数理解析研究所講究録
1066 巻 1998 年 184-188

Convergence of Entanglements into Minimal Uncertainty in Quantum Computing

松 枝 秀 明　　D. W. コーエン
Hideaki Matsueda and David W. Cohen*
Department of Information Science, Kochi University, 2-5-1 Akebono-cho, Kochi 780-8072, Japan
**Department of Mathematics, Smith College, Northampton, Massachusetts 01063, USA*
(September 4, 1998)

A theoretical framework is developed to evaluate the degree of convergence of quantum entangled pure states towards a dispersion-free state of no intrinsic uncertainty. 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.

PACS numbers: 89.70.+c, 03.65.-w, 02.10.B, 32.80.-t

I. INTRODUCTION

Since early 1980's when quantum mechanics was introduced into the study of novel computing processes [1] [2] [3], scientists have conceived various schemes of superparallel computation on the basis of the superposition principle and unitary temporal evolution in quantum mechanics [4] [5] [6].

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

II. THE QUANTUM COMPUTING PROCESS

The quantum computing process begins with an input port, consisting of an 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 $n = a + f$ boxes representing two preparation registers on the left, and some boxes on the right to represent the input register, as shown in Fig.1.

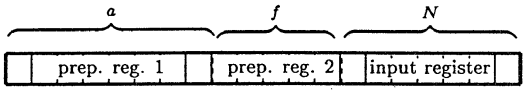

FIG. 1. The input port consisting of preparation registers and an input register.

The computation proceeds via a bank of *row operations*, that are facilitated either by a spatial array of parallel set of quantum gates, or by a temporal series of parallel 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 ground state, driven by the propagation of excited control bit states [7] or by series of external optical excitations.

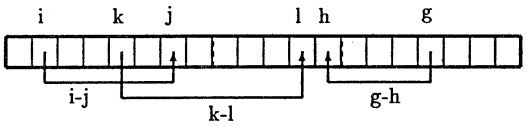

FIG. 2. A parallel collection of C-T operations. Each pair connected by an arrow represents a control-bit/target-bit pair.

The overall process of quantum computation may be understood as consisting of four main steps. Fig.3 represents this situation schematically, for a quantum computer of different methods such as solid state [5], ion trap [8] [9], CQED (cavity quantum electrodynamics) [10], or even NMR (nuclear magnetic resonance) [11] [12].

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 or sessions A,B,C and D.

The first step is to prepare the preparation registers (section A), which is a superposition (minimum entanglement) of the ground state $|0\rangle$ and the excited state $|1\rangle$ in each of a bits, and a ground state in each of f bits. The latter preparation register is used to accomodate intermediate results in some algorithms such as for factoring [4]. We'll call the state of each bit a bit-state [13].

The state of the preparation registers 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 $g_i|0\rangle + e_i|1\rangle$. The initial preparation state is the state of maximum intrinsic uncertainty in the first preparation register, $(\overbrace{\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}}^{a}; \overbrace{0, 0, \ldots, 0}^{f})$ [14], [15]. We'll also call this a state of maximal dispersion, as opposed to a dispersion-free state, where each b_i is either 0 or 1 [15]. It's not hard to see that there are 2^n vectors representing dispersion-free states in the n-dimensional state space.

In the second step, 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'll address that issue in Section III of this paper.

In the case of solid state scheme involving ensemble of quantum dots [5], 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 bit error in an original bit state, stabilization may be increased by dipole-dipole interactions within each ensemble of quantum dots to reduce bit errors [5]. 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.

The third step in the overall computation, represented by section C in Figure 3, is another unitary evolution, converging into the final less dispersive state, or even into a dispersion-free state [16], i.e. a minimal uncertainty state in the first a bits corresponding to the preparation register 1. 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 [4] is an example of such a third step [17] [18] [19]. The iterative combination of two Walsh-Hadamard transforms and a CPS (or conditional phase shift) in a quantum search algorithm [20], and the building up of the correlation function in a quantum simulator [21] may also be considered as examples of the third step.

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

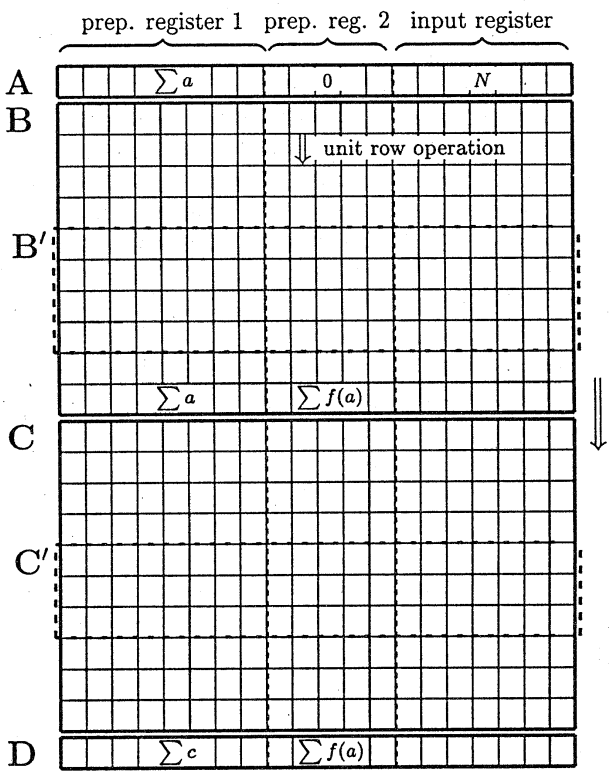

FIG. 3. A schematic diagram representing sequential steps in quantum computing. Section A is the input step, providing the preparation registers 1 and 2 on the left, and the input register on the right. Section B is the first bank of row operations containing the algorithim for making the super-parallel quantum computation. Section C is the bank of row operations such as quantum Fourier transform designed to reduce overall intrinsic uncertainty, and section D is the output step. Sections B and C might contain subsections B′ and C′ for reducing phase errors.

III. DIAGRAM FOR THE EVOLUTION OF LOGICAL STATES

A. 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've created a diagram (Fig.4 [22]) 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 [6].

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 2-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

$$\mathcal{D} = \min_d \{ \| b - d \| \mid d \text{ is a dispersion} - \text{free vector} \}. \quad (1)$$

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 $\mathcal{D}$.

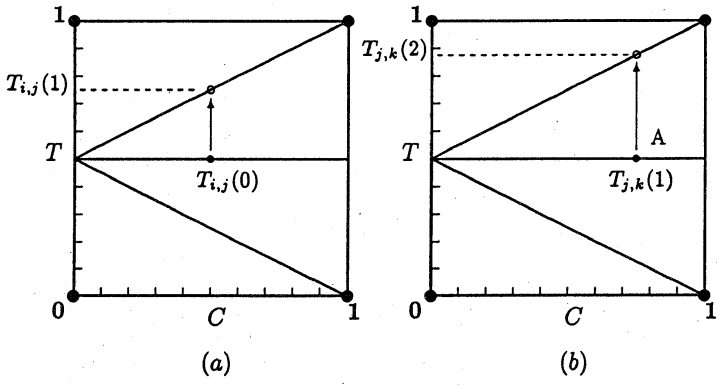

FIG. 4. State space diagrams for control-target bit pairs. The temporal evolution of the truth probability T of the statement *the target bit* b_j *is in state* $|1\rangle$ *at time step* t is plotted with an open circle labled $T_{i,j}(t)$. [The subscript i means that bit b_i is the control bit for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

For a control-target bit (C-T) pair i-j, suppose both the control and target are in an initial superposition of maximal uncertainty: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Then we represent the pair by the closed circle at the center point (0.5, 0.5) in the left diagram, Fig.4 (a). 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're interested in the evolution of the truth values of target bits, we'll label this first point $T_{i,j}(0)$. We'll follow the evolution of the state as it is affected by controlled rotations.

A controlled rotation by angle β around the y axis $\hat{R}^{\beta}_{y\,i,j}$ moves the truth value of the target bit away from the initial superposition point, into some point in the triangular region defined by the ± 45 degree 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.4 (a) or (b). If the angle of rotation is $\pm\frac{\pi}{2}$, the truth value of the target bit increases or decreases so that the C-T pair falls on one of the ± 45 degree lines. This is proven in Subsection III B below.

Suppose the target is subjected to a y-rotation through angle $\frac{\pi}{2}$. 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 $\frac{\pi}{2}$ 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. The states in the sessions B′ and C′ in Fig.3 where phase error is suppressed, are treated separately in the estimation of dispersion.

B. Derivation of the Truth Values

We'll 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 [6] is expressed as

$$\hat{R}^{\beta}_{y} = \begin{pmatrix} \cos\frac{\beta}{2} & -\sin\frac{\beta}{2} \\ \sin\frac{\beta}{2} & \cos\frac{\beta}{2} \end{pmatrix} \quad (2)$$

Applying this to an initial target bit j, in state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with $T_j(0) = \frac{1}{2}$, [we write T_j instead of $T_{i,j}$ because the control bit isn't at issue in this case], we get

$$\hat{R}^{\beta}_{y} \mid T_j(0)\rangle = \begin{pmatrix} \cos\frac{\beta}{2} & -\sin\frac{\beta}{2} \\ \sin\frac{\beta}{2} & \cos\frac{\beta}{2} \end{pmatrix} \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right]$$

$$= \frac{1}{\sqrt{2}} \left[(\cos\frac{\beta}{2} \mp \sin\frac{\beta}{2}) \mid 0\rangle + (\pm\cos\frac{\beta}{2} + \sin\frac{\beta}{2}) \mid 1\rangle \right]. \quad (3)$$

Thus, the free rotation results in

$$T_j(1) = \left| \frac{1}{\sqrt{2}} (\pm\cos\frac{\beta}{2} + \sin\frac{\beta}{2}) \right|^2. \quad (4)$$

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

$$\begin{aligned}\Delta T_{i,j} &= (T_j(1) - T_j(0))C \\ &= \left[\left|\frac{1}{\sqrt{2}}(\pm\cos\frac{\beta}{2} + \sin\frac{\beta}{2})\right|^2 - \left|\frac{1}{\sqrt{2}}\right|^2\right]C \\ &= \left[\frac{1}{2}(1 \pm \sin\beta) - \frac{1}{2}\right]C \\ &= \pm\frac{\sin\beta}{2}C, \end{aligned} \tag{5}$$

which gives the new T value:

$$T_{i,j}(1) = T_{i,j}(0) + \Delta T_{i,j}. \tag{6}$$

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

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

The controlled controlled not (CCN) operation $\hat{P}_{CCNij,k}$ (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:

$$\hat{P}_{CCNij,k} = \hat{S}^{\frac{\pi}{2}}_{j,i}\hat{S}^{\frac{\pi}{2}}_{i,j}\hat{R}^{\pi/2}_{xi,k}\hat{P}_{CNi,j}\hat{R}^{3\pi/2}_{xj,k}\hat{P}_{CNi,j}\hat{R}^{\pi/2}_{xj,k}, \tag{7}$$

where $\hat{R}^{\alpha}_{xj,k}$ denotes a CR operation around the x axis by angle α, $\hat{P}_{CNi,j}$ a CN, and $\hat{S}^{\gamma}_{i,j}$ a CPS by angle γ respectively [6]. Therefore, the overall change $\Delta T_{ij,k}$ 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 y axis $\hat{R}^{\beta}_y$ to a general superposition state $|\, T_k(0)\rangle = g|0\rangle \pm e|1\rangle$ gives

$$\begin{aligned}\hat{R}^{\beta}_y \,|\, T_k(0)\rangle &= \begin{pmatrix}\cos\frac{\beta}{2} & -\sin\frac{\beta}{2} \\ \sin\frac{\beta}{2} & \cos\frac{\beta}{2}\end{pmatrix}\left[g\begin{pmatrix}1\\0\end{pmatrix} \pm e\begin{pmatrix}0\\1\end{pmatrix}\right] \\ &= \left[(g\cos\frac{\beta}{2} \mp e\sin\frac{\beta}{2}) \,|\, 0\rangle + (g\sin\frac{\beta}{2} \pm e\cos\frac{\beta}{2}) \,|\, 1\rangle\right] \end{aligned} \tag{8}$$

where $|\, g\,|^2 + |\, e\,|^2 = 1$. Then, by a procedure simillar to that leading to eq.(5),

$$\Delta T_{i,j} = \left[(|\, g\,|^2 - |\, e\,|^2)\frac{1-\cos\beta}{2} \pm (ge^* + g^*e)\frac{\sin\beta}{2}\right]C, \tag{9}$$

of which eq.(5) is a special case, and * denotes the complex conjugate.

Furthermore, for a controlled rotation by a fractional angle $\beta = \frac{\pi}{2m}$, the following is obtained using eq.(9).

$$\begin{aligned}\Delta T_{i,j} &= \frac{1}{2}\left[(|\, g\,|^2 - |\, e\,|^2)\left(\frac{\beta^2}{2} - \frac{\beta^4}{24} + \frac{\beta^6}{720} - \cdots\right)\right. \\ &\qquad \left.\pm(ge^* + g^*e)\left(\beta - \frac{\beta^3}{6} + \frac{\beta^5}{120} - \cdots\right)\right]C \qquad (10) \\ &= \frac{1}{2}\left[\pm(ge^* + g^*e)\beta\right]C + W \qquad (11)\end{aligned}$$

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

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

$$\frac{1}{\Delta T_{i,j}} = \frac{1}{\beta C + W} \approx \frac{1}{\beta C} = \frac{4m}{\pi} \sim 1.27m, \tag{12}$$

assuming the new target bits always begin in the maximally uncertain state. The upper bound of the accumulated error in the consecutive rotation is estimated as

$$\begin{aligned}W \times (\text{number of steps} \approx \tfrac{1}{\beta C}) &< \frac{\beta}{4} + \frac{\beta^2}{2} \\ \Longrightarrow 0 \quad \text{for } \beta \to 0;\ &i.e.\, m \to \infty. \end{aligned} \tag{13}$$

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

IV. CONCLUSIONS

We have developed a way to estimate intrinsic uncertainties in provisional results of quantum computations. We've also calculated the reduction of uncertainty resulting from particular controlled rotations 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 make the provisional solutions converge into a dispersion-free state having minimal uncertainty, is 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 various kinds of quantum computing schemes. Such a tool may be effective

for designing and refining quantum algorithms, and for implementing quantum systems, as well as an aid for understanding quantum entanglements.

ACKNOWLEDGMENTS

This work is 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.

[1] P. Benioff, J. Statistical Phys., **22**, 563 (1980); Phys. Rev. Lett. **48**, 1581 (1982).

[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); Optics News **11**, 11 (1985); Foundations of Phys. **16**, 507 (1986); *Feynman Lectures on Computation*, eds. A. J. G. Hey and R. W. Allen (Addison-Wesley, Reading, Massachusetts, 1996).

[3] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985); Proc. R. Soc. Lond. A **425**, 73 (1989).

[4] P. W. Shor, in *Proc. of the 35th Annual Symp. on the Foundations of Computer Science (FOCS)*, ed. S. Goldwasser (IEEE Computer Society Press, Los Alamitos, 1994), pp.124–134.

[5] H. Matsueda, and S. Takeno, IEICE Trans. Fundamentals Electron., Commun. and Computer Sci., **E80-A (9)** (1997) 1610-1615; 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) invited paper at Special Session "Toward Nanoelectronics", pp.265-270; in *Unconventional Models of Computation*, eds. C. S. Calude, J. Casti, and M. J. Dinneen (DMTCS Series, Springer-Verlag, Singapor, 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 *Proc. 1998 SPIE Quantum Computation Conference, at AeroSense'98* (Orlando, 1998) SPIE Proc. vol.**3385**, pp.84-94.

[6] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[7] In the case of solid state implementation, the C-T operations are executed by methods of clock signals and biased band gap [5].

[8] S. R. Jefferts, C. Monroe, E. W. Bell, and D. J. Wineland, Phys. Rev. A **51**, 3112 (1995); C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).

[9] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995); M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 44 (1994).

[10] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).

[11] D.G.Cory and T.F.Havel, 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.87-91.

[12] N.A.Gershenfeld and I.L.Chuang, Science **275**, 350 (1997).

[13] In a solid state scheme, to increase resistance of the bits to decohering agitations, each bit better be an ensemble of quantum dots [5], which fact is usually emphasized by writing the bit states as $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$. We'll omit the tildes in this paper, however, with a reminder to the reader that our bits could be ensembles.

[14] P. Pták and S. Pulmannová, *Orthomodular Structures as Quantum Logics* (Kluwar, Dordrecht, 1991) Chap. 5.

[15] D. W. Cohen, *An Introduction to Hilbert Space and Quantum Logic* (Springer, New York, 1989) Chaps. 3 and 6; the intrinsic uncertainty is also called ontological uncertainty.

[16] This convergence and collapses of wave functions into a limited number of states lead to solutions, from which the period of $f(a)$ ($= x^a \ mod \ N$, for a chosen x) will be derived in an algorithm to factor a number N [4]. The state after the partial collapse into one of the groups of $f(a)$, is called disentanglement between registers for a and for $f(a)$, in A. Peres, Superlattices and Microstructures, **23**, 373 (1998).

[17] A. Barenco, A. Ekert, K.-A. Suominen, and P. Törmä, Phys. Rev. A **54**, 139 (1996).

[18] C. Miquel, J. P. Paz, and R. Perazzo, Phys. Rev. A **54**, 2605 (1996).

[19] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A **54**, 1034 (1996).

[20] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[21] S. Lloyd, Science **273**, 1073 (1996).

[22] H. Matsueda, and D. W. Cohen, submitted to Int. J. Theor. Phys. (1998).