



Quantum Computing

James D. Franson and Bryan C. Jacobs

Quantum computers will utilize nonclassical logic operations to perform numerical calculations that are not feasible on conventional computers. The enhanced capabilities of quantum computers result partly from their expected ability to perform many different calculations simultaneously on a single processor. The Applied Physics Laboratory is developing an optical approach to quantum computing. (Keywords: Computers, Optics, Phase, Quantum.)

INTRODUCTION

Many kinds of numerical problems cannot be solved using conventional computers because of the time required to complete the computation. For example, the computer time required to factor an integer containing N digits is believed to increase exponentially with N . It has been estimated that the time required to factor a 150-digit number using the fastest supercomputers currently available would be longer than the age of the universe. Future increases in the speed of conventional computers will clearly be inadequate for problems of that kind, which are often of considerable practical importance. For example, the difficulty in factoring large numbers forms the basis for the most commonly used methods of cryptography.

It was recently shown¹ that quantum-mechanical computers²⁻⁷ could use nonclassical logic operations to provide efficient solutions to certain problems of that kind, including the factoring of large numbers. As an example of a nonclassical logic function, consider the conventional NOT operation, which simply flips a single bit from 0 to 1 or from 1 to 0. In addition to the usual NOT, a quantum computer could also implement

a new type of logic operation known as the square root of NOT. When this operation is applied twice (squared), it produces the usual NOT, but if it is applied only once, it gives a logic operation with no classical interpretation.

In addition to performing nonclassical logic operations, quantum computers will be able to perform a large number of different calculations simultaneously on a single processor, which is clearly not possible for a conventional computer. This quantum parallelism is responsible for much of the increased performance of a quantum computer.

The operation of individual quantum logic gates has been demonstrated recently, but no operational quantum computer has been constructed. The feasibility of an optical approach to quantum computing is currently being investigated at APL. The eventual goal is to produce large numbers of quantum logic gates on a single substrate, in analogy with current semiconductor technology, which would allow the development of quantum computers for practical applications.

QUANTUM BITS AND PARALLEL PROCESSING

Quantum computers will use a binary representation of numbers, just as conventional computers do. An individual quantum bit, often called a qubit, will be physically represented by the state of a quantum system. For example, the ground state of an atom could be taken to represent the value 0, while an excited state of the same atom could represent the value 1. In our optical approach to quantum computing, a 0 is represented by a single photon in a given path. The same photon in a different path represents a 1.

Although classical bits always have a well-defined value, qubits often have some probability of being in either of the two states representing 0 and 1. It is customary to represent the general state of a quantum system by $|\Psi\rangle$, and we will let $|0\rangle$ and $|1\rangle$ represent the states corresponding to the values 0 and 1, respectively. Quantum mechanics allows superpositions of these two states, given by

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

where α and β are complex numbers. The probability of finding the system in the state $|0\rangle$ is equal to $|\alpha|^2$; the probability of the state $|1\rangle$ is $|\beta|^2$.⁸

Quantum-mechanical superpositions of this kind are fundamentally different from classical probabilities in that the system cannot be considered to be in only one of the states at any given time. For example, consider a single photon passing through an interferometer, as illustrated in Fig. 1, with phase shifts ϕ_1 and ϕ_2 inserted in the two paths. A beam splitter gives a 50% probability that the photon will travel in the upper or the

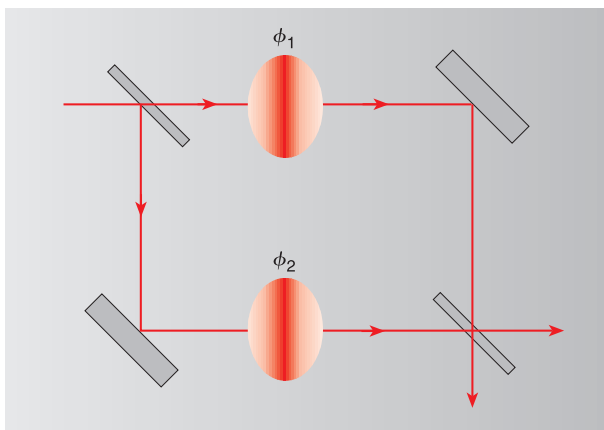


Figure 1. A single photon passing through an interferometer. Such a photon can simultaneously measure the phase shifts in both paths, even though it will always be found in only one path.

lower path. If a measurement is made to determine where the photon is located, it will be found in only one of the two paths. But if no such measurement is made, a single photon can somehow measure both phase shifts ϕ_1 and ϕ_2 simultaneously, since the observed interference pattern depends on the difference of the two phases. This suggests that in some sense a photon must be located in both paths simultaneously if no measurement is made to determine its position. In a more complicated interferometer with many paths, a single photon can simultaneously measure a linear combination of the phase shifts in all of the paths even though it can be detected in only one of the paths. A more detailed discussion of nonclassical effects of this kind can be found in an earlier *Technical Digest* article.⁹

The ability of a quantum computer to perform more than one calculation at the same time is analogous to the properties of the single-photon interferometer just described. A quantum computer can provide results that depend on having performed a large number of calculations, even though a measurement to determine exactly what the computer was doing would show that it was programmed to perform only one specific calculation. To illustrate this, consider a computer programmed to perform a specific calculation based on the value of N input bits, and assume that the result can be described by N output bits, as illustrated in Fig. 2. There are 2^N different combinations of input bits, each of which corresponds to a specific input state denoted by $|\text{input}_j\rangle$, where j takes on all the values from 1 to 2^N . The equal number of specific combinations of output bits is denoted by $|\text{output}_k\rangle$. Each input state can produce a superposition of possible output states,

$$|\text{input}_j\rangle \rightarrow \sum_{k=1}^{2^N} \beta_{jk} |\text{output}_k\rangle, \quad (2)$$

where the complex coefficients β_{jk} describe the calculation performed. In addition, the input state can be a superposition of all of the possible inputs to the computer:

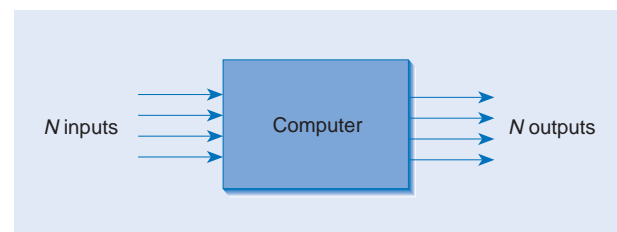


Figure 2. A general-purpose quantum computer with N input bits and N output bits. Superpositions of different input and output states allow the computer to effectively perform many different calculations simultaneously.

$$|input\rangle = \sum_{j=1}^{2^N} \alpha_j |input_j\rangle. \tag{3}$$

In that case, the linearity of quantum mechanics gives an output state of the form

$$|output\rangle = \sum_{j=1}^{2^N} \alpha_j \sum_{k=1}^{2^N} \beta_{jk} |output_k\rangle. \tag{4}$$

The probability P_k of getting a specific output state k is then given by the square of its coefficient in Eq. 4:⁸

$$P_k = \left| \sum_{j=1}^{2^N} \alpha_j \beta_{jk} \right|^2. \tag{5}$$

It can be seen that the probability of getting a particular output depends on all of the coefficients β_{jk} , which represent the results of all possible calculations on the computer. The result also depends on interference between all of the possible inputs, in the sense that P_k will be large if all of the input states contribute in phase with each other. Conversely, P_k will be small if the contributions from all of the initial states cancel out. The goal of quantum computing is to program the computer in such a way that the desired result occurs with high probability while all incorrect results occur with negligible probability.

To illustrate the usefulness of superposition states of this kind, suppose that we want to calculate the quantity Q ,

$$Q = \sum_{j=1}^{2^N} e^{ij} f(j), \tag{6}$$

where $f(j)$ is a highly nonlinear function of j . The quantity Q corresponds to a weighted average of the function f over all possible inputs to the computer, which is a Fourier transform of sorts. Calculations of this kind could be implemented on a quantum computer by programming the computer itself to calculate $f(j)$ and then creating a superposition of input states corresponding to the desired weighted average.

Peter Shor¹ of Bell Labs recently showed that quantum computers could be used to efficiently factor large numbers, which is responsible for much of the current interest in quantum computing. Shor's algorithm uses interference effects to ensure that, with high probability, the output of the computer will correspond to one

of the desired factors. A more detailed discussion of this algorithm, which involves the calculation of functions similar to Q , requires the use of number theory and can be found in the references. Programming a quantum computer is obviously very different from conventional programming, and finding efficient algorithms for the solution of other problems of interest remains an important task.

AN OPTICAL APPROACH TO QUANTUM COMPUTING

Any practical implementation of a quantum computer will probably require a modular approach in which many separate logic gates can be connected with some equivalent of the wiring in a conventional computer. The ability to correct for the growth of errors in the quantum states, known as decoherence, is also essential. Individual quantum gates have been demonstrated using the nuclear spins of ions in a trap.¹⁰ This approach is not modular, however, and the transfer of information from one ion to another is a very complex process.

An optical approach to quantum computing appears to offer a number of practical advantages. All quantum computers are inherently dependent on interference effects and must maintain the appropriate phases. Optical interferometers are widely used in many current applications because their phase is relatively stable and can be controlled using feedback techniques. Interferometers based on charged particles, such as electrons, do exist but are very sensitive to stray electromagnetic fields. In addition, optical fibers or waveguides could readily be used to connect optical quantum gates as needed to perform the desired logic operations. For these and other reasons, we believe that the most practical approach to the construction of quantum computers will be based on the use of optical devices.

It was recently shown that any logic operation or numerical calculation can be implemented by combining a sufficient number of the controlled-NOT gates illustrated in Fig. 3 with additional single-bit operations that are easily implemented. The controlled NOT has

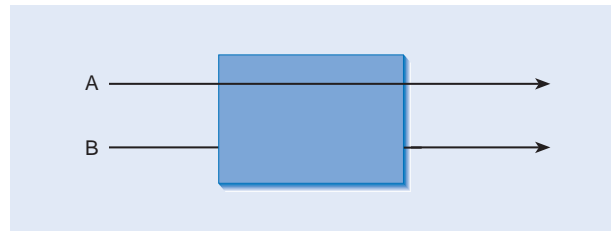


Figure 3. A controlled-NOT gate, which can form the basic logic element of a quantum computer. Bit B is inverted if and only if bit A is 1.

two binary inputs, A and B. Input A is always transferred to the output without change, while input B is inverted (flipped) if and only if input A = 1. Thus, input A can control what happens to input B. The development of a practical controlled-NOT gate is the first step toward the construction of a quantum computer.

A controlled-NOT gate can be implemented using the optical arrangement illustrated in Fig. 4. Here, bit A has the value 1 if a single photon is in the path indicated by the dashed line, whereas it has the value 0 if that photon is in the path indicated by the solid line. Input B is represented in a similar way by a second photon; the two photons have different frequencies ω_1 and ω_2 , which allow them to be distinguished. The two paths for photon B are combined by a beam splitter to form an interferometer with one arm passing through a nonlinear medium. The phase shift experienced by photon B depends on the index of refraction of the medium, which in turn depends on the strength of the electric field at that location (Kerr effect). If photon A passes through the medium at the same time, its electric field will introduce an additional π phase shift, which changes the output path that photon B must take. The net result is that photon A can control the path of photon B.

The primary difficulty in such an optical approach is that nonlinear effects of this kind typically require high-intensity electric fields, whereas the electric field associated with a single photon is normally quite weak. However, the field from a single photon is inversely proportional to the square root of the volume that it occupies, and confining a photon to a sufficiently small volume can produce electric fields as high as 10,000 V/m. A group at the California Institute of Technology recently demonstrated nonlinear phase shifts of this kind at the two-photon level,¹¹ but their approach involves the use of extremely high-quality mirrors, atomic beams, and operation near the resonant frequency of the atoms in the medium, none of which appear to be practical for the construction of a working quantum computer.

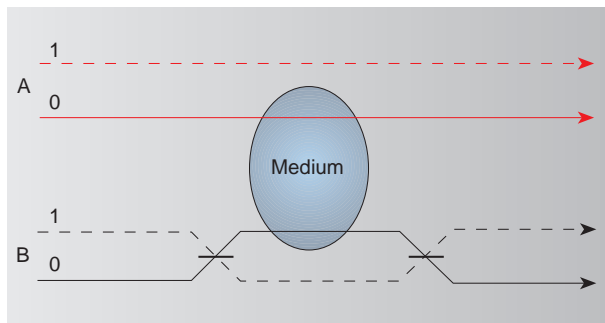


Figure 4. Optical implementation of a controlled-NOT gate based on a nonlinear index of refraction in one arm of an interferometer.

Our approach is based on a new physical effect, recently predicted by one of the authors, that should greatly enhance these kinds of nonlinear phase shifts. Earlier nonlinear mechanisms involved the interaction of two photons with individual atoms, which gives a phase shift proportional to the number N_A of atoms in the medium. The new mechanism involves the interaction of two photons with pairs of atoms, which gives a phase shift proportional to N_A^2 , since that is the number of pairs of atoms in the medium. As Fig. 5 shows, the proposed mechanism consists of the absorption of photon 1 and the emission of photon 2 by atom A, followed by the absorption of photon 2 and the emission of photon 1 by atom B. (The energy of a quantum-mechanical system is uncertain over small time intervals and need not be conserved during the intermediate steps of this process.) This exchange of the photons by a pair of atoms has no net effect other than to cause a shift in the energy of the system, which produces the desired phase shift. An experimental demonstration of this effect is now in progress at APL.

For large values of N_A , this new mechanism should produce much larger phase shifts at the two-photon level. This in turn will allow other design requirements to be relaxed, such as the need for high-quality mirrors or atomic beams. As a result, this approach is eventually expected to allow the construction of large numbers of quantum gates on a single substrate, with optical waveguides to provide the necessary logical connections. We are also investigating the use of some of the same techniques that we previously developed for use in quantum cryptography^{9,12,13} as a means of controlling the growth of quantum phase errors.

SUMMARY

Quantum computing is a promising new technique that may eventually provide the ability to perform

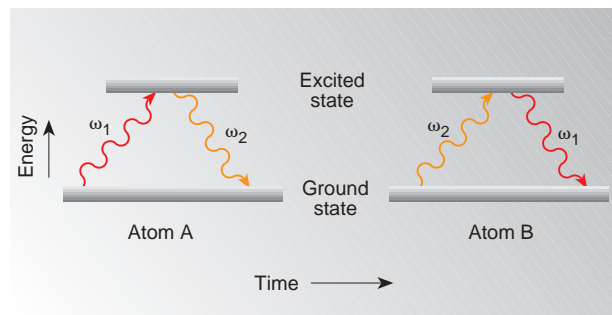


Figure 5. Predicted mechanism for the enhancement of nonlinear phase shifts at the two-photon level. Atom A absorbs photon 1 while making a transition from its ground state to its excited state, after which it re-emits photon 2. Atom B absorbs and re-emits the photons in the opposite order. This interchange of the two photons produces a nonlinear phase shift.

numerical calculations not possible with conventional computers. These enhanced capabilities result from the use of nonclassical logic elements and the ability of a quantum computer to perform many calculations in parallel on a single processor. The advent of quantum computers would revolutionize computer science and information theory. However, a number of practical difficulties must be overcome before quantum computing becomes a reality. APL is currently investigating the feasibility of an optical approach to quantum computing that appears to have a number of advantages over other potential methods.

REFERENCES

¹Shor, P. W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *35th Annual Symposium on Foundations of Computer Science: Proceedings*, S. Goldwasser (ed.), IEEE Computer Society Press (1994).

²Feynman, R. P., "Quantum Mechanical Computers," *Opt. News* **11**, 11-20 (1985).

³Deutsch, D., "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," *Proc. R. Soc. Lond. A* **400**, 97-117 (1985).

⁴Lloyd, S., "Quantum-Mechanical Computers," *Sci. Am.*, 140-145 (Oct 1995).

⁵Bennett, C. H., "Quantum Information and Computation," *Phys. Today*, 24-30 (Oct 1995).

⁶Lloyd, S., "A Potentially Realizable Quantum Computer," *Science* **261**, 1569-1571 (1993).

⁷Glanz, J., "A Quantum Leap for Computers?" *Science* **269**, 28-29 (1995).

⁸Baym, G., *Lectures on Quantum Mechanics*, W. A. Benjamin, London (1969).

⁹Franson, J. D., "Recent Developments in Quantum Optics," *Johns Hopkins APL Tech. Dig.* **16**, 324-332 (1995).

¹⁰Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M., and Wineland, D. J., "Demonstration of a Fundamental Quantum Logic Gate," *Phys. Rev. Lett.* **75**, 4714-4717 (1995).


¹¹Turchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H., and Kimble, H. J., "Measurement of Conditional Phase Shifts for Quantum Logic," *Phys. Rev. Lett.* **75**, 4710-4713 (1995).

¹²Franson, J. D., "Quantum Cryptography," *Opt. Photonics News* **6**, 30-33 (1995).


¹³Franson, J. D. and Jacobs, B. C., "Operational System for Quantum Cryptography," *Electron. Lett.* **31**, 232-234 (1995).

ACKNOWLEDGMENTS: This work is supported by the Independent Research and Development program, the Office of Naval Research, and the National Security Agency.

THE AUTHORS



JAMES D. FRANSON received a B.S. in physics from Purdue University in 1970 and a Ph.D. in physics from the California Institute of Technology in 1977. He joined the Strategic Systems Department at APL in 1978 and transferred to the Milton S. Eisenhower Research and Technology Development Center in 1996. A member of the Principal Professional Staff, his current research activities include quantum optics and the foundations of quantum mechanics. His e-mail address is James.Franson@jhuapl.edu.



BRYAN C. JACOBS received a B.S. in electrical engineering from Drexel University in 1989 and an M.S. in applied physics from The Johns Hopkins University in 1994. While attending Drexel University, he worked on the Tokamak Fusion Test Reactor at the Princeton University Plasma Physics Laboratory. Since joining the Strategic Systems Department at APL in 1989, where he is now a member of the Senior Professional Staff, he has collaborated on several basic research and development projects, including the Advanced Inertial Sensors Project and two quantum cryptography projects. His e-mail address is Bryan.Jacobs@jhuapl.edu.