Lower Bound on the Number of Toffoli Gates in a Classical Reversible Circuit through Quantum Information Concepts

Sandu Popescu,[1,2] Berry Groisman,[1] and Serge Massar[3]

[1]*HH Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom*
[2]*Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, United Kingdom*
[3]*Laboratoire d'Information Quantique and QUIC, Université Libre de Bruxelles, C.P. 165/59,
Boulevard du Triomphe, 1050 Bruxelles, Belgium*

The question of finding a lower bound on the number of Toffoli gates in a classical reversible circuit is addressed. A method based on quantum information concepts is proposed. The method involves solely *concepts* from quantum information—there is no need for an actual physical quantum computer. The method is illustrated in the example of classical Shannon data compression.

In the past ten years we have witnessed the birth and explosive growth of the field of quantum information and computation. The main thrust of this new field is to study how quantum systems (such as quantum computers and quantum communication devices) can be used to solve certain mathematical problems or to improve communication capabilities. The crucial feature of this approach is that although the quantum systems themselves can be studied with pen and paper, gains are obtained only when the quantum systems are actually used in practice. The gains are due to new physical behavior unique to quantum systems and not shared by classical ones. In this Letter we take a different direction. We are not interested in using quantum systems; rather, we want to use the concepts and insights gained in the study of quantum information for solving mathematical problems.

The problem we consider here concerns lower bounds on reversible classical circuits. Although reversible classical computation will probably not be realized in the near future (though increasing attention is being devoted to this issue), its study has yielded profound insights into the theory of complexity and into thermodynamics; see [1] for a review.

A reversible classical computation evaluates a function f which takes n-bit input $\bar{x} \in \{0, 1\}^n$ to n-bit output $f(\bar{x}) \in \{0, 1\}^n$. Each particular input has its own unique output, thus f is invertible. A classical circuit that evaluates f can be reduced to a sequence of elementary reversible logical gates. Examples of reversible one-, two-, and three-bit gates are NOT, Controlled-NOT (C-NOT) and Toffoli (Controlled-Controlled-NOT) gates. C-NOT applies NOT on the second bit only if the value of a first bit is 1; Toffoli applies NOT on the third bit only if the values of both first and second bit are 1. Reversible one- and two-bit gates do not constitute a universal set of gates. The Toffoli gate, however, is a universal basic gate for reversible classical computation; i.e., any reversible classical circuit can be built up from Toffoli gates [2].

Although we can build any reversible circuit out of Toffoli gates alone, an interesting conceptual question is to find the *minimal* number of Toffoli gates required if one allows for *any* number of one- and two-bit gates. The problem is interesting because Toffoli gates are, in a sense, the strongest reversible gates, and the minimal number needed tells us about the complexity of the computation itself. Furthermore, Toffoli gates require *physical interaction* between 3 bits, and are therefore more difficult to implement in practice than one- and two-bit gates, and it might be useful to minimize their use.

We formulate the problem as follows: given a reversible function $f(\bar{x})$, what is the minimum number of Toffoli gates needed to construct a circuit that will evaluate $f(\bar{x})$ for (i) every $\bar{x}$ or (ii) a certain subset of $\bar{x}$?

As far as we know, a systematic approach to this problem does not exist. In this Letter we use quantum information concepts to address it. In quantum information (computation) one classical bit can be encoded in two orthogonal states of a quantum system. The main idea of our method is to *map* the bits onto some special quantum states, and the action of the logic gates onto unitary transformations acting on these states. Then, the study of the properties of the unitary transformation that is associated with the classical reversible computation will give information about the classical circuit. The map is

$$
\begin{aligned}
0 &\rightarrow |\mathbf{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B), \\
1 &\rightarrow |\mathbf{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B).
\end{aligned}
\tag{1}
$$

The states $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$, the "logical" qubits into which the classical bits are mapped, represent entangled states of two "constituent" qubits, denoted by the indexes A and B. (Throughout this Letter we will use boldfaced fonts for the logical qubits and normal fonts for the constituent qubits.) Here the states $|\mathbf{0}\rangle, |\mathbf{1}\rangle$ are associated with orthogonal states of a two-level quantum system.

A string of n bits is mapped on the associated quantum state of n qubit pairs: $x_1 x_2 \ldots x_n \to |\mathbf{x_1}\rangle |\mathbf{x_2}\rangle \ldots |\mathbf{x_n}\rangle$. Any computation $x_1 x_2 \ldots x_n \to f_1(\bar{x}) f_2(\bar{x}) \ldots f_n(\bar{x})$ is mapped on the same transformation of the corresponding quantum states $|\mathbf{x_1}\rangle |\mathbf{x_2}\rangle \ldots |\mathbf{x_n}\rangle \to |\mathbf{f_1}(\bar{\mathbf{x}})\rangle |\mathbf{f_2}(\bar{\mathbf{x}})\rangle \ldots |\mathbf{f_n}(\bar{\mathbf{x}})\rangle$. Since we consider a reversible classical computation, the corresponding quantum transformation is unitary. For example, the action of a C-NOT gate $a, b \to a, a \oplus b$ ($a, b \in \{0, 1\}$) is mapped on the unitary transformation $U_{\text{C-NOT}}$: $|\mathbf{a}\rangle |\mathbf{b}\rangle \to |\mathbf{a}\rangle |\mathbf{a} \oplus \mathbf{b}\rangle$. [Note that this does not define the unitary $U_{\text{C-NOT}}$ completely as the two logical qubits in Eq. (1) do not constitute a basis of the Hilbert space of the two constituent qubits. Similarly the unitary quantum transformation corresponding to any computation acting on n bits is not specified completely by the above mapping. Finally note that if we only specify a partial truth table for the computation, then the unitary is even less specified.]

The most important property of this mapping is that any classical reversible circuit built only from one- and two-bit gates is mapped onto a transformation that requires neither entanglement nor classical communication, i.e., onto a *local* unitary transformation $U = U^A \otimes U^B$ where $U^A(U^B)$ acts only on the $A(B)$ constituent qubits. For example, the $U_{\text{C-NOT}}$ gate can be built from *local* C-NOT gates:

$$U_{\text{C-NOT}} = \tilde{U}^A_{\text{C-NOT}} \otimes \tilde{U}^B_{\text{C-NOT}} \qquad (2)$$

as can be easily checked explicitly. Here $\tilde{U}^A_{\text{C-NOT}}$ ($\tilde{U}^B_{\text{C-NOT}}$) is a C-NOT gate acting on the $A(B)$ constituent qubits in the opposite direction to normal, i.e., with the second bit as the control and the first bit as the target. [Such bi-lateral transformations were considered in [3] for the purpose of density matrix purification.] That the quantum equivalent of *any* reversible one- or two-bit gates can be constructed by a similar local bi-lateral transformation can be verified explicitly. Hence, any circuit built from one- or two-qubit gates is local.

We can use this property of our mapping to analyze general circuits: given a classical reversible computation we construct the associated quantum unitary transformation U; if U is nonlocal, the corresponding classical transformation cannot be constructed solely by two-bit gates. Furthermore, the amount of nonlocality in U gives a lower bound on the number of Toffoli gates we need.

We define *nonlocality of production*, E^{Pr}_U, as the maximum amount of entanglement (measured in ebits) which U is capable to produce. We define *nonlocality of implementation*, E^{Im}_U, as the minimum amount of entanglement which allows one to implement U using local operations and classical communication (LOCC). These quantities satisfy

$$E^{\text{Pr}}_U \leq E^{\text{Im}}_U. \qquad (3)$$

We denote by E^{Pr}_T and E^{Im}_T the appropriate quantities for quantum Toffoli gate U_T (we estimate E^{Pr}_T, E^{Im}_T below).

One possible implementation of U is to realize the classical circuit using the nonlocal quantum Toffoli gates

(which cost E^{Im}_T ebits each) and the local two-bit and one-bit gates. Hence U can be implemented using $N_T E^{\text{Im}}_T$ ebits. This yields the lower bound on N_T:

$$N_T \geq E^{\text{Im}}_U / E^{\text{Im}}_T \geq E^{\text{Pr}}_U / E^{\text{Im}}_T. \qquad (4)$$

We now arrive at the crucial point of the method. To determine E^{Pr}_U, E^{Im}_U may be a very complicated task—it might actually be as complicated as directly determining the required number of Toffoli gates. On the other hand, it is easy to obtain bounds on them.

To obtain lower bound on E^{Pr}_U we apply U on a *test state* $|\Psi^{\text{test}}_{\text{in}}\rangle$:

$$U |\Psi^{\text{test}}_{\text{in}}\rangle = |\Psi^{\text{test}}_{\text{out}}\rangle, \qquad (5)$$

where the test state can be any arbitrary superposition of basic input states $|\mathbf{x_1}\rangle |\mathbf{x_2}\rangle \ldots |\mathbf{x_n}\rangle$. We denote the amount of nonlocality between A and B possessed by $|\Psi^{\text{test}}_{\text{in}}\rangle$ and $|\Psi^{\text{test}}_{\text{out}}\rangle$ by $E^{\text{test}}_{\text{in}}$ and $E^{\text{test}}_{\text{out}}$, respectively, where $E = S(\text{Tr}_A |\Psi\rangle\langle\Psi|) = S(\text{Tr}_B |\Psi\rangle\langle\Psi|)$ is the von Neumann entropy of the reduced density matrix. (Applying U to the test state and computing $E^{\text{test}}_{\text{in}}$ and $E^{\text{test}}_{\text{out}}$ is straightforward.) The nonlocality of production in U is not less than the entanglement difference between the two states:

$$E^{\text{Pr}}_U \geq |E^{\text{test}}_{\text{in}} - E^{\text{test}}_{\text{out}}|. \qquad (6)$$

How good are these bounds on E^{Pr}_U? First of all, note that *any* test state leads to a lower bound. However, different test states may lead to different lower bounds because the nonlocal content of U may not be realized in full when U acts on a particular state. (For example, a test state of the form $|\Psi^{\text{test}}_{\text{in}}\rangle = |\mathbf{x_1}\rangle |\mathbf{x_2}\rangle \ldots |\mathbf{x_n}\rangle$ is transformed into $|\Psi^{\text{test}}_{\text{out}}\rangle = |\mathbf{f_1}\rangle |\mathbf{f_2}\rangle \ldots |\mathbf{f_n}\rangle$ and leads to no increase in entanglement.) Good test states can be found either by trial and error or by systematic optimization.

A more important restriction is due to the fact that Eq. (4) can be far from tight. This is because when implementing the classical circuit some of the Toffoli gates may increase the entanglement whereas others may decrease it. Thus there may be more efficient ways of implementing U than realizing the classical circuit. For instance, if U acts on states composed of n logical qubits, then $E_U \leq 2n$, because one can always implement U by teleporting Alice's qubits to Bob, letting Bob implement U locally, and teleporting Alice's qubits back to her. This shows that our method can only provide bounds that grow linearly in n. On the other hand, it is known that for some problems of classical reversible computation the number of Toffoli gates grows exponentially [4] and for these problems our method is very inefficient. Nevertheless we expect that in many cases the number of Toffoli gates will grow linearly with, or as a fractional power of, n. Bounding the actual power may give an interesting—indeed, sometimes fundamental—insight.

Let us now consider the case of the Toffoli gate itself and prove the basic fact that classical Toffoli gates cannot be built from reversible two-bit gates. We will do this by

showing that under our map the quantum equivalent of the Toffoli gate is nonlocal. Specifically we will obtain the upper and lower bounds

$$1 \leq E_T^{\text{Pr}} \leq E_T^{\text{Im}} \leq 2. \tag{7}$$

Then, from Eqs. (4), (6), and (7) we obtain the following lower bound on the number N_T of Toffoli gates required to carry out a computation

$$N_T \geq \frac{|E_{\text{in}}^{\text{test}} - E_{\text{out}}^{\text{test}}|}{2}. \tag{8}$$

(Note that it is not essential for our method to find the exact value of E_T^{Im} since in general we are interested only in the scaling of the number of Toffoli gates with the size of the problem.)

The lower bound $E_T^{\text{Pr}} \geq 1$ is obtained by showing that under our map the quantum Toffoli gate is capable of producing at least one ebit of entanglement. Consider the test state

$$|\Psi_{\text{in}}^{\text{test}}\rangle = \frac{1}{2}(|\mathbf{0}\rangle_1|\mathbf{0}\rangle_2|\mathbf{0}\rangle_3 + |\mathbf{1}\rangle_1|\mathbf{0}\rangle_2|\mathbf{0}\rangle_3 + |\mathbf{0}\rangle_1|\mathbf{1}\rangle_2|\mathbf{0}\rangle_3$$
$$- |\mathbf{1}\rangle_1|\mathbf{1}\rangle_2|\mathbf{1}\rangle_3)$$
$$= \frac{1}{\sqrt{2}}|001\rangle_A|001\rangle_B + \frac{1}{2\sqrt{2}}(|000\rangle_A|000\rangle_B$$
$$+ |010\rangle_A|010\rangle_B + |100\rangle_A|100\rangle_B$$
$$- |110\rangle_A|110\rangle_B),$$

where the third logical bit is the target of the Toffoli gate. After acting with U_T on $|\Psi_{\text{in}}^{\text{test}}\rangle$ we obtain

$$|\Psi_{\text{out}}^{\text{test}}\rangle = \frac{1}{2}(|\mathbf{0}\rangle_1|\mathbf{0}\rangle_2|\mathbf{0}\rangle_3 + |\mathbf{1}\rangle_1|\mathbf{0}\rangle_2|\mathbf{0}\rangle_3 + |\mathbf{0}\rangle_1|\mathbf{1}\rangle_2|\mathbf{0}\rangle_3$$
$$- |\mathbf{1}\rangle_1|\mathbf{1}\rangle_2|\mathbf{0}\rangle_3)$$
$$= \frac{1}{2\sqrt{2}}(|000\rangle_A|000\rangle_B + |001\rangle_A|001\rangle_B$$
$$+ |010\rangle_A|010\rangle_B + |100\rangle_A|100\rangle_B + |011\rangle_A|011\rangle_B$$
$$+ |101\rangle_A|101\rangle_B - |110\rangle_A|110\rangle_B - |111\rangle_A|111\rangle_B).$$

The Schmidt coefficients of $|\psi_{\text{in}}^{\text{test}}\rangle$ and $|\psi_{\text{out}}^{\text{test}}\rangle$ are found to be $\{\alpha_i\} = \{\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, 0, 0, 0\}$ and $\{\beta_i\} = \{\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}\}$, respectively. Hence $E_{\text{in}}^{\text{test}} = 2$ ebits and $E_{\text{out}}^{\text{test}} = 3$ ebits and $E_T^{\text{Pr}} \geq 1$. (In passing we note that the quantum Toffoli gate cannot be implemented without classical communication: if such an implementation were possible it would violate relativistic causality.)

To obtain the upper bound $E_T^{\text{Im}} \leq 2$ we will describe explicitly a method for realizing the quantum map of the Toffoli that requires 2 ebits. Consider three pairs of qubits on which we are going to apply U_T, where the states $|\Phi\rangle_1$, $|\Psi\rangle_2$ are control and $|\Theta\rangle_3$ is a target (see Fig. 1). It is convenient to analyze in parallel the cases where $|\Phi\rangle_1$ is $|0\rangle_1$ or $|1\rangle_1$. The two parties start by performing local Hadamard rotations $H_{A(B)}$ [acting as $H|0\rangle = \frac{1}{\sqrt{2}} \times (|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$] of A_1 and B_1 of the first
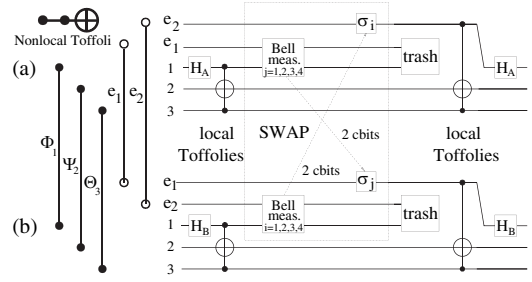

FIG. 1. Implementation of nonlocal Toffoli using 2 ebits as a resource.

pair, obtaining

$$|0\rangle_1 \rightarrow |0'\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle_1^A|0\rangle_1^B + |1\rangle_1^A|1\rangle_1^B),$$
$$|1\rangle_1 \rightarrow |1'\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle_1^A|1\rangle_1^B + |1\rangle_1^A|0\rangle_1^B). \tag{9}$$

Then the parties proceed by performing local Toffoli gates on their particles, which can be written as

$$U_T^{A(B)} = |0\rangle\langle 0|_1 \otimes I_2 \otimes I_3 + |1\rangle\langle 1|_1 \otimes U_{23}, \tag{10}$$

where U_{23} is a local C-NOT between particles 3 and 2 (with particle 3 as the control and particles 2 as the target). As a result the initial states evolve to:

$$|0'\rangle_1|\Psi\rangle_2|\Theta\rangle_3 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_1^A|0\rangle_1^B$$
$$+ |1\rangle_1^A|1\rangle_1^B U_{23}^A U_{23}^B)|\Psi\rangle_2|\Theta\rangle_3,$$
$$|1'\rangle_1|\Psi\rangle_2|\Theta\rangle_3 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_1^A|1\rangle_1^B U_{23}^B$$
$$+ |1\rangle_1^A|0\rangle_1^B U_{23}^A)|\Psi\rangle_2|\Theta\rangle_3.$$

Next they swap the states of A_1 and B_1. This operation utilizes two ebits and can be performed using two ordinary teleportations in both directions. This yields

$$\frac{1}{\sqrt{2}}(|0\rangle_1^A|0\rangle_1^B + |1\rangle_1^A|1\rangle_1^B U_{23}^A U_{23}^B)|\Psi\rangle_2|\Theta\rangle_3,$$
$$\frac{1}{\sqrt{2}}(|1\rangle_1^A|0\rangle_1^B U_{23}^B + |0\rangle_1^A|1\rangle_1^B U_{23}^A)|\Psi\rangle_2|\Theta\rangle_3.$$

Next, they perform (10) again. The resulting states are

$$|0'\rangle_1|\Psi\rangle_2|\Theta\rangle_3 \quad \text{and} \quad |1'\rangle_1 U_{23}^A U_{23}^B|\Psi\rangle_2|\Theta\rangle_3.$$

Finally, they apply H_A and H_B again and obtain

$$|0\rangle_1|\Psi\rangle_2|\Theta\rangle_3 \quad \text{and} \quad |1\rangle_1 U_{23}^A U_{23}^B|\Psi\rangle_2|\Theta\rangle_3.$$

As we have already noted, two local C-NOT transformations are equivalent to a nonlocal C-NOT transformation. Thus, from the last expression it follows that a nonlocal C-NOT is applied on pairs 2 and 3 (with pair 2 as the control and pair 3 as the target) if and only if the state of the first

pair is $|\mathbf{1}\rangle$. Thus this protocol implements the nonlocal Toffoli gate and utilizes two ebits, which are needed to swap two states in the intermediate stage. Because of linearity of quantum mechanics all these arguments will hold also in the case of arbitrary superposition of initial states.

We illustrate our result (8) on the example of Shannon data compression. We were led to consider this particular example by our research in multiparticle entanglement compression [5]. In fact, this is how we discovered this method in the first place.

The method of classical compression of n-bit source string of 0's and 1's, where p is the probability of each bit to be equal 1, is based on the fact that the most probable (typical) strings generated by the source will contain np ones when n is large [6]. If $p \neq \frac{1}{2}$ then the Shannon entropy of the source $H(p)$ is smaller than 1 and the number of typical strings, $2^{nH(p)}$, is less than the total number of strings 2^n. Thus, a message generated by the source can be compressed to a shorter message.

We consider a "Shannon compressor"—a classical reversible circuit which receives as input an n-bit string which contains np ones (i.e., a typical string) and outputs a compressed version of the string in which only the first $\log\binom{n}{np} \simeq nH(p)$ bits carry information and the other $n(1 - H(p))$ redundant bits are set to some standard sequence, e.g., to all 0's:

$$x_1 x_2 \ldots x_n \rightarrow f_1 f_2 \ldots f_{nH} 0_{nH+1} \ldots 0_n. \qquad (11)$$

Our goal is to find a lower bound on the number of Toffoli gates needed to build the "Shannon compressor." We take the initial test state to be the uniform superposition of states with np ones:

$$|\Psi_{\text{in}}^{\text{test}}\rangle = N \sum_{x_i \in \{0,1\}, \sum_i x_i = np} |\mathbf{x_1}\rangle |\mathbf{x_2}\rangle \ldots |\mathbf{x_n}\rangle,$$

where $N = \binom{n}{np}^{-1/2}$. The output state is:

$$|\Psi_{\text{out}}^{\text{test}}\rangle = N \sum_{f_i \in \{0,1\}} |\mathbf{f_1}\rangle |\mathbf{f_2}\rangle \ldots |\mathbf{f_{nH}}\rangle |\mathbf{0_{nH+1}}\rangle \ldots |\mathbf{0_n}\rangle.$$

For fixed value of p we can calculate the entanglement of $|\Psi_{\text{in}}^{\text{test}}\rangle$ and $|\Psi_{\text{out}}^{\text{test}}\rangle$. The entanglement $E_{\text{out}}^{\text{test}}$ is easy to calculate: it equals the number of output redundant pairs, i.e., $E_{\text{out}}^{\text{test}} = n(1 - H(p))$. We have calculated $E_{\text{in}}^{\text{test}}$ using a combination of analytical and numerical techniques which are described in [5]. Figure 2 presents our results for $p = 0.8$. A linear dependence of $E_{\text{in}}^{\text{test}} - E_{\text{out}}^{\text{test}}$ on n is obtained. Thus, the number of Toffoli gates needed to perform Shannon compression grows at least linearly with n. For instance, for $p = 0.8$ we need at least $0.2332n$ Toffoli gates. Inspired by our numerical result, Buhrman has found, using a completely different technique, an analytical proof of this lower bound [7].

In summary, we have addressed the problem of evaluating the number of Toffoli gates needed to perform classical
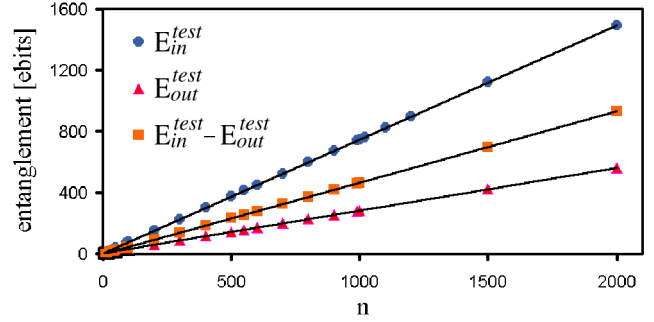

FIG. 2 (color online). Entanglement as a function of string length n for $p = 0.8$.

reversible computations. We have proposed a method based on quantum information concepts in which strings of classical bits are mapped into sequences of special nonlocal quantum states and classical reversible computations are mapped onto unitary transformations of these quantum states. The nonlocal properties of these transformations provide information about the classical reversible computation. In particular, if the unitary transformation is nonlocal then the corresponding classical reversible circuit cannot be built solely from one- and two-bit gates. The amount of nonlocality possessed by the unitary transformation associated with any classical reversible computation provides a lower bound on the number of Toffoli gates needed for this computation.

As an example we considered classical Shannon compression and calculated the amount of nonlocality of the associated unitary transformation. According to our numerical results, the lower bound on the number of Toffoli gates grows linearly with the size of the string n. Thus quantum methods can provide fundamental insights about classical computation.

We hope that our approach may prove useful for other problems concerning classical reversible computation.

[1] C. H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).
[2] T. Toffoli, MIT Report No. MIT/LCS/TM-151, 1980 (unpublished).
[3] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[4] Scott Aaronson (private communication).
[5] B. Groisman, N. Linden, and S. Popescu, quant-ph/0508001.
[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[7] Harry Buhrman (private communication).