Entanglement Purification for Quantum Computation

W. Dür and H.-J. Briegel

Sektion Physik, Ludwig-Maximilians-Universität München, Theresienstrasse 37, D-80333 München, Germany

(Received 10 October 2002; published 13 February 2003)

We show that thresholds for fault-tolerant quantum computation are solely determined by the quality of single-system operations if one allows for d-dimensional systems with $8 \leq d \leq 32$. Each system serves to store one logical qubit and additional auxiliary dimensions are used to create and purify entanglement between systems. Physical, possibly probabilistic two-system operations with error rates up to 2/3 are still tolerable to realize deterministic high-quality two-qubit gates on the logical qubits. The achievable error rate is of the same order of magnitude as of the single-system operations. We investigate possible implementations of our scheme for several physical setups.

DOI: 10.1103/PhysRevLett.90.067901 PACS numbers: 03.67.Lx, 03.65.Ud

Much of the theoretical and experimental interest in quantum information theory in the last decade has been devoted to quantum computation. The finding of quantum algorithms which offer an (exponential) speedup over their best known classical counterparts [1] as well as the possibility to operate a quantum computer in a noisy environment in a fault-tolerant way [2] can be counted as milestones of this investigation. Since then, many theoretical proposals to implement quantum computation in various physical systems, ranging from trapped atoms or ions to NMR and quantum dots, have been put forward and experimental implementation of basic quantum logic gates was demonstrated in several of these systems [3]. Unfortunately, there are stringent requirements which have to be fulfilled before a universal quantum computer can operate in a fault-tolerant way. These include gate error rates below a threshold value which is of the order of 10^{-4}–10^{-5}, still far beyond experimentally reachable accuracies. On the other hand, in quantum communication it was found [4,5] that the requirements to ensure secure communication over arbitrary distances are much less stringent. Indeed, error rates of the order of several percent are tolerable in this case [4,5]. The main tool to achieve secure [6] quantum communication over arbitrary distances is *entanglement purification* [7]. But is entanglement purification also useful for quantum computation? Does it allow one to increase thresholds for tolerable errors? In this Letter, we answer these questions in a positive way. We show that one can indeed use entanglement purification to increase the quality of two-system operations by several orders of magnitude. This in turn implies that *the requirements for fault-tolerant quantum computation can be met if the quality of single-system operations is sufficiently high* (almost) independently of the quality of two-system operations.

We consider a collection of distinct physical systems which shall be used to perform a quantum computation. Each of the systems serves to store at least one qubit of information. That such a setup can be used for fault-tolerant quantum computation requires — among others — the ability to perform both arbitrary unitary operation on each of the distinct systems and controlled interactions between different systems (i.e., nonlocal operations) with error rates below 10^{-4}–10^{-5} [8]. However, not all of these operations are equally difficult to perform. For example, it may be easy to manipulate each of the distinct systems in a controlled way while interactions between different systems may be very difficult to achieve. Consider the example where each system corresponds to the polarization degrees of freedom of a photon. While the state of each photon may be manipulated quite easily by means of linear optical elements, controlled deterministic interactions between photons (e.g., using Kerr nonlinearities) are very difficult to achieve. Also for trapped neutral atoms or ions, it is much easier to manipulate the electronic states of each particle by means of well controllable laser pulses than to achieve a controlled interaction between two particles.

Having already initiated the discussion with atoms and ions, we refer to each physical system as "particle." It is, however, not a necessary requirement of our analysis that each distinct system corresponds to a real particle; it could also be some abstract system. In what follows, we carefully distinguish between operations on a single particle and operations which require controlled interaction between two particles. Our results are applicable to all situations where single-particle operations are much easier to implement than two-particle operations.

In order to simplify the description and discussion of our scheme, we impose a virtual tensor-product structure; that is, we divide each physical d-level system (particle) into n virtual qubit subsystems [9], i.e., $d = 2^n$. We refer to different particles as $A, B, C, \ldots, Z$, while virtual subsystems of, say, particle A are denoted by $A_1, A_2, A_3, \ldots, A_n$. The corresponding Hilbert space is denoted by $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \ldots \mathcal{H}_Z$ with $\mathcal{H}_X = \mathcal{H}_{X_1} \otimes \mathcal{H}_{X_2} \otimes \ldots \mathcal{H}_{X_n} \cong (\mathbb{C}^2)^{\otimes n}$, $X \in \{A, B, \ldots, Z\}$.

A brief summary of the scheme follows. Each particle X serves to store and manipulate one logical qubit in its virtual subsystem X_1. A (noisy) two-particle interaction is used to create entanglement between the additional virtual subsystems X_k, $k \geq 2$ of different particles. This noisy entanglement is efficiently purified using a novel entanglement purification scheme based on nested entanglement pumping which requires less than five virtual subsystems, i.e., $d \leq 32$. The entanglement is then used—together with high-quality single-particle operations—to implement in a deterministic way two-particle gates between the logical qubits. For instance, a CNOT gate [10] between A_1 and B_1 can be realized using schemes presented in Refs. [11–13]. We find that the physical two-particle gate need only be weakly entangling or may even be probabilistic (i.e., the operation needs to be successful only with some nonzero probability) and the error rate can be as high as $2/3$. This still allows one to realize deterministic logical two-qubit gates whose quality is of the same order of magnitude as the single-particle operations. This means that the thresholds for fault-tolerant quantum computation are solely determined by the quality of *single*-particle operations. The requirements to build a scalable quantum computer thus reduce to provide small ($d \leq 32$), well controllable systems which interact by some means, where the interaction may be very noisy or even probabilistic. In what follows, we discuss this scheme in detail for two particles, A and B.

We start with the creation and purification of noisy entanglement. Consider a situation where several, say n_0, (noisy) entangled states shared between systems A_k and B_k, $k \geq 2$, have been created using the physical two-particle interaction. Standard entanglement purification methods, e.g., the recurrence protocol of Ref. [7], can be applied to purify the n_0 noisy entangled pairs and eventually to end up with a single entangled pair of higher quality shared between A_2 and B_2. Imperfections in single-particle operations still allow us to increase the quality of the entangled pairs up to a certain point, depending on the quality of single-particle operations; however, no maximally entangled states can be created under these circumstances [4,5]. Nevertheless, we consider such a situation in the following. Using the standard recurrence methods [7,14] (or other methods such as hashing or breeding [7]) typically requires the storage of hundreds of entangled pairs. However, storing n_0 entangled pairs plus the logical qubits requires $d = 2^{n_0+1}$ levels for each particle, which quickly becomes impractical simply because no sufficient number of controllable levels is available. To avoid this exponential overhead in the number of dimensions, we propose to use a novel, modified entanglement purification scheme which consists of *nested entanglement pumping*.

The main idea is to use this entanglement pumping, that is, to use the (noisy) two-particle gate to repeatedly create noisy entangled pairs between systems A_2, B_2, which are used to purify another pair shared between systems A_3, B_3 [4]. The advantage of such a scheme is that only two virtual subsystems per particle are required. However, as the purification process has to be restarted from the beginning as soon as one purification step fails, the time required to implement entanglement pumping as compared to the standard recurrence method is (polynomially) higher. It should be mentioned that even under ideal conditions, no maximally entangled states can be created using entanglement pumping, but the fidelity of the pairs can be increased only by a certain amount. This last problem can be overcome by using a nested scheme in such a way that the pair stored in A_3, B_3 is purified (almost) up to its highest reachable value and then used to purify another such pair (which was created in the same way) stored in systems A_4, B_4. For each nesting level, one additional virtual subsystem per particle is required. We have performed numerical investigation of the nested entanglement pumping scheme and found that when considering imperfect operations, the minimal required fidelity as well as the reachable fidelity of the pairs is the same as in the recurrence method of Ref. [14], and only a few nesting levels are required [15]. For all practical purposes, that is, when the error rates for for single-particle operations are above 10^{-7}, three nesting levels are sufficient (i.e., a total of $d \leq 32$ dimensions per particle). In this case, the achievable error rate of the *logical* two-qubit gate is of the same order of magnitude as the error rate of single-particle operations, provided that error rates for *physical* two-particle gates are at the order of 0.2 or lower. That is, the nested entanglement pumping combines the high tolerable error rates with few physical resources at the price of (polynomial) time overhead. Note that since entanglement pumping is itself a probabilistic process, the creation of the entangled pairs (and thus the two-particle gate) does not need to be deterministic. It only has to be known when the gate was successful. While such a probabilistic gate may completely destroy the performance of a quantum computation when applied directly to data qubits (as the whole computation has to be restarted each time a gate fails), this is not the case in our proposal, since the information carrying qubits are unaffected by the probabilistic gate.

The purified entangled pair created in this way can then be used to implement *deterministically* a two-particle gate (e.g., a CNOT) between the logical qubits stored in A_1 and B_1. In case the pair is maximally entangled and the single-particle operations are perfect, this can be accomplished with unit fidelity. Given a maximally entangled state shared between A_2, B_2, $|\Phi\rangle \equiv 1/\sqrt{2}(|00\rangle + |11\rangle)$, the following sequence of single-particle operations realizes a CNOT gate between A_1, B_1 [11]: (i) CNOT_{A_1,A_2}, (ii) measurement of A_2 in the z basis, depending on the outcome of measurement, applies $\mathbb{1}_{B_2}$ (outcome "0") or $\sigma_x^{B_2}$ (outcome "1"), (iii) CNOT_{B_2,B_1}, and (iv) measurement of B_2 in the x basis, depending on the outcome of measurement, applies $\mathbb{1}_{A_1}$ (outcome "0") or $\sigma_z^{A_1}$ (outcome "1"). In a similar way one may also realize arbitrary two-qubit operations (instead of CNOT) or even a multiqubit operation by purifying and consuming certain (multipartite) entangled states, following, e.g., the scheme proposed in Ref. [13]. For nonmaximally entangled pairs and imperfect single-particle operations, the two-particle gate is realized only in an imperfect way. The corresponding completely positive map $\mathcal{E}$ can be obtained by carrying out (i)–(iii), taking imperfections of single-particle gates and measurement into account, and considering a nonmaximally entangled mixed state, e.g., of Werner form, $\rho_{A_2B_2} = x|\Phi\rangle\langle\Phi| + (1-x)/4\mathbb{1}$, which can always be achieved using depolarization. The average gate fidelity,

$$\bar{F}(\mathcal{E}, U_{\mathrm{CNOT}}) \equiv \int d\psi \langle\psi|U^\dagger_{\mathrm{CNOT}}\mathcal{E}(\psi)U_{\mathrm{CNOT}}|\psi\rangle, \qquad (1)$$

is used as a measure of the quality of the imperfect operation $\mathcal{E}$ and we refer to $p \equiv (1 - \bar{F})$ as the *error rate of the operation.* Note that given $\mathcal{E}$, $\bar{F}$ can be easily evaluated using the results of Ref. [16].

We have analyzed the influence of imperfections on the scheme described above. In order to illustrate our results, we describe imperfect single-particle operations by a simple error model; however, the application of our scheme is not restricted to such an error model but is universal. We describe imperfect single-particle operations acting on two virtual subsystems as follows:

$$\mathcal{E}_{U_{A_1A_2}}(\rho) = qU_{A_1A_2}\rho U^\dagger_{A_1A_2} + \frac{1-q}{4}\mathbb{1}_{A_1A_2} \otimes \mathrm{tr}_{A_1A_2}\rho. \qquad (2)$$

While with probability q the desired gate is performed, with probability $(1-q)$ the gate fails and a completely depolarized state is produced. The average gate fidelity $\bar{F}$ for this imperfect operation is given by $\bar{F} = (3q+1)/4$, which implies an error rate $p = 3/4(1-q)$. Such an error model may be used to reflect our restricted knowledge on the kind of error. Imperfect projective measurements are described by the positive operators $\mathcal{P}^{(0)}_{A_2} = \eta|0\rangle_{A_2}\langle 0| + (1-\eta)|1\rangle_{A_2}\langle 1|$, $\mathcal{P}^{(1)}_{A_2} = \eta|1\rangle_{A_2}\langle 1| + (1-\eta)|0\rangle_{A_2}\langle 0|$, where, e.g., in the case of $\rho = |0\rangle\langle 0|$ the correct measurement outcome, $'0'$, is obtained with probability η. For simplicity, we consider $\eta = q$. Our analysis considers both (nested) entanglement purification with imperfect means as well as realization of the logical two-particle gate using noisy entangled states and imperfect single-particle operations. Figure 1 shows the achievable gate error rate for logical two-qubit operations as a function of the single-particle gate error rate. The different curves correspond to different numbers of nesting levels for entanglement pumping and different gate fidelities of physical two-particle interaction. Single-particle operations with a low error rate allow us to decrease error rates of two-particle operations by several orders of magnitude.

In order to realize the scheme, it is necessary that the operations we perform respect the virtual tensor-product structure we imposed. In particular, our scheme requires the realizability of the following operations: (i) entangling two-particle gate $\mathcal{E}$ acting only on specific virtual subsystems of each particle, e.g., A_2, B_2, without affecting other virtual subsystems; (ii) single-particle measurement on one virtual subsystem without affecting other virtual subsystems; (iii) arbitrary unitary operations on one virtual subsystem; and (iv) CNOT and SWAP gates [10] between arbitrary virtual subsystems A_j, A_k.

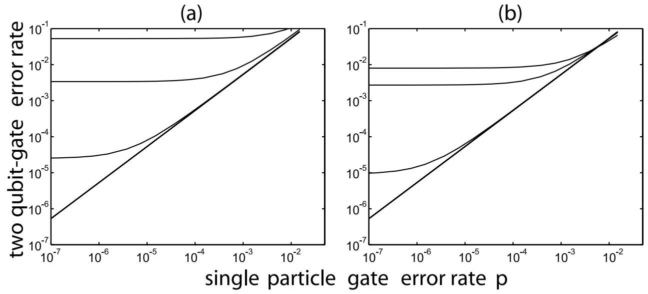

FIG. 1. Double logarithmic plot of achievable logical two-qubit gate error rate against single-particle error rate p for fixed error rate of physical two-particle interaction of (a) $1.5 * 10^{-1}$ and (b) 10^{-2}. Curves from top to bottom correspond to no entanglement purification and entanglement pumping using 1, 2, and 3 (or more) nesting levels, respectively.

On the one hand, (i) imposes conditions on the (nonlocal) two-particle interactions, namely, that the completely positive map $\mathcal{E}$ representing the two-particle operation between virtual subsystems A_2 and B_2 should act as $\mathbb{1}$ on the remaining virtual subsystems. Note that the division of d-dimensional Hilbert space into virtual subsystems is arbitrary and may we chosen in such a way that this condition can be fulfilled. In addition, $\mathcal{E}$ needs to be able to create entanglement, which can, e.g., be checked using the results of Ref. [13]. For imperfect two-particle operations which can be described by a map $\mathcal{E}'_{U_{A_1B_1}}$ similarly to Eq. (2) with $U_{A_1B_1} = \mathrm{CNOT}$, the gate is entangling if and only if $q' > 1/9$. For high fidelity single-particle operations, this also determines the highest tolerable error rate $p \approx 2/3$ of physical two-particle gates for which our scheme is applicable. Conditions (ii)–(iv) concern (local) single-particle operations and may be replaced by the ability to perform arbitrary single-particle operations; however, this may be more difficult to achieve. While (iii) ensures the ability to manipulate the logical qubit, (ii) and (iv) are required to realize nested entanglement pumping and for the realization of the logical two-qubit gate by consuming entanglement. For example, CNOT and SWAP operations between virtual subsystems X_2 and X_3, together with $\mathcal{E}$, are required to create and purify two noisy pairs. The purification step also involves measurements on virtual subsystems X_2, which clearly should not affect other virtual subsystems that are used to store logical qubits or other entangled pairs.

We also emphasize that metastable states (i.e., long decoherence times) are solely required for the virtual subsystems X_1, as the additional virtual subsystems are used only when implementing a two-qubit interaction. To be specific, coherence of the additional virtual subsystems is required only on time scales needed to implement a logical two-qubit gate using the scheme described above, while coherence of logical qubits (X_1) has to be maintained, as usual, over the whole time required for the quantum computation. This allows one to use, e.g., motional states of ions or neutral atoms as virtual subsystems whose decoherence time is much shorter than that of the electronic states.

We now briefly discuss possible implementations of our scheme, taking conditions (i)–(iv) into account. As an example consider an array of ions trapped in microtraps, following the proposal of Ref. [17]. The electronic and motional states of trapped ions provide the additional levels required to implement our scheme. The motional states (in x and y directions) are used to temporally store logical qubits and previously generated entangled states, while electronic states of ions are used to generate entanglement between neighboring ions by applying the two-particle gate proposed in Ref. [17] which is based on Coloumb interaction. Requirements (i), (iii), and (iv) can be met in such a setup using present-day technology [15]. In fact, several ingredients, e.g., local CNOT gates between electronic and motional states, have already been experimentally demonstrated [18]. However, (ii), the measurement of electronic states using spectroscopic methods seems to require either tighter traps (smaller Lamb-Dicke parameter) or more efficient detectors. Alternatively, one may embed each ion into a cavity, thereby directing the emission of photons into the z direction to avoid recoil kicks in the x and y directions which would otherwise destroy the coherence of the motional states. Similarly, neutral atoms trapped in dipole traps or optical lattices may be used and, e.g., the two-particle gate proposed in Ref. [19] is applied.

Our scheme is also applicable in a *concatenated* scenario, e.g., in distributed quantum computation [20]. Consider the situation where several ions are stored in a Paul trap, with at least one ion embedded into a cavity. Several such systems may be placed in the same lab and connected by optical fibers, while several such labs form the setup for quantum computation. In this case, operations at different concatenation levels are not equally difficult to realize and the quality of operations at the lowest concatenation level completely determine the quality of operations at the highest level [15].

We have shown that entanglement purification is a useful tool also for quantum computation and allows one to reduce error thresholds for two-particle operations by several orders of magnitude. This in turn implies that small ($d \leq 32$), well controllable physical systems which interact (in a possible very noisy or even probabilistic way) are sufficient to build a fault-tolerant quantum computer. We have illustrated our proposal with trapped neutral atoms and ions. We, however, believe that they are applicable to other existing proposals for quantum computation (e.g., based on linear optics [21,22]) or may even trigger the design of fault-tolerant proposals especially suitable to meet the requirements of our scheme.

We thank J. I. Cirac for many useful comments and valuable discussions. This work was supported by the DFG and by the European Union [HPMF-CT-2001-01209 (W. D.), IST-1999-13021].

[1] P.W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124; L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[2] P. Shor, quant-ph/9605011; A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997); D. Aharonov and M. Ben-Or, quant-ph/9611025; A. Yu. Kitaev, Russ. Math. Surv. **52**, 1191 (1997); E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).

[3] Special issue on experimental proposals for Quantum Computation, Fortschr. Phys. **48**, No. 9–11 (2000).

[4] H.-J. Briegel *et al.*, Phys. Rev. Lett. **81**, 5932 (1998); W. Dür *et al.*, Phys. Rev. A **59**, 169 (1999).

[5] G. Giedke *et al.*, Phys. Rev. A **59**, 2641 (1999).

[6] H. Aschauer and H.-J. Briegel, Phys. Rev. Lett. **88**, 047902 (2002).

[7] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).

[8] The bound 10^{-4} was recently derived for a general error model by D. Aharonov *et al.* (unpublished), who also gave a relaxed bound if higher dimensional systems are used.

[9] P. Zanardi, Phys. Rev. Lett. **87**, 077901 (2001).

[10] The CNOT (SWAP) operation is defined by the following mapping of states, written in the standard basis: $|i\rangle_A|j\rangle_B \rightarrow |i\rangle_A|i \oplus j\rangle_B$ [$|i\rangle_A|j\rangle_B \rightarrow |j\rangle_A|i\rangle_B$], where $\oplus$ denotes addition modulo 2.

[11] D. Gottesman, quant-ph/9807006; A. Chefles, C. R. Gilson, and S. M. Barnett, Phys. Rev. A **63**, 032314 (2001); J. Eisert *et al.*, Phys. Rev. A **62**, 052317 (2000); D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).

[12] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[13] J. I. Cirac *et al.*, Phys. Rev. Lett. **86**, 544 (2001); W. Dür and J. I. Cirac, Phys. Rev. A **64**, 012317 (2001).

[14] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).

[15] W. Dür, M. Hein, and H.-J. Briegel (to be published).

[16] M. A. Nielsen, e-print quant-ph/0205035 (unpublished).

[17] J. I. Cirac and P. Zoller, Nature (London) **404**, 579 (2000).

[18] B. DeMarco *et al.*, Phys. Rev. Lett. **89**, 267901 (2002).

[19] D. Jaksch *et al.*, Phys. Rev. Lett. **85**, 2208 (2000).

[20] J. I. Cirac *et al.*, Phys. Rev. Lett. **78**, 3221 (1997); S. J. van Enk *et al.*, Science **279**, 205 (1998).

[21] E. Knill *et al.*, Nature (London) **409**, 46 (2001).

[22] J.-W. Pan *et al.*, Nature (London) **410**, 1067 (2001).