International Journal of Theoretical Physics, Vol. 38, No. 2, 1999

Reduction of Theoretical Uncertainty in Quantum Computing

Hideaki Matsueda[1] and David W. Cohen[2]

Received May 18, 1998

A theoretical framework is developed to evaluate the amount of intrinsic uncertainty, as distinguished from operational uncertainty (noise), inherent in quantum computation. The temporal evolution of states in quantum computing is analyzed diagramatically, providing a visual tool for the refining of quantum algorithms to help achieve minimal uncertainty and maximal efficiency, as well as for better understanding of the quantum entanglements crucial to quantum computing.

1. INTRODUCTION

Since the introduction of quantum mechanics into the study of novel computing processes in the early 1980s [4,6,7] and the quantum mechanical algorithms for discrete logarithms and factoring in 1994 [13] scientists have conceived various schemes of super-parallel computation on the basis of the superposition principle and unitary temporal evolution in quantum mechanics [1, 10].

So far, however, the most fundamental questions of how and to what degree the quantum mechanical parallelism supplies a nearly unique solution that can be read by classical devices is not clearly understood. This may be one of the reasons why there is still considerable ambiguity and skepticism in this field.

This paper provides a diagrammatic method to visualize and assess limitations due to intrinsic uncertainty inherent in quantum states. This intrinsic uncertainty is not the same as operational uncertainty, which is the noise

[1] Department of Information Science, Kochi University, 2-5-1 Akebono-cho, Kochi 780-8072, Japan; e-mail: matsueda@is.kochi-u.ac.jp.
[2] Department of Mathematics, Smith College, Northampton, Massachusetts 01063.

0020-7748/99/0200-070 1$16.00/0

Fig. 1. The input port consisting of a preparation register and an input register.

accumulated by inefficiencies of physical devices. The goal is to help build quantum circuit algorithms that reduce intrinsic uncertainty to a level low enough so that reduction in operational uncertainty becomes effective.

2. THE QUANTUM COMPUTING PROCESS

The computing process begins with an input port, including a n-bit preparation register in a superposition state of maximal uncertainty, together with an input register. We can visualize this input port as a row of boxes, with n boxes representing the preparation register on the left, and some boxes on the right to represent the input register, as shown in Fig. 1.

The computation proceeds via a bank of *row operations*. A row operation consists of a parallel collection of control-bit/target-bit (C-T) operations, such as controlled not (CN), controlled rotation (CR), and controlled phase shift (CPS), as represented in Fig. 2. Each C-T operation produces the unitary (or quasiunitary) evolution of the target bits, initially kept in the ground state, driven by the propagation of excited control bit states. The C-T operations are executed by methods of clock signals and biased band gap [10].

The overall process of quantum computation may be understood as consisting of four main steps. In Fig. 3 we show a schematic example of a solid-state quantum computer as proposed in refs. 10.

Each small box in Fig. 3 represents a quantum bit. Each row represents a quantum state, which evolves from row to row to the final solution state through row operations. The four main steps for the computation are represented by sections A, B, C, and D.

The first step is to prepare the preparation register (section A), which is a superposition (minimum, or zero, entanglement) of the ground state $|0\rangle$ and the excited state $|1\rangle$ in each of n bits. Part of the preparation resister may be kept in the ground state if necessary. We'll call the state of each bit

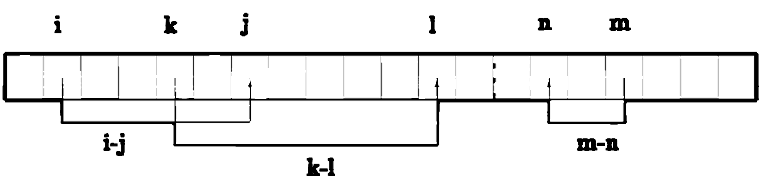

Fig. 2. A parallel collection of C-T operations. Each pair connected by an arrow represents a control-bit/target-bit pair.

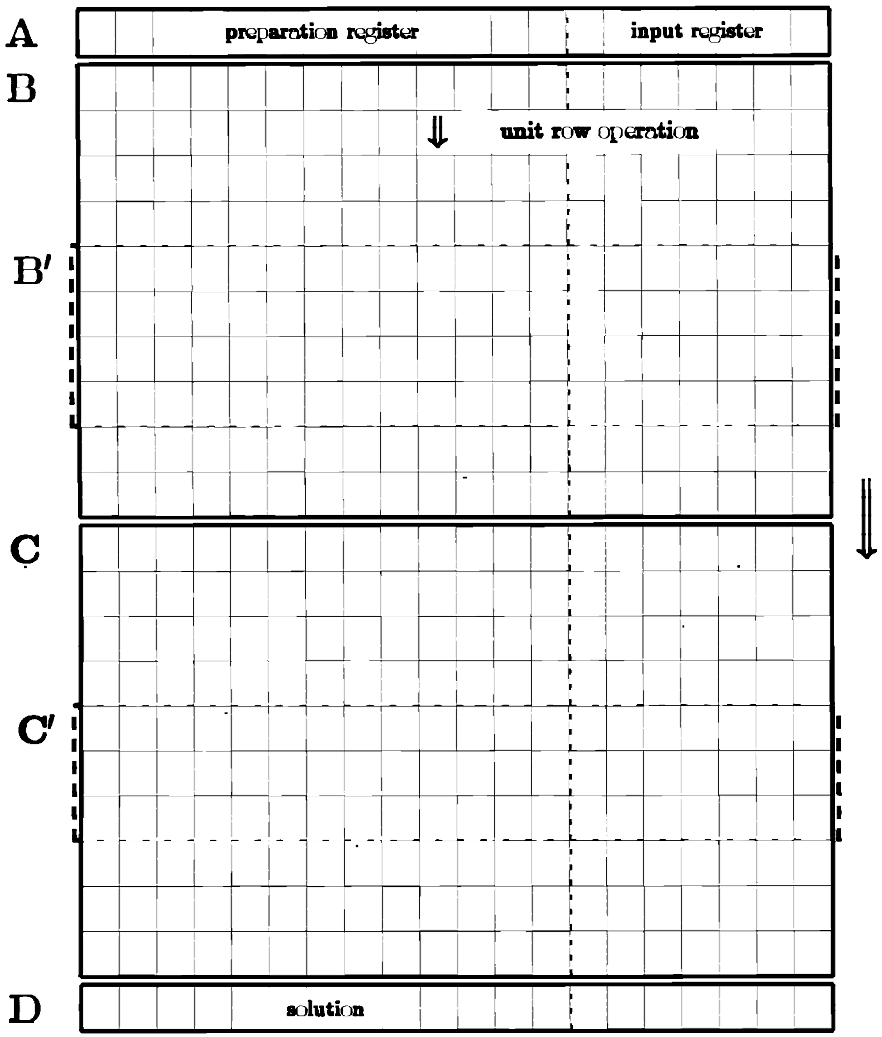

Fig. 3. A schematic diagram representing a solid-state quantum computer. Section A is the input port, consisting of the preparation register on the left and the input register on the right. Section B is the first bank of row operations containing the algorithim for making the super-parallel quantum computation. Section C is the bank of row operations designed to reduce overall intrinsic uncertainty, and section D is the output port. Sections B and C might contain subsections B′ and C′ for reducing phase errors.

a bit-state. (To increase resistance of the bits to decohering agitations, each bit is an ensemble of quantum dots [10], which fact is usually emphasized by writing the bit states as $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$. We omit the tildes in this paper, however, with a reminder to the reader that our bits are ensembles.)

The state of the preparation register can be represented by an n-dimensional vector $(b_1, b_2, \ldots, b_n)$, where each b_i is a number between 0 and 1, representing the probability that bit i is in the excited bit-state $|1\rangle$. The number b_i is obtained by $b_i = |e_i|^2$, where each bit is in a superposition $g|0\rangle + e|1\rangle$. The initial preparation state is the state of maximum intrinsic uncertainty, $(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$ [5,12]. We also call this a state of maximal dispersion, as opposed to a dispersion-free state, where each b_i is either 0 or 1 [5]. It is not hard to see that there are 2^n vectors representing dispersion-free states in the n-dimensional state space (folded diagram of state space).

Computation proceeds as the downward sequential execution of a bank of row operations (section B). Each row operation results in an evolution of the preparation state, generating the quantum mechanical entangled states. A row operation may increase or decrease the intrinsic uncertainty (dispersion) of the preceding state. We address that issue in Section 3 of this paper.

Within section B there may be subsections B′ where bit states might be transformed by a Hadamard transformation

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

for increased resistance to phase errors. Because a phase error in the transformed state corresponds to a pair of bit errors in an original bit state, stabilization may be increased by dipole–dipole interactions within each ensemble of quantum dots to reduce bit errors [10]. After a phase-sensitive row operation, the reverse Hadamard transformation may be applied to the bits. We denote a bank of rows accomplishing these transformations by B′. There may be many such banks within B and same for C^1 within C.

The third step in the overall computation, represented by section C in Fig. 3, is another unitary evolution, converging into the final less dispersive state, or even into a dispersion-free state. This is achieved as the cumulative effects of rotary operations causing interference among the quantum bits. The quantum Fourier transform for the case of the factoring algorithm [13] is an example of such a third step [2,3,11]. The iterative combination of two Walsh–Hadamard transforms and a CPS (or conditional phase shift) in a quantum search algorithm [8] and the building up of the correlation function in a quantum simulator [9] may also be considered as examples of the third step.

The fourth step, which we represent as section D in Fig. 3, is the reading or measuring of the final solution state in the output port. The less the uncertainty in this final state is, the more accurately one can read it.

3. DIAGRAM FOR THE EVOLUTION OF LOGICAL STATES

3.1. State Space Diagram

The third step in our quantum computing schematic is crucial for making quantum computing useful, because without this all we can achieve is an utterly unreadable superposition of all the provisional solutions. We have created a diagram (Fig. 4) to visualize the evolution of uncertainty in the quantum logical process of a pair of bits working as an elemental gate, such as a CN, CR, or CPS gate. Each such gate can be represented as an operation on bit-states by an $SU(2)$ matrix [1].

Figure 4 (a) represents the state space for a single pair of bits, consisting of a control bit c_i and target bit t_j. The horizontal axis represents the probability C that the control bit is in state $|1\rangle$, and the vertical axis represents the same probability T for the target bit. In the terminology of quantum logic, we are plotting the temporal change of the truth value of the proposition *the target bit is in state* $|1\rangle$ together with the truth value of the proposition *the control bit is in state* $|1\rangle$.

The temporal evolution of the state of a provisional solution (an entire row in the quantum computer) may be tracked in the n-dimensional state space, by considering the two-dimensional subspaces generated by control–target pairs for each row. With that in mind we define the *dispersion of the state represented by row-vector* $b = (b_1, b_2, \ldots, b_n)$ as

$$\mathcal{D} = \min_{d} \{\| b - d \| \,|\, d \text{ is a dispersion-free vector}\} \tag{3.1}$$

This is a measure of how close b is to one of the 2^n dispersion-free vectors in the state space. We now consider the effect that row operations have on $\mathcal{D}$.

For a control–target bit (C-T) pair i–j, suppose both the control and target are in an initial superposition of maximal uncertainty: $(1/\sqrt{2})(|0\rangle + |1\rangle)$. Then we represent the pair by the closed circle at the center point (0.5, 0.5) in the left diagram (Fig. 4a). The theoretical dispersion for a pair of bits is maximal in this initial superposition, because the shortest distance to any one of all the dispersion-free states (0, 0), (0, 1), (1, 0), or (1, 1) is maximal at this middle point. Since we are interested in the evolution of the truth values of target bits, we label this first point $T_{i,j}(0)$. We follow the evolution of the state as it is affected by controlled rotations.

A controlled rotation by angle β around the y axis $\hat{R}^{\beta}_{yi,j}$ moves the truth value of the target bit away from the initial superposition point into some

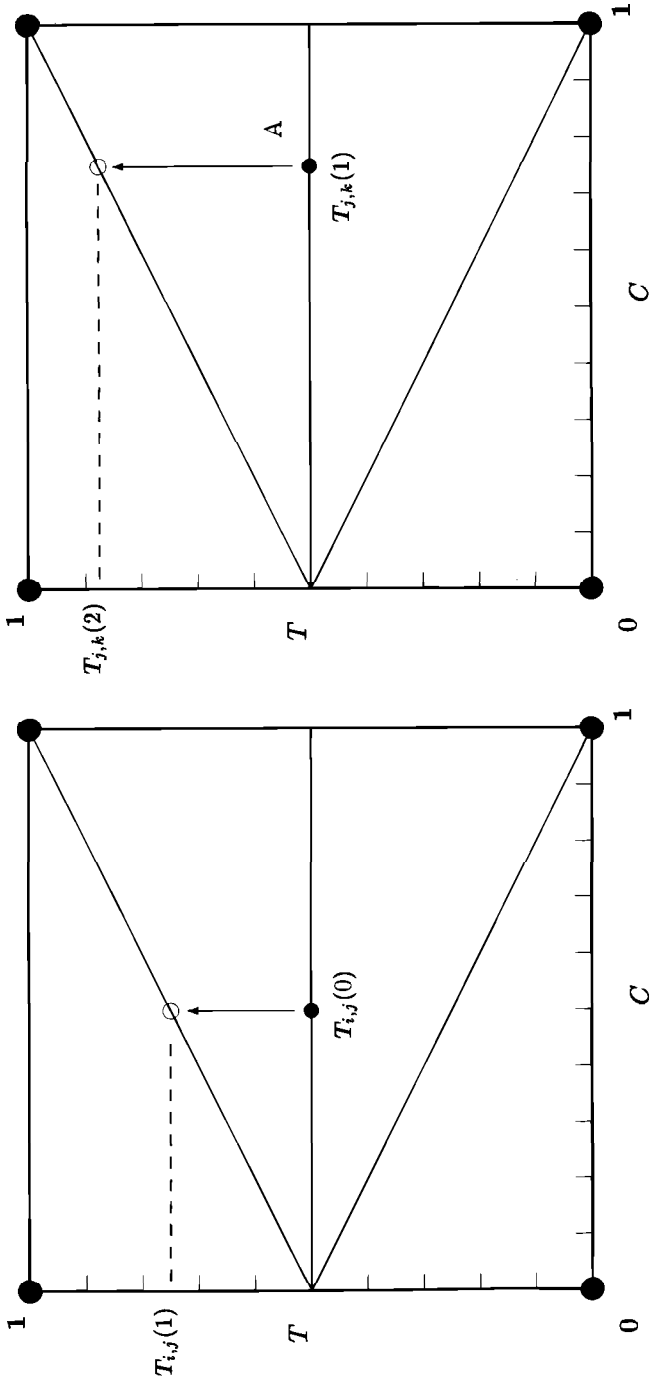

Fig. 4. State space diagrams for control–target bit pairs. The temporal evolution of the truth probability T of the statement *the target bit* b_j *is in state* $|1\rangle$ *at time step* t is plotted with an open circle labled $T_{i,j}(t)$. (The subscript i means that bit b_i is the control bit for this target.)

point in the triangular region defined by the ±45-deg lines connecting the points (0, 0.5) and (1, 1) or (0, 0.5) and (1, 0), and the vertical line at $C = 1$, as shown in Fig. 4a or 4b. If the angle of rotation is $\pm\pi/2$, the truth value of the target bit increases or decreases so that the C-T pair falls on one of the ±45-deg lines. This is proven in Section 3.2 below.

Suppose the target is subjected to y rotation through angle $\pi/2$. Then the pair state is moved from the center of the left diagram [with $T_{i,j}(0)$] to a state with truth value $T_{i,j}(1)$.

Now suppose that target becomes a control bit b_j with truth value $C_{j,k}(1) = T_{i,j}(1)$ for a new target bit b_k in a state of maximal dispersion [point A with $T_{j,k}(1)$ in the right diagram]. Another y rotation through angle $\pi/2$ moves the new target to a bit state with probability $T_{j,k}(2)$.

Consecutive similar rotations for C-T pairs, where the control is the target from the preceding rotation and the target is in a maximally uncertain state, produce targets with truth values converging to 1.

As a matter of course, these dispersions are measured relative to the fixed basis, which may be preferentially determined by experimental situation.

3.2. Derivation of the Truth Values

We show the method for calculating the probability T for the case of a controlled rotation around the y axis.

A free rotation around the y axis by angle β [1] is expressed as

$$\hat{R}_y^{\beta} = \begin{pmatrix} \cos(\beta/2) & -\sin(\beta/2) \\ \sin(\beta/2) & \cos(\beta/2) \end{pmatrix} \tag{3.2}$$

Applying this to an initial target bit j in state $(1/\sqrt{2})(|0\rangle + |1\rangle)$ with $T_j(0) = 1/2$ (we write T_j instead of $T_{i,j}$ because the control bit is not at issue for this calculation), we get

$$\begin{aligned} \hat{R}_y^{\beta}|T_j(0)\rangle &= \begin{pmatrix} \cos(\beta/2) & -\sin(\beta/2) \\ \sin(\beta/2) & \cos(\beta/2) \end{pmatrix} \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] \\ &= \frac{1}{\sqrt{2}} \left[\left(\cos\frac{\beta}{2} \mp \sin\frac{\beta}{2} \right) |0\rangle + \left(\pm\cos\frac{\beta}{2} + \sin\frac{\beta}{2} \right) |1\rangle \right] \end{aligned} \tag{3.3}$$

Thus, the free rotation results in

$$T_j(1) = \left| \frac{1}{\sqrt{2}} \left(\pm\cos\frac{\beta}{2} + \sin\frac{\beta}{2} \right) \right|^2 \tag{3.4}$$

Then the change of T in the controlled rotation for control bit i and target bit j is given as

$$\begin{aligned}\Delta T_{i,j} &= (T_j(1) - T_j(0))C \\ &= \left[\left|\frac{1}{\sqrt{2}}\left(\pm\cos\frac{\beta}{2} + \sin\frac{\beta}{2}\right)\right|^2 - \left|\frac{1}{\sqrt{2}}\right|^2\right]C \\ &= \left[\frac{1}{2}(1 \pm \sin\beta) - \frac{1}{2}\right]C \\ &= \pm\frac{\sin\beta}{2}C \end{aligned} \tag{3.5}$$

which gives the new T value:

$$T_{i,j}(1) = T_{i,j}(0) + \Delta T_{i,j} \tag{3.6}$$

Similar calculations give the change $\Delta T_{i,j}$ for other operations such as CRs around the x axis.

It is not difficult to establish that a CN operation $\hat{P}_{\mathrm{CN}}$, which can be represented in terms of a $\pm\pi$ rotation around the x axis by $\hat{P}_{\mathrm{CN}} = \pm i\hat{R}_x^{\pm\pi}$, does not change the truth value of the target bit ($\Delta T_{i,j} = 0$) if it is initially in the superposition $(1/\sqrt{2})(|0\rangle + |1\rangle)$, leaving the target bit always on the horizontal line at $T = 0.5$ for any initial state of the control bit.

The controlled controlled not (CCN) operation $\hat{P}_{\mathrm{CCN}ij,k}$ (i, j control bits, k target bit), which is useful to construct NAND gates for classical computing, can be decomposed into C-T operations as follows:

$$\hat{P}_{\mathrm{CCN}ij,k} = \hat{S}_{j,i}^{\pi/2}\hat{S}_{i,j}^{\pi/2}\hat{R}_{xi,k}^{\pi/2}\hat{P}_{\mathrm{CN}i,j}\hat{R}_{xj,k}^{3\pi/2}\hat{P}_{\mathrm{CN}i,j}\hat{R}_{xj,k}^{\pi/2} \tag{3.7}$$

where $\hat{R}_{xj,k}^{\alpha}$ denotes a CR operation around the x axis by angle α, $\hat{P}_{\mathrm{CN}i,j}$ a CN, and $\hat{S}_{i,j}^{\gamma}$ a CPS by angle γ, respectively [1]. Therefore, the overall change $\triangle T_{ij,k}$ can be estimated as the sum of the changes of these elemental operations, resulting in $\Delta T_{ij,k} = 0$ when applied to a target initially in the maximally uncertain state.

Moreover, application of the controlled rotation around the y axis $\hat{R}_y^{\beta}$ to a general superposition state $|T_k(0)\rangle = g|0\rangle \pm e|1\rangle$ gives

$$\begin{aligned}\hat{R}_y^{\beta}|T_k(0)\rangle &= \begin{pmatrix}\cos(\beta/2) & -\sin(\beta/2)\\ \sin(\beta/2) & \cos(\beta/2)\end{pmatrix}\left[g\begin{pmatrix}1\\0\end{pmatrix} \pm e\begin{pmatrix}0\\1\end{pmatrix}\right] \\ &= \left[\left(g\cos\frac{\beta}{2} \mp e\sin\frac{\beta}{2}\right)|0\rangle + \left(g\sin\frac{\beta}{2} \pm e\cos\frac{\beta}{2}\right)|1\rangle\right] \end{aligned} \tag{3.8}$$

where $|g|^2 + |e|^2 = 1$. Then, by a procedure simillar to that leading to Eq. (3.5),

$$\Delta T_{i,j} = \left[(|g|^2 - |e|^2) \frac{1 - \cos\beta}{2} \pm (ge^* + g^*e) \frac{\sin\beta}{2} \right] C \tag{3.9}$$

of which Eq. (3.5) is a special case, and the asterisk denotes the complex conjugate.

Furthermore, for a controlled rotation by a fractional angle $\beta = \pi/2m$, the following is obtained using Eq. (3.9):

$$\Delta T_{i,j} = \frac{1}{2} \left[(|g|^2 - |e|^2) \left(\frac{\beta^2}{2} - \frac{\beta^4}{24} + \frac{\beta^6}{720} - \cdots \right) \right. \tag{3.10}$$

$$\left. \pm (ge^* + g^*e) \left(\beta - \frac{\beta^3}{6} + \frac{\beta^5}{120} - \cdots \right) \right] C$$

$$= \frac{1}{2} [\pm (ge^* + g^*e)\beta] C + W \tag{3.11}$$

where the remainder of the Taylor expansion W is estimated to be less than $(\beta^2/4 + \beta^3/2)C$, because $|g|, |e| \leq 1$.

Then the number of steps for consecutive controlled rotations $\hat{R}_y^{\pi/2m}$ to reach the dispersion-free state at (1, 1) in Fig. 4 can be estimated to be no more than

$$\frac{1}{\Delta T_{i,j}} = \frac{1}{\beta C + W} \approx \frac{1}{\beta C} = \frac{4m}{\pi} \sim 1.27m \tag{3.12}$$

assuming the new target bits always begin in the maximally uncertain state, i.e. $g = e = 1/\sqrt{2}$. The upper bound of the accumulated error in the consecutive rotation is estimated as

$$W \times \left(\text{number of steps} \approx \frac{1}{\beta C} \right) < \frac{\beta}{4} + \frac{\beta^2}{2}$$

$$\Rightarrow 0 \qquad \text{for} \quad \beta \to 0, \quad i.e., \quad m \to \infty \tag{3.13}$$

The convergence of this process is also verified by a Bloch vector making up an angle π by consecutive $\beta = \pi/2m$ rotations.

4. CONCLUSIONS

We have developed a way to estimate intrinsic uncertainties in provisional results of quantum computations. We also calculated the reduction of uncertainty resulting from particular controlled rotations ($\hat{R}_y^{\beta}$) applied to control–target bit pairs, and also showed that other C-T operations do not reduce

target bit uncertainty when the initial state is the maximal uncertainty superposition.

A lower bound in the number of computational steps to achieve the solution without the intrinsic uncertainty was estimated by this method, within a finite error which decreases with the angle of controlled rotation. In this way the intrinsic or theoretical efficiency could be maximized for any quantum computing process, so that efforts to reduce operational uncertainty should become effective.

This method could be applied to other kinds of quantum computing schemes in addition to the solid-state implementation focused on in this paper. Such a tool may be effective for designing and refining quantum algorithms, and for implementing quantum systems, as well as aid in understanding quantum entanglements.

ACKNOWLEDGMENTS

This work was partially supported by the Proposal-Based New Industry Creative Type Technology R&D Promotion Program of the New Energy and Industrial Technology Development Organization (NEDO) of Japan.

REFERENCES

1. A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Physical Review A*, **52**, 3457 (1995).
2. A. Barenco, A. Ekert, K.-A. Suominen, and P. Törmä, *Physical Review A*, **54**, 139 (1996).
3. D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, *Physical Review A*, **54**, 1034 (1996).
4. P. Benioff, *Journal of Statistical Physics*, **22**, 563 (1980); *Physical Review Letters*, **48**, 1581 (1982).
5. D. W. Cohen, *An Introduction to Hilbert Space and Quantum Logic*, Springer, New York (1989), Chaps. 3 and 6.
6. D. Deutsch, *Proceedings of the Royal Society of London A*, **400**, 97 (1985); **425**, 73 (1989).
7. R. P. Feynman, *International Journal of Theoretical Physics*, **21**, 467 (1982); *Optics News*, **11**, 11 (1985); *Foundations of Physics*, **16**, 507 (1986); *Feynman Lectures on Computation*, eds. A. J. G. Hey and R. W. Allen, Addison-Wesley, Reading, Massachusetts (1996).
8. L. K. Grover, *Physical Review Letters*, **79**, 325 (1997).
9. S. Lloyd, *Science*, **273**, 1073 (1996).
10. H. Matsueda, and S. Takeno, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E80-A**(9), 1610–1615 (1997); in *Proc. 4th Workshop on Physics and Computation (PhysComp96)*, eds. T. Toffoli, M. Biafore, and J. Leão, New England Complex Systems Institute, Cambridge, Massachusetts (1996), pp. 215–222; H. Matsueda, in *Proc. European Conference on Circuit Theory and Design (ECCTD'97)*, Budapest (1997), pp. 265–270; in *Unconventional Models of Computation*, eds. C. S. Calude, J. Casti, and M. J. Dinneen, Springer-Verlag, Singapore (1998), pp. 286–292; in *Proc. The First NASA International Conference on Quantum Computing and Quantum Communications (NASA-QCQC'98)*, Lecture Notes in Computer Science, Springer-Verlag

(1998); in *Photonic Quantum Computing II,* SPIE Proceedings **3385**, 84–94 (1998); Superlattices and Microstructures, **24**(4), (1998) 11 pp.
11. C. Miquel, J. P. Paz, and R. Perazzo, *Physical Review A*, **54**, 2605 (1996).
12. P. Pták and S. Pulmannová, *Orthomodular Structures as Quantum Logics*, Kluwer, Dordrecht (1991), Chap. 5.
13. D. R. Simon, in *Proc. of the 35th Annual Symposium on the Foundations of Computer Science (FOCS)*, ed. S. Goldwasser, IEEE-Computer Society Press, Los Alamitos (1994), pp. 116–123; P. W. Shor, *Ibid.*, pp. 124–134.