On Research Funding in Quantum Information Science and Engineering by NSF/CISE/CCF Emerging Models and Technologies Program Cluster

Pinaki Mazumder
Program Director
Emerging Models and Technologies
Computing and Communications Division
National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22203
April 6, 2008

I. What is Quantum Computing?

Imagine an intelligent life form dwelling several light years away in a Milky Way star staring curiously at a peta-scale IBM Blue Gene machine on the earth and wondering somewhat skeptically whether that infinitesimal object possesses at all any form of intelligence or computational power! Imagine the same machine at that time is spewing out calculations in the battle of the millennium, the Chip v. Champ chess match on the earth while the clueless beholder from the Milky Way star is ignorantly questioning its very intelligence form! Only the Champ (Gary Kasparov), the best of human chess minds, sitting fidgety opposite to the placid Chip (Blue Gene) can quantify and fathom the complex reasoning and lightning computational prowess of the Chip. Now, imagine the distances between objects in the universe have contracted exponentially and the observer in the Milky Way is now standing on the earth, beholding at sub-atomic tiny particles as if they were like the Blue Gene as appeared to the observer from the Milky Way star.

The above thought experiment can unravel the hidden power of quantum computing, where sub-atomic particles like electrons, protons and photons can be manipulated to unlock their collective information processing capability that can outperform even the fastest supercomputers in solving computationally intractable problems such as factoring and discrete log. In his 1957 visionary talk at the annual meeting of the *American Physical Society* at the California Institute of Technology, titled "There is Plenty of Room at the Bottom", the renowned quantum physicist, Richard Feynman had alluded for the first time to the computational power trapped in atomic particles and challenged physicists to build denser computer circuitry, and more powerful microscopes that can observe tinier objects than scanning electron microscopes could do.

II. Evolution of Quantum Computing

Since Feynman's seminal lecture in the late Fifties, sporadic efforts were made until the Eighties by several scientists who developed the foundation of this emerging field of study. In 1973, Alexander Holevo published a paper establishing a relationship between quantum bits and classical binary bits of information, while Charles H. Bennett showed that computation can be done reversibly. In 1975, R. P. Poplavskii published an article which showed that simulating quantum systems on classical computers are

computationally infeasible due to the “superposition principle” used in quantum systems. In 1976, a Polish mathematical physicist Roman Ingarden showed that Shannon’s information theory cannot directly be generalized to the quantum case. However, it is possible to construct a quantum information theory which is a generalization of Shannon's theory.

In 1981, almost two decades after his seminal lecture, Richard Feynman in his talk at the *First Conference on the Physics of Computation*, held at Massachusetts Institute of Technology, rekindled interest in the emerging field by proposing a basic model for a quantum computer that would be capable of simulation of an evolution of a quantum system. Following Bennett’s idea of reversible computing, Tommaso Toffoli introduced the reversible Toffoli gate, which, along with the NOT and XOR gates provides a universal set for quantum computation. In 1985, David Deutsch, at the University of Oxford, described the first universal quantum computer that like its benchmark counterpart in classical computing, the Turing machine, can simulate any other quantum computer with at most a polynomial time overhead.

However, it is not until 1994, when Peter Shor at AT&T Bell Laboratories defined the most important milestone in quantum computing by demonstrating theoretically how quantum computers can break many of the seemingly secure cryptosystems in use today. Following the works of Charles Bennett, Giles Brassard, Artur Ekert and Dan Simon in cryptography and entanglement based secure system, Peter Shor invented a path-breaking quantum algorithm that solved both the factoring problem and the discrete log problem in polynomial time. In 1995, Peter Shor and Andrew Steane simultaneously proposed the first schemes for quantum error correction that showed how quantum computers can be built to perform reliably. In 1996, Lov Grover at Bell Laboratories demonstrated quadratic speedup by developing the quantum database search algorithm. This new application of quantum computer opened the vista of applications of quantum computers for a much wider variety of problems where random, brute-force search algorithms can be accelerated quadratically. Simultaneously, Christopher Monroe and David Wineland at the National Institute of Technology and Standard (NIST) used trapped ions to experimentally realize the first quantum logic gate - the C-NOT gate.

III. Government Funding in Quantum Computing Research

As the quantum algorithm for cryptography was discovered in 1995 showing exponential speed advantages of quantum computers over classical computers, the United States Government funding agencies turned their attention to this emerging transformative field of research by holding workshops on quantum computing at NIST in Gaithersburg, Maryland and at the University of Arizona in Tucson. Then the Army Research Office and the National Security Agency issued the first public call for research proposals in quantum information processing in 1996. Since then numerous federal, state and private funding agencies have spent considerable amount of research dollars to build working quantum computers. Several universities and government laboratories have demonstrated entanglement and superposition principles in solving experimental quantum algorithms over up to 7-qubit quantum computers. The first privately invested

commercial company, D-Wave in Canada claimed that its 28-qubit quantum computer could solve several quantum algorithms.

The National Science Foundation had started funding numerous university research projects on quantum computing (QC) and quantum information processing (QIP) through its three major directorates: CISE, MPS and ENG. Large and medium QC and QIP research projects were funded by NSF along with regular single-investigator type research projects by leveraging the Information Technology Research (ITR) initiative that spanned over 6 years between 1999 and 2005. To further stimulate and sustain funding for QC and QIP research projects, the CISE established a new research program, called Quantum and Biologically Inspired Computing (QuBIC). Then about five years ago, a new program cluster, named Emerging Models and Technologies (EMT) for computing, was created within the CCF Division of CISE Directorate in order to promote a wide gamut of nascent disruptive technologies that can radically transform the ways computers and communication systems will function in the future. Presently, the EMT Program is a major funding source for research projects in quantum information science and engineering (QISE). The research projects being supported under the EMT Program can be broadly divided into the following five categories:

1. Physical Implementation of Quantum Computers
2. Measurements and Sensing of Quantum Information
3. Quantum Algorithms and Complexity
4. Error Correction and Fault-tolerance
5. Algorithms and Device Architectures

IV. Research Accomplishments and Challenges Discussed in 2007 EMT Workshop

On September 10 and 11, 2007, the EMT Program held a workshop on QISE to highlight the accomplishments of on-going EMT research projects in above-mentioned areas of research within the QISE field. The workshop report also makes several recommendations for future research funding to overcome critical challenges before the quantum computing can be transformed into reality to solve intractable and computationally hard problems in real time. The following sections are primarily extracted from the EMT Workshop report, which was distributed to the NSF administrators in February 2008.

1. Physical Implementation of Quantum Computers

The leading candidates for physical implementation of quantum computers consist of the following technologies: 1) Superconductor-based quantum computers, 2) Trapped ion quantum computer, 3) Electrons on helium quantum computers, 4) Nuclear magnetic resonance on molecules in solution"-based, 5) Quantum dot on surface (e.g. the Loss-DiVincenzo quantum computer), 6) Cavity quantum electrodynamics (CQED), 7) Molecular magnet, 8) Fullerene-based ESR quantum computer, 9) Solid state NMR Kane quantum computers, 10) Optic-based quantum computers (Quantum optics), 11)

Topological quantum computer, 12) Spin-based quantum computer, 13) Adiabatic quantum computation, 14) Bose–Einstein condensate-based quantum computer, and 15) Transistor-based quantum computer - string quantum computers with entrainment of positive holes using a electrostatic trap. EMT Program has funded some of the above physical implementations of quantum computer. Besides the EMT Program, the other directorates within NSF and federal agencies including DARPA, NSA, ARO, and NASA have funded quite heavily to build large-scale quantum computers that can demonstrate quantum entanglements over a several quantum bits.

Several types of condensed matter semiconductor qubits were discussed in the EMT workshop. A few types of spin based qubits that were identified as highly promising for implementation of the quantum computers include optically addressed spin qubits, electrically controlled spin qubits in III-V quantum dots, spin qubits in silicon quantum dots**,** hybrid and orbital qubits, excitonic qubits, and non-Abelian topological qubits.

The EMT workshop recognized that "the goal of constructing a quantum computer is useful in that it helps to focus attention and effort on multidisciplinary issues, but answering some of these questions may prove to be as important as the original goal. The devices that are being contemplated and developed are stretching our fundamental understanding of many-body systems, simultaneously involving hyperfine coupling, spin-orbit interactions, as well as electron-phonon, electron-photon, and electron-electron processes. The quantum systems must interact with the macroscopic world for control and measurements, while at the same time this interaction should introduce minimal decoherence for quantum information applications. Understanding these issues and how better to utilize uniquely quantum properties such as entangled states will lead to enhanced quantum sensors, higher resolution lithography, and other applications that are yet to be identified."

2. Measurements and Sensing of Quantum Information

Since quantum computers must interact with the outside world and must have the I/O capability to interface with other technologies, an essential part of quantum computation is quantum measurement. Revolutionary methods are being pursued under the EMT funded projects to make "practical measurements of tiny signals with unprecedented sensitivity at noise levels so low that the measurement precision is limited by the Heisenberg uncertainty principle. This ability to do 'quantum sensing' and quantum limited measurement is of interest both in terms of fundamental science and a variety of practical applications ranging from ultra-sensitive high bandwidth magnetometers and electrometers to single microwave photon detectors".

Recently there has emerged a new approach to quantum measurements. It employs several types of nonlinear micro- and mesoscopic vibrational systems based on Josephson junctions, dc SQUIDs, and nano-resonators. They have extremely small damping, with a Q-factor 10^4-10^5. This type of devices have been successfully used for fast and sensitive measurements of the states of different types of Josephson junction based qubits.

With mechanical resonant frequencies from the kilohertz to gigahertz range, low internal dissipation, and small masses, $10^{-15} – 10^{-17}$ kg, nano-electromechanical systems (NEMS) are poised to enable new types of fundamental measurements at the quantum limit. Their small dimensions make them extremely susceptible to *local* forces, as epitomized in the recent success at IBM Research in detecting a single electron spin using a MEMS resonator. But perhaps of even greater interest is that it is possible to integrate and tightly couple NEMS with a variety of interesting electronic systems that manifest quantum mechanical coherence, such as solid-state qubits.

Emerging efforts are beginning to focus upon coupling NEMS to Cooper-Pair Box (CPB) qubits and to superconducting transmission-line resonators. Nanomechanical resonators will become increasingly useful for fundamental explorations of quantum mechanics, whether as ultra-sensitive probes of quantum and mesoscopic forces, detectors of single quantum systems, as a "bus" in a quantum information device or as a device to allow the study of quantum behavior in an ordinary bit of matter. With NEMS we can explore what it takes to observe the quantum nature of an ordinary system. Our hope and expectation is that experiments with NEMS at the quantum limit will serve to further illuminate the boundary between the microscopic realm, governed by quantum mechanics, and our macroscopic world, governed by classical mechanics.

3. Quantum Algorithms and Complexity

New algorithms continue to be developed, and the insights obtained promise to yield avenues for other problems. An important direction is exploration of novel quantum algorithmic primitives from mathematical first principles or from analogies with physical processes. Recent developments include algorithms based on the quantum adiabatic theorem, a fast quantum algorithm for evaluating two-player games inspired by scattering theory, and algorithms using representations of Temperley Lieb algebras to approximate the Jones polynomial and the partition function of the Potts model. Limits on possible quantum speedup, such as the recent results on the difficulty of solving the subgroup isomorphism problem using quantum algorithms, shed light into the ultimate power of quantum computers. The recent result that the quantum version of satisfiability with Hamiltonian couplings restricted to qudits arranged in a line is as difficult as with a general arrangement has been an enormous surprise to many in the scientific community. There are many theoretical issues that promise to maximize the impact of quantum information devices.

One key area will be to understand and maximize the power of quantum information processing performed with restricted quantum resources. Advances in this area will have great impact in optimizing the usefulness and power of early generations of quantum information processing devices, which inevitably will have limited numbers of qubits. Some specific questions are:

- Quantum cryptography is an example of a useful application that can be done with limited quantum resources. Can the ideas underlying quantum cryptography be used in more general settings?

- What interesting and useful quantum information processing can be done with devices with small numbers of qubits? Do quantum games have interesting applications?

- There are fundamental unsolved problems in communication complexity. Can using classical and quantum correlations together yield new capabilities? It is known that there are some problems for which the quantum communication complexity is exponentially smaller than the classical communication complexity. Is this true for total Boolean functions (Boolean functions that depend on all their arguments)?

- How much systematic understanding can we obtain of when a quantum algorithm can be efficiently simulated classically, or with restricted quantum resources?

The design of cryptographic methods immune to quantum cryptanalysis is an example of a potentially large payoff from increasing our understanding of inherent limits to quantum algorithms. The challenge is to design a cryptosystem that can be implemented efficiently on classical computers, but for which there is credible evidence that even quantum computers will not compromise their security.

An area that promises to have enormous impact on both physics and computer science is applying quantum information viewpoints to physics problems, which yields deeper insight in both subfields. It has been shown that understanding entanglement sheds a great deal of light into the fundamental nature of quantum phase transitions and also provides a method to understand when quantum algorithms can be simulated efficiently by classical computers. Quantum algorithms for interesting mathematical objects also yield new insight into mathematical problems. Some interesting questions in this area are:

- What new insight is gained by applying quantum information viewpoints to physics problems? There has been a great deal of recent progress on identifying which quantum many-body systems can be simulated efficiently using classical computers. Matrix product states have elucidated the fundamental properties of entanglement and of strongly interacting physical systems.

- Examples of extremely fruitful research directions are the relationships between satisfiability problems and spin glasses, many-particle quantum dynamics and localization in disordered systems and systems with controlled nonperiodic potential, and quantum chaos. Studies in these areas are just beginning, and the characterization of strongly interacting physical systems using the tools of quantum information will continue to yield new understanding.

- Simulating physical and biological materials systems promises to be a truly transformative application of quantum computation. Can quantum information processors with limited quantum capability solve interesting materials problems?

- What is the power of quantum computation in solving difficult classical problems such as calculating the partition functions of Potts and Ising spin models, and simulating the Navier-Stokes equations governing hydrodynamics?

- The interpretation of quantum computation using topological quantum field theory and unitary braid group representations has yielded important insights into the evaluation of mathematically important polynomials such as the Jones polynomial; it has been shown that quantum algorithms can be used to evaluate efficiently values of the Jones polynomial, which is important in characterizing knots in mathematics. Could quantum algorithms speed up evaluation of other properties, such as roots of Jones polynomials? Can the relationship between quantum computation and braid groups be exploited further to yield new algorithms characterizing objects of mathematical importance?

An example of a close interconnection between quantum algorithms and physical systems is algorithmic cooling. It can be applied in nuclear magnetic resonance and MRI imaging, where the scanning time may be dramatically decreased by effectively cooling down nuclear spins. It can also help in quantum computing, since it provides a means for preparing qubits in the ground state and, if necessary, bringing them into the register.

4. Error Correction and Fault-tolerance

Another important role of quantum theory is to develop new architectures that enable and facilitate different physical implementations of quantum information processing devices. The impact of this type of research could be truly enormous if one of these novel architectures enables the construction of the first large-scale quantum information processor. Some examples of recent developments in this area are the linear optics quantum computer, the cluster state or one-way quantum computer, and the adiabatic quantum computer. Decoherence-free subspaces and subsystems have also enabled new physical implementations of quantum computation. Some important outstanding questions are:

- In one-way quantum computation, an initial entangled state is prepared and the computational steps are done using single-qubit measurements. It could be important to developing physical quantum processing devices because the architecture obviates the need for fast and reliable two-qubit gates. Does one-way computation enable new physical implementations? What topologies of connections between qubits yield universal one-way computation?

- Adiabatic algorithms, in which computations are performed by slowly changing the Hamiltonian of a system until its ground state configuration encodes the solution to the question of interest, have been proven to be computationally universal and also expand the range of possible device implementations. What computationally interesting questions can the adiabatic algorithm solve efficiently? What are the connections between the behavior of adiabatic algorithms and quantum phase transitions?

- Topological quantum computation uses the broken topological symmetry in certain condensed matter systems to achieve fault-tolerance from the architecture and not from explicit quantum error correction. Can the fractional quantum Hall effect be exploited to build a working topological quantum computer? Are there other systems with broken topological symmetries that could be similarly exploited?

- Can combining novel architectures yield new advantages? For example, it has been claimed that using cluster state ideas in linear optics quantum computing leads to improved feasibility of the hybrid approach. Does this strategy improve the feasibility of the architecture? Can other combinations of approaches improve device feasibility and robustness?

- Are special purpose quantum computers useful for specific problems? For example, physical realizations of spin glasses could be used to for complex optimization problems. What are the connections between spin glass dynamics in experimental quantum and classical systems and the properties of algorithms?

- Coded qubits and decoherence-free subspaces enable universal quantum computation in a system with rotationally-invariant gates, which improves the feasibility of spin-based architectures with Heisenberg interactions and also increases error-resistance. Can related strategies provide further progress for semiconductor device architectures?

5. Algorithms and Device Architectures

There has been steady progress in understanding how to improve the robustness of quantum information processing since Shor demonstrated the feasibility of quantum error correction in 1996. In the last couple of years, fault-tolerance schemes with very high thresholds (decoherence rates that can be tolerated) of 1-5% have been obtained. These decoherence rates are high enough to be realized in practice. Progress in this area has been multi-faceted, because different types of errors prevail in different device implementations, and some strategies for fault-tolerance involve the fundamentals of the device architecture, as described above for the topological quantum computer.

One important area of investigation is to understand fault-tolerance for novel device architectures. The magnitudes of fault-tolerant thresholds for nontraditional computational architectures will be important in determining whether these alternate computational models have significant advantages over gate-based quantum computation. Some specific questions are:

- What is the fault-tolerance threshold of adiabatic quantum computation?
- What are the fault-tolerance properties of non-circuit models of quantum computation, such as the cluster state quantum computation and linear optics quantum computation?

- What are the fault-tolerance properties of the holonomic (geometric) quantum computation model?
- What fault-tolerance properties are needed for operation of moderately large quantum computers that will be used to study physical phenomena and quantum systems of intermediate size?
- How much can combining topological error correction and algorithmic error correction improve the fault-tolerance of quantum computers?
- We know that quantum information can be preserved. What is the general form of preserved information, both quantum and classical? Is there an "information conservation law"?

Another important avenue of investigation in this area is to understand the fundamental physics of the interaction of the quantum information processor and the external environment, which gives rise to many of the errors that need to be corrected. This understanding is vital to obtaining coherence times that are long enough for useful quantum information processing (moreover, recent work on superconducting quantum computing architectures demonstrates that remarkable progress in this area is possible). Some questions of importance in this area are:

- Can error correction and robustness in quantum systems give new insights into how to improve robustness of classical systems, particularly as device sizes become smaller and smaller?
- Much current work on error correction and robustness assumes that the computational device and the environment, or bath, are only slightly correlated at the end of each error correction cycle. Can this assumption be relaxed?

Finally, a potentially important area is the development of novel error-correction strategies with the potential to increase the fault-tolerant threshold. Some questions in this area include:

- It has been shown that entanglement can enhance error correction in the context of quantum communication. Can the ideas underlying entanglement-enhanced error correction be used in other quantum information contexts?
- How much additional error-correcting power is obtained if one uses post-selection in combination with other error correction techniques?
- The theory of quantum error correction has focused on finding solutions for specific error models. Thus existing error correction procedures perform very well at isolated points in the space of errors, but their performance deteriorates rapidly away from these points. Can we find procedures that are robust, in the sense that they perform uniformly well in a large neighborhood of their optimal points? This is important as error correction moves into the real world, where conditions can change unexpectedly and a quantum information processor should be able to perform well in the face of uncertainty.

The open questions listed above are just some examples of exciting research questions that are growing out of recent advances. As physical quantum information

processors are built, implementation-specific theoretical work will facilitate future implementation advances and also enable more efficient use of the quantum information processing power that is available. In addition, we expect surprising advances that will lead to entirely new directions in algorithms. These research directions have the potential to greatly advance our understanding of the power of quantum computation as well as our fundamental understanding of quantum mechanics.

Acknowledgement: Section IV is primarily derived from the final report of EMT Workshop on Quantum Information Science and Engineering that was held at the National Science Foundation on September 10 and 11, 2007 under the sponsorship of the Emerging Models and Technologies program cluster. The panel members who contributed to writing the final report include: D. Awschalom (UCSB), S. Coppersmith (UWM), M. Dykman (MSU; organizer), E. Farhi (MIT), S. Girvin (Yale), B. Golding (MSU), L. Grover (Bell Labs), L. Kauffman (UIUC), A. Korotkov (UCR), D. Lidar (USC), M. Lukin (Harvard), S. Lyon (Princeton), C. Marcus (Harvard), J. Martinis (UCSB), M. Roukes (Caltech), L. Sham (UCSD), V. Smelyanskiy (NASA), D. Steel (U. Michigan), U. Vazirani (UCB), E. Yablonovitch (UCLA).