Communication Capacity of Quantum Computation

S. Bose, L. Rallan, and V. Vedral
Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, England

(Received 17 March 2000)

By considering quantum computation as a communication process, we relate its efficiency to its classical communication capacity. This formalism allows us to derive lower bounds on the complexity of search algorithms in the most general context. It enables us to link the mixedness of a quantum computer to its efficiency and also allows us to derive the critical level of mixedness beyond which there is no quantum advantage in computation.

PACS numbers: 03.67.Lx, 03.65.Bz, 03.67.Hk

Any computation, both classical and quantum, is formally identical to a communication in time. At time $t = 0$, the programmer sets the computer to accomplish any one of several possible tasks. Each of these tasks can be regarded as embodying a different message. Another programmer can obtain this message by looking at the output of the computer when the computation is finished at time $t = t_1$. A surge of interest in both quantum computation [1–3] and quantum communication has been witnessed in recent years [4,5]. Computation based on quantum principles allows for more efficient algorithms for solving certain problems than algorithms based on purely classical principles. Quantum communication, on the other hand, can be used for unconditionally secure secret key distribution [6]. However, to date, the relationship between these two areas (i.e., quantum computation and quantum communication) has not been fully explored. Although some work interrelating quantum communication and computation does exist [7], this does not utilize any entropic results from communication theory to study computational complexity. An entropic approach to computational complexity exists in classical complexity theory from the point of view of Kolmogorov complexity [8,9]. In this Letter we connect the classical capacity of a quantum communication channel [4] with the efficiency of quantum computation using entropic arguments. This approach allows us to derive lower bounds on the complexity of search algorithms in the most general context. It also enables us to link the mixedness of a quantum computer to its efficiency. This offers a unifying framework for quantum information processing.

Let us first introduce a few definitions and a communication model of quantum computation. We have two programmers, the sender and the receiver, and two registers, the memory (M) register and the computational (C) register. The sender prepares the memory register in a certain quantum state $|i\rangle_M$ which encodes the problem to be solved. For example, in the case of factorization [2], this register will store the number to be factored. In case of a search [3], this register will store the state of the list to be searched. The number N of possible states $|i\rangle_M$ will, of course, be limited by the greatest number that the given computer could factor or the largest list that it could search. The receiver then prepares the computational register in some initial state ρ_C^0. Both the sender and the receiver feed the registers (prepared by them) to the quantum computer. The quantum computer implements the following general transformation on the registers:

$$(|i\rangle\langle i|)_M \otimes \rho_C^0 \rightarrow (|i\rangle\langle i|)_M \otimes U_i \rho_C^0 U_i^\dagger . \qquad (1)$$

The resulting state $\rho_C(i) = U_i \rho_C^0 U_i^\dagger$ of the computational register contains the answer to the computation and is measured by the receiver. As the quantum computation should work for any $|i\rangle_M$, it should also work for any mixture $\sum_i^N p_i(|i\rangle\langle i|)_M$, where p_i are probabilities. For the sender to use the above computation as a communication protocol, he has to prepare any one of the states $|i\rangle_M$ with an *a priori* probability p_i. The entire input ensemble is thus $\sum_i^N p_i(|i\rangle\langle i|)_M \otimes \rho_C^0$. Because of the quantum computation, this becomes

$$\sum_i^N p_i(|i\rangle\langle i|)_M \otimes \rho_C^0 \rightarrow \sum_i^N p_i(|i\rangle\langle i|)_M \otimes \rho_C(i) . \qquad (2)$$

Whereas before the quantum computation, the two registers were completely uncorrelated (mutual information is zero), at the end, the mutual information becomes

$$\begin{aligned} I_{MC} &:= S(\rho_M) + S(\rho_C) - S(\rho_{MC}) \\ &= S(\rho_C) - \sum_i^N p_i S[\rho_C(i)] , \end{aligned} \qquad (3)$$

where ρ_M and ρ_C are the reduced density operators for the two registers, ρ_{MC} is the density operator of the entire $M + C$ system, and $S(\rho) = -\mathrm{Tr}\rho \log\rho$ is the von Neumann entropy (for conventional reasons we will use $\log_2$ in all calculations). Notice that the value of the mutual information (i.e., correlations) is equal to the Holevo bound $H = S(\rho_C) - \sum_i^N p_i S[\rho_C(i)]$ for the classical capacity of a quantum communication channel [4] [note that $\rho_C = \sum_i^N p_i \rho_C(i)$]. This tells us how much information the receiver can obtain about the choice $|i\rangle_M$ made by the sender by measuring the computational register. The maximum value of H is obtained when the states $\rho_C(i)$ are pure and orthogonal. Moreover, the sender conveys the maximum information when all the message states have equal *a priori* probability (which also maximizes the channel capacity). In that case the mutual information (channel capacity) at the end of the computation is $\log N$. Thus the communication capacity I_{MC} [given by Eq. (3)] gives an index of the efficiency of a quantum computation. *A necessary target of a quantum computation is to achieve the maximum possible communication capacity consistent with given initial states of the quantum computer.* We cannot give a sufficiency criterion from our general approach as this depends on the specifics of an algorithm. If one breaks down the general unitary transformation U_i of a quantum algorithm into a number of successive unitary blocks, then the maximum capacity may be achieved only after the number of applications of the block. In each of the smaller unitary blocks, the mutual information between the M and the C registers (i.e., the communication capacity) increases by a certain amount. When its total value reaches the maximum possible value consistent with a given initial state of the quantum computer, the computation is regarded as being complete.

We now proceed to illustrate one immediate application of the above formalism. Any general quantum algorithm has to have a certain number of queries into the memory register [10–12] (this is necessitated by the fact that the transformation on the computational register has to depend on the problem at hand, encoded in $|i\rangle_M$). These queries can be considered to be implemented by a black box into which the states of both the memory and the computational registers are fed. The number of such queries needed in a certain quantum algorithm gives the black box complexity of that algorithm [10–12] and is a lower bound on the complexity of the whole algorithm. Recently, Ambainis [12] showed in a very elegant paper that if the memory register was prepared initially in the superposition $\sum_i^N |i\rangle_M$, then, in a search algorithm, $O(\sqrt{N})$ queries would be needed to completely entangle it with the computational register. This gives a lower bound on the number of queries in a search algorithm. In a manner analogous to his, we will calculate the change in mutual information between the memory and the computational registers [from Eq. (3)] in one query step. The number of queries needed to increase the mutual information to $\log N$ (for perfect communication between the sender and the receiver), is then a lower bound on the complexity of the algorithm.

Any search algorithm (whether quantum or classical, irrespective of its explicit form) will have to find a match for the state $|i\rangle_M$ of the M register among the states $|j\rangle_C$ of the C register and associate a marker to the state that matches (here $|j\rangle_C$ is a complete orthonormal basis for the C register). The most general way of doing such a query in the quantum case is the black box unitary transformation [12]

$$U_B|i\rangle_M|j\rangle_C = (-1)^{\delta_{ij}}|i\rangle_M|j\rangle_C\,. \tag{4}$$

Any other unitary transformation performing a query matching the states of the M and the C registers could be constructed from the above type of query. We would like to put a bound on the change of the mutual information in one such black box step. Let the memory states $|i\rangle_M$ be available to the sender with equal *a priori* probability so that the communication capacity is a maximum. His initial ensemble is then $\frac{1}{N}\sum_i^N(|i\rangle\langle i|)_M$. Let the receiver prepare the C register in an initial pure state ψ^0 (in fact, the power of quantum computation stems from the ability of the receiver to prepare pure state superpositions of form $\frac{1}{N}\sum_j^N|j\rangle_C$). This is an equal weight superposition of all $|j\rangle_C$ as there is no *a priori* information about the right $|j\rangle_C$. This can be done by performing a Hadamard transformation to each qubit of the C register. In general, there will be many black box steps on the initial ensemble before a perfect correlation is set up between the M and the C registers. Let, after the kth black box step, the state of the system be

$$\rho^k = \frac{1}{N}\sum_i^N(|i\rangle\langle i|)_M \otimes [|\psi^k(i)\rangle\langle\psi^k(i)|]_C\,, \tag{5}$$

where

$$|\psi^k(i)\rangle_C = \sum_j \alpha_{ij}^k|j\rangle_C\,. \tag{6}$$

The $(k+1)$th black box step changes this state to $\rho^{k+1} = \frac{1}{N}\sum_i^N(|i\rangle\langle i|)_M \otimes [|\psi^{k+1}(i)\rangle\langle\psi^{k+1}(i)|]_C$ with

$$|\psi^{(k+1)}(i)\rangle = \sum_{i,j}^N \alpha_{ij}^k(-1)^{\delta_{ij}}|j\rangle_C\,. \tag{7}$$

Thus we only have to evaluate the difference of mutual information between the M and the C registers for the states. This difference of mutual information [when computed from Eq. (3)] can be shown to be the difference $|S(\rho_C^{k+1}) - S(\rho_C^k)|$ [13]. This quantity is bounded from the above by [14]

$$|S(\rho_C^{k+1}) - S(\rho_C^k)| \le d_B(\rho_C^k,\rho_C^{k+1})\log N - d_B(\rho_C^k,\rho_C^{k+1})\log d_B(\rho_C^k,\rho_C^{k+1})\,, \tag{8}$$

where, $d_B(\sigma,\rho) = \sqrt{1 - F^2(\sigma,\rho)}$ is the Bures metric and $F(\sigma,\rho) = \mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}$ is the fidelity. Using methods similar to Ambainis [12], it can be shown that $F^2(\rho_C^0,\rho_C^1) \ge \frac{N-2}{N}$ from which it follows that the change in the first step

$$|S(\rho_C^0) - S(\rho_C^1)| \le \frac{3}{\sqrt{N}}\log N\,. \tag{9}$$

The change $|S(\rho_C^k) - S(\rho_C^{k+1})|$ in the subsequent steps has to be less than or equal to the change in the first step. This is because the Bures metric does not increase under general completely positive maps (which is what the query represents when we trace out the M register). Any other operations performed only on the C register in between two queries can only reduce the mutual information between the C and the M registers. This means that at least $O(\sqrt{N})$ steps are needed to produce full correlations (maximum mutual information of value $\log N$) between the two registers. This gives the black box lower bound on the complexity of any quantum search algorithm. Of course, we know that there also exists an algorithm achieving this bound due to Grover [3] and this has been proven to be optimal [10,12,15]. However, our proof is the most general as it holds even when any type of completely positive map is allowed between the queries (only in Ref. [15] a heuristic argument was made for the optimality of Grover's algorithm under general operations).

We now use Grover's algorithm to show how the mutual information varies with time in a quantum search. The general sequence described by Cleve *et al.* [16] for Grover's algorithm will be used in this Letter. The algorithm consists of repeated blocks, each consisting of a Hadamard transform on each qubit of the C register, followed by a U_B (our black box transformation), followed by another Hadamard transform on each qubit of the C register and finally a phase flip f_0 of the $|00\cdots 0\rangle_C$ state of the C register (see Fig. 1). This block can then be repeated as many times as is necessary to bring the mutual information to its maximum value of $\log N$, which, as we have shown in Eq. (9), is $O(\sqrt{N})$. Note that the only transformation correlating the M and C registers is the black box transformation U_B and all the other transformations are done *only* on the C register and therefore do not change the mutual information between the two registers. In Fig. 2 we have plotted the variation of mutual information between the M and the C registers (i.e., the communication capacity of the quantum computation) with the number of iterations of the block in Grover's algorithm. It is seen that the mutual information oscillates with the number of iterations. Figure 2 is plotted for a four qubit computational register which can search a database of 16 entries. It is seen that the period is roughly 6, which means that the number of steps needed to achieve maximum mutual information is roughly 3. This is well above our bound for the minimum number of steps, which is 4/3 in this case.

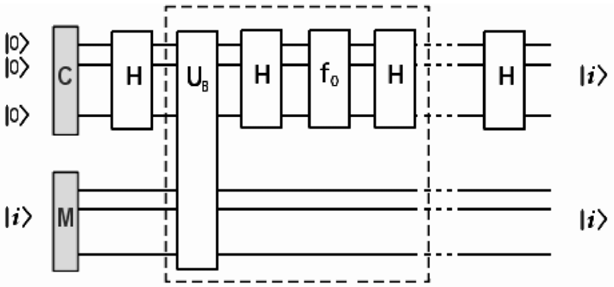

FIG. 1. The figure shows the circuit for Grover's algorithm. C is the computational register and M is the memory register. U_B is the black box query transformation, H is a Hadamard transformation on every qubit of the C register, and f_0 is a phase flip in front of the $|00\cdots 0\rangle_C$. The block consisting of H, U_B, H, and f_0 is repeated a number of times.

The three graphs (a), (b), and (c) in Fig. 2 are for different values of initial mixedness of the C register. We find that the mutual information fails to rise to the maximum value of $\log N$ when the state of the computational register is mixed. Our formalism thus allows us to calculate the performance of a quantum computation as a function of the mixedness (quantified by the von Neumann entropy) of the computational register. We can put a bound on the entropy of the second register after which the quantum search becomes as inefficient as the classical search. Suppose the initial entropy $S(\rho_C^0)$ of the C register exceeds $\frac{1}{2}\log N$. Then Eq. (3) implies that the increase in mutual information between the M and the C registers in the course of the entire quantum computation would be at most $\log\sqrt{N}$. This can already be achieved by a classical database search in $\sqrt{N}$ steps. So there is no advantage in using quantum evolution when the initial state is more mixed than a certain amount. This value of the initial entropy of the C register above which you do not get any advantage from the quantum search is

$$S(\rho_C^0) \geq \frac{1}{2}\log N\,. \tag{10}$$

The above condition for no quantum advantage in the search algorithm is only a sufficient condition and not a necessary condition. This is similar to the entropic conditions sufficient to ensure no quantum benefit from teleportation and dense coding [17]. Note that it is not that the algorithm is slowed down in any way by mixedness of the C register, but that we have lower than the amount of correlations that can be obtained in the same amount of time by classical querying. This result would

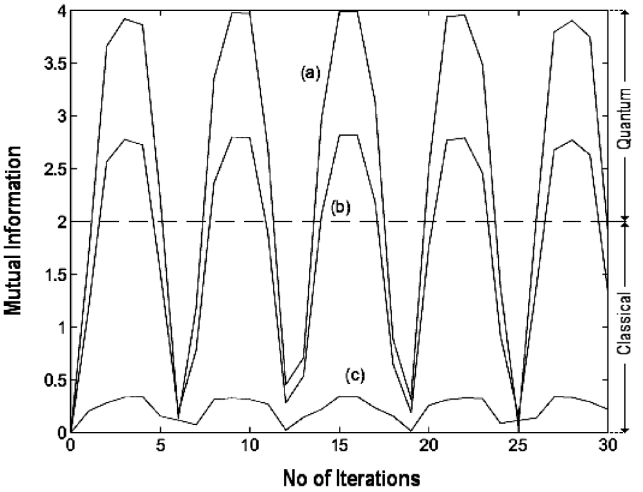

FIG. 2. The figure shows the dependence of the mutual information between the M and the C registers as a function of the number of times the block in Grover's algorithm is iterated for various values of initial mixedness of the C register. Each qubit of the C register is initially in the state $p|0\rangle\langle 0| + (1-p) \times |1\rangle\langle 1|$, ($a$) $p = 1$, (b) $p = 0.95$, and (c) $p = 0.7$. The (a) and (b) computations achieve higher mutual information than classically allowed in the order of root N steps, while (c) does not.

tell an experimentalist the temperature below which a system has to be cooled in order to begin to see quantum advantages in computation. For example, suppose the difference in energy between the levels $|0\rangle$ and $|1\rangle$ is ΔE for the system being used by an experimentalist. Then the critical temperature T_c beyond which there is no quantum advantage in computation can be calculated from the relation $\log(1 + \alpha) - \frac{\alpha}{1+\alpha}\log\alpha \geq \frac{1}{2}$ where $\alpha = \exp(-\Delta E/KT_c)$ in which K is the Boltzmann constant. Analogous analysis can be applied to other algorithms.

Finally, we point out that the states of the M register need not be a mixture, but could be an arbitrary superposition of states $|i\rangle_M$ (such a state was used by Ambainis in his argument [12]). All the above arguments still hold in that case, and the M and the C registers become quantum mechanically entangled and not just classically correlated. Thus our analysis implies that any quantum computation can be viewed as a quantum measurement process [18] (though there is more to quantum computation than just the concepts of measurement and communication). The system being measured is the M register and the apparatus is the C register of the quantum computer. As the time progresses the apparatus (register C) becomes more and more correlated (or entangled) to the system (register M). This means that the states of register C become more and more distinguishable which allows us to extract more information about the M register by measuring the C register. The analysis in the last paragraph, where we showed the limitations on the efficiency of quantum computation imposed by the mixedness of the C register, applies also to the efficiency of a quantum measurement when the apparatus is in a mixed state. Mixedness of an apparatus, to the best of our knowledge, has been considered only in a quantum measurement for treating foundational issues (such as the origin of a statistical nature of a quantum measurement [18]) and never for analyzing efficiency. In general practice, any apparatus, however macroscopic, is considered to be in a pure quantum state before the measurement. Our approach highlighting the formal analogy between measurement and computation offers a way to analyze measurement in a much more general context.

We thank Y. Shi for useful discussions on the subject of this paper. L. R. would like to thank Invensys Plc for financial support. Funding by the European Union project EQUIP (Contract No. IST-1999-11053) is also acknowledged.

[1] D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).

[2] P. Shor, SIAM J. Comput. **26**, 1484 (1997). Also FOCS'94.

[3] L. Grover, in *Proceedings of the 28th ACM Symposium on Theory of Computing* (ACM, Philadelphia, 1996), p. 212.

[4] A. S. Kholevo, Probl. Peredachi Inf. **9**, 177 (1973); see also A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).

[5] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179; C. H. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992); A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[6] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[7] A. C.-C. Yao, in *Proceedings of the 34th FOCS, 1993* (IEEE, Palo Alto, 1993), p. 352; H. Buhrman, R. Cleve, and A. Wigderson, quant-ph/9802040.

[8] A. N. Kolmogorov, Probl. Inf. Transm. **1**, 1 (1965); R. J. Solomonoff, Inf. Control **7**, 1–22 (1964); **7**, 224–254 (1964); G. J. Chaitin, J. Assoc. Comput. Mach. **16**, 145 (1969).

[9] M. Li and P. M. B. Vitanyi, in *Kolmogorov Complexity and its Applications,* edited by J. van Leeuwen, Handbook of Theoretical Computer (Elsevier Science Publishers, Amsterdam, 1990), pp. 197–254; M. Li and P. M. B. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications* (Springer-Verlag, Berlin, 1997), 2nd ed.

[10] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, SIAM J. Comput. **26**, 1510 (1997).

[11] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, in *Proceedings of FOCS'98* (IEEE, Palo Alto, 1998), pp. 352–361.

[12] A. Ambainis, quant-ph/0002066.

[13] L. Henderson and V. Vedral, Phys. Rev. Lett. **84**, 2263 (2000).

[14] M. Fannes, Commun. Math. Phys. **31**, 291 (1973); M. Nielsen, Phys. Rev. A **61**, 4301 (2000).

[15] C. Zalka, Phys. Rev. A **60**, 2746 (1999).

[16] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Philos. Trans. R. Soc. London A **454**, 339 (1997).

[17] S. Bose and V. Vedral, Phys. Rev. A **61**, 040101(R) (2000).

[18] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1955); H. Everett III, in *The Many-Worlds Interpretation of Quantum Mechanics,* edited by B. S. DeWitt and N. Graham (Princeton University Press, Princeton, 1973).