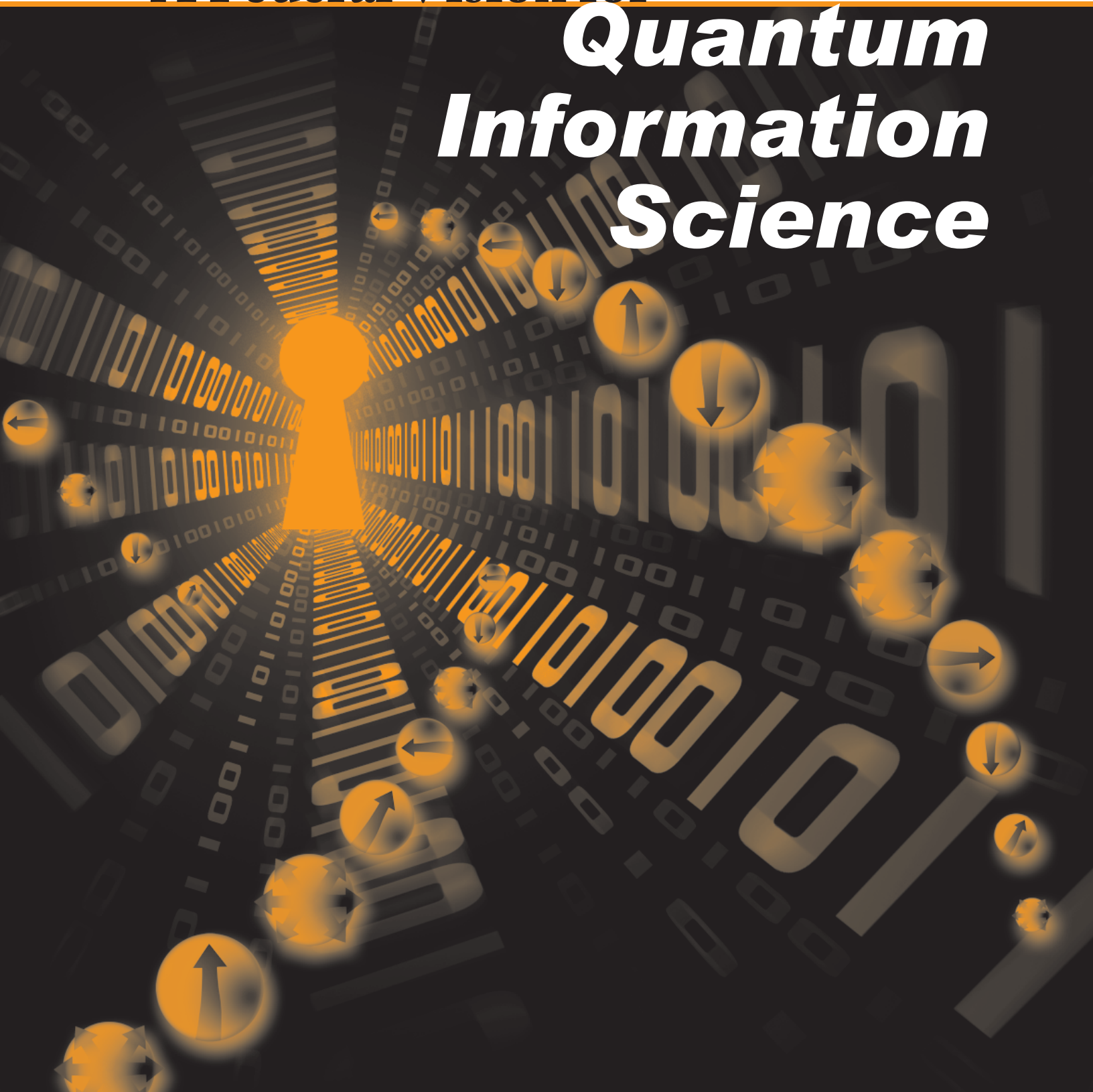




A Federal Vision for ***Quantum Information Science***



ABOUT THE NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This cabinet-level council is the principal means by which the President coordinates science, space, and technology policies across the Federal government. NSTC coordinates diverse paths of the Federal research and development enterprise.

An important objective of the NSTC is the establishment of the clear national goals for Federal service and technology investments in areas ranging from information technologies and health research to improving transportation systems and strengthening fundamental research. The Council prepares research and development strategies that are coordinated across the Federal agencies to form a comprehensive investments package aimed at accomplishing multiple national goals.

For more information visit http://www.ostp.gov/nstc/html/NSTC_Home.html/.

ABOUT THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization and Priorities Act of 1976. OSTP's responsibilities include advising the President in policy formulation and budget development on all questions concerning science and technology (S&T); articulating the President's S&T policies and programs; and fostering strong partnerships among Federal, state and local governments and the scientific communities in industry and academe.

Every fiscal year, OSTP and the Office of Management and Budget (OMB) issue a memorandum entitled "Administration Research and Development Budget Priorities." The memorandum highlights the Administration's research and development priorities and emphasizes improving management and performance to maintain excellence and leadership in science and technology. The FY 2008 memorandum is available at <http://www.ostp.gov/html/budget/2008/m06-17.pdf>.

For more information visit <http://www.ostp.gov>.

This report was prepared under the guidance of the NSTC Subcommittee on Quantum Information Science. The NSTC Subcommittee on Quantum Information Science would like to thank the following individuals who contributed to this report: Ron Boisvert (NIST), Denise Caldwell (NSF), Charles Conover (NSF), Wendy Fuller-Mora (NSF), Evelyn Goldfield (NSF), Susan Hamm (NSF), Daryl Hess (NSF), Sampath Kannan (NSF), Dmitry Maslov (NSF), Charles Pibel (NSF), Barry Schneider (NSF), and Henry Warchall (NSF).

Report Prepared by

The Subcommittee on Quantum Information Science (SQIS)
Committee on Technology (COT)
National Science and Technology Council (NSTC)

December 2008
Washington, D.C.

EXECUTIVE OFFICE OF THE PRESIDENT
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
WASHINGTON, DC 20502

January 5, 2009

Dear Colleague,

I am pleased to forward this document, “A Federal Vision for Quantum Information Science.” It was developed by the Subcommittee on Quantum Information Science (SQIS), an interagency group formed under the National Science and Technology Council to examine and coordinate Federal efforts in quantum information science and related fields. The case for federal action in this new field is so unusual that I am stating it here in concise form so readers will see at the outset why this work is necessary.

Our society is being transformed by an information technology revolution that began with the first electronic computer in the early years of World War II. At the core of this revolution is the concept of a programmable digital computer which turned out to be the foundation for what economists call a disruptive technology, actually a whole family of technologies.

These technologies all have limits inherited from the original model. We know today that some important problems are just too hard to solve with any computer based on the original principles. And these limitations are not easy to overcome because they are embedded in the foundations of logic itself. This fact reassures us that important information applications can be protected by wrapping them within one of the “impossible” problems.

Today we know this reasoning is flawed. Another platform exists that has capabilities beyond conventional logic, and therefore not subject to its limitations. That any actual physical system could behave in an “illogical” way is almost unbelievable, and the early discoverers struggled against ingrained preconceptions that were only surmounted by hard data from many experiments. Scientists have been aware for eight decades that quantum mechanics describes nature in a way that surpasses conventional logic. But it was not until quite recently that practical applications have become apparent. The odd quantum behavior is prominent at atomic scales but fades rapidly away in larger assemblies.

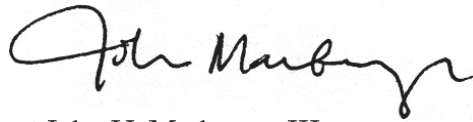
Now we know that devices can be made that allow the non-intuitive quantum logic to reveal itself in practical systems. Some of the physical phenomena involved are familiar and have already been captured in applications: superconductivity, laser light, atomic clocks. It appears that these and similar phenomena can be employed to process information in a way that transcends at least some of the built-in limitations of conventional computing. Some of the “impossible” problems are known to be solvable by a large scale quantum device.

This development has very significant implications. It creates a new conceptual platform for a family of potentially disruptive technologies, adding a new stage to the already staggering impact of conventional information technology. The ability to solve some of the “impossible” problems would enhance discovery and economic strength. But applications that rely on the “impossibility” of certain problems – widespread

in data protection – would be rendered obsolete. The United States' large stake in all these potential applications warrants a cohesive national effort to achieve and maintain leadership in the rapidly emerging field of quantum information science.

Agencies and departments across the Federal Government that perform or sponsor research in quantum information sciences should look to this report as a basis for establishing research priorities and should rely on the Subcommittee on Quantum Information Science as a primary mechanism for identifying research priorities and gaps, sharing results and addressing the challenges that lie ahead. By working together we will maximize the effects of our investments and ensure that the United States continues to lead the world.

Sincerely,

A handwritten signature in black ink, reading "John Marburger". The signature is fluid and cursive, with the first name "John" and last name "Marburger" clearly legible.

John H. Marburger, III

Director, Office of Science and Technology Policy



A Federal Vision for Quantum Information Science

Table of Contents

Background	1
The Call for a Coordinated Approach	1
Prioritizing the Research Challenge	2
Power of a Quantum Computer	4
Fundamental Limits	8
Complex Quantum Systems	11
Conclusion	14

Background

Two of the great scientific and technological revolutions of the 20th century are *quantum mechanics* and *information theory*. *Quantum mechanics* describes nature at or near the atomic scale and is the theoretical basis for the semiconductor microelectronic and photonic technologies that underpin our post-industrial “information economy.” *Information theory* quantifies information content and provides a framework for efficiently communicating and processing information, thereby revolutionizing our world and making vast information resources available to billions of people. Together these two revolutionary 20th century developments have had enormous impact socially, economically and technologically.

New discoveries in the latter part of the 20th century revealed the intimate relationship between these two previously disparate fields and led to their merger under a single unifying viewpoint now known as *Quantum Information Science* (QIS). In the early 1980’s, scientists suggested that a computer based on quantum principles would be able to perform calculations beyond the capabilities of any classical computer. Scientists now know that the physical and technological realization of information is limited by the laws of physics and that information can be characterized, quantified, and processed using the basic rules of quantum mechanics. However, scientists do not fully understand the true capabilities that a general purpose *quantum computer* would have should it be realized.

Quantum Information Science will enable a range of exciting new possibilities including: greatly improved sensors with potential impact for mineral exploration and improved medical imaging and a revolutionary new computational paradigm that will likely lead to the creation of computing devices capable of efficiently solving problems that cannot be solved on a classical computer. The development of a general purpose quantum computer would provide radical new computational methods and powerful new tools to scientists.

The Call for a Coordinated Approach

A number of government agencies and national laboratories have research efforts in QIS, including the National Security Agency, the Intelligence Advanced Research Projects Activity, the Defense Advanced Research Projects Agency, the National Science Foundation, the National Institute of Standards and Technology, the Department of Energy, the Army Research Laboratory, the Air Force Research Laboratory, and the Naval Research Laboratory.

These agencies have distinct missions that will be influenced by QIS and have differing approaches to basic research in this area. Achieving the potential of quantum information science and ensuring US leadership in this revolutionary area will require long-term, focused attention by the Nation for a decade or more. Creating the scientific basis for manipulating, exploiting, and controlling quantum matter and identifying the physical, mathematical, and computational capabilities and limitations of QIS systems will require coordination and prioritization of research activities among these agencies.

To this end, the President's Science Advisor under the auspices of the National Science and Technology Council's Committee on Technology, established the Subcommittee on Quantum Information Science (SQIS) and tasked it with developing a vision for Federal QIS research. The SQIS is a multiagency, multidisciplinary group whose long term goal is to foster research and development, expedite the exploration of the fundamentals of quantum systems and the discovery of potential applications, foster the conditions that will advance the state of the science, ensure an expert workforce and sustain US competitiveness in QIS.

A Federal Vision for Quantum Information Science

The United States will create a scientific foundation for controlling, manipulating, and exploiting the behavior of quantum matter and identifying the physical, mathematical, and computational capabilities and limitations of quantum information processing systems in order to build a knowledge base for this 21st century technology. To succeed the US must identify the critical scientific elements and target them as research priorities, train a new generation of scientists in the underlying disciplines that contribute to QIS, and share results and coordinate efforts.

Prioritizing the Research Challenge

QIS is fundamentally restructuring our approach to quantum mechanics and teaching us how to examine quantum systems in an entirely new way. QIS is also providing a more transparent perspective into some of the *counter-intuitive aspects* of quantum physics that will be essential in advancing 21st century technology. The scope of the scientific challenge that must be addressed if we are to fully exploit the potential possibilities that QIS provides for 21st century technology is encompassed in the following three fundamental questions.

- What is the true power of a general purpose quantum computer, what problems does it allow us to compute efficiently, and what does it teach us about nature?
- Are there fundamental limits to our ability to control and manipulate quantum systems, and what constraints do they place on technology and QIS?

- Are there exotic new states of matter that emerge from collective quantum systems, what are they useful for, how robust are they to environmental interactions, and do these collective quantum phenomena limit the complexity of the quantum computing devices we can build?

This set of questions provides a guideline for agencies as they develop their research programs. Their answers will help us discover the limits that quantum mechanics imposes on our world and understand the range of possibilities that are allowed, including the role of quantum mechanics in nature. Federal research activities should be focused in technical and scientific areas that have the greatest chance of helping answer these three fundamental questions. Mathematical models of quantum systems must be developed concurrently so that discoveries in the physical domain can be fully exploited. Answering these questions will advance the field and reveal other questions that need to be answered in turn.



Unlocking the secrets of the quantum realm, where qubits can be simultaneous 0 and 1, may allow us to perform calculations that are impossible on a classical computer and to create technologies that have yet to be imagined.

Pursuing this course will involve exploring some of the most fundamental questions of physics, including the limits of quantum mechanics and how well individual quantum particles and states, including macroscopic quantum states, can be detected and manipulated. Classical information processing is built on the concept of a bit that like a light switch has two possible states – on and off or “0” and “1”. The bits of a classical computer obey classical mechanics and classical *everyday* logic. QIS is largely based on the concept of a two level or two state quantum system, referred to as a *quantum bit or qubit*. Unlike a bit in a classical computer, the qubit can be both “0” and “1” simultaneously – an “illogical” but thoroughly verified concept. If QIS and qubits are to lead to a 21st century technological revolution as much as classical information and classical bits did to

the 20th century, it is essential to fully understand the possibilities and limitations that arise from quantum mechanics and QIS.

The ways we teach and understand quantum mechanics are currently undergoing radical changes and now mathematicians, computer scientists, and engineers are being exposed to aspects of quantum mechanics once thought to be esoteric. Within the physics community

Atomic, Molecular, and Optical physicists are now engaging with their Condensed Matter colleagues as these two subfields of physics begin to coalesce after a half-century of divergence. New breakthroughs are occurring at an accelerating pace. There is now very strong evidence that a quantum computer could revolutionize quantum chemistry, which could have a dramatic impact on drug design and the development of exotic materials with applications from sensing to highly efficient solar cells.

QIS promises to have important implications not only for national security but also for future economic competitiveness in areas ranging from wholly new and innovative technologies to improvements in the global positioning system and to everyday concerns like health care. The remainder of this document expands upon the three scoping questions and provides a framework for establishing research priorities in this area.

Power of a Quantum Computer

What is the true power of a general purpose quantum computer, what problems does it allow us to compute efficiently, and what does it teach us about nature?

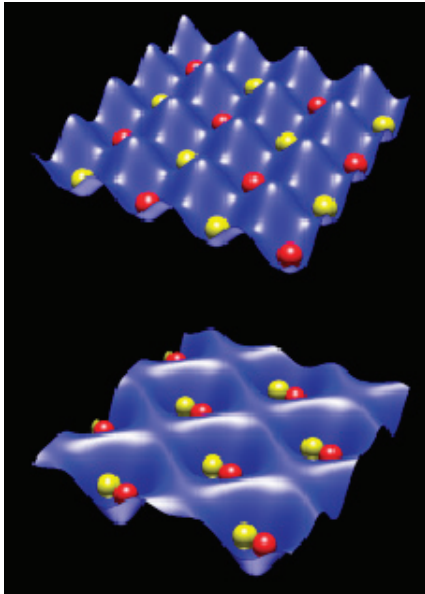
“... and if you want to make a simulation of Nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem, because it doesn’t look so easy.”
— Richard P. Feynman, “Simulating Physics with Computers”, May 1981

The important ideas of what is computable or equivalently, what problems are solvable on a computer, were laid down by two distinguished mathematicians, Alonzo Church and Alan Turing in the 1930s, well before the first electronic computer was built in 1943. Church defined computability in two ways using two different mathematical formalisms – general recursion and the λ -calculus. Turing described a very simple mechanical computing device, now called the Turing Machine, and defined a solution to a problem to be computable only if it could be computed by his machine. These two approaches were ultimately shown to be equivalent and thus led to the Church-Turing principle, which posits that any effectively computable function is also computable on a Turing Machine.

In all known models of quantum computing, the quantum computable functions can still be computed by a Turing Machine¹. What then is the point of building quantum devices and exploring their computing power?

¹ The one exception is the problem of generating a random number, which is not really a problem of computing a mathematical function. Quantum computers can do this while the basic Turing Machine, being purely deterministic, cannot.

To answer this question we need to consider the *efficiency* of computation on different types of computers. Computer scientists define the efficiency of a computation in terms of the number of steps required to obtain the solution. A problem has an efficient solution if it has an algorithm which takes a number of steps that is at most a *polynomial function* (P class – standing for “solvable by a Polynomial-time algorithm on the Turing Machine”) of the input size. For example, finding the product of two n -bit integer numbers is easily solvable in at most n^2 steps using long multiplication (although faster algorithms exist). As such, integer multiplication is very efficient, which is a good thing given how frequently the multiplication operation is used in computations.



Quantum logic requires controlled, pair wise interaction between atoms. The requirements for such control can be studied with dynamically configurable optical lattices.

Here, initially isolated individual atoms are merged in pairs into the same sites, where they can interact and become “entangled”.

Some computational problems, many that arise in practical applications, have no known polynomial time solutions. Some examples include: determining if two given chemical molecules are isomers, finding the 3-dimensional folded configuration of a protein molecule, determining low-energy configurations of lattice structures of fundamental particles or atoms, integer factorization, or deciding whether there is a plan for achieving a desired objective under a given set of constraints. All of these problems share an interesting feature: while a polynomial time solution is not known, one can *verify* that a given solution is indeed correct with a polynomial time procedure. As a simple example, no polynomial time solution has been discovered for factoring an arbitrary integer N into its constituent factors p and q (say); however given the solution consisting of the numbers p and q , verifying that this solution is correct reduces to simple multiplication and comparison of the result to the number N . The latter task is accomplished trivially. Problems whose solution is easy to verify but hard to find are said to belong to NP (class of Non-deterministic Polynomial time problems).

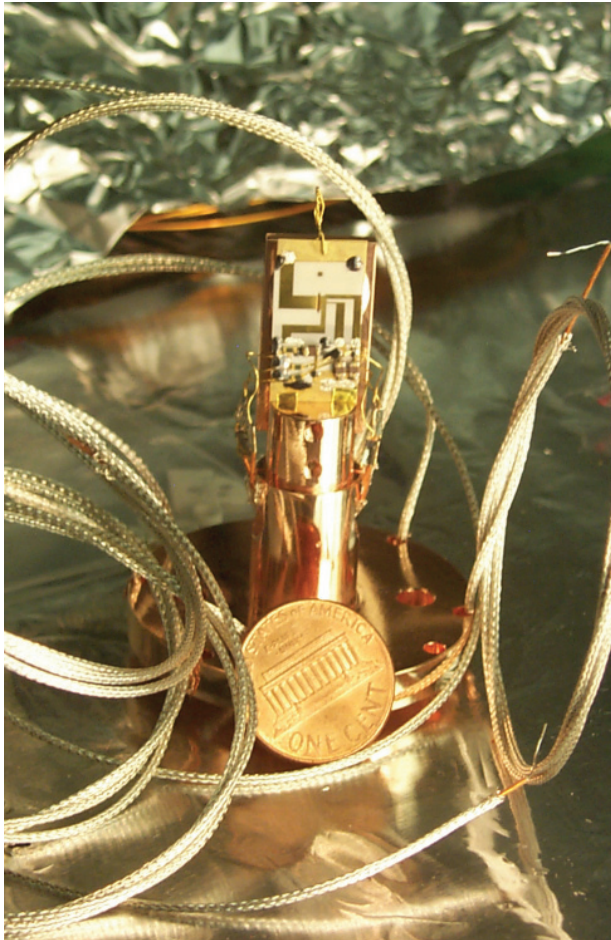
The question of whether P and NP are identical sets is one of the most important unsolved problems in mathematics. It is arguably also the problem with the greatest practical importance. If it is proved that $P=NP$, then most forms of cryptography would become obsolete, we would have near perfect learning algorithms and predictions of weather, and we would be able to automate the discovery process. Because these implications are difficult to imagine being possible, it is generally accepted that NP probably does contain some problems that are not in the set P.

The original Church-Turing Thesis was later extended to make an even bolder claim. The Extended Church-Turing thesis states that any problem that is *efficiently* solvable on any computer is also *efficiently* solvable on a Probabilistic Turing Machine, *i.e.*, a Turing Machine equipped with the ability to toss coins and use the results of these coin tosses as random inputs to its computation. On the surface this claim sounds preposterous; nevertheless, it has been proved that the Extended Church-Turing thesis holds for all computers based on *classical* (Newtonian) *physics* and even for radically different computers that are envisioned based on nanotechnology and/or inspired by biology. The one intriguing exception is the quantum computer, a computing paradigm based on employing the laws of *quantum mechanics* to perform a computation. Although probably difficult to prove, there are good reasons for conjecturing that there are problems that are intractable for the Turing Machine but are efficiently computable using a quantum computer. This is the conjecture first suggested by Richard Feynman in a 1981 speech where he observed that building a computer based on *quantum mechanics* should allow for the efficient simulation of quantum systems – something that could not be done efficiently on a classical computer. Feynman made this conjecture while noting that nature is not classical.

How can we even talk about what is efficiently computable on a quantum computer when we don't yet know for certain how to build a quantum computer? Just as with the Turing machine, the theoretical construct that predated the construction of a physical, general-purpose computer, scientists have already developed an abstract, mathematical model of how quantum computation works. There are in fact several quantum computing models and a number of competing technologies proposed for their realization. However, it has already been proved that no matter which one of them is ultimately realized, the resulting computer will be correctly described by a model that is equivalent to any of the standard theoretical models of quantum computation. So far, history repeats itself but this *new, as yet non-existent, quantum computer* appears to be *exponentially more efficient* for a special class of problems.

Although there is no proof that the problem of factoring an integer is hard (this would imply $P \neq NP$), centuries of attempts to find an efficient algorithm to solve it have failed. As a result, public key cryptography based on the difficulty of efficient factoring has become the standard cryptographic protocol protecting much of our information infrastructure.

However, in 1994 Peter Shor showed that factoring can be done efficiently on a quantum computer if one could be built. This discovery sparked significant interest in quantum algorithms in general and specifically in generalizations of Shor's algorithm.



NIST researchers trapped aluminum and beryllium ions in the device above in experiments designed to produce an atomic clock that could be significantly more precise than today's most accurate atomic clocks.

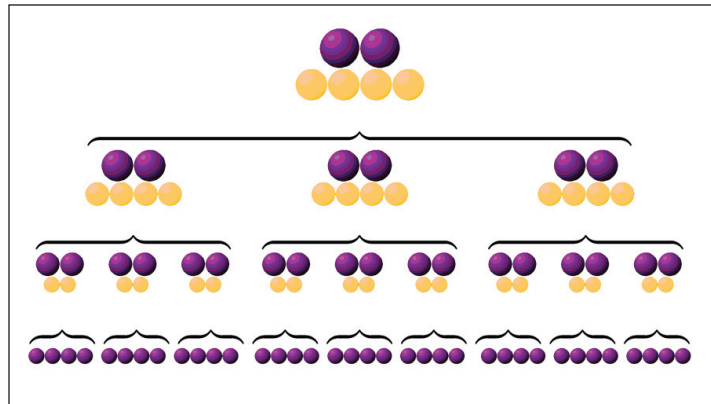
Complete miniaturization of the device and the uses of more exotic quantum states could one day lead to improved GPS devices.

An important group of problems is the ability to simulate quantum mechanical systems on a quantum computer, a problem that appears to be intractable for classical computers. This would result in accurate predictions of chemical properties, and thus assist in the design of better materials. Quantum “noon” states may be used in atomic clocks to dramatically increase their precision, and as a result improve the accuracy of GPS devices. Quantum algorithms are available for communication purposes allowing parties to exchange significantly fewer bits to solve such basic problems as set disjointness and equality with communication to a referee. Learning from the history of classical computation, we are perhaps not yet in a good position to judge which of the emerging applications will have maximal impact.

To summarize, the fundamental questions to be answered in understanding the power of quantum computation include:

- What is the class of problems that are efficiently solvable on a quantum computer but not on a classical computer?
- What problems remain intractable even for quantum computers?
- Which currently tractable problems can be sped up further using quantum algorithms?

- Quantum computations are inherently prone to errors due to imperfect isolation of quantum mechanical systems from the environment. What error correction schemes can be developed to allow quantum computation to be done free of errors? (Good ideas to address this problem are already being developed.)



Architecture for quantum computing relies on several levels of error checking to ensure the accuracy of quantum bits (qubits). The image illustrates how qubits are grouped in blocks to form the levels. To implement the architecture with three levels, a series of operations is performed on 36 qubits (bottom row) each one representing either a 1, a 0, or both at once. The operations on the nine sets of qubits produce two reliably accurate qubits (top row). The purple spheres represent qubits that are either used in error detection or in actual computations. The yellow spheres are qubits that are measured to detect or correct errors but are not used in final computations.

Fundamental Limits

Are there fundamental limits to our ability to control and manipulate quantum systems, and, if so, what constraints do they place on technology and QIS?

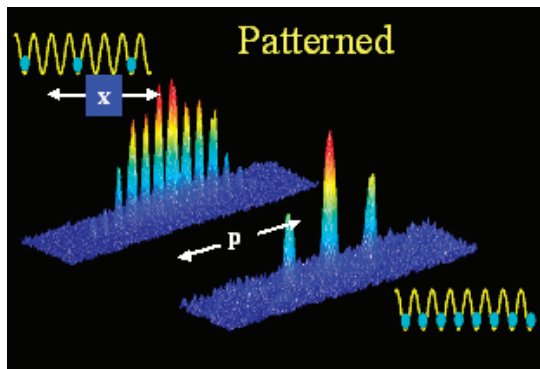
“When we get to the very, very small world—say circuits of seven atoms—we have a lot of new things that would happen that represent completely new opportunities for design. We can manufacture in different ways. We can use, not just circuits, but some system involving the quantized energy levels, or the interactions of quantized spins, etc.” — Richard P. Feynman, “Plenty of Room at the Bottom”, December 1959

At the heart of classical information processing is the principle that its implementation can be made very reliable and robust, almost totally immune from noise. However, achieving a robust QIS system that is immune from noise is a bigger challenge. Quantum information is fragile; even weak interactions with the environment can destroy it. If physical realizations of quantum systems are ever to be a reality, then questions about the sources of *decoherence*, the weak interactions that destroy quantum information and the main impediment to exploiting quantum phenomena, must be answered:

- What are these weak interactions?
- Do mechanisms exist for either eliminating or controlling these interactions?

- Are there fundamental limits on the control and read-out of quantum information in quantum systems that are also interacting with an environment?
- How can the tendency toward decoherence that destroys quantum information be suppressed?
- What constructs, such as decoherence-free subspaces and topological methods, can be employed to manage or avoid decoherence?

Exploration of multiple approaches to physical systems that can robustly process quantum information while employing “fragile” quantum states is a key issue in the goal of assembling real, complex, interacting quantum systems together in robust, fault-tolerant ways. While individual atoms or ions may constitute the best qubits for memory, electron or nuclear spins in semiconductors may be more easily manufactured and provide better qubits for processing, and photons may be better suited for communications – especially over longer distances. However, to take advantage of these various strengths we must develop the means to interconvert between various types of qubits. Finally, what are the advantages and disadvantages that emerge as we move from isolated quantum systems to integrated quantum systems?



Atoms can be uniquely positioned in an optical lattice. The two patterns shown in the middle of the figure are the resulting interference pattern for atoms released from an optical trap. The interference pattern at the top occurs when every third site of the lattice is filled as shown in the small inset at the top while the lower interference pattern occurs when every site of the lattice is filled as shown in the small inset at the very bottom.

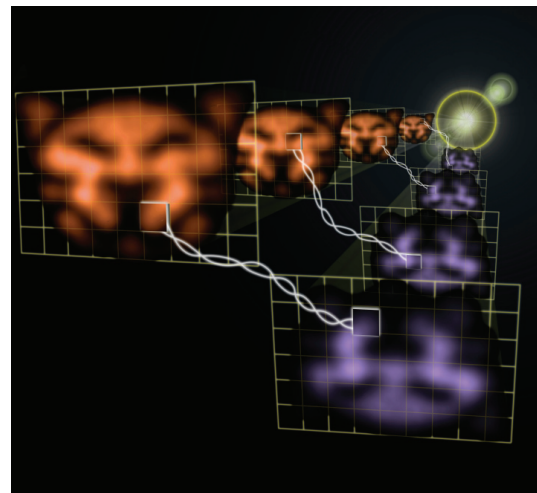
Unlike traditional experiments, which are carried out on ensembles of many objects (e.g. large collections of atoms or molecules), the technology underlying quantum information processors requires manipulation and measurement at the level of individual quantum objects. Only in recent years has it become possible to interact with and control the state behavior of an individual quantum object in the presence of the surrounding environment, and the number of systems in which this has been successfully implemented is limited. Making measurements on individual quantum systems requires both sensitive detection and a more general framework and deeper understanding of quantum processes. The tools and theoretical constructs required to control and interrogate quantum systems with exquisite precision need to be developed and employed in challenging

experiments involving many independent quantum systems that cannot be simultaneously disturbed. These challenges require the development of new measurement tools and test the limits of measurement science, requiring extreme sensitivity and precision.

QIS depends intimately on *entanglement*, the striking feature of quantum mechanics that leads to strong correlations between the various components of a physical system, regardless of the distance separating them. Information processing that exploits this entanglement gives rise to a *quantum parallelism* that has no analog in classical information processing. While entanglement is a well established feature of quantum systems, measurements and understanding of entanglement have largely been limited to systems of two quantum objects. Entanglement in meaningful quantum processors will need to be spread among many objects, where even theoretical constructs for understanding entanglement are only beginning to be understood.

- Are there fundamental limits to how large an entangled system can become?
- How can we best quantify “multi-partite” entanglement?
- How does one characterize a highly entangled state or at least confirm that it is the state one intended to create?
- What is the power of distributed entanglement and what unique capabilities does this provide?

Two of the great theoretical constructs of the 20th century, quantum mechanics and the general theory of relativity, appear to be mutually exclusive. Even though quantum mechanics as a tool has been extraordinarily successful in providing a description of the behavior of physical systems of very small sizes, the question still remains whether quantum mechanics as we now know it is a correct and complete description of the physics of the universe. Is it true that quantum theory describes all attainable information about a physical system? Measurements on individual quantum systems make it



In this photo montage of actual quantum images, two laser beams coming from the bright glare in the distance transmit images of a cat-like face at two slightly different frequencies (represented by the orange and the purple colors). The twisted lines indicate that the seemingly random changes or fluctuations that occur over time in any part of the orange image are strongly interconnected or “entangled” with the fluctuations of the corresponding part in the purple image. Though false color has been added to the cats’ faces, they are otherwise actual images obtained in the experiment. Credit for montage: Vincent Boyer/JQI

feasible to ask this question, pushing into a frontier that was closed only a decade or so ago. Investigators are exploring how big an object can be and still demonstrate quantum behavior. Is there a smooth transition between quantum and classical behavior? Others are performing ultra-sophisticated precision measurements on systems that test the fabric of space and time, such as searching for the electric dipole moment of the electron or the time variation of the fine structure constant. Understanding the fundamental limits of quantum mechanics will tell us what we can accomplish in QIS.

Complex Quantum Systems

Are there new states of matter that emerge from collective quantum systems, what are they useful for, how robust are they to environmental interactions, and do these collective quantum phenomena limit the complexity of the quantum computing devices we can build?

“The workings of our minds and bodies, and of all animate and inanimate matter of which we have any detailed knowledge, are assumed to be controlled by the same set of fundamental laws, which except under certain extreme conditions we feel we know pretty well... that the state of a really big system does not at all have to have the symmetry of the laws which govern it ... But sometimes, as in the case of superconductivity, the new symmetry – now called broken symmetry because the original symmetry is no longer evident – may be of an entirely unexpected kind and extremely hard to visualize.” — P. W. Anderson, “More Is Different”, *Science* 177, 393 1972

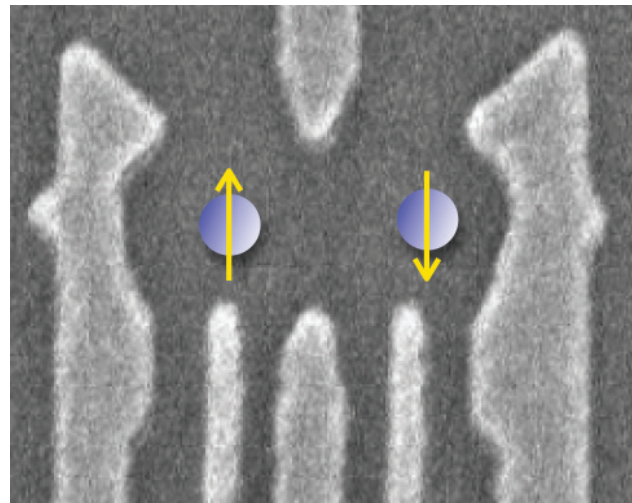
There is a fundamental connection between QIS and the study of quantum systems composed of many particles. By their nature, quantum many-body systems contain many degrees of freedom and can give rise to new symmetries that are not evident in the individual atoms or components from which they are built. The interactions among these degrees of freedom lead to entangled quantum mechanical states and finally to emergent states that have unexpected properties that cannot be foreseen from the properties of the individual atoms. The best known example of such emergent states is that associated with superconductivity. Some emergent states exhibit quantum mechanical properties that persist to macroscopic length scales that are significantly larger than the original microscopic or atomic length scales. Understanding emergent states of matter, their unusual properties, and how to control them on both microscopic scales and macroscopic scales provides an essential connection to QIS and the physical realization of a quantum computer. Any realization of a quantum computer will connect to the macroscopic world in ways both desirable and undesirable. The quantum properties of some emergent states of matter

appear to be protected, that is, they are robust quantum mechanical states with some immunity from decoherence. The levels of immunity vary from that present in superconducting qubits to the believed robustness of some topological qubits that may give rise to nearly error free quantum computers.

Entanglement in a many-body system appears to play a key role in the emergence of new states of matter and in exotic behavior such as quantum phase transitions. Controlled entanglement of many qubits also appears essential to physically realizing a quantum computation.

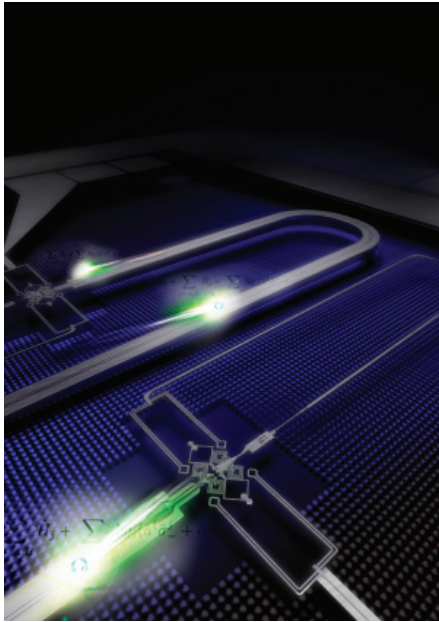
- Do the phenomena and quantum states of matter that arise in quantum many-body systems, such as quantum phase transitions, occur as the number of qubits is scaled up in a quantum computer?
- How does this behavior affect the operation of the computer?
- Can this behavior be exploited or should it be avoided?
- Can the methods to understand entanglement developed by QIS scientists be adapted to understand entanglement in quantum many-body systems?
- Is this a fruitful way to think about or understand how new states of matter emerge from systems described by simple mathematical models used by Condensed Matter physicists?

Fractional quantum Hall states, topological insulators, and superconducting states are among the emergent states of matter from which candidates for quantum computation have been proposed. The notion of topological symmetry at low energy links many of these states and leads to intriguing properties that form the basis for their suggested application in quantum computing. Topological states promise to have the property of being resistant to random events in the environment that lead to decoherence and therefore may enable long-



A double quantum dot fabricated with metal gates on top of a gallium arsenide semiconductor heterostructure. Individual electrons, illustrated as blue circles, each carrying quantized angular momentum, or spin, can be held indefinitely, coupled, and measured by applying electrical pulses on the confining gates. The up-down orientation of the spin arrows represents spins prepared in an entangled singlet configuration before separation. Device fabricated by J. R. Petta, micrograph courtesy of C. M. Marcus/ Harvard University

lived quantum mechanical states that can be manipulated for robust quantum processing. Developing decisive experiments that can confirm or rule out the unusual theoretical predicted properties of the fractional quantum Hall states is an exciting and intellectually stimulating endeavor with potentially tremendous implications.



Artist's rendition of the NIST superconducting quantum computing wire used to couple two superconducting Josephson phase qubits. The superconducting quantum wire allows the two qubits to interact and become entangled.
Illustration by: Michael Kemper

Superconducting states may play an important role as well. Superconductivity can be thought of as a macroscopic quantum state. Using charge and magnetic fields, superconducting qubits may be entangled and manipulated for computation purposes. These systems offer another potential route to the physical realization of a quantum computer that is being pursued in the community. Other routes to using superconductivity for quantum processors appear possible using topological insulators that appear to share many of the advantages of fractional quantum Hall states. Finally, superconductivity provides an example of perhaps the most direct way that an emergent state of matter may influence the evolution of QIS as a practical endeavor. Research to discover new superconducting materials with more advantageous properties, such as higher temperatures and longer coherence times may enable more practical quantum devices that are more robust for general applications.

Advanced theoretical techniques require approximations to make progress in understanding the possibilities in quantum many-body systems. Looking to classical computation for guidance and validation has met with only limited success, because the

simulations of these quantum systems grow exponentially with system size. As a result, the problems quickly become intractable on classical computers for all but the smallest systems. The development of an *analog quantum simulator* holds the promise of being able to *efficiently emulate* these systems. The idea of an analog quantum simulator is in a nascent stage but has the potential of exploring some of these exotic emergent states of quantum many-body systems. The development of a quantum simulator and its applications to these systems could have profound influence on problems critical to fundamental physics, QIS, and the design of new materials potentially useful in commercial applications, including energy systems.

Exploring problems like high temperature superconductivity and other quantum many-body systems on an analog quantum simulator could potentially lead to new states of matter that arise through *quantum phase transitions*. Such quantum phase transitions can separate emergent states of matter and may provide a useful paradigm to understand surprising phenomena such as the emergence of fractionally charged electrons in the quantum Hall effect. Does the notion of entanglement provide a fruitful way to think about this problem? How does one measure entanglement in a system containing upwards of 10^{19} particles? How does entanglement change as we cross a quantum phase transition and a new state of matter appears as another vanishes? The methods of QIS may contribute productive ways to understand how unexpected quantum states with amazing properties and unexpected symmetries emerge from deceptively ordinary models.

Conclusion

The impact of QIS is not yet known, nor is the schedule on which working systems might be available. The potential is enormous, since all technology is constrained by the laws of physics. In the 19th century, our technology was constrained by thermodynamics and classical mechanics; in the 20th century quantum mechanics shattered these constraints, ushering in the age of lasers, transistors, computers and information technology. However, our 20th century technology was too crude to exploit the full potential of quantum mechanics, and was constrained by semiclassical approximations. Now it appears plausible that in the 21st century the stranger properties of quantum mechanics may allow a host of new possibilities based on QIS. Because QIS is a basic research thrust it is much broader in scope than the earlier breakthroughs of the transistor or the laser. Yet the astonishing impact of these two technologies proved impossible to predict. QIS phenomena are at an early pre-application stage, but possess a novelty and a richness that suggests the likelihood of even greater unanticipated impact.

Quantum Information Science is an emerging research area that will require sustained, focused attention if the US is to maintain its position as global leader. Agencies that fund basic research in the physical sciences or that have significant mission-related equities must work together to ensure that all promising avenues are addressed, that priorities are set and that the results of scientific breakthroughs are properly shared. Departments and agencies will require adaptive structures that allow scientific breakthroughs to move effectively from research institutions to experimental applications. In accomplishing this, we must train the future scientists who will be active in creating this new field and ensuring US competitiveness.

