Ortiz, O., J. E. Gubernatis, E. Knill, and R. Laflamme. 2001. Quantum Algorithms for Fermionic Simulations. *Phys. Rev. A* **64**: 022319.

Papadimitriou, C. H. 1994. *Computational Complexity*. Reading, MA: Addison-Wesley.

Raz, R. 1999. Exponential Separation of Quantum and Classical Communication Complexity. In *Proceedings of the 3lst Annual ACM Symposium on the Theory of Computation* (STOC), p. 358. El Paso, TX: ACM Press.

Ribordy, O., J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden. 2001. Long-Distance Entanglement-Based Quantum Key Distribution. *Phys. Rev. A* **63**: 012309.

Shor, P. W. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings of the 35'th Annual Symposium on Foundations of Computer Science*. p. 124. Los Alamitos, CA: IEEE Press.

———. 1995. Scheme for Reducing Decoherence in Quantum Computer Memory. *Phys. Rev. A* **52**: 2493.

———. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **26**: 1484.

Simon, D. R. 1994. On the Power of Quantum Computation. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, p. 116. Los Alamitos, CA: IEEE Press.

Steane, A. 1996. Multiple Particle Interference and Quantum Error Correction. *Proc. R. Soc. London, Ser. A* **452**: 2551

Terhal, B. M., and D. P. DiVincenzo. 2000. Problem of Equilibration and the Computation of Correlation Functions on a Quantum Computer. *Phys. Rev. A* **61**: 022301.

Townsend, P. D. 1998. Quantum Cryptography on Optical Fiber Networks. *Opt. Fiber Tech.: Mat., Dev., Sys.* **4**: 345.

von Neumann, J. 1932a. Der Messprozess. Ch. VI. In *Mathematische Grundlagen der Quantenmechanik.* Berlin: Springer Verlag.

———. 1932b. "Messung und Reversibilität." Allgemeine Betrachtungen. Ch. V. In *Mathematische Grundlagen der Quantenmechanik.* Berlin: Springer Verlag.

Wiesner, S. 1983. Conjugate Coding. *Sigact News* **15**: 78.

———. 1996. Simulations of Many-Body Quantum Systems by a Quantum Computer. [Online]: http://eprints.lanl.gov. (quant-ph/9603028).

Yao, A. 1993. Quantum Circuit Complexity. In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*. p. 352. Los Alamitos, CA: IEEE Press.

Zalka, C. 1998. Simulating Quantum Systems on a Quantum Computer. *Proc. R. Soc. London, Ser. A* **454**: 313.

Glossary

Algorithm. A set of instructions to be executed by a computing device. What instructions are available depends on the computing device. Typically, instructions include commands for manipulating the contents of memory and means for repeating blocks of instructions indefinitely or until a desired condition is met.

Amplitude. A quantum system with a chosen orthonormal basis of "logical" states $|i\rangle$ can be in any superposition $\Sigma_i \alpha_i \, |i\rangle$ of these states, where $\Sigma_i |\alpha_i|^2 = 1$. In such a superposition, the complex numbers α_ι are called the amplitudes. Note that the amplitudes depend on the chosen basis.

Ancillas. Helper systems used to assist in a computation involving other information systems.

Bell basis. For two qubits A and B, the Bell basis consists of the four states $1/\sqrt{2}(|00\rangle_{AB} \pm |11\rangle_{AB})$ and $1/\sqrt{2}(|01\rangle_{AB} \pm |10\rangle_{AB})$.

Bell states. The members of the Bell basis.

Bit. The basic unit of deterministic information. It is a system that can be in one of two possible states, 0 and 1.

Bit sequence. A way of combining bits into a larger system whose constituent bits are in a specific order.

Bit string. A sequence of 0s and 1s that represents a state of a bit sequence. Bit strings are the words of a binary alphabet.

Black box. A computational operation whose implementation is unknown. Typically, a black box implements one of a restricted set of operations, and the goal is to determine which of these operations it implements by using it with different inputs. Each use of the black box is called a "query." The smallest number of queries required to determine the operation is called the "query complexity" of the restricted set. Determining the query complexity of sets of operations is an important area of computational complexity.

Bloch sphere. The set of pure states of a qubit represented as points on the surface of the unit sphere in three dimensions.

Bra. A state expression of the form $\langle\psi|$ considered to be the conjugate transpose of the ket expression $|\psi\rangle$.

Bra-ket notation. A way of denoting states and operators of quantum systems with kets (for example, $|\psi\rangle$) and bras (for example, $\langle\phi|$).

Circuit. A combination of gates applied to information units in a prescribed order. To draw circuits, one often uses a convention for connecting and depicting gates. See also "network."

Circuit complexity. The circuit complexity of an operation on a fixed number of information units is the smallest number of gates required to implement the operation.

Classical information. The type of information based on bits and bit strings and more generally on words formed from finite alphabets. This is the information used for communication between people. Classical information can refer to deterministic or probabilistic information, depending on the context.

Computation. The execution of the instructions provided by an algorithm.

Computational states. See "logical states."

Computer. A device that processes information.

Density matrix or operator. A representation of pure and mixed states without redundancy. For a pure state $|\psi\rangle$, the corresponding density operator is $|\psi\rangle\langle\psi|$. A general density operator is a probabilistic combination $\Sigma_i\lambda_i|\psi_i\rangle\langle\psi_i|$, with $\Sigma_i\lambda_i = 1$.

Deterministic information. The type of information that is based on bits and bit strings. Deterministic information is classical, but it explicitly excludes probabilistic information.

Distinguishable states. In quantum mechanics, two states are considered distinguishable if they are orthogonal. In this case, a measurement exists that is guaranteed to determine which of the two states a system is in.

Efficient computation. A computation is efficient if it requires, at most, polynomially many resources as a function of input size. For example, if the computation returns the value $f(x)$ on input x, where x is a bit string, then it is efficient if there exists a power k such that the number of computational steps used to obtain $f(x)$ is bounded by $|x|^2$, where $|x|$ is the length (number of bits) of x.

Entanglement. A nonclassical correlation between two quantum systems most strongly exhibited by the maximally entangled states, such as the Bell states for two qubits, and considered to be absent in mixtures of product states (which are called separable states). Often, states that are not separable are considered to be entangled. However, nearly separable states do not exhibit all the features of maximally entangled states. As a result, studies of different types of entanglement are an important component of quantum information theory.

Gate. An operation applied to information for the purpose of information processing.

Global phase. Two quantum states are indistinguishable if they differ only by a global phase. That is, $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ are in essence the same state. The global phase difference is the factor $e^{i\phi}$. The equivalence of the two states is apparent from the fact that their density matrices are the same.

Hilbert space. An n-dimensional Hilbert space consists of all complex n-dimensional vectors. A defining operation in a Hilbert space is the inner product. If the vectors are thought of as column vectors, then the inner product $\langle x, y\rangle$ of x and y is obtained by forming the conjugate transpose $x^\dagger$ of x and calculating $\langle x,\ y\rangle\ =\ x^\dagger y$. The inner product induces the usual squared norm $|x|^2 = \langle x, x\rangle$.

Information. Something that can be recorded, communicated, and computed with. Information is fungible; that is, its meaning can be identified regardless of the particulars of the physical realization. Thus, information in one realization (such as ink on a sheet of paper) can be easily transferred to another (for example, spoken words). Types of information include deterministic, probabilistic, and quantum information. Each type is characterized by information units, which are abstract systems whose states represent the simplest information of each type. The information units define the “natural” representation of the information. For deterministic information, the information unit is the bit, whose states are symbolized by $\mathsf{0}$ and $\mathsf{1}$. Information units can be put together to form larger systems and can be processed with basic operations acting on few of them at a time.

Inner product. The defining operation of a Hilbert space. In a finite dimensional Hilbert space with a chosen orthonormal basis $\{e_i : 1 \leq i \leq n\}$, the inner product of two vectors $x = \Sigma_i x_i e_i$ and $y = \Sigma_i y_i e_i$ is given by $\Sigma_i \bar{x}_i y_i$. In the standard column representation of the two vectors, this is the number obtained by computing the product of the conjugate transpose of x with y. For real vectors, that product agrees with the usual “dot” product. The inner product of x and y is often written in the form $\langle x, y\rangle$. Pure quantum states are unit vectors in a Hilbert space. If $|\phi\rangle$ and $|\psi\rangle$ are two quantum states expressed in the ket-bra notation, their inner product is given by $(|\phi\rangle)^\dagger\langle\psi| = \langle\phi|\psi\rangle$.

Ket. A state expression of the form $|\psi\rangle$ representing a quantum state. Usually, $|\psi\rangle$ is thought of as a superposition of members of a logical state basis $|i\rangle$. One way to think about the notation is to consider the two symbols $|$ and $\rangle$ as delimiters denoting a quantum system and ψ as a symbol representing a state in a standard Hilbert space. The combination $|\psi\rangle$ is the state of the quantum system associated with ψ in the standard Hilbert space via a fixed isomorphism. In other words, one can think of $\psi \leftrightarrow |\psi\rangle$ as an identification of the quantum system's state space with the standard Hilbert space.

Linear extension of an operator. The unique linear operator that implements a map defined on a basis. Typically, we define an operator U on a quantum system only on the logical states $U : |i\rangle \rightarrow |\psi_i\rangle$. The linear extension is defined by $U(\Sigma_i \alpha_i |i\rangle) = \Sigma_i \alpha_i |\psi_i\rangle$.

Logical states. For quantum systems used in information processing, the logical states are a fixed orthonormal basis of pure states. By convention, the logical basis for qubits consists of $|\mathsf{0}\rangle$ and $|\mathsf{1}\rangle$. For larger dimensional quantum systems, the logical basis is often indexed by integers, $|0\rangle$, $|1\rangle$, $|2\rangle$, and so on. The logical basis is often called the computational basis, or sometimes, the classical basis.

Measurement. The process used to extract classical information from a quantum system. A general projective measurement is defined by a set of projectors P_i, satisfying $\Sigma_i P_i = \mathbb{1}$ and $P_i P_j = \delta_{ij} P_i$. Given the quantum state $|\psi\rangle$, the outcome of a measurement with the set $\{P_i\}_i$, is one of the classical indices i associated with a projector P_i. The index i is the measurement outcome. The probability of outcome i is $p_i = |P_i|\psi_i\rangle|^2$, and given outcome i, the quantum state “collapses” to $P_i|\psi_i\rangle/\sqrt{p_i}$.

Mixture. A probabilistic combination of the pure states of a quantum system. Mixtures can be represented without redundancy with density operators. Thus, a mixture is of the form $\Sigma_i \lambda_i |\psi_i\rangle\langle\psi_i|$, with $\lambda_i \geq 0$ and $\Sigma_i \lambda_i = 1$ being the probabilities of the states $|\psi_i\rangle$. This expression for mixtures defines the set of density operators, which can also be characterized as the set of operators ρ satisfying $\mathrm{tr}(\rho) = 1$ and for all $|\psi\rangle$, $\langle\psi|\rho|\psi\rangle \geq 0$ ("positive semidefinite operator").

Network. In the context of information processing, a network is a sequence of gates applied to specified information units. Networks can be visualized as displaying horizontal lines that denote the timeline of an information unit. The gates are represented by graphical elements that intercept the lines at specific points. A realization of the network requires applying the gates to the information units in the specified order (left to right).

Operator. A function that transforms the states of a system. Operators may be restricted depending on the system's properties. For example, in talking about operators acting on quantum systems, one always assumes that they are linear.

Oracle. An information processing operation that can be applied. A use of the oracle is called a query. In the oracle model of computation, a standard model is extended to include the ability to query an oracle. Each oracle query is assumed to take one time unit. Queries can reduce the resources required for solving problems. Usually, the oracle implements a function or solves a problem not efficiently implementable by the model without the oracle. Oracle models are used to compare the power of two models of computation when the oracle can be defined for both models. In 1994, for example, Dan Simon showed that quantum computers with a specific oracle O could efficiently solve a problem that had no efficient solution on classical computers with access to the classical version of O. At the time, this result was considered the strongest evidence for an exponential gap in power between classical and quantum computers.

Overlap. The inner product between two quantum states.

Pauli operators. The Hermitian matrices σ_x, σ_y, and σ_z acting on qubits, which are two-level quantum systems. They are defined in Equation (12). It is often convenient to consider the identity operator to be included in the set of Pauli operators.

Polynomial resources. To say that an algorithm computing the function $f(x)$, where x is a bit string, uses polynomial resources (in other words, is efficient) means that the number of steps required to compute $f(x)$ is bounded by $|x|^k$ for some fixed k. Here, $|x|$ denotes the length of the bit string x.

Probabilistic bit. The basic unit of probabilistic information whose state space consists of all probability distributions over the two states of a bit. The states can be thought of as describing the outcome of a biased coin flip before the coin is flipped.

Probabilistic information. The type of information obtained by extending the state spaces of deterministic information to allow arbitrary probability distributions over the deterministic states. This is the main type of classical information with which quantum information is compared.

Probability amplitude. The squared norm of an amplitude with respect to a chosen orthonormal basis $\{|i\rangle\}$. Thus, the probability amplitude is the probability with which the state $|i\rangle$ is measured in a complete measurement that uses this basis.

Product state. For two quantum systems A and B, product states are of the form $|\psi\rangle_{\mathrm{A}}|\phi\rangle_{\mathrm{B}}$. Most states are not of this form.

Program. An algorithm expressed in a language that can be understood by a particular type of computer.

Projection operator. A linear operator P on a Hilbert space that satisfies $P^2 = P^\dagger P = P$. The projection onto a subspace V with orthogonal complement W is defined as follows: If $x \in V$ and $y \in W$, then $P(x + y) = x$.

Pseudocode. A semiformal computer language intended to be executed by a standard random-access machine, which is a machine model with a central processing unit and access to a numerically indexed unbounded memory. This machine model is representative of the typical one-processor computer. Pseudocode is similar to programming languages such as BASIC, Pascal, or C but does not have specialized instructions for human interfaces, file management, or other "external" devices. Its main use is to describe algorithms and enable machine-independent analysis of the algorithms' resource usage.

Pure state. A state of a quantum system that corresponds to a unit vector in the Hilbert space used to represent the system's state space. In the ket notation, pure states are written in the form $|\psi\rangle = \Sigma_i \alpha_i |i\rangle$, where the $|i\rangle$ form a logical basis and $\Sigma_i |\alpha_i|^2 = 1$.

Quantum information. The type of information obtained when the state space of deterministic information is extended by normalized superpositions of deterministic states. Formally, each deterministic state is identified with one of an orthonormal basis vector in a Hilbert space, and normalized superpositions are unit-length vectors expressible as complex linear sums of the chosen basis vectors. It is convenient to extend this state space further by permitting probability distributions over the quantum states (see the entry for "mixtures"). This extension is still called quantum information.

Qubit. The basic unit of quantum information. It is the quantum extension of the deterministic bit, which implies that its state space consists of the unit-length vectors in a two-dimensional Hilbert space.

Readout. A method for obtaining human-readable information from the state of a computer. For quantum computers, readout refers to a measurement process used to obtain classical information about a quantum system.

Reversible gate. A gate whose action can be undone by a sequence of gates.

Separable state. A mixture of product states.

States. The set of states for a system characterizes the system's behavior and possible configurations.

Subspace. For a Hilbert space, a subspace is a linearly closed subset of the vector space. The term can be used more generally for a system Q of any information type: A subspace of Q or, more specifically, of the state space of Q is a subset of the state space that preserves the properties of the information type represented by Q.

Superposition principle. One of the defining postulates of quantum mechanics according to which if states $|1\rangle, |2\rangle, \ldots$ are distinguishable, then $\Sigma_i \alpha_i |i\rangle$ with $\Sigma_i |\alpha_i|^2 = 1$ is a valid quantum state. Such a linear combination is called a normalized superposition of the states $|i\rangle$.

System. An entity that can be in any of a specified number of states. An example is a desktop computer whose states are determined by the contents of its various memories and disks. Another example is a qubit, which can be thought of as a particle whose state space is identified with complex, two-dimensional, length-one vectors. Here, a system is always associated with a type of information that determines the properties of the state space. For example, for quantum information, the state space is a Hilbert space. For deterministic information, it is a finite set called an alphabet.

Unitary operator. A linear operator U on a Hilbert space that preserves the inner product. That is, $\langle Ux, Uy\rangle = \langle x, y\rangle$. If U is given in matrix form, then this expression is equivalent to $U^\dagger U = \mathbb{1}$.

Universal set of gates. A set of gates that satisfies the requirement that every allowed operation on information units can be implemented by a network of these gates. For quantum information, it means a set of gates that can be used to implement every unitary operator. More generally, a set of gates is considered universal if, for every operator U, there are implementable operators V arbitrarily close to U.