quantum solutions to the SAT problem. For problems like satisfiability or other NP-complete problems, “the quantum benefits appear to be inherently more restricted” than for factoring.

**Quantum State, Gates, and Registers**

Researchers in quantum computing have described notions of quantum state, analogous to the state of a computation on a classical machine, and quantum gates, analogous to logic gates in classical computing. On an ordinary computer, state is the set of values of all bits in the machine, or equivalently, the values of all variables in a computation. The state of a quantum computer is described by a vector that is a linear superposition of all bits in the vector.

State transitions are described by a unitary operator on the vector space. A 3-qubit register, for example, may have the state \( |010\rangle \), also written \( |2\rangle \), also written \( (0, 0, 1, 0, 0, 0, 0, 0, 0) \), where the 1 is the probability that the register has the value 2 and the 0s are the probabilities that is has the values 0, 1, or 3 to 7.

All the allowed operations on qubit registers are rotations. Since rotations...
copying qubits is not possible, because their quantum state is destroyed in the copying

Determinism: A Foundation of Computer Science

The notions that observable entities, such as particles, are in indeterminate, undefined, or probabilistic states seems to collide with the necessary foundations of computer science. This discipline is concerned with the execution of algorithms and algorithm-based interactive processes in the real world. Algorithms compute mathematical functions on representations of parts of the real world. A function on natural numbers or strings of symbols is, by definition, a mapping from one discrete value x to another, y, such that for any x a unique y exists. Here x is called input and y is output.

In computer science, a notion of nondeterminism exists; namely, that for a given x, y may be a set. Thus we could make x a city and y the set of cities with direct airline connections to x. If we consider where we could be after taking some plane on one flight from city x, then the set y would contain all the possibilities. If we imagine boarding a random plane, the one city where we will land is constrained but could be considered nondeterministic. Non-deterministic automata (simple abstract mathematical machines) are of great theoretical value in computer science.

On the other hand, to compute such a set y of one-stop destination cities would require a representation of y, a representation of sets. Such digital representations exist, and they are by no means random, nor probability distributions.

Thus quantum computing challenges those of us who are trained in computer science to stretch our imaginations and our notions of what computing is. In the same way, quantum theory challenged physicists trained in the Newtonian assumptions about physics and in the much more recent theory of relativity.

Fundamental Obstacles to Some Speedup Prospects?

Possibly a final negative answer to the question posed by this article is a result reported in 2003[10]. According to a theorem by Jozsa and Linden, the quantum entanglement of multiple elements, with a number unbounded with respect to input size, is needed for exponential speedup. Shor’s algorithm, for example, entails entanglement of an unbounded number of particles. A widely respected 2008 paper affirms this result in passing[11].

Thus, the cost of exponential speedup may be exponential quantum processing hardware. This is similar to the requirement, for some parallel computation, that an exponential number of processors be available in order to provide exponential speedup. The superposition of 2^{1000} states and pathways may be physically possible under quantum theory. The entanglement of 2^{1000} particles, more than can exist in the universe, is not. If the result by Jozsa and Linden holds, then despite the power of quantum computing, it will not break the performance-to-resources barrier established tentatively by complexity theorists forty years ago.

Is Quantum Computing Better Adapted to Fuzzy Problems?

Whereas the formal descriptions of the hard problems encountered by humans and all other life forms are discrete, and these problems (called NP-complete) give evidence of being intractable and not worth solving precisely, these life forms nevertheless survive by finding satisfactory approximate and probabilistic solutions. (In fact, since these problems are in continuous physical space and time, they are in that form unsolvable by any digital computer, anyway[11].)

Some researchers have noted that these fuzzy problems are well suited to quantum computing[12]. A sequence of fuzzy numbers may correspond to our uncertainty about the inputs to a computation. A fuzzy number x is a generalization of a real number, in that it is a set of values v that may be x, each with an extent to which it is x. Thus it is similar to a fuzzy set, such as tall, the set of all possibly tall people together with the degrees to which each person is deemed tall.

Two ideas of these researchers for quantum algorithms that speed up fuzzy computing are as follows:

1. Since fuzzy numbers may be represented as classes of real intervals, fast quantum interval algorithms may solve problems involving fuzzy numbers. (Whereas classically computing the range of an interval is NP-hard, quantum algorithms offer tractable solutions.)

2. Computing a function on a sequence of fuzzy numbers on a quantum computer may reduce the classical running time to its square root for the most time-consuming step, which is the minimum of all possible combinations of inputs.

Thus the cost of exponential speedup may be exponentially large quantum processing hardware

... the work on quantum algorithms for fuzzy computing may point the way toward fruitful avenues of research leading to practical contributions

Readers of this article may wish to consider looking into these optimistic claims. Though a speedup of √n is not
exponential, or even linear, the work on quantum algorithms for fuzzy computing may point the way toward fruitful avenues of research leading to practical contributions.

References

About the Author
Prof. David M Keil has taught at Framingham State University, USA, since 1997. He has acted as Director of Assessment for computer science since 2009. Additional responsibilities include as Search Committee chair in Spring 2001 and member of search committee in 2004 and 2013-2014. He was Acting chair in Spring 2000-Fall 2000 and 2003-2004 and Faculty coordinator for computer-science lab during 1997-1998.

He has presented at workshops on theory and practice of open computational systems, evolutionary computation, environments for multi-agent systems, foundations of interactive computing, and teaching and assessment in computer science. His research interests include interactive models of computation, evolutionary computation, artificial intelligence, database theory and Kolmogorov complexity.
Quantum Information Processing with Quantum Dots in a Cavity

Introduction
Communication and computing are the heart of information processing whether classical or quantum. Photonics dominates the development of modern day classical communication based on transfer of light over free space or fibers. Quantum communication or quantum key distribution is also demonstrated and in fact commercial systems are available now from different companies like idquantique, magiqtech, smartquantum and quintessencelabs. Crucial single photon sources are mostly based on very weak light sources. Deterministic single photon sources, that is, sources that emit single photons at precise times are still not very efficient. Some of the possibilities that are demonstrated are based on single quantum dots[1], nitrogen vacancies in diamond[2], ZnTe, GaP among others. Quantum dots[1], nitrogen vacancies in diamond[2], ZnTe, GaP among others. The quantum dots are demonstrated based on single quantum dots[1], nitrogen vacancies in diamond[2], ZnTe, GaP among others. The quantum dots are shown to increase the channel capacity[4].

Efficient single photon detectors are available in the form of avalanche photodiodes (APDs), photomultiplier tubes and more recently superconducting detectors with very high efficiency. One may note that InGaAs APDs that work in visible to near infrared wavelengths and superconducting detectors require cryogen temperatures to operate. In the context of making use of quantum principles, sources that generate entangled photons, photons with at least one of their properties (like polarization) correlated, or photons that are in superposition states are very useful. For example, entanglement is shown to increase the channel capacity[4]. So, the role of photonics in the field of communications is well established.

In the context of making use of quantum principles, sources that generate entangled photons, photons with at least one of their properties (like polarization) correlated, or photons that are in superposition states are very useful.

A quantum computer is envisaged for different applications like Shor’s algorithm for factoring large numbers and eventually to study quantum mechanical systems that are useful for futuristic applications in diverse fields.

On the other hand, as is well known, computing in the classical domain is still ruled by Silicon technologies and the Moore’s law governs the growth of the field. Shrinking transistor sizes, possibly, approaching the single molecule size limits the future and this lead to the search for alternate technologies. There are several alternatives being pursued to overcome the limitations set by shrinking sizes including alternate designs being pursued at University of Illinois (SONIC), and optical, DNA, and Nano-computing. The quest to realize a truly powerful computer that utilizes the unparalleled parallelism offered by quantum principles is still on. A quantum computer is envisaged for different applications like Shor’s algorithm for factoring large numbers and eventually to study quantum mechanical systems that are useful for futuristic applications in diverse fields.

In the standard quantum computing schemes, a system is required to have universal quantum logic gates. A Hadamard gate prepares the input state in a superposition state, a Controlled NOT gate (cNOT) whose second input is negated only when the first input is true, a Toffoli gate which copies the first two inputs to the first two outputs and the third output is the Exclusive Or of the third input and the AND of the first two inputs and the Fredkin gate which swaps the last two inputs if the first input is 0. Some of the quantum logic gates are described in Fig.1. To explain the complexity in realizing the quantum logic gates with existing technologies, a schematic of the quantum phase gate which was proposed in 1995 by Kimble’s group is shown in the bottom row of Fig.1[5]. A cNot gate has been demonstrated in different systems including in trapped ions and linear optics based integrated circuits. However, a quantum computer need not be similar in architecture to the present day digital computer. That is, there are other schemes where logic gates are not essential. For example, in adiabatic quantum computing the system with a large network of interacting qubits is turned on by preparing various states appropriately and let the system evolve through the interactions. The final state of the system after all the interactions gives the answer to the problem being computed. Another quantum computing.
scheme that does not require universal gates is cluster state quantum computing. It may be noted that, the present day computers evolved a long way from first generation computers that occupied big rooms and required high power and punch cards. The invention of transistor was a big game changer which, probably, came at the most opportune time. Regarding quantum computer, though there are proof of concept demonstrations and several technologies being pursued, we are at a stage where we are looking for major breakthroughs which will help us realize a quantum computer.

Of the several technologies that are being pursued, the success of any system depends on the scalability so that larger number of qubits is possible. In addition, the qubits should have long decoherence times which is a measure of interaction of the system with the environment. For high fidelity devices, long decoherence times (time before which the coherence is lost) are required. To put it in a nutshell, to realize a quantum computer, one needs a system in which we can address and measure individual quantum systems while keeping them isolated from the environment. Three major fields that gave the initial breakthroughs are nuclear magnetic resonance (NMR), trapped atoms and ions and linear optic quantum computing. In the NMR technique, liquid molecules with a large number of resonances, each of which can be a qubit were used. Logic operations with about 12 qubits were demonstrated by Nakamura et al. We are at a stage where we are looking for major breakthroughs which will help us realize a quantum computer.

Table 1: A comparison of some of the qubit systems studied so far

<table>
<thead>
<tr>
<th>Qubit system</th>
<th>Decoherence time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$^{29}$Si nuclear spins in $^{28}$Si</td>
<td>25 sec</td>
</tr>
<tr>
<td>Spin of trapped ions</td>
<td>15 sec</td>
</tr>
<tr>
<td>Spin of trapped atoms</td>
<td>3 sec</td>
</tr>
<tr>
<td>Nuclear spin (NMR)</td>
<td>2 sec</td>
</tr>
<tr>
<td>Electron spin bound to $^{11}$p</td>
<td>0.6 sec</td>
</tr>
<tr>
<td>NV centre in diamond</td>
<td>2 msec</td>
</tr>
<tr>
<td>Photon polarization</td>
<td>0.1 msec</td>
</tr>
<tr>
<td>Electron spin in QD</td>
<td>3 μsec</td>
</tr>
<tr>
<td>Superconducting Charge/Flux/Phase</td>
<td>4 μsec</td>
</tr>
</tbody>
</table>

The basic requirements for a quantum computer are qubits with long decoherence time (that is, very low interaction with the surroundings), logic gates, scalability among others. The choice of qubit limits the technology that can be used. For example, after an initial lull, superconducting qubits have come back in vogue thanks to some innovative recent research. NMR computing which showed the feasibility of quantum computing is still limited by the number of possible qubits, bulkier size etc. Table 1 shows a comparison of some of the qubit systems that are studied. The most feasible and well accepted scheme for quantum computing networks is to have localized logic operations of qubits and connect different parts of the circuit or network by “flying” qubits which carry information from one part to the other. Photons with their interesting properties like being the fastest, non-interacting etc offer to be the best possible flying qubits. In the following, various basic components required for quantum dot based quantum information processing circuits are described.
**Quantum Dots as Solid State Equivalent of Atoms**

QDs are semiconductor nanostructures that confine electrons to regions comparable to the electron wavelength (Bohr radius). This confinement of electrons to smaller regions discretizes the energy levels like the particle in a box problem one studies in basic quantum mechanics course. These discrete states help use QDs as solid state equivalent of atoms. One major difference though is that, atoms in vacuum interact very little with surroundings and thus have very long lifetimes. Interaction of electrons in a quantum dot with surroundings reduces the coherence time of the electrons. For fault tolerant quantum computing, the short coherence time in QDs is considered a setback. However, electron spins are shown to have long coherence times of the order of milli seconds making them good candidates for qubits. Several atom like properties of QDs are demonstrated like discrete energy levels, dressed states, single photon emission, entanglement, driven Rabi oscillations and control of single charge and spin excitation.

**Photonic Crystal Cavities**

Electrons in a periodic array of ions or atoms experience spatially varying field which eventually results in the energy band structure for electrons. Band structure defines the allowed energy levels for the electrons. Similarly, it was proposed and demonstrated in 1984 that, photons can also be subjected to periodic modulation of refractive index which leads to band structure for photons. Analogous to crystals for electrons, crystals that exhibit energy band structure for photons are called Photonic crystals. They exist in nature like the patterns that give vibrant colours to butterfly wings, peacock feathers etc. These can be made by having a stack of different materials with different refractive indices (1-dimensional) or can be 2-dimensional like an array of holes in a dielectric material or array of dielectric rods in a different dielectric. These are shown schematically in the top row of Fig. 3. One useful feature of photonic crystals is, by a suitable modification (a defect) to the structure one can have field localization. That is, as the rest of the photonic crystal does not allow a photon, with energy in the bandgap region, it is reflected by the periodic structures surrounding and thus leads to localization of a photon in a small volume. Schematics of the defect in a periodic lattice for 1-d and 2-d are shown in the bottom row of Fig. 3. By solving Maxwell’s equations, by finite difference time domain or finite element method, the resonances, field profiles and the cavity parameters are calculated. Simulation results of a cavity structure with the central holes displaced from their lattice sites (so called, LO cavity) is shown in Fig.4 on the left. Also shown is a scanning electron micrograph image of a fabricated photonic crystal cavity on the right side of Fig. 4. While, in the plane, light is confined by the periodic arrangement of holes the out of plane confinement is achieved by having a suspended bridge structure.

As photons can be localized or trapped to very small regions comparable to or smaller than the wavelength of light), the photonic crystals with defects are called microcavities. Light localization to smaller regions results in increasing the probability of interaction of photons with any material in the defect region. Thus, if one has a quantum dot in the defect region, one can achieve cavity enhanced coupling of light to quantum dot. Modulation of light emission
of the QD inside the cavity, controlling the dimensions and shape of the QDs etc.

The quality factor achieved in a fabricated structure depends on the quality of the lithography which limits the quality of nonlinear elements as well as the QD wafer itself. To make a microcavity centered about a QD of dimensions of few 10s of nanometer, either one makes a large number of cavities on a wafer and tests all of them to identify cavities which have a QD in them or first gets a map of the QD positions (by imaging the luminescence) and makes a cavity around a QD that is spatially identified. The highest Q reported with QD embedded in a cavity is still not sufficient to observe single photon-QD coupling. Thus, the quest is on to reach the strong coupling regime where one may expect single photon level coupling to the QD.

Coupling to and from photonic crystals is still a challenging issue but tapered waveguides have been shown to have very high coupling efficiencies. One of the biggest advantages of planar architectures presented in Fig. 2 is that one would be able to study entanglement (coupled cavities) in addition to single photon logic operations and having single photon emitters embedded in the circuit.

For the future, the strong local field generated at the interfaces when plasmon polaritons are excited could also be useful for QD based architectures below the diffraction limit. Coupling of broadband light incident at any angle can be coupled to the active layer by plasmonic quasicrystal patterns(19).

To summarize, it is too early to answer questions like, when a quantum computer will be realized, what technology will it be based on or what will be the qubits or qudits it will use, will it require logic gates like present day computers... The current lead is, probably, with trapped atoms and ions as well as superconducting circuits, both of which require complex experimental setups. The lead may change as several technologies are simultaneously being pursued.

References


Fig. 4: Schematic of a photonic crystal cavity structure formed by air holes in GaAs wafer along with the calculated field profile in the defect region is shown on the left. Scanning electron micrograph image of a fabricated suspended air bridge cavity is shown on the right

Light localization to smaller regions results in increasing the probability of interaction of photons with any material in the defect region

Achanta Venu Gopal obtained his Ph.D. (Physics) from Solid State Electronics group at TIFR, Mumbai and Ph.D. (Electronics) from Tokyo University. He worked as a NEDO Fellow at FESTA Laboratories, Tsukuba, headquarters of Japanese national Femtosecond Technology Project between 2000 and 2003 and as a JST Fellow in the Quantum Information Technology group at NEC, Tsukuba, Japan between 2003 and 2004. He joined Department of Condensed Matter Physics and Materials Science at TIFR in 2004 where he is currently an Associate Professor. His current research interests are in plasmonics for manipulating the optical properties of materials as well as light harvesting and in photonic crystal cavity based planar architectures. He is a Senior Member of IEEE and a Member of OSA.
Introduction
Quantum computing, also known as atomic computing is the research area persistent on development of the computer technology based on quantum theory and principles. The quantum theory describes the behaviour and nature of energy and substance on the quantum, which is atomic and subatomic, level. Development of the quantum computer, if realistic, would mark a leap forward in computing capacity far superior than from the abacus to a modern day supercomputer, with recital grows in the billion-fold realm and further than. By following laws of quantum physics, the quantum computer, would gain huge processing power through facility to be in multiple states, and use all possible permutations simultaneously to perform tasks.

Now, it is essential to understand Quantum Theory before we are going to apply it in our Information Technology and Communication Networking (ICTN) which becomes quantum computing. Actually, in 1990 Max Planck has introduced the concept of quantum theory in which he has introduced the idea that energy exists in individual units, to which he has given the name quanta, as does matter. Then after, many scientists have worked for more than 30 years to have modern understand of quantum theory.

The Necessary Fundamentals of Quantum Theory
• Energy, for example matter, consists of separate units, rather than exclusively as a constant wave.
• Basic particles of energy as well as matter may behave like either particles or waves. Generally it depends on the conditions.
• Basic particles’ movement is inherently random and because of that it is unpredictable.
• The concurrent dimension of two complementary values, such as the location and momentum of a basic particle, is unavoidably flawed. It is something like that more precise measurement of one value will give more flawed measurement of the other value.

In Fig. 1, we have explained classical computing system in which there are electrical signals as inputs and electrical signals as outputs. The in-between of these two there are classical Gates which are working on input signals and generating output signals. This is known as classical computing system.

Where as in Fig. 2, we have tried to explain quantum computing system in which there is quantum state as an input on which quantum Gates has been applied which generates measurement results as an output.

The fundamental difference between quantum computing and conventional or classical computing is, in quantum computing we are architecturally using all possibilities to solve computational problems where as conventional or classical computing is the small part or subset of all these possibilities. Apart from this difference, a quantum computing system is thousands of time faster than conventional computing to solve very important types of problems. A really tough problem like the big number factorisation, that would take a supercomputer years or decades to crack, can be crunched by a quantum computer in very little time at all. It doesn't stop over here. In conventional computing a
program and process has to operate in sequence of the information it stored and one bit at a time, whereas as in quantum computing process of all information stored in all QBITs simultaneously. It is a kind of imagination that instead of millions of desktops are running side by side rather than just one working on the same problem.

Let us take an example to understand quantum computing more effectively. The classical NOT-gate, we are trying to convert it into quantum analogue.

The Classical NOT-gate, the left side of above figure, flips its input bit over; NOT (1) = 0, NOT (0) = 1. The quantum analogue, the QNOT also does this, but it flips all states in a superposition at the same time is available on right hand side of above figure. So if we start with 3 qbits in the state $|000\rangle + |001\rangle + 2|010\rangle - |011\rangle - |100\rangle + 3i|101\rangle + 7|110\rangle$ and apply QNOT to the first qbits, we get $|100\rangle + |101\rangle + 2|110\rangle - |111\rangle - |000\rangle + 3|001\rangle + 7|010\rangle$.

Quantum Computing is a kind of imagination where instead of millions of desktops running side by side there is rather just one working on the same problem.

Quantum Machine Learning Relevance
Many services available by Google or others are classy depends on Artificial Intelligence technologies includes Pattern Reorganization as well as Machine Learning. If any individual takes closer look at capabilities, they can come across with the solution of hard combinatorial optimization problems, called by mathematicians. The requirement of solving such kind of hardest problem is so large server farms which are very next to impossible to build.

The quantum computing is a new type of machine system can be helpful here. The laws of quantum physics and its advantages provide new computational capabilities represents as Quantum Computing. While quantum mechanics has been foundational to the theories of physics for about a hundred years the picture of reality it paints remains enigmatic. This is principally as of the scale of our regulatory experience quantum consequences are vanishingly small and can typically not be pragmatic directly. Subsequently, quantum computers surprise us with these capabilities.

In Fig. 4, we have endeavoured model of quantum computing with Machine Learning. In middle of the figure there is quantum Gates are available based on quantum computing and encircle of it there are machines which learns continuously from quantum gates. To understand quantum computing with machine learning let’s look at an example of unstructured search.

**Example with Algorithm 1:** Consider a situation in which we are hiding ball in a cabinet of million drawers. How many drawers, an individual has to open to find out the ball? It is possible, if anyone is a lucky person, to find the ball in the foremost few drawers but we can not deny the situation in which an individual has to inspect almost all of them. If we are computing this example we can find out an average peaks the ball will be 500,000. By using quantum computing technique, it is possible to perform such kind of searching into 1000 drawers only. This wonderful achievement is possible by using Grover’s algorithm. This algorithm is the quantum algorithm to search a database which is not sorted with many entries in $O(\sqrt{N})$ time by using $O(\log N)$ storage space.

**Example with Algorithm 2:** Apart from Grover’s algorithm there is another algorithm of quantum computing with machine learning is Shor’s Algorithm. This algorithm is most frequently used method for sending encrypted data. Shor’s algorithm permits tremendously quick factoring of large numbers. A classical computer can be sketchy at taking 10 million or billion years to factor a 1000 digit number, where as by using quantum computing it would take approx 20 minutes.

**Example with Algorithm 3:** This is most interesting and effective example of best usage of quantum machine learning. In a banking transaction system...
it is very hard to detect fraudulent bank transactions. It is time consuming as well. In this situation quantum computing with machine learning can help here. This mathematical problem can be optimized by using consensus algorithms which is also known as Boyd’s system. In this algorithm we are using past data to train the model in hopes that it will work on future data. It is a pattern which means each node updates its local variable with weighted average of its neighbour’s values, and each new value is corrupted by an additive noise with zero mean. The quality of consensus can be measured by the total mean-square deviation of the individual variables from their average, which converges to a steady state value. This can be prepared on a single computer, with all the data in one place. Many processors are used by machine learning typically, each handling a little bit of problem. But for a single machine a consensus optimization approach can work better if the problem becomes too large. In this, dataset is spited into bits and disseminated across 1,000 agents which analyse their bit of data and each produce a model based on the data they have processed. By applying this we can decrease incredible time of computing which means a few movements instead of many years. This model is not only useful for detecting fraudulent bank transactions but also useful for creating an effective spam filter.

Benefits of Quantum Computing
- It is useful to solve complex discrete combinatorial optimization problems easily.
- In processing it is very faster
- It provides better methods of Machine learning, which is really high-quality instead of improving classical methods.
- There are other artificial intelligence problems which can also easily solved by quantum computing.

The above benefits are not limited but prime consideration. There are also some drawbacks of quantum computing, while applies for machine learning, in the terms of computational formulation and implementation.

Drawbacks of Quantum Computing
- It requires more memory to solve complex problem includes more summation.
- Just like we are talking, it is not easy to design or formulate quantum computing.
- The cost and other hardware related expenses are very high in the implementation of quantum computing.
- The major drawback is, quantum computing is not used in practice till date.

Conclusion
Quantum computing is the technique which provides better and faster machine learning. It is a current research trend in the field of computer science and technology having some drawbacks which we have discussed above. Machine learning is a process which requires past data to predict future and it is only possible by using high demanding computational operations. These operations always require very long time which can be avoided by using quantum computing technique. There are other applications and algorithms of quantum computing apart from those discussed above. Finally, it is high time to implement quantum computing on practical basis as it is not in exercise at the present.

References

About the Authors
Hardik A Gohel an Academician and Researcher, he is an Assistant Professor at AITS, Rajkot and active member of CSI. His research spans Artificial Intelligence and Intelligent Web Applications and Services. He also focuses on "How to make popular, Artificial Intelligence in study of Computer Science for various reasons" He has 28 publications in Journals and proceedings of national and international conferences. He is also working as a Research Consultant. He has published cover stories in CSI Communication Magazine by last year. He can be reached at hagohel@gmail.com

Dr. Priyanka Sharma has worked in IT education field in teaching and research at Masters level for 16 years, published more than 100 papers, carried out Funded research projects, reviewers and editors of various journals and conferences and guiding PhD students in GTU and other recognized studies. Her area of interest is Knowledge Based systems and Information system security.
Quantum Leap into High Performance Computing Environment

Introduction

Quantum theory or quantum mechanics or quantum physics all refer to that branch of physics that deals with study of nature and behaviour of matter and energy on the atomic and subatomic level (i.e., at nanoscopic scales). German physicist Max Planck (1900) is credited with identifying the existence of these units that became the first instance of quantum theory. For his experiment presenting before the world the reasons for radiation of glowing body that changes the colour from red to orange through to blue as the temperature (of the body) rises; assumption that energy existed not only in matters but also within individual units (termed as quanta) and famous mathematical equation quantifying the concepts, was awarded Nobel Prize in Physics in 1918.[10]

Copenhagen interpretation and the many-worlds theory are the two major interpretations of quantum theory.

The Copenhagen interpretation of quantum theory was proposed by Niels Bohr conceptualising that state of any object remains unknown and in reality it exists in all possible states concurrently till it remains unchecked. This he referred to as a principle of superposition.[10]

The many-worlds (or multiverse theory) states that as soon as a potential exists for any object to be in any state, the universe of that object transmutes into a series of parallel universes equal to the number of possible states in which that the object can exist, with each universe containing a unique single possible state of that object.[10]

Since then there has been several outstanding contribution to quantum theory, notable being – (see table 1)

Field of computing technology too have been exploring the use of quantum theory into creating environment that is more and more efficient. It all started in 1959, when Richard P. Feynman proposed an idea of creating more massive computers using quantum effects. 1985 saw David Deutsch proposing the concept of quantum logic gates in order to enhance processing power of computers. Peter Shor created an algorithm in 1984 that used only 6/7-qubits (quantum bits) to make some basic factorization. First 2-qubit computer was developed in 1998 and in 2000 4-qubit and 7-qubit computers were developed.[1]

Quantum Computing Fundamentals

Any operation having either of the two possible outcomes is referred to as binary or two-state operations. A number system using a base number or radix of 2 is known as a binary number system. Only two symbols, 0 and 1, are used to represent the numbers of this system. Each of these symbols is referred to as binary digit or more simply a bit. Classical computer understand, process and store using bit as a smallest unit of measurement. This is analogous to quantum computing principles.

In physics every object in the real world is considered to be made up of atoms, smallest unit of existence of matter.

It was in 1937 when Alan Turing developed a machine comprising of lines of cell (referred to as tapes later on) which could move back and forth that laid to evolution of quantum computing. Cells were made up of squares which could hold either 0 or 1 and alternatively can be left blank. This Turing machine also contained an active element called ‘head’ or ‘state’ which eventually would change the property namely ‘color’ of the underneath active cell. Also, read/write head component would read the symbol (0/1 or blank) and accordingly give instructions to perform the specified task. (See Fig. 1)

David Deutsch modified the Turing Machine in 1985, by replacing binary

<table>
<thead>
<tr>
<th>Year</th>
<th>Scientist</th>
<th>Theorized</th>
</tr>
</thead>
<tbody>
<tr>
<td>1905</td>
<td>Albert Einstein</td>
<td>Not just the energy, but the radiation too is quantized</td>
</tr>
<tr>
<td>1924</td>
<td>Louis de Broglie</td>
<td>The principle of wave-particle duality</td>
</tr>
<tr>
<td>1927</td>
<td>Werner Heisenberg</td>
<td>Proposed Uncertainty Principle</td>
</tr>
<tr>
<td>1935</td>
<td>Erwin Schrödinger</td>
<td>Famous Schrödinger’s cat illustration</td>
</tr>
</tbody>
</table>

Table 1: Contributors to quantum theory[10]
computing gates with quantum logic gates and called this new version as Quantum Turing Machine (QTM). In which ‘state’ of the tape could not only be either 0 or 1 but also superposition of 0 and 1 (see figure 2);

Put simply, if there is a quantum computer using n qubits, it can be in any superposition of up to $2^n$ different states simultaneously (see Fig. 3). 

**Quantum Computing Application Areas**

**Factorization**

Factorization has always been an area that attracted attention of most of the researchers in the field of computing, mainly so because of its application in the area of security (RSA algorithm) and artificial intelligence (robotics). For instance, a 129 digit number would take about 8 months and 1600 workstations (using conventional computers - 1994).

A thousand digit number(s) would therefore take 1025 years to complete the task. Shor’s algorithm using capability of quantum computers (using qubits) superpositioning can help expedite the task of factorization in about a million steps.\(^1\)

**Optimization with Artificial Intelligence**

Object detection technology which sense particular object, video compression etc.\(^6\)

**Simulations**

Any real life object that can be converted into a model that replicates its behaviour under a particular situation can be referred to as a simulation. Creating such models require large number of variables (having different domains and ever changing range) is a difficult proposition. For instance, Monte Carlo simulation is a mathematical model of simulation that employs large number of sample data. Such scenarios can be explored using quantum computing techniques.\(^8\)

**Cloud Security (majorly cryptography)**

One of the distinct features of cloud computing environment is that central servers placed at remote locations are used for storage as well as processing of data. This means that their exists an obvious challenge for the service providers to create an environment that is secure and ensures complete privacy of users data. Researchers, using the power of quantum mechanics have created cryptographic algorithm that aims at providing complete secure cloud computing environment.\(^9\)
The user’s data staying perfectly encrypted using quantum computing was first demonstrated by the scientists of the Vienna Research Group and was referred to as “blind quantum computing” in the said experiment.[4]

**Conclusions**

The exponential changes in the science of numbers and computing techniques have made mankind scale newer and greater heights. The principles of quantum physics are now being applied in an increasing number of areas, including quantum optics, quantum chemistry, quantum computing. Furthermore, having achieved maturity level when it comes to information technology arena, the focus for scientists across the globe has shifted to making cloud-based transactions more secure by applying quantum theory concepts into providing security through quantum cryptography.

**References**


Call for Contributions - CSI Communications – Programming.Learn() section

Contributions are called for Programming.Learn section under Practitioner Workbench column of the CSIC magazine. You would be aware that recently we covered various articles on R language in this section.

Prospective contributors are requested to send articles (1 page in length – around 1000 words). Those who intend to contribute a series of articles on a specific programming language are requested to send 2 or 3 sample articles and general plan of covering various aspects of the chosen language. These will be reviewed and then decision will be informed.

Please send your contribution at the earliest to csic@csi-india.org with subject title as Contribution for Programming.Learn.

(Issued on behalf of Editorial Board of CSI Communications)
Quantum Computing: Fusion of Physics and Computers

We are talking about a novel way to incorporate physics into the computers. Silicon and semiconductor phenomena have long since dominated the computer design and hardware, now we shift gears and come around with a totally new computer unknown to our predecessors. Google and NASA have teamed up for this paradigm shift and as expected, the results are mind-boggling. A Quantum computer has been designed by Google and NASA, fabricated by D-Wave Systems and installed at NASA - California.

History

Our classical computers have been around since long but Quantum computer are the most recent development. If we go by the Moore’s Law then every 18 months the processor capacity doubles; in that case we can only imagine the amount of processing power we shall need by the need of this century. Thanks to Paul Bernioff at Argonne National Laboratory who theorized the quantum computers in 1981. Actually he came up with quantum Turing Machine where in the bits can be stored as qubits. Qubits are actually the superimposition phenomena of quantum physics. At a particular memory location a bit can have value either 0 or 1 in our current classical computer, whereas qubits can be the values both 0 and 1. This allows many parallel calculations on the processor at the same time. As a memory location can have multiple values at any point in time, different values can be used for different calculations, hence allowing inherent parallelism.

We are not keen on going into too much detail about the timeline of development of quantum computers post 1982 as that would make this article a plain history informative. We rather aim at making it more interesting.

Background and Concepts

As said earlier, by Moore’s law, by the year 2020 or 2030 we shall need the circuits on microprocessor measured on atomic scale. And hence logically the next generation should steer us to quantum computers where we harness the power of atoms and molecules to perform memory and processing tasks. We use several concepts of quantum physics which are discussed as under:

1. Superposition: As discussed in the opening already, with QC (we shall refer quantum computer s as QC henceforth) we store the data as qubits where the memory can have the values 0 or 1 or a superposition of 0 and 1. The superposition is actually the symbols both 0 and 1 and all the points in between them. As a QC can have multiple states at the same time they can be multifold powerful than today’s classical systems. This can be quantified with a fact as this: a 30-qubit system is equivalent to 10 teraflops of today’s typical desktop system.

Look at the diagram below. We know that atom can have only two spins determining the value to be 0 or 1 (or at some places we choose them as +1 and -1). In case of the qubits, they can spin in any direction, allowing us values 0 and 1 at same time or any value between them.

2. Entanglement: When we try to look at a qubit in superposition we can only find whether the value is 0 or 1 whereas it actually would be having both the values. So in such a case, we may not directly look at the value of qubit. We need some indirect way to know the value of a qubit. As the law of entanglement goes, we can make two atoms closely related by applying outside force to two atoms. When this happens, the second atom takes on the properties of first atom. And from the second atom, applying some quantum physics methods, we can know the value of our atom of interest.

3. Multiverse: Quantum computing does not deny, rather support the idea of parallel universe. John Gribbin, a popular science writer believes that QC can work because they get their processing power from some other parallel universe. That said, can be interpreted as if you successfully build a quantum computer, you have all the computers from some other universe at your disposal. Well, to us, this may seem a little vague as we do...
not know the cosmology behind all this; yet what should fascinate us is the processing power of these QCs.

4. **Tunneling:** The idea of quantum tunneling; i.e. a manifest of Heisenberg’s uncertainty principle which ports the data to some other universe is also said to be used in design of quantum computers. The atoms, electrons, photons or other such subatomic particles are seen to cross a barrier without seeming to have crossed it. The MIT Technology Review reports to have simulated quantum tunneling on a QC. That is to say that the mathematical behavior of one computer is reproduced on the other hence looking at one system tells you all how another one would behave. (http://www.technologyreview.com/view/427931/first-simulation-of-quantum-tunneling-on-a-quantum-computer/)

All these concepts, due to brevity of the mention here, may seem so uncanny and weird to the field of computing but trust us, if you can, these behavior of subatomic particles in a QC can open the avenues of astro-physics that we have only heard off or scientists have only imagined thus far.

Quantum computing has now created a new class of algorithmic problems in the complexity theory too called BQP and BPP viz. Bounded error, Quantum, Polynomial time and Bounded error, probabilistic, polynomial time. These are the problems which can only be solved using probability theory in polynomial time. And these probabilistic problems can only be solved on a QC as it is the only set of problems QC can solve.

### Applications Development

Being the newest research development there are a few applications that are being targeted to the use of Quantum computers. As many researchers of the field also agree, we still do not know the right kind of the question to ask this computer. We are still not fully aware of the applications that can really harness the computing power of this magnitude. One of the many applications that are being developed by the pioneers such as Google is, Google aims to use these for improving its search and advertising capabilities. Given the large amount of data that is generated in search and adverts, Google is optimistic about making correct use of this computing power. Given that Google earns its more than two-thirds of revenue from advertisements, it wants to ensure its advertising technology can outperform that of any other company.

The biggest and complex problem in mathematics is to factorize a large number into two prime numbers. This is an important problem because almost all encryption methods are based on this problem. The quantum computer must be quickly able to identify these prime numbers. If quantum computers become commonly available, which surely is not going to happen soon, the current security and encryption algorithms are bound to fail. Currently the security algorithms that we use be it RSA or SHA, are bound only by the computations that they require. But with this magnitude of computing power, they can easily break-in to.

Our favorite and a wonderful example has been given by Google in a short video they have made for introducing this concept to the world (https://www.youtube.com/watch?v=CMdHDHeuOUE)

### Challenges

There are various challenges that are foreseen with QC. Well, we are no extra-ordinnaire to list them all but depending on the understanding and case studies that have been done to write this article, we can list a few to give you all a flavor of them.

1. A problem is because you have deal with the subatomic particles, you can change their values inherently without even knowing it. Hence, the data integrity becomes critical. If we try to look at a qubit in superposition,
it will return us the values either 0 or 1 where as it should be operating at a value in between 0 and 1 or both the values.

2. Quantum computer can run only probabilistic algorithms and that too with a rigid limit that the answer/solution will be right with high probability. Hence, our classical algorithms that we have been using it so far cannot be used directly, not even the overwhelmingly computational part of classical algorithms be accelerated.

3. Current 16-qubit QC that has been designed by D-Wave systems requires a rigorous temperature control to be maintained on the chip. And hence, thought the chip is quite small in dimensions, the housing is quite huge. And thus expensive to maintain and operate.

4. There are people who doubt whether QC designed and fabricated by D-Wave systems really operate as a QC or not. As we cannot look inside the hood of quantum computing because that would disturb the computation reason being that when we see the state of atom which is its spin then the superposition gets disturbed as explained earlier), these doubts are raised and so far there is no way out found to prove it. And this also questions the stability of the quantum states.

5. Programming of these computers has also been a problem. The current state of art is to use software that has been designed by D-Wave systems such as LIQuiD, which is a software architecture and language that can represent quantum algorithms, to technology specific lower level program.

Current Research
Researchers of Princeton University have built a rice grain-sized device laser power-driven by single electrons tunneling through artificial atoms known as quantum dots. They built the device on a single atom, which translated high level program, representing quantum algorithm, to technology specific lower level program.

Conclusion
So, we are taking the macro to the micro level; or actually we are taking the phenomena of Universe to the chips in the computer. Of course, the currently built computers are of the size of a room, keeping the legacy of their ancestors going. But eventually they will evolve to fit into our laptops. We no longer live in an age where we see or need an entire lifetime to see the research output materialize especially not if it is to build a machine.

References

About the Authors

Tadrash Shah has completed his B.E. in Computer Engineering from Gujarat Technological University in 2012. Prior to starting his M.S. in Computer Science from State University of New York at Stony Brook, he worked on projects with IIT-Gandhinagar, IIT-Bombay, IIM-Ahmedabad and United Nations. He has been serving as Technical Program Committee Member on several conferences and has many research publications. Currently he is working at Technology Analyst at Bank of America Merrill Lynch in New York. His research areas include - High Performance Computing, Algorithms and Database. Teaching also interests him apart from his coveted corporate job.

Chintan M Bhatt has received B.E. and M. Tech. Degrees from Gujarat University (CITC now CSPIT) and Dharmsinh Desai University in Computer Engineering. He is currently pursuing PhD in Computer Science. He is a member of CSI, AIIRCC (Academy & Industry Research Collaboration Center), IAENG (International Association of Engineers), ISTE, IEEE, SDIWC, EIA etc. His areas of interest include Data Mining, Web Mining, Networking, Mobile Computing Security and Software Engineering. He has more than 4 years of teaching and research experience. He is working as a Technical Program Committee member/Reviewer in many reputed international journals/conferences.
CSI Communications – Suggestions Invited for Cover Themes of forthcoming issues

Greetings from the Editors of CSI Communications! We are in the process of planning themes for future issues from April 2015 onwards and think that your inputs at this stage would be valuable. So here is a request to all of you to give suggestions regarding Cover Themes for forthcoming issues. This will help us to be on the same wavelength as you all.

So start scratching your heads and provide suggestions and send these as soon as possible. We shall finalize the topics before end of February 2015 and so please send your email to csic@csi-india.org with subject title as Cover Themes for CSIC Future Issues on or before 28th Feb. 2015.

(Issued on behalf of Editorial Board of CSI Communications)
Researchers at the Institute for Quantum Computing (IQC) are uncovering the reality of the microscopic world and harnessing the power of quantum mechanics to create next-generation technologies that promise to transform our world. Ultra-powerful computers, unbreakable cryptography, quantum devices, quantum materials, and nanotechnologies of unprecedented precision are some of the discoveries being pioneered at the institute based at the University of Waterloo.

**World-Class Science**

IQC at the University of Waterloo was founded to conduct world-leading fundamental and applied research in quantum information science and technology. That research will lead to applications in computing, communications, sensing, and applications that we haven’t yet imagined. IQC attracts the world’s top researchers and provides them with cutting-edge infrastructure, collaborative opportunities, and intellectual freedom necessary for breakthroughs to happen. Researchers are appointed to both IQC and one of six departments across three faculties at the University of Waterloo.

**Research Focus**

**Quantum Computation**

Quantum computation involves manipulating information using the rules of quantum mechanics. These rules offer a much richer environment and allow researchers to solve problems that are deemed intractable using the classical laws of physics. From material science to database search to optimization problems, the impact of quantum computation are as varied as they are transformational.

**Quantum Communication**

From the transmission of classical and quantum information to unbreakable information security, research in quantum communication will lead to new efficiencies and protocols with no classical counterpart. Short distance quantum key distribution networks are being established around the world and IQC has active projects for satellite-based global quantum communication.

**Quantum Sensors**

Sensors that behave uniquely according to the laws of quantum mechanics have the potential to achieve the highest precision, selectivity, and efficiencies allowed by nature. Quantum sensors will play a critical role in material science, neuroscience, personalized medicine, geological exploration and more.

**Quantum Materials**

Quantum systems are inherently fragile. The investigation of novel types of materials that exhibit stable quantum behaviors will be critical in bringing quantum technologies out of the lab and into the marketplace.

**Ongoing Outreach Activities**

A vibrant outreach program complements and showcases the research to bring IQC’s research to the world — and bring the world to IQC. IQC holds public lectures throughout the year featuring world-class researchers in the quantum world. In the past, we hosted talks from faculty members such as IQC Executive Director, Raymond Laflamme, Canada Excellence Research Chair David Cory and distinguished guests including John Preskill, Alain Aspect and Physics Nobel Prize co-recipient, Serge Haroche.

Every couple of years, IQC welcomes the local community to learn more about our research through an Open House visited by more than 1,200 visitors. This featured hands-on science exhibits in the

---

**Fig.1:** Deposition system to engineer novel quantum materials for application in quantum science and technology at IQC, University of Waterloo

**Fig.2:** IQC researchers discussing low-temperature experiments
Kids Zone and Discovery Zone hosted by IQC students and various local outreach initiatives, a “Meet a Scientist” zone where visitors could speak directly to IQC researchers about their work, as well as tours of state-of-the-art laboratories focused on optics, low-temperature physics, quantum cryptography and nanofabrication. It also included a Quantum Kids Science Show for children of all ages.

**Bringing Quantum to the High School Crowd**

At IQC, we host high school students and teachers throughout the year for tours and hands-on workshops. This introduces both students and teachers to quantum research through short tours of our advanced facilities or a full-day workshop. Our workshops include an introduction to Quantum Information Science and Technology, an introduction to quantum cryptography and a demonstration of superconductivity.

IQC also visits several high schools through partnerships with other local scientific outreach initiatives. Working with our partners, we look to generate widespread interest and involvement in science through quantum-themed activities and workshops.

Each summer we accept about 40 high school students into the Quantum Cryptography School for Young Students (QCSYS). It aims to teach students the tricky mathematics and physics behind quantum cryptography in just eight days. The team encourages these exceptional young adults from around the world to be bold and curious, to keep pushing the limits of what they know and to help them develop an intuition about quantum physics. Not only do they collaborate and learn about one of the most rapidly developing fields in science today, but they experience living on a university campus while being surrounded by peers who share the same interests.

**Giving Undergrads Hands-on Experience**

For those students looking to gain more knowledge about quantum information, the Undergraduate School on Experimental Quantum Information Processing (USEQIP) gives third-year undergraduate students an unprecedented experience. Each summer, this two-week program inspires students to pursue graduate studies in quantum information.

Approximately 20 students attend this workshop from all over the globe. They attend classroom lectures on the fundamentals of experimental quantum information – such as magnetic resonance, optics, superconducting qubits, quantum dots and more many. The students also spend more than 25 hours working on experiments in IQC labs to put what they have learned from the lectures into practice.

Many students stay at IQC following USEQIP with an Undergraduate Research Award (URA). It provides students the opportunity to work alongside an IQC...
faculties member or a Research Assistant Professor for the rest of the summer. This unique opportunity to interact within an interdisciplinary research community allows students to prepare for graduate studies and research careers while gaining a broad exposure to the field of quantum information processing. URAs are also available during the fall and winter terms.

Preparing for a Career in Quantum

The University of Waterloo, in collaboration with IQC, offers graduate students a unique opportunity to learn about and engage in world-leading research in quantum information. The research-based interdisciplinary graduate program in Quantum Information leads to Master’s and PhD degrees from one of six departments within the Faculties of Mathematics, Science and Engineering. Potential research topics are varied but can essentially be classified in four categories: quantum computing, quantum communication, quantum sensors and quantum materials. Students particularly interested in cryptography are not only able to pursue it through our degree program, but also IQC’s Quantum Key Distribution Summer School (QKD) every second summer. This five-day program concentrates on the theoretical and experimental aspects of quantum communication with a focus on quantum cryptography. By providing a solid foundation in relevant approaches and techniques, QKD Summer School enables graduate students to perform their own independent research.

Getting Ready for the Next Quantum Revolution

By preparing future generations with the knowledge to lead us through the next quantum revolution, IQC will continue to be a leading force with significant advancements in quantum information research. The drive for excellence will see the research spark new technologies, employ future generations and change the way we live, work and play.

Table 1: Training and Outreach offerings of IQC

<table>
<thead>
<tr>
<th>Training and Outreach offerings of IQC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique collaborative Master’s and PhD programs in Quantum Information</td>
</tr>
<tr>
<td>Strong postdoctoral fellowship program</td>
</tr>
<tr>
<td>Collaborative Research and Training Experience (CREATE) programs: Neutron Science and Engineering of Functional Materials and Building a Workforce for the Cryptographic Infrastructure of the 21st Century (CryptoWorks21)</td>
</tr>
<tr>
<td>Undergraduate School of Experimental Quantum Information Processing (USEQIP)</td>
</tr>
<tr>
<td>Quantum Cryptography School for Young Students (QCSYS)</td>
</tr>
<tr>
<td>Quantum Key Distribution (QKD) Summer School</td>
</tr>
<tr>
<td>Collaboration with high school programs for gifted students</td>
</tr>
</tbody>
</table>

Fig. 5: The Institute for Quantum Computing is hosted in the Mike & Ophelia Lazaridis Quantum-Nano Centre. The Lazaridis Centre was built with the most stringent scientific controls against vibration, temperature fluctuations, electromagnetic radiation and more, enabling research and discovery at the forefront of science.

About the Author

Martin Laforest is the Senior Manager, Scientific Outreach at Institute for Quantum Computing, University of Waterloo, Canada. The major part of his role is to bring science out of the lab and into people’s lives. Martin leads IQC’s strategic outreach programs including the Undergraduate School on Experimental Quantum Information Processing (USEQIP) and the Quantum Cryptography School for Young Students (QCSYS). He also leads the academic outreach for the collaborative graduate program in quantum information at the University of Waterloo. He is actively involved in industry and government relations at IQC bringing my scientific knowledge and experience to the discussions.

Martin Laforest holds a PhD in quantum physics from the University of Waterloo, as well as an undergraduate degree in Mathematics and Physics at McGill University. He is a passionate advocate for communicating science and share my passion with audiences around the world as a guest speaker and lecturer.

He can be reached at mlaforest@uwaterloo.ca, and 519-888-4567 x38931
Software Engineering.Tips() »

A New Software Engineering

Reprinted from ACM Queue, Volume 12, issue 10, November 29, 2014 with permission from authors

What happened to software engineering? What happened to the promise of rigorous, disciplined, professional practices for software development, like those observed in other engineering disciplines?

What has been adopted under the rubric of “software engineering” is a set of practices largely adapted from other engineering disciplines: project management, design and blueprinting, process control, and so forth. The basic analogy was to treat software as a manufactured product, with all the real “engineering” going on upstream of that—in requirements analysis, design, modeling, etc.

Doing the job this way in other engineering disciplines makes sense because the up-front work is based on a strong foundational understanding, so the results can be trusted. Software engineering has had no such basis, so “big up-front design” often has just not paid off. Indeed, the ethos of software engineering has tended to devalue coders (if not explicitly, then implicitly through controlling practices). Coders, though, are the ones who actually have to make the software work—which they do, regardless of what the design “blueprints” say should be done.

What has been adopted under the rubric of “software engineering” is a set of practices largely adapted from other engineering disciplines: project management, design and blueprinting, process control, and so forth

Not surprisingly, this has led to a lot of dissatisfaction.

Today’s software craftsmanship movement is a direct reaction to the engineering approach. Focusing on the craft of software development, this movement questions whether it even makes sense to engineer software. Is this the more sensible view?

Since it is the code that has to be made to work in the end anyway, it does seem sensible to focus on crafting quality code from the beginning. Coding, as a craft discipline, can then build on the experience of software “masters,” leading the community to build better and better code. In addition, many of the technical practices of agile development have made it possible to create high-quality software systems of significant size using a craft approach—negating a major impetus for all the up-front activities of software engineering in the first place.

In the end, however, a craft discipline can take you only so far. From ancient times through the Middle Ages, skilled artisans and craftsmen created many marvelous structures, from the Pyramids to Gothic cathedrals. Unfortunately, these structures were incredibly expensive and time consuming to build—and they sometimes collapsed in disastrous ways for reasons that were often not well understood.

Modern structures such as skyscrapers became possible only with the development of a true engineering approach. Modern construction engineering has a firm foundation in materials science and the theory of structures, and construction engineers use this theoretical foundation as the basis of a careful, disciplined approach to designing the structures they are to build.

Of course, such structures still sometimes fail. When they do, however, a thorough analysis is again done to determine whether the failure was caused by malfeasance or a shortcoming in the underlying theory used in the original design. Then, in the latter case, new understanding can be incorporated into the foundational practice and future theory.

Construction engineering serves as an example of how a true engineering discipline combines craftsmanship with an applied theoretical foundation. The understanding captured in such an accepted foundation is used to educate entrants into the discipline. It then provides them with a basis for methodically analyzing and addressing engineering problems, even when those problems are outside the experience of the engineers.

From this point of view, today’s software engineering is not really an engineering discipline at all.

What is needed instead is a new software engineering built on the experience of software craftsmen, capturing their understanding in a foundation that can then be used to educate and support a new generation of practitioners.

What is needed instead is a new software engineering built on the experience of software craftsmen, capturing their understanding in a foundation that can then be used to educate and support a new generation of practitioners. Because craftsmanship is really all about the practitioner, and the whole point of an engineering theory is to support practitioners, this is essentially what was missing from previous incarnations of software engineering.

How does the software community go about this task of “refounding” software engineering?

The SEMAT (Software Engineering Method and Theory) initiative is an international effort dedicated to answering this question (http://www.semat.org). As the name indicates, SEMAT is focusing both on supporting the craft (methods) and on building foundational understanding (theory).

This is still a work in progress, but the essence of a new software engineering is becoming clear. The remainder of this article explores what this essence is and what its implications are for the future of the discipline.

Engineering is Craft Supported by Theory

A method (equivalently, methodology or process) is a description of a way of working to carry out an endeavor, such as developing software. Ultimately, all methods are derived from experience with what does and does not work in carrying out the subject endeavor. This experience is distilled, first into rules of thumb and then into guidelines and, when there is consensus, eventually into standards.
In a craft discipline, methods are largely developed by masters, who have the long experience necessary. In older times, the methods of a master were closely guarded and passed down only to trusted apprentices. In today’s world, however, various approaches based on the work of master craftsmen are often widely published and promoted.

As a craft develops into an engineering discipline, it is important to recognize commonality between the methods of various masters, based on the underlying shared experience of the endeavor being carried out. This common understanding is then captured in a theory that can be used as a basis for all the different methods to be applied to the endeavor.

In this sense, theory is not the bad word it is sometimes treated as in our culture (“Oh, that’s just a theory”). As noted earlier, having a theoretical foundation is, in fact, the key that allows for disciplined engineering analysis. This is true of materials science for construction engineering, electromagnetic theory for electrical engineering, aerodynamics for aeronautical engineering, and so forth.

Of course, the interplay between the historical development of an engineering discipline and its associated theory is generally more complicated than this simple explanation implies. Engineering experience is distilled into theory, which then promotes better engineering, and back again. Nevertheless, the important point to realize here is this: traditional software engineering did not have such an underlying theory.

One might suggest that computer science provides the underlying theory for software engineering—and this was, perhaps, the original expectation when software engineering was first conceived. In reality, however, computer science has remained a largely academic discipline, focused on the science of computing in general but mostly separated from the creation of software engineering methods in industry. While “formal methods” from computer science provide the promise of some useful theoretical analysis of software, practitioners have largely shunned such methods (except in a few specialized areas such as methods for precise numerical computation).

As a result, there have often been cycles of dueling methodologies for software “engineering,” without a true foundational theory to unite them. In the end, many of these methods didn’t even address the true needs of the skilled craft practitioners of the industry.

So, how to proceed?

The creation of a complete, new theory of software engineering will take some time. Rather than starting with an academic approach, we can begin, as already mentioned, by capturing the commonality among the methods that have proven successful in the craft of software development. This, in turn, requires a common way of describing, understanding, and combining various software-development techniques, instead of setting them up in competition with each other.

To see how this might be accomplished, let’s take a closer look at methods and the teams of practitioners that really use them.

**Agility is for Methods, not Just Software**

The current movement to promote agility in software development complements the recognition of software craftsmanship. As the name suggests, agile software development is about promoting flexibility and adaptability in the face of inevitably changing requirements. This is done by producing software in small increments, obtaining feedback in rapid iterations, and continually adjusting as necessary.

Agile software development teams take charge of their own way of working. Such a team applies the methods it feels it needs for the project at hand as they are needed, adapting the development process throughout a project. In effect, an agile team needs to evolve and improve its methods in as agile a fashion as it develops its software.

... agile development focuses on supporting the practitioner in building quality software, rather than requiring the practitioner to support the process.

A lack of agility in methods is a central failure of traditional software engineering.

Software is, by its very nature, malleable and (physically) easy to change. A complicated software system, however, can exhibit a kind of intellectual rigidity in which it is hard to make changes correctly, with each change introducing as many or more errors as it resolves. In the face of this, the response of traditional software engineering was to adopt process-control and project-management techniques such as those used to handle similar problems with complicated hardware systems.

From an agile viewpoint, however, the application of hardware-engineering techniques was a mistake. Agile techniques, instead, take advantage of the changeable nature of software, using quick feedback cycles allowed by continuous integration and integrated testing to manage complexity, rather than process control. As a result, agile development focuses on supporting the practitioner in building quality software, rather than requiring the practitioner to support the process.

So, how do you introduce agility into software-engineering methods? By looking at the basic things that practitioners actually do—their practices.

**Methods Are Made from Practices**

A method may appear monolithic, but any method may be analyzed as being composed of a number of practices. A practice is a repeatable approach to doing something with a specific purpose in mind. Practices are the things that practitioners actually do.

For example, the agile method of Extreme Programming is described as having 12 practices, including pair programming, test-driven development, and continuous integration. The agile framework Scrum, on the other hand, introduces practices such as maintaining a backlog, daily sprints, and sprints. Scrum is not really a complete method but a composite practice built from a number of other practices designed to work together. Scrum, however, can be used as a process framework combined with practices from, say, Extreme Programming, to form the method used by an agile team.

That exemplifies the power of explicitly considering how methods are made up of practices. Teams can pull together the practices that best fit the development task at hand and the skills of the team members involved. Further, when necessary, a team can evolve its method not only in small steps, but also in more radical and bigger steps such as replacing an old practice with a better practice (without having to change any other practices).

Note how the focus is on teams and the practitioners in teams, rather than “method engineers,” who create methods for
other people to carry out. Creating their own way of working is a new responsibility for a lot of teams, however, and it is also necessary to support a team’s ability to do this across projects. It is also useful, therefore, to provide for groups interested in creating and extending practices, outside of any specific project, so they can then be used as appropriate by project teams.

This can be seen as a separation of concerns: practices can be created and grown within an organization, or even by cross-organization industry groups (such as is effectively the case with Extreme Programming and Scrum); practitioners on project teams can then adopt, adapt, and apply these practices as appropriate.

What assurance do project teams have that disparately created practices can actually be smoothly combined to produce effective methods? This is where a new software-engineering foundation is needed, independent of practices and methods but able to provide a common underpinning for them.

**The Kernel is the Foundation for Practices and Methods**

The first tangible result of the SEMAT initiative is what is known as the kernel for software engineering. This kernel can be thought of as the minimal set of things that are universal to all software-development endeavors. The kernel consists of three parts:

- A means for measuring the progress and health of an endeavor.
- A categorization of the activities necessary to advance the progress of an endeavor.
- A set of competencies necessary to carry out such activities.

Of particular importance is having a common means for understanding how an endeavor is progressing. The SEMAT kernel defines seven dimensions for measuring this progress, known as alphas. (The term alpha was originally an acronym for abstract-level progress health attribute but is now simply used as the word for a progress and health dimension as defined in the kernel. Many other existing terms were considered, but all had connotations that clashed with the essentially new concept being introduced for the kernel. In the end, a new term was adopted without any of the old baggage.) The seven dimensions are: opportunity, stakeholders, requirements, software system, work, team, and way of working.

These alphas relate to each other as shown in Fig. 1.

Each alpha has a specific set of states that codify points along the dimension of progress represented by the alpha. Each of the states has a checklist to help practitioners monitor the current state of their endeavor along a certain alpha and to understand the state they need to move toward next. The idea is to provide an intuitive tool for practitioners to reason about the progress and health of their endeavors in a common, method-independent way.

One way to visualize the seven-dimensional space of alphas is using the spider chart shown in Fig. 2. In this chart, the shaded area represents how far an endeavor has progressed, while the white area shows what still needs to be completed before the endeavor is done. A quick look at such a diagram provides a good idea of where a project is at any point in time.

The alphas can be made even more tangible by putting each of the alpha states on a card, along with the state checklist in an abbreviated form (see Fig. 3). The deck of all such cards can then fit easily into a person’s pocket. Although more detailed guidelines are available, these cards contain key reminders that can be used by development teams in their daily work, much like an engineer’s handbook in other disciplines.

A more complete discussion of the kernel and its application is available in previous work.[2,3] The kernel itself is formally defined as part of the Essence specification that has been standardized through the Object Management Group.[4] In addition to the full kernel, the Essence standard also defines a language that can be used both to represent the kernel and to describe practices and methods in terms of the kernel. Importantly, this language is intended to be usable by practitioners, not just method engineers; for basic uses, it can be learned in just a couple of hours (the alpha state cards are a simple example of this).

Of course, this ability to use the kernel to describe practices is exactly what is needed as a foundation for true software engineering methods.

**Practices Built on the Kernel Enable Method Agility**

A practice can be expressed in terms of the kernel by:

- Identifying the areas in which it advances the endeavor.
- Describing the activities used to achieve this advancement.

These alphas relate to each other as shown in Fig. 1.

Each alpha has a specific set of states that codify points along the dimension of progress represented by the alpha. Each of the states has a checklist to help practitioners monitor the current state of their endeavor along a certain alpha and to understand the state they need to move toward next. The idea is to provide an intuitive tool for practitioners to reason about the progress and health of their endeavors in a common, method-independent way.

One way to visualize the seven-dimensional space of alphas is using the spider chart shown in Fig. 2. In this chart, the shaded area represents how far an endeavor has progressed, while the white area shows what still needs to be completed before the endeavor is done. A quick look at such a diagram provides a good idea of where a project is at any point in time.

The alphas can be made even more tangible by putting each of the alpha states on a card, along with the state checklist in an abbreviated form (see Fig. 3). The deck of all such cards can then fit easily into a person’s pocket. Although more detailed guidelines are available, these cards contain key reminders that can be used by development teams in their daily work, much like an engineer’s handbook in other disciplines.

A more complete discussion of the kernel and its application is available in previous work.[2,3] The kernel itself is formally defined as part of the Essence specification that has been standardized through the Object Management Group.[4] In addition to the full kernel, the Essence standard also defines a language that can be used both to represent the kernel and to describe practices and methods in terms of the kernel. Importantly, this language is intended to be usable by practitioners, not just method engineers; for basic uses, it can be learned in just a couple of hours (the alpha state cards are a simple example of this).

Of course, this ability to use the kernel to describe practices is exactly what is needed as a foundation for true software engineering methods.

**Practices Built on the Kernel Enable Method Agility**

A practice can be expressed in terms of the kernel by:

- Identifying the areas in which it advances the endeavor.
- Describing the activities used to achieve this advancement.
A practice can also extend the kernel with additional states, checklists, or even new alphas.

The critical point is that the kernel provides a common framework for describing all practices and allowing them to be combined into methods. Bringing a set of practices into this common system allows gaps and overlaps to be more easily identified. The gaps can then be filled with additional practices and the overlaps resolved by connecting the overlapping practices together appropriately.

For example, consider two practices: one about using a backlog to manage the work to be carried out by a team (advancing the work alpha), the other about defining requirements using user stories (advancing the requirements alpha). The backlog practice does not prescribe what the items on the backlog must be, while the user-story practice does not prescribe how the team should manage the implementation of those stories. The two practices are thus complementary and can be used together—but, when so combined, they overlap. The two practices can be connected in a smooth and intuitive way within an overall method by identifying backlog items from the one with user stories from the other, so that user stories become the items managed on the backlog.

Note, in particular, how the common framework of the kernel provides a predictive capability. A construction engineer can use materials science and the theory of structures to understand at an early stage whether a proposed building is likely to stand or fall. Similarly, using the kernel, a software developer can understand whether a proposed method is well constructed, and, if there are gaps or overlaps in its practices, how to resolve those.

Further, through the separation of concerns discussed earlier, an organization or community can build up a library of practices and even basic methods that a new project team may draw on to form its initial way of working. Each team can then continue to agilely adapt and evolve its own methods within the common Essence framework.

Ultimately, the goal will be, as an industry, to provide for the standardization of particularly useful and successful practices, while enhancing, not limiting, the agility of teams in applying and adapting those practices, as well as building new ones as necessary. And that, finally, is the path toward a true discipline of software engineering.

Conclusion

The term paradigm shift may be a bit overused these days; nevertheless, the kernel-based Essence approach to software engineering can quite reasonably be considered to be such a shift. It truly represents a profound change of viewpoint for the software-engineering community.

When Thomas Kuhn introduced the concept of a paradigm shift in his influential book, The Structure of Scientific Revolutions, he stressed the difficulty (Kuhn even claimed impossibility) of translating the language and theory of one paradigm into another. The software-development community has actually seen such shifts before, in which those steeped in the old paradigm have trouble even understanding what the new paradigm is all about. The move to object orientation was one such shift, as, in many
ways, is the current shift to agile methods.

In this regard, Essence can, indeed, be considered a paradigm shift in two ways. First, those steeped in the “old school” of software engineering have to start thinking about the true engineering of software specifically, rather than just applying practices largely adapted from other engineering disciplines. Second, those in the software craftsmanship and agile communities need to see the development of a true engineering discipline as a necessary evolution from their (just recently hard-won!) craft discipline.

In regard to the second point, in his foreword to The Essence of Software Engineering: Applying the SEMAT Kernel,[3] Robert Martin, one of the SEMAT signatories, describes a classic pendulum swing away from software engineering toward software craftsmanship. Martin’s assessment is correct, but it is important to note that this proverbial pendulum should not simply swing back in the direction it came. To the contrary, while swing it must, it now needs to swing in almost a 90-degree different direction than the one from which it came, in order to move toward a new discipline of true software engineering.

There is, perhaps, hardly a better image for a paradigm shift than that. In the end, the new paradigm of software engineering, while building on the current paradigm of software craftsmanship, must move beyond it, but it will also be a shift away from the old paradigm of traditional software engineering. And, like all paradigm shifts before, this one will take considerable time and effort before it is complete—at which point, as the new paradigm, everyone will consider its benefits obvious.

Even as it stands today, though, using Essence can provide a team with some key benefits. Essence helps teams to be agile when working with methods and to measure progress in terms of real outcomes and results of interest to stakeholders. These progress measurements are not only on one dimension, but along the seven dimensions of the kernel alphas, all of which need to be measured to reflect the true state of the project and the software product. Essence can, indeed, be considered a paradigm shift . . . those steeped in the “old school” of software engineering have to start thinking about the true engineering of software specifically, rather than just applying practices largely adapted from other engineering disciplines.

The real shift, however, will only come as teams truly realize the benefits of Essence today and as SEMAT builds on Essence to complete the new software engineering paradigm. Further, Essence can allow organizations to simplify governance of methods, using a pool of practices that may be adopted and adapted by project teams. Having Essence as a common foundation for this also allows practitioners to learn from one another more readily.

The real shift, however, will only come as teams truly realize the benefits of Essence today and as SEMAT builds on Essence to complete the new software engineering paradigm. A community of practitioners is now contributing their experience and becoming part of this “refounding” of software engineering—or, perhaps, really founding it for the first time.

References
Quantum Computing – Boon or Bane?

Quantum computing uses an entirely different approach than classical computing. Classical computers that record, store and process data in bits (using two states 0 and 1) use transistors. Quantum computers use Qubits that can take multiple states 0, 1 or 0 and 1 and all points in between at the same time which is called superposition. This “quantum superposition”, along with the quantum effects of entanglement and quantum tunneling, enable quantum computers to consider and manipulate all combinations of bits simultaneously, making quantum computation powerful and fast. This inherent parallelism allows a quantum computer to work on a million computations at once, while your desktop PC works on one. A 30-qubit quantum computer would equal the processing power of a conventional computer that could run at 10 teraflops (trillions of floating-point operations per second). Today’s typical desktop computers run at speeds measured in gigaflops (billions of floating-point operations per second). Some of the systems under development use “quantum annealing” to solve problems. Quantum annealing “tunes” qubits from their superposition state to a classical state to return the set of answers scored to show the best solution. For a relatively new field which is about 30 years old, Quantum computing has taken giant strides. Although quantum computers for practical computing are still a far away possibility, quantum computers are being built, albeit with restricted uses and capabilities.

These capabilities and the enhanced speed and ability of Quantum Computers will enable tasks that have long been thought impossible (or “intractable”) for classical computers, which will now be achieved quickly and efficiently by a quantum computer.

But, all is not roses all the way and there are problems and issues too. One of the obvious issues is the threat that it poses to cryptography based security that uses symmetric algorithms, and even RSA and DSA. Quantum computing definitely poses a threat to internet security and security in the business, medical and even personal world of people who use computers. It will now be possible to use quantum computing to break the keys – which essentially require factorization of a very large number, in a very short time, making this kind of security vulnerable to compromise.

But there are some ethical issues involved in Quantum computing too. Qubits as we have seen have a number of properties that distinguish them from classical bits. Most significantly, the physics of qubits envisages that the state of a qubit at any given moment cannot be known in a classical sense. A qubit can be thought of as being both a 0 and a 1 simultaneously (in superposition). When the superposition is destroyed, the qubit becomes a classical bit, either a 0 or a 1, with a certain probability. The very nature of quantum computation is to manipulate that probability so that the correct result is most likely. The implication is that while most of the time the result will be correct, sometimes it will be wrong. Because the quantum sub process is efficient, it is practical to compute in this way, in cases where a relatively easy check for correctness of the solution is available. Unfortunately, it will also be possible to use quantum sub processes to speed up algorithms for problems that do not have an easy check for correctness, thus calling the reliability of the results into question.

What can go wrong or what issues could arise using such systems more frequently and on larger scale especially using quantum computers of different power and capacity? Is it really safe to depend on systems for important business, welfare / social / health and personal decisions? Especially are users of these computers aware of their limitations and also really aware as to the true meaning and significance of the solutions provided by these computers? These are significant issues especially in the context of Ethics, Governance, and Security. Businesses and society need to consider these issues before progressively adopting and relying on these systems. Since research is at present ongoing and it is early days of Quantum Computing it is necessary to look into these aspects more closely.

Given this background the current Case in Information Systems is being presented. The facts of the case are based on information available in media reports online information and real life incidents. Although every case may cover multiple aspects it will have a predominant focus on some aspect which it aims to highlight.

A case study cannot and does not have one right answer. In fact answer given with enough understanding and application of mind can seldom be wrong. The case gives a situation, often a problem and seeks responses from the reader. The approach is to study the case, develop the situation, fill in the facts and suggest a solution. Depending on the approach and perspective the solutions will differ but they all lead to a likely feasible solution. Ideally a case study solution is left to the imagination of the reader, as the possibilities are immense. Readers’ inputs and solutions on the case are invited and may be shared. A possible solution from the author’s personal viewpoint is also presented.
A Case Study of Niti Aayog of the State of Surashtra

NITI Aayog is a dynamic institution in the State of Surashtra, which will provide a concrete plan based on changing global socio-economic structure and its impact on the economy. It is expected to play a pivotal role in the development of the state in the years to come.

Yogiraj, the CEO of Niti Aayog has decided it’s high time to introduce Quantum Computing in the planning process. After his recent US trip where he has seen these systems work on problems at lightning speed, he is convinced that in these days of complex decisions involving interconnected economies in a globalised scenario adopting Quantum Computing is the way forward for the Aayog.

He calls a meeting of his management team and shares his viewpoint. He emphasizes that adopting Quantum Computing will enable Niti Aayog to:

- Open up and capitalize on greater opportunities with less human error
- Profit from opportunities between multiple scenarios and possibilities at a rapid pace
- Curtail computing and decision making costs and
- Enable a reasoned decision in an otherwise imperfect economy by using quantum computing to tunnel through to the optimal solution.

Purandas a renowned economist is an old timer. He and the chief secretary Manibhadra are not happy. The chief statistician Kalpesh is elated at the prospect and is all set to work on the new system. In fact he anticipates a fair reduction in staffing and computing costs which can substantially fund the acquisition of the system. He is also happy that being the latest and state of the art technology and generally unintelligible to the masses as well as to the politicians and little understood even by the cream of society, results generated and decisions taken based on these would need little explaining and would rarely be questioned. It is amidst these conflicting opinions in the Niti Aayog team that a go ahead is given and a time frame of one year is given to implement and roll out the system.

Purandas concerned as he was pointed out two significant reports:

The first about Quantum Computers and the End of Security:

“The cryptosystem setup assumes that a spy can eavesdrop on the connection, but it will take an unreasonable amount of time (from dozens to millions of years depending on key length) to calculate a secret key and decrypt the connection. It turns out that quantum computers might help here. Using Shor’s algorithm, a quantum computer comes to a final state corresponding to solved mathematical problems very quickly, almost as fast, as an ordinary computer multiplying a couple of numbers. A quantum computer might find the required large numbers very quickly, helping an attacker calculate the secret key and decrypting the message.”

The second one was the report that discussed “Is quantum computing inherently evil?”

The report highlights –

- Ethical Concerns about the Probability of Incorrect Results
- Ethical Concerns about Debugging Quantum Computing Solutions
- Ethical Concerns about Quantum Computing and Encryption

The quantum state is destroyed in order to gain access to its classical information. In the destruction of the quantum state, all quantum information is lost. The argument is that in this case, the info sphere has been negatively affected by the loss of the quantum information which at the very least is not commendable according to Information Ethics.

Kalpesh points out that in any computational setting; it is not the computation that is the potential source of damage to the info sphere. The potential damage comes from the (incorrect) choice of probability thresholds and insufficient software safeguards to protect against incorrect responses. Computers do exactly as they have been programmed to do, and there will be large errors only if they aren’t monitored properly. According to him all these were human errors and blaming the Quantum Computing systems was just witch-hunting.

Yogiraj who had already made up his mind, pointed out that at this stage any debate was pointless and inputs provided by Purandas were aberrations and could be taken care of by improving the system.

To reassure the old timers and the opponents, Yogiraj decides to call in Sumati an experienced analyst who had experience and expertise in Quantum Computing to help them adopt it expeditiously. Sumati has been approached and has suggested a way forward.

Solution

The Situation

Quantum Computing is still under development and it will take a while before it reaches a large number of serious users. It will take even more time before it becomes available to a large section of society. Currently Quantum Computing is able to solve so-called “optimization” problems, where there are a series of criteria all simultaneously competing to be met, and where there is one optimum solution that satisfies the majority of them.

But there is no denying that Quantum computing is a practical tool for extremely complex predictive analysis, and machine learning where you need to assess many variables and many patterns and test models against it. This is relevant in the area of drug discovery, cyber security, business, finance, investment, health care, logistics, and above all in planning. There are a number of government, professional, business and other applications—that those that involve solving complex optimization problems—that today would be too difficult to address with silicon computing.

Traditional computers, including supercomputers, require substantial time to crunch that kind of big data. But scientists

---

The quantum state is destroyed in order to gain access to its classical information. In the destruction of the quantum state, all quantum information is lost. The argument is that in this case, the info sphere has been negatively affected by the loss of the quantum information which at the very least is not commendable according to Information Ethics.
have long theorized that a computer that harnesses the often-peculiar principles of quantum mechanics could perform these kinds of calculations in a flash, and even solve problems that would take years for a normal computer to churn through. This is now becoming a reality with the advent and use of quantum computing.

**The Consequences**
The State of Surashtra and its Niti Aayog has to understand and appreciate this and be alive to these issues which cannot be ignored when implementing and using quantum computing. It is a situation that needs to be handled with care; quantum computing can only be ignored at peril and as of now adopted with peril too.

**The Strategy**
The right strategy for the Niti Aayog will be to deal with each of these issues:

1. **Ethical issues in Quantum Computing - Security Concerns** - These need to be addressed by developing security solutions based on Post-Quantum Cryptography. E.g. Use of Lattice-based systems. Developments such as these in Post-Quantum Cryptography are indeed required to keep us secure well into the future.

2. **Ethical issues in Quantum Computing - Probability of Incorrect Results** - The low-level of awareness of technical details about quantum computing poses a serious trust issue. Future quantum developers will be well aware of the probabilistic nature of qubits. But most computer users will not be aware of this, nor will they want to be bothered about it. On one hand users will have to be shielded from the consequences of qubit uncertainty through ethical care in development. On the other hand, it will be the responsibility of developers, to inform the users of the probabilistic nature of the results of computations based on qubits. Users’ trust of computational accuracy will be based on how much users trust the developers. If the widespread introduction of quantum computing is done in such a way that mistrust in computing becomes significantly higher, this will have adverse societal effects.

3. **Debugging Quantum Computing Solutions** - It is impossible to make copies of quantum registers and it is impossible to inspect quantum registers part way through a computation without destroying the computation that is in progress. At an ethical level, as new debugging techniques are developed, the probabilistic nature of quantum computation should serve as a constant reminder to the debugger of quantum software that no two quantum registers prepared and treated identically can be assumed to register identical information as is so often done (and rightly so) with the information stored in classical memory.

4. **Human errors, unauthorized changes / alterations and Rogue elements** - The nature of Quantum Computing brings additional ethical responsibilities that quantum developers and those in charge of the systems have with respect to the roll-out of large quantum computers.

5. **Unforeseen Issues and Problems** - If quantum developers are careless and secretive about the uncertainty of their algorithms and applications, the info sphere will be harmed.

---

**If quantum technologies are anticipated wisely and gracefully introduced by the experts, decision makers and users, the info sphere could be enhanced; but if quantum technologies are allowed to undermine trust due to inadequate care, malicious use and negligent oversight, then the info sphere will be harmed.**

---

If quantum technologies are anticipated wisely and gracefully introduced by the experts, decision makers and users, the info sphere could be enhanced; but if quantum technologies are allowed to undermine trust due to inadequate care, malicious use and negligent oversight, then the info sphere will be harmed. Niti Aayog and its key functionaries will do well to put in place adequate controls, sensitize the developers and take due care to address these and newer threats and issues as they emerge and follow best practices to make good and beneficial use of Quantum Computing.

An effective solution is generally expected to proceed on these lines.

---

**About the Author**

Dr. Vishnu Kanhere

Dr. Vishnu Kanhere is an expert in taxation, fraud examination, information systems security and system audit and has done his PhD in Software Valuation. He is a practicing Chartered Accountant, a qualified Cost Accountant and a Certified Fraud Examiner. He has over 30 years of experience in consulting, assurance and taxation for listed companies, leading players from industry and authorities, multinational and private organizations. A renowned faculty at several management institutes, government academies and corporate training programs, he has been a key speaker at national and international conferences and seminars on a wide range of topics and has several books and publications to his credit. He has also contributed to the National Standards Development on Software Systems as a member of the Sectional Committee LITD17 on Information Security and Biometrics of the Bureau of Indian Standards, GOI. He is former Chairman of CSI, Mumbai Chapter and has been a member of Balanced Score Card focus group and CGeIT-QAT of ISACA, USA. He is currently Convener of SIG on Humane Computing of CSI and Topic Leader - Cyber Crime of ISACA(USA). He can be contacted at email id vkanhere@gmail.com
Solution to January 2015 crossword

**CLUES**

**ACROSS**

4. Uses entangled states and classical communication to transfer arbitrary quantum states from one location to another (7, 13)
5. Uses atomic quantum states to effect computation (7, 8)
7. A device which can be used to store or transfer information between independent quantum bits (7, 3)
8. Type of integer greater than 1 with no positive integer divisors other than 1 and itself (5)
9. A geometrical representation of the pure state space of a quantum bit (5, 6)
12. Term used in theoretical physics to express hypothetical “shortcut” through space and time (8)
14. A communication text in cipher or code (10)
15. A stable subatomic particle with a charge of negative electricity (8)
17. A mathematician who devised a quantum algorithm for integer factorization (5, 4)
18. A type of Quantum Logic Gate that prepares the input state in a superposition state (8)
22. The orientation of a photon’s vibrations (12)
23. A type of quasiparticle having properties intermediate between those of bosons and fermions (5)
24. A possible implementation of a quantum bit (7, 3)
25. Type of crystals that exhibit energy band structure for photons (8)
26. Term used to describe the stable superposition of states (8)

**DOWN**

1. Quantum bit (5)
2. The vertical and horizontal polarizations (11)
3. A collection of n quantum bits (7, 8)
6. Data Encryption Standard (3)
10. Originator of the Grover database search algorithm used in quantum computing (3, 6)
11. A property of waves that can oscillate with more than one orientation (12)
12. An oscillation that travels through matter or space, accompanied by a transfer of energy (4)
13. An ambiguous state in which a particle can be both a “0” and a “1” (13)
16. A spectroscopic technique that detects species that have unpaired electrons (3)
17. Light particle (6)
19. An elementary particle and a fundamental constituent of matter (5)
20. A self-reinforcing solitary wave that maintains its shape while it propagates at a constant velocity (7)
21. A type of Quantum Logic Gate whose second input is negated only when the first input is true (4)

---

**Did you know role of Doped Diamond in Quantum Computing?**

A defect is intentionally added to make a diamond doped. Physicists claim these defects can be used to manipulate the spin of quantum particles. Diamonds can play a major role towards better quantum computers and nanoscale sensors.

(More details can be found in http://www.bbc.com/future/story/20130218-diamond-idea-for-quantum-computer)

---

We are overwhelmed by the responses and solutions received from our enthusiastic readers.

**Congratulations!**

NEAR ALL correct answers to January 2015 month’s crossword received from the following reader:

Er. Aruna Devi (Surabhi Softwares, Mysore) and Surendra Khatri (Senior CSI Member, Retired From Survey of India).
The following are the ICT news and headlines of interest in January 2015. They have been compiled from various news & Internet sources including the dailies - The Hindu, Business Line, and Economic Times.

**Voices & Views**

- Kerala will be the first State to go on NFN. In two years, the entire Kerala population will move to smartphones – BBNL chief.
- The cost of a transaction at a bank branch is Rs. 40-50 on an average. But at an ATM the cost drops to Rs. 10-12, and on the debit card, it drops further to Rs. 2-3 a transaction – Banking experts.
- At present the IT sector in Karnataka provides direct and indirect employment to 40 lakh people besides contributing Rs. 1.80 lakh crore to export revenue - 5R Patil, Karnataka Minister for Planning and Statistics, IT, BT, Science & Technology.
- Cashless transactions only way to curb black money - Modi.
- Artisans take e-comm route to better their life.
- Kerala will be the first State to go on Mee Kosam – to let people post their grievances online.
- TCS issues pink slips: techies scramble to unison.
- The trading of ‘used’ software licences is set to help rural Indians derive the benefits of IT in daily activities.
- India's BT industry sources.

**New Initiatives**

- NITI - National Institutions for Transforming India Aayog replaces Planning Commission.
- Free land among sops Karnataka is offering to IT firms moving to Tier-II/III cities.
- Online approval system soon for moving heavy cargo.
- India, US to discuss social security, visas ahead of Obama’s visit.
- Centre to implement Rs. 1,900-cr e-governance project for ESIC.
- Cabinet approves 2G spectrum auction, hopes to garner Rs. 64,800 crore.
- Rural BPO policy to improve skills, economic conditions soon – Prasad, IT Minister.
- Telecom industry fears excessive auction as Centre squeezes 3G spectrum supply.
- Digital knowledge bridge - ‘Gyan Setu’ is set to help rural Indians derive the benefits of IT in daily activities.
- AP Govt. proposes a 6000 Crore optical fibre project which aims at making available 10-15 Mbps broadband connections each to 12 million homes at about Rs. 150 per month and on-demand availability of 100 Mbps to one Gbps connection to every business enterprise.
- In a first, Kerala allows mobile towers on govt land, buildings.
- Centre refers plea on banning porn websites to Cyber Law Division.
- Pre-Budget meet: IT industry wants tax incentives to set up data centres.
- Coming soon, policy on Net neutrality, security - IT Minister.
- The digitisation of about 73 lakh SHGs is expected to result in better participation in financial inclusion scheme.
- DoT agrees to Microsoft’s proposal to tap unused spectrum in terrestrial TV frequency bands for offering broadband services.
- Modi’s Digital India project delayed by cable tangle.
- Pricing 3G spectrum at Rs. 3.705 cr/MHz, Centre eyes Rs. 1-lakh crore mop-up.
- India asks for US comments on draft IPR policy.
- US, India to formulate smart city action plan in 3 months for Visakhapatnam, Allahabad, Ajmer.
- Hyderabad to have the country’s first home-grown Conditional Access System (CAS) for cable television.
- Samsung, known for its phones running own Tizen OS.
- Google unveils Flight search tool.
- BPO firm Omega Healthcare to hire 2,300 this year.
- Google India MD Rajan Anandan made in charge of S-E Asia too.

**Govt, Policy, Telecom, Compliance**

- 3G spectrum: TRAI proposes 18% cut in reserve price at Rs. 2,720 cr/MHz.
- The Rs. 30,000-crore project NOFN will be the digital backbone of India and aims to take high-speed broadband connectivity to 2.5 lakh gram panchayats.
- RBI is looking to remove the two-factor authentication requirement for small-value transactions up to Rs. 3,000 to make transactions easier.
- The AP Govt., to start an online window - Mee Kosam - to let people post their
e-commerce transactions are taking off, 50,000 jobs likely in 2-3 years. In India, most e-commerce firms increased salaries by 10-40 per cent in 2013 and 2014 and are paying annual salaries of Rs. 10 lakh to Rs. 23 lakh at the entry level.
- Foxconn deadlock continues as union, management dig in. The factory has stopped production since December 22 as there was no order from customers.
- We must encourage students to look at entrepreneurship as a career option – IITM Director.
- Online furniture vendor Urban Ladder will add 1,400 employees to its workforce this year.
- The demand is set to increase to 30,000 skilled VLSI engineers per annum after 12 months.
- Data analysis skills vital for jobs in the banking sector – Bankers.
- Govt. to use 43,000 km of optical fiber network and 6,000 railway stations across India in the skill development revolution.
- TCS says only 1% about 3000 staff will be involved in ‘involuntary attrition’ this year.
- Capgemini plans to recruit 20,000 in India by 2016.
- TCS extends research scholarship programme for students abroad.
- Pre-Budget meet: IT industry wants tax incentives to set up data centres.
- Coming soon, policy on Net neutrality, security - IT Minister.
- The digitisation of about 73 lakh SHGs is expected to result in better participation in financial inclusion scheme.
- DoT agrees to Microsoft’s proposal to tap unused spectrum in terrestrial TV frequency bands for offering broadband services.
- Modi’s Digital India project delayed by cable tangle.
- Pricing 3G spectrum at Rs. 3.705 cr/MHz, Centre eyes Rs. 1-lakh crore mop-up.
- India asks for US comments on draft IPR policy.
- US, India to formulate smart city action plan in 3 months for Visakhapatnam, Allahabad, Ajmer.
- Hyderabad to have the country’s biggest start-up facility T-Hub funded and promoted by the Telangana State Govt.
- E-commerce may soon come under the lens of nine ministries, RBI.

**Company News: Tie-ups, Joint Ventures, New Initiatives**

- Tata Group will invest in future and emerging technologies in the digital and physical space – Mistry.
- IndusInd Bank has a special innovation team and was the first to launch video banking, whereby bank officials can see and talk to the customers over the phone.
- Broadcom pledges support to cable TV digitisation in India – to developing country’s first home-grown Conditional Access System (CAS) for cable television.
- Online classified portal Quikr.com, which is the business of used goods, plans to provide delivery services to its subscribers.
- Google unveils Flight search tool.
- Recently launched intelligent ATM (ATM) developed by Chennai-based Leo Prime Payment Solutions comes with a button and also will give non-fatal shock to crooks.
- New software technology known as Hotknob to transfer big files to another phone.
- Samsung, known for its phones running on Google’s Android operating system (OS), has launched its first phone on its own Tizen OS.
- Infosys creates $250-million fund for start-ups.
- E-tailers setting up labs to innovate on customer experience.
- Yu Televentures has sold 10,000 Yureka smartphones on Amazon in just 3 seconds.
- Airtel-Cisco to launch video conferencing service.
- Pearson takes digital learning to classrooms with new mobile app – MyPedia which will cost $2,000 annually for a child.
- Infibeam introduces logistics platform www.shipdroid.com for online merchants.
CSI Reports

From CSI SIG and Divisions »

Please check detailed news at:
http://www.csi-india.org/web/guest/csic-reports

<table>
<thead>
<tr>
<th>SPEAKER(S)</th>
<th>TOPIC AND GIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division-V (Educations and Research) and IEEE Kolkata Section and C.V. Raman College of Engineering, Bhubaneswar</td>
<td></td>
</tr>
<tr>
<td>Dr. V Chandrasekhar, Dr. Anirban Basu, Dr. KC Patra, Dr. RK Das, Dr. Rachita Misra, Dr. Ajith Abraham, Dr. Dhamendra Prakash Sharma, Bhanu Pratap Dash, Dr Anil Kumar, Manoj Nambiar &amp; Dr. Uma Charan Mohanty</td>
<td></td>
</tr>
</tbody>
</table>

Conference was inaugurated by Dr. Chandrasekhar who emphasized need of innovative research in India by citing Dr. CV Raman’s achievements. Dr. Basu discussed how supercomputing has changed from single core architecture to multi-core, distributed and hybrid models for the present day HPC demands. Organizers released book of program & abstracts and proceedings in CD form which was distributed to all. Around 150 delegates attended included delegates from China, Japan as well as IITs, NITs, IIITs, BITS, Central & State Universities, Engineering colleges, Corporate research departments & Govt of India research laboratories and faculty & students from local colleges. There were 8 technical sessions & 81 peer reviewed papers were presented which will be published in IEEE Xplore. Speakers delivered lectures on many aspects of efficient architecture, networking, computational intelligence & applications of HPC. On closing day Dr. Mohanty spoke emphasizing demand for high performance computing in the Indian Context and encouraged researchers and students pursuing studies in this field.

Annual Student Convention of CSI

ESL Narasimhan, SV Raghavan, Dr. SS Mantha, TS Kohli, GS Kohli, HR Mohan, Dr. HS Saini, Dr. DD Sarma, Raju Kanchibotla, Sanjay Mohapatra, ML Saikumar, Gautam Mahapatra and Chandra Dasaka

3-4 January 2015: Annual Student Convention of CSI

Chief Guest Narasimhan said that IT has changed entire global order making world a global village. He mentioned 3 parameters in taking up this challenge - Economic Power, Environment Security and Good Governance. Prof. Raghavan deliberated on convention objectives: To motivate students in engineering and other disciplines in state of art developments in ICT & to facilitate initiative to understand expectations of industry from freshers. Dr. Mantha explained role of AICTE in maintaining standards in engineering education. Dr. Saini briefed on courses run at GNI and on projects being executed in areas such as Solar Energy, Robotics, Entrepreneurship & Software development at GNI’s Innovative Centre. Sessions were conducted on - Campus to Corporate, Carrier Opportunities, Entrepreneurship & Career Opportunities in Government & PSUs and Technology Enablement in Education. Certificates of merit and mementoes were presented for best papers and to first two teams of Hackathon and Devthon.

Patna Women’s College in Technical Collaboration with Division – I (Systems) Division – III (Applications) & Patna Chapter

Dr. Ranjit Verma, UK Singh, Atul Sinha, Dr. AK Nayak, Dr. MN Hoda, Dr. Marie Jessie AC, Bhawana Sinha

22 January 2015: National Seminar on “ICT and Women Empowerment”

Seminar was inaugurated by Prof. Ranjit Verma. Prof. UK Singh and Atul Sinha were guests of honour. Ms. Bhawana Sinha introduced seminar theme & Prof. Nayak explained contribution of ICT for Women empowerment. Prof. Hoda talked about different areas where women should empower themselves. Prof. Singh stressed upon larger participation of women in technical sector in general & ICT sector in particular. Atul Sinha advised women to be empowered without depending on others. Dr. Verma explained action & activities of empowered women of Indian history and pointed out that women can do everything good as their male counterpart. Altogether there were 5 keynote lectures, 4 invited lectures and presentations of 40 technical papers in two parallel sessions apart from 30 contributions in Poster Presentation.
## CSI News

### From CSI Chapters »


<table>
<thead>
<tr>
<th>SPEAKER(S)</th>
<th>TOPIC AND GIST</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DELHI (REGION I)</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Prof. (Dr) Gurdeep S Hura, VK Gupta and SD Sharma | 17 December 2014: Golden Jubilee Celebrations Technical Talk on “Cyber Infrastructure for Emerging Computing Technologies: A New Global Perspective”  
Mr. Sharma said that cyber infrastructure is a challenging topic. Understanding its various aspects needs formation of information assurance curriculum & related research by students of multi-disciplinary majors. Dr. Hura explained that internet grew rapidly as general-purpose enabling infrastructure, upon which controls had to be superimposed in an ad hoc manner. However knowledge infrastructure is human-centered & optimized for particular resources and communities. Cyber infrastructure offers advanced knowledge infrastructure for research & education that integrates diverse resources across barriers of geography & time & across subtle & complex barriers of discipline, community sector & jurisdiction. | [Dr. Ratan Datta presenting memento to speaker](http://www.csi-india.org/web/guest/csic-chapters-sbs-news) |
| **NASHIK (REGION VI)** | |
| Chairman Girish Pagare and Hon. Secretary Sandeep Karkhanis | 11 January 2015: Golden Jubilee Program and SWOT Analysis Group Work  
Program was attended by 40 participants. Girish Pagare shared journey of CSI for last fifty years. He expressed gratitude towards all past & present Execom, Divisional, Regional and Chapter MC members of CSI, guidance provided by various professionals, support by educational institutes and mainly people of Nashik. Group work cum workshop was organized to conduct SWOT analysis of the chapter to make it more vibrant and effective. Workshop was moderated by Sandeep Karkhanis; based on ‘Kaizen’ principles. The brainstorming brought many insights. | [Golden Jubilee Program participants](http://www.csi-india.org/web/guest/csic-chapters-sbs-news) |
| **CHENNAI (REGION VII)** | |
| Dr. S Kannan, Ph.D.,CA, CISA, CISM | 7 January 2015: Talk on “Vedic Self-Management”  
Talk was organized jointly with IEEE Computer Society, Madras chapter. Vedic self-management refers to the art of managing self as a wholesome entity at the physical, emotional, intellectual and creative levels. Talk was delivered by Dr. S Kannan who holds a Ph.D. in Commerce and another inter-disciplinary Ph.D. in Management and Sanskrit in the domain of Vedic Management. | [Resource person while delivering the talk](http://www.csi-india.org/web/guest/csic-chapters-sbs-news) |
| **CHENNAI (REGION VII)** | |
| Ms. Mythili Prakash | 28 January 2015: Model Exam for Plus Two State Board Students  
Chapter conducted Model Exam for plus two state board students for last 15 years to guide them to score good marks at final examination. As part of spreading Institutional Membership to Schools, Ms. Mythili Prakash, an active CSI woman member gave tips to present plus two students to score high marks in Government Examination. She also stressed upon the importance of Institutional Membership for Schools. | [Ms Mythili Prakash delivering tips to students at local school](http://www.csi-india.org/web/guest/csic-chapters-sbs-news) |
SPEAKER(S) | TOPIC AND GIST
---|---
COCHIN (REGION VII) | 30 October 2014: Annual Kerala State Student Convention of CSI, on “Empowering Villages through Emerging ICTs”
The event was inaugurated by Chief Guest Dr. PT Mathew, GM, BBNL and felicitation was given by SP Soman. Panel discussion on the theme was conducted. More than 100 participants registered. Few Contests like ICT Quiz, Poster Designing and Web designing were conducted and winners were awarded cash prizes and certificates. Website address is http://www.amrita.edu/asas/kochi/CSIevents.html

VELLORE (REGION VII) | 15 September to 16 October 2014: Seminar series as a part of Golden Jubilee Celebration

From Student Branches »

(REGION - IV) | (REGION - V )
---|---
SILICON INSTITUTE OF TECHNOLOGY, BHUBANESWAR | HKBK COLLEGE OF ENGINEERING, BENGALURU

23-12-2014: In Student Research Symposium, Dr. Satyananda Champatirai, Dr. Jaideep Talukdar, Dr. Manas Senapati, Dr. Saraju P. Mohanty, Mr. Sanjay Mohapatra | 06-11-2014 : Dr. Mala V Patil, HOD, Dr. T C Marunath, Principal, Mr. Rajesh R Nambiar, EMC Corporation, Mr. Abdul Hameed, Mr. Chandar P Mannar, Chairman, CSI-BC, Mr. H R Mohan, President CSI and Mr. Vishwas Bondade, RSC-CSI during Karnataka State Students Convention.
<table>
<thead>
<tr>
<th>REGION-V</th>
<th>REGION-VI</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMR TECHNICAL CAMPUS, HYDERABAD</td>
<td>K. K. WAGH INSTITUTE OF ENGINEERING EDUCATION RESEARCH, NASHIK</td>
</tr>
<tr>
<td>24-01-2015: Resource Persons Addressing to Participants from various Colleges during the FDP on “Research Methodologies and preparation of research proposals”</td>
<td>26-12-2014: Mr. Prashant, Saurabh, Varad, Shruti and Chaitali during Demo Session on IT Security at CAN Expo 2014</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION-VI</th>
<th>REGION-VII</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. N. J. B’S KBJ COLLEGE OF ENGINEERING, CHANDWAD, NASHIK</td>
<td>VELAMMAL ENGINEERING COLLEGE, CHENNAI</td>
</tr>
<tr>
<td>01-10-2015: Prof. M M Rathore, Prof. M R Sanghavi, SBC, Staff Coordinators for the Inauguration of the Swachata Abhiyaan by CSI Student Members</td>
<td>23-12-2014: Dr. B Rajalakshmi, Dean-IT and CSI-SBC, Mr. Vanlin Sathya, Research scholar, Indian Institute of Technology, Hyderabad, Dr. B Venkatalakshmi, Chief co-ordinator-TIFAC CORE during “Recent trends in mobile communication” seminar</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION-VII</th>
<th>REGION-VII</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA ENGINEERING COLLEGE, AVADI</td>
<td>SCAD COLLEGE OF ENGINEERING AND TECHNOLOGY, CHERANMADEVI</td>
</tr>
<tr>
<td>17-12-14: Dr. S. Suyambazhahan-Principal, Dr. G. Umarani Srikanth HOD-CSE, Prof. V Vaidehi-, MIT &amp; VP Dr. T. Sasilatha during the one week FDP on “Recent Trends in Wireless Sensor Networks”</td>
<td>18-09-2014: International Workshop On Sixth Sense Technology by Mr. Lohit Malik, Ms. Norma Marcia, Speech Therapist, UK is present along with Prof. S Balaji, HOD, Dr. P Venkumar, Principal</td>
</tr>
</tbody>
</table>

**CSI ED EVENT**

**BOSS MOOL WORKSHOP AT COIMBATORE**

KPR Institute of Technology, Coimbatore joined with CSI ED, IITM, CDAC hosted the BOSS MOOL workshop for the benefit of academicians at Coimbatore during 21st and 22nd January, 2015. This is the third BOSS MOOL Workshop conducted by CSI followed at Chennai, Ananthapur. There are extensive opportunities for the students to have their academic project work in this area and teaching faculties are trained to train the students.

21-01-15 : Prof. Janakiraman, IIT Madras inaugurating the BOSS MOOL Workshop. Prof. Nadarajan, Div II chair with Mr. Rajan Joseph, Director CSI ED looking on.

Please send your student branch news to Education Director at director.edu@csi-india.org. News sent to any other email id will not be considered. Please send only 1 photo per event, not more.
## CSI Calendar 2015

### Bipin V Mehta

**Vice President, CSI & Chairman, Conf. Committee**  
Email: bvmehta@aesics.ac.in

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Details &amp; Organizers</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>February 2015 events</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 19-22 Feb 2015 | **Second International Conference on Inter-disciplinary Research in Engineering Management, Pharmacy and Science (ICIREMPS)**  
http://www.rajeshkshukla.com | Prof. V P Saxena  
Chair: iciremps@sirtbhopal.ac.in  
Dr. Surendra K. Jain  
Conference Co-Chair: iciremps@sirtbhopal.ac.in  
Prof. Rajesh Shukla  
Convener Computer Science, Information Technology & Computer Application: rkumardmh@gmail.com |
| 20 Feb 2015   | **First National Conference on Computational Technologies-2015 (NCCT'15)** organised by CSI, Siliguri Chapter, Dept of Computer Science and Application, University of North Bengal and CSI Div-V.  
http://www.nbucsaevents.in | Prof. Ardhendu Mandal  
am.csa.nbu@gmail.com |
| 23-24 Feb 2015 | **5th International Engineering Project Competition & Exhibition** at the Vel Tech University Campus in Avadi, Chennai. Organised by Vel Tech University and supported by CSI & IEEE CS.  
http://veltechuniv.edu.in/VISAI2015/index.html | P Chandra Kumar  
veltech@vsnl.com |
| 26 Feb-6 Mar 2015 | **Annual Symposium on Information Technology Research, Innovation and Entrepreneurship Development award (ITRIED)** | gjagadeesh@vit.ac.in  
kgovinda@vit.ac.in |
| **March 2015 events** |                                                                                          |                                                                                      |
| 11-13 Mar 2015 | **9th INDIACom; 2015 2nd International Conference on “Computing for Sustainable Global Development”** Organized by Bharati Vidyapeeth’s Institute of Computer Applications and Management (BVICAM), New Delhi | Prof. M N Hoda  
conference@bvicam.ac.in,  
indiacom2015@gmail.com |
| 12-13 Mar 2015 | **International Symposium in honour of Dr Ravi Ravindran** at Bangalore. Jointly organised by ORSI, IIMM, IIITB, CSI and RIMSR.  
http://www.ravisymposium.org | Dr. M Mathirajan  
(+919945668905) or  
Mr. Ganesh Kumar  
(+919739011141) |
| 27-28 Mar 2015 | **International Conference on ICT in Healthcare** organized by Sri Aurobindo Institute of Technology, Indore in association with CSI Indore, Udaipur Chapter and CSI Division III and Division IV Communication.  
http://www.csi-udaipur.org/icthc-2015/ | Dr. Durgesh Kumar Mishra  
drdurgeshk mishra@gmail.com  
Prof. AK Nayak  
aknayak@iibm.in  
Prof. Amit Joshi  
amitjoshiudr@gmail.com |
| **April 2015 events** |                                                                                          |                                                                                      |
| 3-4 Apr 2015  | **National Conference on Creativity and Innovations in Technology Development (NCCITD’15)** at Udaipur. Organised by CSI Udaipur Chapter, Division IV, ACM Udaipur Chapter and S S College of Engineering, Udaipur.  
www.csi-udaipur.org | Amit Joshi  
amitjoshiudr@gmail.com  
Dr. Jaydeep Ameta  
jaydeep_ameta@yahoo.com |
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
<th>Organizers</th>
</tr>
</thead>
</table>
| 11-12 Apr 2015 | Two Day National Conference on ICT Applications “CONICTA-2014” at IIIBM Auditorium, Patna, organized by CSI Patna Chapter in association with Div-III and Div-IV of Computer Society of India | Prof. A K Nayak
aknayak@iibm.in
Prof. Durgesh Kumar Mishra
drdurgeshmanishra@gmail.com |
| 24-25 Apr 2015 | ICON’15 “All India Conference On “Sustainable product in Computer Science & Engineering organized by Chhatrapati Shivaji Institute of association with CSI Division IV, CSI Region IV. | Prashant Richhariya
prashantrichhariya@csitdurg.in |
| May 2015 events | International Conference on Emerging Trend in Network and Computer Communication (ETNCC2015) at Department of Computer Science, School of Computing and Informatics Polytechnic of Namibia in Association with Computer Society of India Division IV and SIG-WC http://etncc2015.org/ | Prof. Dharm Singh
dsingh@polytechnic.edu.na |
| 15-17 May 2015 | International Conference on Computer Communication and Control (IC42015) at Medicaps Group of Institutions, Indore in association with CSI Division IV, Indore Chapter and IEEE MP Subsection. | Prashant Richhariya
prashantrichhariya@csitdurg.in |
| Sept 2015 events | International Conference on Computer Communication and Control (IC42015) at Medicaps Group of Institutions, Indore in association with CSI Division IV, Indore Chapter and IEEE MP Subsection. | Prashant Richhariya
prashantrichhariya@csitdurg.in |
| 10-12 Sep 2015 | International Conference on Computer Communication and Control (IC42015) at Medicaps Group of Institutions, Indore in association with CSI Division IV, Indore Chapter and IEEE MP Subsection. | Prashant Richhariya
prashantrichhariya@csitdurg.in |
drycbhatt@hotmail.com
Amit Joshi
amitjoshiudr@gmail.com |
drycbhatt@hotmail.com
Amit Joshi
amitjoshiudr@gmail.com |
| 16-17 Oct 2015 | 6th Edition of the International Conference on Transforming Healthcare with IT to be held at Hotel Lalit Ashok, Bangalore, India. http://transformhealth-it.org/ | Mr. Suresh Kotchatill,
Conference Coordinator,
mail@transformhealth-it.org |
prashantrichhariya@csitdurg.in |
Kind Attention: Prospective Contributors of CSI Communications

Please note that Cover Theme for forthcoming issue of March 2015 is planned as follows:

- **March 2015 – Machine Translation**

Articles may be submitted in the categories such as: Cover Story, Research Front, Technical Trends and Article. Please send your contributions before 20th February 2015. The articles may be long (2500-3000 words maximum) or short (1000-1500 words) and authored in as original text. Plagiarism is strictly prohibited.

Please note that CSI Communications is a magazine for membership at large and not a research journal for publishing full-fledged research papers. Therefore, we expect articles written at the level of general audience of varied member categories. Equations and mathematical expressions within articles are not recommended and, if absolutely necessary, should be minimum. Include a brief biography of four to six lines for each author with high resolution author picture.

Please send your articles in MS-Word and/or PDF format to the CSI Communications Editorial Board via email id csic@csi-india.org.

(Issued on behalf of Editorial Board of CSI Communications)
Computer Society of India (CSI), India’s longest serving premier society of Information Technology and Computer Science professionals, has been rendering yeoman service to IT Education, Research and Industry.

As you are aware, computers and communication technologies have become pervasive and their usage in our daily life continues to increase in several areas including education, entertainment, banking, travel, hospitality, healthcare, and commerce. Our country is well known for providing IT solutions to the entire world. Indian IT industry earns over $120 billion per year representing about 6% of our GDP and employs over 3.5 million people in the areas of IT and IT-enabled services. By 2020, the earnings are expected to be about $300 billion along with increasing employment in all sectors. This tremendous growth, of course, demands continuous learning and updating ones knowledge in computing, IT, Communication and related areas.

CSI has been playing a key role in fostering this growth and in harnessing ICT (Information and Communication Technology) for improving nation’s socioeconomic status and quality of life through its various activities - awareness creation, improving digital literacy, providing updates on advances in ICT, training and educational programs, conferences and seminars. The primary focus for CSI, now in its Golden Jubilee (50th) year has been serving the needs and interest of IT professionals, academics, college students, and the IT industry. Consistent with realizing the enhanced and ambitious vision of “IT for Masses”, CSI has launched an initiative that extends its services to schools through Institutional Membership (IM) to schools. Some schools have already become IMs and enjoying the benefits.

This Institutional Membership scheme is aimed at helping schools in computer education and use. As can be seen from the brochure at [http://goo.gl/aXYd2S](http://goo.gl/aXYd2S) the Institutional Membership provides significant, long lasting benefits of value to the school - its management, teachers and students. Becoming an Institutional Member is easy. The website at [http://goo.gl/zFQTUK](http://goo.gl/zFQTUK) provides the details on how a school can become an Institutional Member.

We look forward to having schools as Institutional Members, joining us in the exciting journey of taking ICT in India to the next levels.

We request our members to promote the IM in CSI among the schools in their area / in which their or their friends or contacts children are studying. Student members, may please promote the IM in CSI among the schools in which their or their friends brothers & sisters are studying.

If the schools have any queries or need assistance to become an IM, they may please contact: Mr. Y. Kathiresan, Senior Manager (Promotions), Computer Society of India, Education Directorate, C.I.T. Campus, IV Cross, Taramani, Chennai - 600113. Phone: 044 - 2254 1102 / 1103; Mobile: 09444896312; email: csipromotions@csi-india.org
Computer Society of India announces CSI Summer Internship for CSI Student volunteers. The scheme will be implemented in 2015 during the months of April, May and June. The internship programme envisages engaging the CSI Student Volunteers in an industrial environment, giving them a chance to glance at the work practices, development, deployment etc.

*Calling Student Volunteers to make use of this opportunity!*

For all details and application forms