## **Preserving Coherence in Quantum Computation by Pairing Quantum Bits**

Lu-Ming Duan and Guang-Can Guo\*

Department of Physics and Nonlinear Science Center, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China

(Received 24 March 1997)

A scheme for protecting quantum states from both independent and cooperative decoherence is proposed. The scheme operates by pairing each qubit (two-state quantum system) with an ancilla qubit and by encoding the states of the qubits into corresponding coherence-preserving states of qubit pairs. In this scheme, amplitude damping (loss of energy) as well as phase damping (dephasing) is prevented by a strategy called "free-Hamiltonian elimination." We further extend the scheme to include quantum gate operations and show that loss and decoherence during such operations can also be prevented. [S0031-9007(97)03897-0]

PACS numbers: 89.70.+c, 03.65.Bz, 42.50.Dv

Soon after the idea of quantum computation became an active part of current research, through the innovative work of Shor on factorization [1,2], decoherence was recognized as a major problem that cannot be ignored [3], especially when one is interested in practical applications. Quantum computers act as sophisticated nonlinear interferometers. The coherent interference pattern between the multitude of superpositions is essential for taking advantage of quantum parallelism. However, decoherence of the qubits caused by the interaction with environment will collapse the state of the quantum computer and make the information no longer correct. To overcome this fragility of quantum information, Shor, and independently Steane, inspired by the theory of classical error correction, proposed the first two quantum errorcorrecting codes (QECCs), i.e., the nine-bit code [4] and the seven-bit code [5], which are able to correct errors that occur during the storage of qubits. Furthermore, a general theory for quantum error correction was presented by Calderbank and Shor [6], and independently by Steane [7]. Following this work, many new QECCs have since been discovered [8–21]. The discovery of QECCs has revolutionized the field of quantum information.

Quantum errors are induced by the interaction of the qubits with environment. If we know more about this interaction, simpler codes can be found. In the previous analyses of decoherence [3], the qubits are assumed to interact independently with separate environments. In practice, however, cooperative effects may take place between the qubits. For example, the qubits in ion-trapped computers are believed to be decohered cooperatively [22,23]. References [24,25] considered another extreme case, i.e., all the qubits interact with the same environment. If only the phase damping is considered, as the result, the qubits are found to be decohered collectively. For some of the input states (called the subdecoherent states), the qubits are decohered much slower; and for some others (called the superdecoherent states), they are decohered much faster. The phenomenon of superdecoherence vs subdecoherence is very similar to, but not the same as, the process of superradiance vs subradiance more commonly encountered in literature [26]. As was pointed out in Ref. [24], superradiance is a process of collective radiation by a group of closely spaced atoms, while superdecoherence is due to collective entanglement between qubits and environment. A simple code has been suggested in [24] for reducing this collective decoherence.

Independent decoherence and collective decoherence are extreme cases. With these two ideal circumstances, we ask, what about the real situation? It seems a combination of these two cases may be more practical. If the qubits are close, they tend to be decohered collectively; and if they are departed, the assumption of independent decoherence may be more reasonable. In this Letter, we propose a scheme for reducing decoherence in general cases. The scheme operates by pairing each qubit with an ancilla. The two qubits in each pair are set close so that they interact with the same modes of the environment. But the qubits in different pairs are allowed to be decohered independently or cooperatively. Because of the collective dissipation in each pair, coherence-preserving states of the qubit pairs are found to exist. The stored information is protected from decoherence by encoding the states of the qubits into the corresponding coherence-preserving states of the qubit pairs. In fact, the use of coherence-preserving states for preventing errors induced by the pure dephasing has been described by Chuang and Yamamoto [27,28] and also by Palma et al. [24]. Here we adopt the previously known idea of using such states of qubit pairs. We propose a strategy called the "free-Hamiltonian elimination" to provide a general method to set up the coherence-preserving states. By this strategy, amplitude damping is prevented as well as phase damping. Amplitude damping sometimes is the main source of decoherence [23,29,30]. Furthermore, we show in this Letter that the scheme can be extended to prevent decoherence in quantum gate operations. Coherence is preserved in the gate operations by substituting the logic gates for the qubits with those for the qubit pairs. Preserving coherence during quantum gate operations is a significant step towards realizing the fault-tolerant quantum computation [15].

First, we consider the stored information, i.e., the qubits in quantum memory, which can be described by Pauli's operators  $\vec{\sigma}_l$  (*l* marks different qubits). The environment is modeled by a bath of oscillators with infinite degrees of freedom. Each qubit interacts with some (usually infinite) modes of the environment. The bath modes coupling with the *l* qubit are indicated by  $a_{\omega l}$  ( $\omega$  varies from 0 to  $\infty$ ). For different  $l_1$  and  $l_2$ , some of the modes  $a_{\omega l_1}$  and  $a_{\omega l_2}$  are possibly the same and some of them are different. We use the notation  $\bigcup_{l=1}^{L} A_l$  to indicate the joint sum of  $A_l$ , where all  $A_l$  are bath operators. For example,  $\bigcup_{l=1}^{2} A_l = A_1 + A_2$  if  $A_1$  and  $A_2$  belong to different modes; and  $\bigcup_{l=1}^{2} A_l = A_1$  if  $A_1$  and  $A_2$  are the same. With this notation, the whole Hamiltonian describing the general dissipation of the qubits, including the phase damping and the amplitude damping, has the following form (setting  $\hbar = 1$ ):

$$H_{L} = \omega_{0} \sum_{l=1}^{L} \sigma_{l}^{z} + \sum_{\omega} \bigcup_{l=1}^{L} (\omega a_{\omega l}^{+} a_{\omega l}) + \sum_{l=1}^{L} \sum_{\omega} [(\lambda^{(1)} \sigma_{l}^{x} + \lambda^{(2)} \sigma_{l}^{y} + \lambda^{(3)} \sigma_{l}^{z}) g_{\omega l} (a_{\omega l}^{+} + a_{\omega l})],$$
(1)

where *L* is the number of qubits and the coupling constants  $g_{\omega l}$  may be dependent of  $\omega$  and *l*. The ratio  $\lambda^{(1)}:\lambda^{(2)}:\lambda^{(3)}$  is determined by the type of dissipation. For example, if  $\lambda^{(1)} = \lambda^{(2)} = 0$ , it describes the phase damping; and if  $\lambda^{(3)} = 0$ , it is the amplitude damping.

Now we pair each qubit with an ancilla. The ancilla of the *l* qubit is indicated by l'. The two qubits *l* and l' in the pair are set close so that they interact with the same modes of the environment. With this condition, the dissipation of the *L* qubit pairs is described by the Hamiltonian

$$H_{2L} = \omega_0 \sum_{l=1}^{L} (\sigma_l^z + \sigma_{l'}^z) + \sum_{\omega} \bigcup_{l=1}^{L} (\omega a_{\omega l}^+ a_{\omega l}) + \sum_{l=1}^{L} \sum_{\omega} \{ [\lambda^{(1)} (\sigma_l^x + \sigma_{l'}^x) + \lambda^{(2)} (\sigma_l^y + \sigma_{l'}^y) + \lambda^{(3)} (\sigma_l^z + \sigma_{l'}^z) ] g_{\omega l} (a_{\omega l}^+ + a_{\omega l}) \}.$$
(2)

The following step of our strategy is to eliminate the influence of the free Hamiltonian  $H_0 = \omega_0 \sum_{l=1}^{L} (\sigma_l^z + \sigma_{l'}^z)$  of the qubits. To attain this goal, we introduce a homogeneous classical driving electromagnetic field which acts on all the qubit pairs. The ancillary Hamiltonian describing the driving process is

$$H_{\rm drv} = \sum_{l=1}^{L} [g(\sigma_l^+ + \sigma_{l'}^+) + g^*(\sigma_l^- + \sigma_{l'}^-)] = \sum_{l=1}^{L} [g_1(\sigma_l^x + \sigma_{l'}^x) + g_2(\sigma_l^y + \sigma_{l'}^y)].$$
(3)

By adjusting the intensity and the phase of the driving field, we can choose the driving constants  $g_1$  and  $g_2$  to

satisfy  $g_1:g_2:\omega_0 = \lambda^{(1)}:\lambda^{(2)}:\lambda^{(3)}$ . Then the whole Hamiltonian is simplified to

$$H = H_{2L} + H_{drv}$$

$$= \sum_{l=1}^{L} \left\{ (S_l + S_{l'}) \left[ \frac{\omega_0}{\lambda^{(3)}} + \sum_{\omega} g_{\omega l} (a_{\omega l}^+ + a_{\omega l}) \right] \right\}$$

$$+ \sum_{\omega} \bigcup_{l=1}^{L} (\omega a_{\omega l}^+ a_{\omega l}), \qquad (4)$$

where we have let  $S_l = \lambda^{(1)} \sigma_l^x + \lambda^{(2)} \sigma_l^y + \lambda^{(3)} \sigma_l^z$ .

Suppose the initial state of the qubit pairs is a coeigenstate of all the operators  $S_l + S_{l'}$ , with the eigenvalues  $m_l$ , respectively. The environment state is indicated by  $|\Psi_{env}(0)\rangle$ . Under the Hamiltonian (4), at time *t* the state of the whole system evolves into

$$|\Psi(t)\rangle = e^{-iHt} (|\Psi(0)\rangle \otimes |\Psi_{\rm env}(0)\rangle) = |\Psi(0)\rangle \otimes e^{-it\left\{\sum_{l=1}^{L} m_l \left[\omega_0/\lambda^{(3)} + \sum_{\omega} g_{\omega l}(a_{\omega l}^+ + a_{\omega l})\right] + \sum_{\omega} \bigcup_{l=1}^{L} (\omega a_{\omega l}^+ a_{\omega l})\right\}} |\Psi_{\rm env}(0)\rangle.$$
(5)

So in this case all the qubit pairs undergo no decoherence, though they are interacting with the environment. Because of this property, we call the eigenstates of all the operators  $S_l + S_{l'}$  the coherence-preserving states.

We briefly discuss the coherence-preserving states. The Hermitian operator  $S_l$  satisfies  $tr(S_l) = 0$ , so its two eigenstates, without loss of generality, can be indicated by  $|\pm 1\rangle_l$ , with the eigenvalues  $\pm a$ , respectively. The computation basis states  $|\pm\rangle_l$  are eigenstates of the operator  $\sigma_l^z$ . The

states  $|\pm 1\rangle_l$  may differ with  $|\pm\rangle_l$  by a single-qubit rotation operation  $R_l(\theta)$ , i.e.,  $|\pm 1\rangle_l = R_l(\theta) |\pm\rangle_l$ , where  $\theta$  depends on the type of the dissipation. The coherence-preserving states can be easily constructed from the states  $|\pm 1\rangle_l$ . The largest eigenspace of the operator  $S_l + S_{l'}$  is a twodimensional space spanned by the eigenstates  $|+1, -1\rangle_l$ and  $|-1, +1\rangle_l$ , with the eigenvalue  $m_l = 0$ . So there exists a one-to-one map from the two-dimensional space of a qubit onto the two-dimensional coherence-preserving state space of a qubit pair. The general input states of *L* qubits can be expressed as

$$|\Psi_L\rangle = \sum_{\{i_l\}} c_{\{i_l\}} |\{i_l\}\rangle, \qquad (6)$$

where  $\{i_l\}$  is an abbreviation of the notation  $i_1, i_2, ..., i_L$ and  $i_l = \pm 1, l = 1, 2, ..., L$ . We encode the state (6) into the following coherence-preserving state of *L* qubit pairs

$$|\Psi_{2L}\rangle_{\rm coh} = \sum_{\{i_l\}} c_{\{i_l\}} |\{i_l, -i_l\}\rangle,$$
 (7)

where  $\{i_l, -i_l\}$  indicates  $i_1, -i_1, i_2, -i_2, ..., i_L, -i_L$ . The encoding can be fulfilled by the quantum CNOT (Controlled NOT) operations  $C_{ij}$ , where the first subscript of  $C_{ij}$ refers to the control bit and the second to the target. The ancillas are prearranged in the state  $|\Psi_{1'2'\cdots L'}\rangle = |+1\rangle_{1'} \otimes$  $|+1\rangle_{2'} \otimes \cdots \otimes |+1\rangle_{L'}$ . Let the joint operation  $C'_{ij}(\theta) =$  $R_i(\theta)R_j(\theta)C_{ij}R_i(-\theta)R_j(-\theta)$ , where  $R_i(\theta)$  is the rotation operation acting on the *i* qubit, we thus have

$$|\Psi_L\rangle \otimes |\Psi_{1'2'\cdots L'}\rangle \xrightarrow{C'_{11'}(\theta)C'_{22'}(\theta)\cdots C'_{LL'}(\theta)} |\Psi_{2L}\rangle_{\rm coh} .$$
(8)

The decoding can be similarly realized by applying the operation  $C'_{11'}(\theta)C'_{22'}(\theta)\cdots C'_{LL'}(\theta)$  again. The encoded states  $|\Psi_{2L}\rangle_{\text{coh}}$  undergo no decoherence in the memory.

By pairing the qubits, the number of qubits is expanded from *L* to 2*L*. So the efficiency  $\eta$  of this scheme is  $\frac{1}{2}$ . There is a possible way to raise the efficiency. If 2*m* qubits are set close so that they all interact with the same modes of the environment, the largest eigenspace of the operator  $S_1 + S_2 + \cdots + S_{2m}$  becomes a  $\binom{2m}{m}$ -dimensional state space, with the eigenvalue  $m_l = 0$ . By encoding the input states of 2mL qubits into the coherence-preserving states of the qubit clusters, each cluster consisting of 2m qubits, the maximum efficiency  $\eta_m$  attains

$$\eta_m = \frac{L}{2mL} \log_2 {\binom{2m}{m}} \approx 1 - \frac{1}{4m} \log_2(\pi m), \quad (9)$$

where the approximation is taken under the condition  $m \gg 1$ . So the efficiency  $\eta_m$  is near to one if *m* is large. Of course, with *m* increasing, it becomes harder and harder to set all the *m* qubits close so that they are decohered collectively.

In the above, we have dealt with the qubits in the memory. Now we extend the scheme to include quantum gate operations. In quantum error-correction schemes, a significant step forward in this direction has recently been made by the idea of fault-tolerant implementation of quantum logic gates [15–17]. Here we show our coherence-preserving scheme can, at least in principle, prevent decoherence during the gate operations as well as during the storing process. The Hamiltonian for the gate operation is indicated by  $H_g$ . The initial state  $|\Psi(0)\rangle_{\{m_i\}}$  of the qubit pairs is a co-eigenstate of all the operators  $S_l + S_{l'}$ , with the eigenvalue  $m_l$ , respectively. If the gate Hamiltonian  $H_g$  satisfies the following condition:

$$[H_g, S_l + S_{l'}] = n_l, \qquad l = 1, 2, \dots, L, \qquad (10)$$

where all  $n_l$  are numbers, at time *t* the whole system, including the environment, will evolve into

$$|\Psi(t)\rangle = e^{-iH_g t} |\Psi(0)\rangle_{\{m_l\}} \otimes e^{-it \left\{ \sum_{l=1}^{L} (m_l - (1/2)n_l) \left[ \omega_0 / \lambda^{(3)} + \sum_{\omega} g_{\omega l} (a_{\omega l}^+ + a_{\omega l}) \right] + \sum_{\omega} \bigcup_{l=1}^{L} (\omega a_{\omega l}^+ a_{\omega l}) \right\}} |\Psi_{\text{env}}(0)\rangle.$$
(11)

Therefore, in this case no decoherence occurs during the gate operation. Equation (10) is also a necessary condition for preserving coherence during the gate operation.

Now we show, with the constraint (10), any unitary transformations can still be constructed. To demonstrate this, we need only give a universal gate operation satisfying Eq. (10). It has been proven that almost any two-bit gates are universal [31,32]. In particular, the following is a universal gate operation [33]:

$$U_{l_1 l_2} = |-1\rangle_{l_1 l_1} \langle -1|I_{l_2} + |+1\rangle_{l_1 l_1} \langle +1|V_{l_2}, \qquad (12)$$

where  $I_{l_2}$  is a 2 × 2 unit matrix and the unitary matrix  $V_{l_2}$  is given by

$$V_{l_2}(\alpha, \theta, \phi) = \begin{pmatrix} e^{i\alpha}\cos(\theta) & -ie^{i(\alpha-\phi)}\sin(\theta) \\ -ie^{i(\alpha+\phi)}\sin(\theta) & e^{i\alpha}\cos(\theta) \end{pmatrix}.$$
(13)

The parameters  $\alpha$ ,  $\theta$ ,  $\phi$  are irrational multiples of  $\pi$  and of each other. Now we consider the following gate operation for two qubit pairs  $l_1 l'_1, l_2 l'_2$ :

$$U_{l_1 l'_1 l_2 l'_2} = |-1, +1\rangle_{l_1 l'_1 l_1 l'_1} \langle -1, +1|I_{l_2 l'_2} + |+1, -1\rangle_{l_1 l'_1 l_1 l'_1} \langle +1, -1|V_{l_2 l'_2}, \quad (14)$$

where  $I_{l_2 l'_2}$  is a 4 × 4 unit matrix and  $V_{l_2 l'_2}$  becomes (in the basis { $|-1, -1\rangle$ ,  $|-1, +1\rangle$ ,  $|+1, -1\rangle$ ,  $|+1, +1\rangle$ })

$$V_{l_2 l'_2}(\alpha, \theta, \phi) = \begin{pmatrix} 1 & e^{i\alpha} \cos(\theta) & -ie^{i(\alpha-\phi)} \sin(\theta) \\ -ie^{i(\alpha+\phi)} \sin(\theta) & e^{i\alpha} \cos(\theta) & 1 \end{pmatrix}.$$
(15)

After decoding the coherence-preserving states of the qubit pairs into the original states of the qubits, the operation (14) for the qubit pairs just corresponds to the operation (12) for the qubits. So Eq. (14) gives a universal gate operation for the qubit pairs. For any parameters  $\alpha$ ,  $\theta$ ,  $\phi$ , it is easy to check that  $U_{l_1l'_1l_2l'_2}$  satisfies

$$[U_{l_1l'_1l_2l'_2}, S_{l_1} + S_{l'_1}] = [U_{l_1l'_1l_2l'_2}, S_{l_2} + S_{l'_2}] = 0, \quad (16)$$

so the generators of  $U_{l_1l'_1l_2l'_2}$ , i.e., the gate Hamiltonians, also commute with the operators  $S_l + S_{l'}$ . The constraint (10) is therefore satisfied.

In the above, we have shown coherence can be preserved during gate operations if one substitutes the gates for the qubits with those for the qubit pairs. Of course, after this substitution, the demonstration of these logic gates becomes more involved.

Finally, we compare this scheme with quantum error correction. In the error correction schemes, the decoherence time for a qubit is not increased. One retrieves the useful information from the decohered state by introducing some redundancy. Contrary to this, in our scheme, the decoherence time for the qubits is much increased. (In the ideal case, it is increased to infinity.) We prevent error rather than correct error. So, like Refs. [34,35], this scheme belongs to the class of error prevention schemes. The schemes of Refs. [34,35] are based on the quantum Zeno effect. The decoherence is reduced by continuously measuring the qubits in some basis. The critical idea of our scheme is pairing the qubits and substituting the gate operations for the qubits with those for the qubit pairs. This scheme has some attractive features. First, it covers a large range of decoherence, including the cooperative decoherence and the independent decoherence. The scheme works whether the decoherence is caused by the amplitude damping or by the phase damping. Second, it has a high efficiency. We need at most two qubits to encode a qubit. Third, the encoding and the decoding in this scheme is quite simple. It needs only L times quantum CNOT operations and some single-bit rotation operations to encode and decode the qubits. Last, the scheme is relatively easy to extend for preventing decoherence in quantum gate operations. Of course, compared with QECCs, this scheme also has an obvious disadvantage, that is, the noise parameters  $\lambda^{(i)}$  in the Hamiltonian (1) should be known accurately and must not change in an unknown way.

A crucial assumption for this scheme is that two gubits can be set close so that they are decohered collectively. Reference [36] shows this is the case if distance *d* between the two qubits satisfies  $d \ll \overline{\lambda}$ , where  $\overline{\lambda}$  is the mean effective wave length of the noise field. In practice, such as in the ion-trapped quantum computers, where the noise is from the thermal variation of the qubits [23], this assumption seems reasonable. It is now well understood that quantum errors are harder to correct than classical errors, since there appear new kinds of errors, such as phase errors and bit-phase errors. Here we show, if we have some knowledge of the interaction of the qubits with the environment, quantum errors are easier to prevent. This supports a commonplace, but fundamentally important, observation that the more one knows about the noise, the easier it is to correct for it.

This project was supported by the National Natural Science Foundation of China.

Society Press, New York, 1994), pp. 124-134.

- [2] L. L. Chuang, R. Laflamme, P. W. Shor, and W. K. Zurek, Science 270, 1633 (1995).
- [3] W.G. Unruh, Phys. Rev. A 51, 992 (1995).
- [4] P.W. Shor, Phys. Rev. A 52, R2493 (1995).
- [5] A. M. Steane, Phys. Rev. Lett. 77, 793 (1996).
- [6] A. R. Calderbank and P. W. Shor, Phys. Rev. A 54, 1098 (1996).
- [7] A. M. Steane, Proc. R. Soc. London A 452, 2551 (1996).
- [8] R. Laflamme, C. Miguel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. 77, 198 (1996).
- [9] A. Ekert and C. Macchiavello, Phys. Rev. Lett. 77, 2585 (1996).
- [10] D. Gottesman, Phys. Rev. A 54, 1844 (1996).
- [11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996).
- [12] E. Knill and R. Laflamme, Phys. Rev. A 55, 900 (1997).
- [13] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Phys. Rev. Lett. 78, 465 (1997).
- [14] A. M. Steane, Phys. Rev. A 54, 4741 (1996).
- [15] P.W. Shor, LANL eprint quant-ph/9605011.
- [16] D. P. DiVincenzo and P. W. Shor, Phys. Rev. Lett. 77, 3260 (1996).
- [17] W. H. Zurek and R. Laflamme, Phys. Rev. Lett. 77, 4683 (1996).
- [18] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, LANL eprint quant-ph/9608006.
- [19] A. Steane, LANL eprint quant-ph/9608026.
- [20] P.W. Shor and R. Laflamme, Phys. Rev. Lett. 78, 1600 (1997).
- [21] R. Cleve, LANL eprint quant-ph/9612048.
- [22] J. I. Cirac and P. Zoller, Phys. Rev. Lett. 74, 4091 (1995).
- [23] A. Garg, Phys. Rev. Lett. 77, 964 (1996).
- [24] G. M. Palma, K. A. Suominen, and A. K. Ekert, Proc. R. Soc. London A 452, 567 (1996).
- [25] L.M. Duan and G.C. Guo, LANL eprint quant-ph/ 9612003.
- [26] See, for example, E. A. Power, J. Chem. Phys. 46, 4297 (1967); G. S. Agarwal, *Quantum Optics*, Springer Tracts in Modern Physics Vol. 70 (Springer-Verlag, Berlin, 1974); R. G. DeVoe and R. G. Brewer, Phys. Rev. Lett. 76, 2049 (1996).
- [27] I.L. Chuang and Y. Yamamoto, Phys. Rev. A 52, 3489 (1995).
- [28] I. L. Chuang and Y. Yamamoto, Phys. Rev. Lett. 76, 4281 (1996).
- [29] M.B. Plenio and P.L. Knight, Phys. Rev. A 53, 2986 (1996).
- [30] D.F.V. James, E.H. Knill, R. Laflamme, and A.G. Petschek, Phys. Rev. Lett. **77**, 3240 (1996).
- [31] S. Lloyd, Phys. Rev. Lett. 75, 346 (1995).
- [32] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London A 449, 669 (1995).
- [33] A. Barenco, Proc. R. Soc. London A 449, 679 (1995).
- [34] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A 54, R1745 (1996).
- [35] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello, LANL eprint quant-ph/ 9604028.
- [36] L.M. Duan and G.C. Guo, LANL eprint quant-ph/ 9703036.

<sup>\*</sup>Electronic address: gcguo@sunlx06.nsc.ustc.edu.cn

<sup>[1]</sup> P.W. Shor, in *Proceedings of the 35th Annual Symposium* on Foundations of Computer Science (IEEE Computer