Power of One Bit of Quantum Information

E. Knill[1] and R. Laflamme[2]
[1]*MS B265, Los Alamos National Laboratory, Los Alamos, New Mexico 87455*
[2]*MS B288, Los Alamos National Laboratory, Los Alamos, New Mexico 87455*
(Received 6 March 1998)

In standard quantum computation, the initial state is pure and the answer is determined by making a measurement of some of the bits in the computational basis. What can be accomplished if the initial state is a highly mixed state and the answer is determined by measuring the expectation of σ_z on the first bit with bounded sensitivity? This is the situation in high temperature ensemble quantum computation. We show that in this model it is possible to perform interesting physics simulations that have no known efficient classical algorithms, even though the model is less powerful than standard quantum computation in the presence of oracles. [S0031-9007(98)07808-9]

PACS numbers: 03.67.Lx, 89.70.+c

Recent discoveries show that quantum computers can solve problems of practical interest much faster than known algorithms for classical computers [1,2]. This has lead to widespread recognition of the potential benefits of quantum computation. Where does the apparent power of quantum computers come from? This power is frequently attributed to "quantum parallelism," interference phenomena derived from the superposition principle, and the ability to prepare and control pure states according to the Schrödinger equation. Real quantum computers are rarely in pure states and interact with their environments, which leads to nonunitary evolution. Furthermore, recent proposals for using NMR at high temperature to study quantum computation involve manipulations of extremely mixed states [3,4]. Recent research in error-correction and fault-tolerant computation has shown that nonunitary evolution due to weak interactions with the environment results in no loss of computational power, if sufficiently pure states can be prepared [5–8]. Here we consider the situation where there are no errors or interactions with the environment, but the initial state is highly mixed. We investigate the power of *one* bit of quantum information available for computing, by which we mean that the input state is equivalent to having one bit in a pure state and arbitrarily many additional bits in a completely random state. The model of computation that consists of a classical computer with access to a state of this form is called *deterministic quantum computation with one quantum bit* (DQC1). We demonstrate that in the presence of oracles, such a computer is less powerful than one with access to pure state bits. However, it can solve problems related to physics simulations (e.g., spectral density estimation) for which no efficient classical algorithms are known. We also show that both DQC1 and deterministic quantum computation with pure states (DQCp) can be defined in terms of estimation problems for coefficients of unitary operators and give a simple method for making pseudopure states in DQC1. Our work suggests that DQC1 is a nontrivial model of computation that is between classical and standard quantum computation.

There are many kinds of problems that one might like to solve using a computational device. In this Letter we focus on deterministic function evaluation, which reduces to the problem of evaluating the bits of the output string one at a time.

The most important resources used in computation are time and space. How much of either is required depends on the model of computation. For a given problem, one usually tries to determine the resources required as a function of the *problem size*, which for one-bit functions is the number of bits in the input string. An algorithm is considered to be *efficient* if the resource requirements are polynomial in the problem size. The powers of two models are considered to be the same if for any algorithm in one model, there is an equivalent algorithm in the other model that uses at most a polynomial multiple of the resources. For a comprehensive treatment of classical computational complexity theory, see [9]. A good reference for quantum complexity theory is [10].

The available computational devices are assumed to include a classical probabilistic computer conforming to the model of an abstract random access machine with access to random bits, and a quantum system consisting of as many (quantum) bits as needed. We assume that the procedure used to evaluate the function f on input b consists of the generation of a sequence of unitary operations using a classical computer and the application of these operations to the quantum system in a specified initial state. A measurement of the quantum system then yields the answer. Answers from one repetition may be used to make decisions in the next ones. The models studied here differ in what are the permitted initial states and measurements. Function evaluation is performed probabilistically and we are satisfied with a high enough probability of success.

The state space of the quantum system of n bits is the complex Hilbert space $\mathcal{Q}^n$ generated by the computational basis. This basis is labeled by binary strings of length n; the basis element corresponding to string b is denoted by $|b\rangle$. $\mathcal{Q}^n$ is the n-fold tensor product of $\mathcal{Q}^1$. To describe

 0031-9007/98/81(25)/5672(4)$15.00

unitary operators and states, it is convenient to use the operator basis consisting of tensor products of the Pauli operators [11]

$$I \doteq \sigma_{00} \doteq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \qquad \sigma_x \doteq \sigma_{01} \doteq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (1)$$

$$\sigma_y \doteq \sigma_{10} \doteq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \qquad \sigma_z \doteq \sigma_{11} \doteq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (2)$$

A Pauli operator acting on the kth bit is denoted by $\sigma_b^{(k)}$. A general tensor product of Pauli operators is denoted by σ_b, where $b_{2k-1}b_{2k}$ is the index of the operator acting on the kth bit.

A *pure state* of a quantum system consisting of n bits is a unit vector in $\mathcal{Q}^n$. In general, the quantum system can be correlated with other systems that we do not have access to. As a result, the general state of the system can be described by a density operator. When using highly mixed (far from pure) states, it is convenient to describe a state by means of deviations from the identity expressed as sums of Pauli operators. In general, a state ρ can be written in the form

$$\rho = \frac{1}{2^n}\left(I + \sum_{b \neq \mathbf{0}} a_b \sigma_b\right), \quad (3)$$

where the a_b are real and $\mathbf{0}$ is the bit string of all 0's. The deviation of ρ is the nonidentity component of the sum given by $\sum_{b\neq\mathbf{0}} a_b\sigma_b$. For example, the deviation of the state where the first bit is 0 and the other bits are completely random is given by $\sigma_z^{(1)}$.

The effect of an operation on the quantum system can be described by a unitary operator U that maps an input state $|\psi\rangle$ to the output state $U|\psi\rangle$. In terms of operators, U takes the state ρ to $U\rho U^\dagger$.

In both of the models of quantum computation to be discussed in this Letter, the elementary operations (quantum gates) that can be applied are a complete set of one- and two-bit unitary operators [12,13]. A network implementation of a unitary operator U is a decomposition of U as a product of elementary gates.

Deterministic quantum computation with pure states (DQCp).—The initial state of the quantum system is $|\mathbf{0}\rangle$. In the standard model of quantum computation, the final (one-bit) answer is obtained by a measurement of the first bit. In DQCp, this measurement is replaced by a process that yields the noisy expectation of $\sigma_z^{(1)}$ for the final state. There is no loss of power by making this restriction on the final measurement. To be specific, if the state of the quantum system is ρ, the measurement process returns a number that is sampled from a distribution with mean $\langle\sigma_z^{(1)}\rangle = \mathrm{tr}(\sigma_z^{(1)}\rho)$ and variance s, where s is independent of the number of bits used. We call such a measurement an *estimate* of the quantity measured. Repeating the computation and measurement is assumed to yield independent instances of this distribution. Thus, the mean can be estimated to within ϵ with probability of error at most p using $O(\log(1/p)/\epsilon^2)$ repetitions of the computation [14]. DQCp is realized by an idealized bulk NMR quantum computer, where all molecules are initially perfectly polarized, with no decoherence or operational errors.

If U is a unitary operator with a network implementation, then DQCp yields an estimate of $\mathrm{tr}(\sigma_z^{(1)}U|\mathbf{0}\rangle\langle\mathbf{0}|U^\dagger)$. The values of $\mathrm{tr}(\sigma_b U|c\rangle\langle c|U^\dagger)$ can be obtained by pre- and postprocessing the state using individual bit rotations. Since the resources required for pre- and postprocessing are linear in the number of bits, we can identify (the power of) DQCp with the ability to estimate these expressions.

Deterministic quantum computation with one bit (DQC1).—The deviation of the initial state of the quantum system is $\sigma_z^{(1)}$. The final answer is obtained as in DQCp by a bounded variance process yielding $\langle\sigma_z^{(1)}\rangle$. The initial state corresponds to having one bit in a pure state and the rest completely random.

DQC1 is realized by an idealized high temperature NMR quantum computer where there is no decoherence and no operational error. This is the regime where the initial deviation state can be approximated by $e^{-\beta H}/Z \sim \frac{1}{2^n}(I - \beta\sum_i e_i\sigma_z^{(i)})$ (noninteracting bits), with negligible higher order terms. The one-bit initial state can be obtained by eliminating polarization in bits other than the first. Exploiting the additional polarization can reduce the time resource required by at most a factor of $1/n$, so that no additional power can be gained. Constraints on the amount of polarization extractable from arbitrary initial states have been investigated by Sörensen [15]. DQC1 is not robust against many error models because fresh ground-state bits cannot be introduced during the computation [16].

Let U be a unitary operator with a network implementation. Using DQC1 and pre- and postprocessing similar to that introduced with DQCp, we can estimate $\mathrm{tr}(\frac{1}{2^n}\sigma_a U\sigma_b U^\dagger)$ for any a and b. We can therefore identify DQC1 with the ability to obtain these estimates.

Theorem 1.—DQCp is at least as powerful as DQC1.

Proof.—Since

$$\mathrm{tr}\left(\frac{1}{2^n}\,\sigma_z^{(1)}U\sigma_z^{(1)}U^\dagger\right) = \frac{1}{2^n}\sum_c (-1)^{c_1}\,\mathrm{tr}(\sigma_z^{(1)}U|c\rangle\langle c|U^\dagger), \quad (4)$$

the estimate obtained with DQC1 can be obtained with DQCp by randomly sampling a few of the $(-1)^{c_1}\,\mathrm{tr}(\sigma_z^{(1)}U|c\rangle\langle c|U^\dagger)$ and estimating the average.

If Eq. (4) is inverted one finds that the estimates available in DQCp are expressed as a *sum* rather than as an *average* of DQC1 estimates. As a result, the proof cannot be used to obtain the converse of Theorem 1.

DQCp and DQC1 can be used to estimate any coefficient of certain operator expansions of U. For DQC1, write $U = \sum_b \alpha_b\sigma_b$, with $\alpha_b = \frac{1}{2^n}\mathrm{tr}(\sigma_b U)$. This is the *Pauli operator* expansion of U. To determine α_b, use the network for U to construct a network for the operator V that maps $|0\rangle|b\rangle \rightarrow |0\rangle U|b\rangle$ and $|1\rangle|b\rangle \rightarrow |1\rangle|b\rangle$. This is a "conditional" U operator and can be implemented with

a linear amount of additional resources [13]. Then

$$\frac{1}{2^{n+1}}\,\mathrm{tr}[(\sigma_x^{(1)} + i\sigma_y^{(1)})V\sigma_x^{(1)}\sigma_b V^\dagger] =$$

$$\frac{1}{2^{n+1}}[\mathrm{tr}(U\sigma_b) + \mathrm{tr}(\sigma_b U^\dagger)] = \alpha_b\,. \qquad (5)$$

Since $U\sigma_b U^\dagger$ is a unitary operator easily implemented given networks for U, we have proved the following result.

Theorem 2.—The ability to efficiently estimate the coefficients of the Pauli operator expansion of the operator implemented by a quantum network is equal in power to DQC1.

If the trick of the previous paragraph is used with DQCp, where U is replaced by $\sigma_c U\sigma_d$, with c and d chosen so that $\sigma_c|\mathbf{0}\rangle = |b\rangle$ and $\sigma_d|\mathbf{0}\rangle = |a\rangle$, then we can obtain $\mathrm{tr}(U|a\rangle\langle b|)$. Therefore any of the transition amplitudes of U can be determined to get coefficients of the *matrix* U in the computational basis. Because $\mathrm{tr}(\sigma_z^{(1)}U|\mathbf{0}\rangle\langle\mathbf{0}|U^\dagger) = \mathrm{tr}(U^\dagger\sigma_z^{(1)}U|\mathbf{0}\rangle\langle\mathbf{0}|)$, we have established the following.

Theorem 3.—The ability to efficiently estimate the transition amplitudes of an operator implemented by a quantum network is equal in power to DQCp.

Let the evolution of a quantum mechanical system be described by a (possibly time varying) Hamiltonian H on a Hilbert space $\mathcal{H}$. To efficiently simulate this evolution using a quantum computer with n bits, it is sufficient to have a unitary embedding of $\mathcal{H}$ into $\mathcal{Q}^n$ and an extension H' of the embedded Hamiltonian for which there are efficient quantum networks approximating $e^{-iH'(t)\delta}$ (taking $\hbar = 1$) for small δ to within $O(\delta^2)$. A class of such Hamiltonians consists of those that are a polynomially bounded sum of two bit Hamiltonians [17]. Whether it is useful to implement this simulation depends on what information one wants to obtain. If one simply wants to predict the outcome of a measurement in an experiment involving this system, it is possible to do that by simulation, provided that the initial state can be computed and the final measurement can be represented as a measurement in the computational basis or expectations of operators that can be approximated as a sum of a reasonable number of computable conjugates of $\sigma_z^{(1)}$.

Even if the initial state is restricted to the deviation $\sigma_z^{(1)}$, there are no known classical algorithms for simulating an arbitrary sum of two-bit Hamiltonians as described above. Since many real-world situations involve highly mixed initial states (e.g., most NMR experiments), such an algorithm is very interesting. In fact, there are ongoing experiments exploiting the fact that many $\frac{1}{r^3}$ interactions can be simulated in solid state systems such as calcium-fluoride by modifying the dipolar interaction but are difficult to simulate using classical computation [18]. The observation that one can efficiently implement such simulations in DQC1 makes this model useful and the question of the relationship between the powers of DQC1 and DQCp or classical computation nontrivial.

For any Hamiltonian, one of its physical properties of interest is the energy spectrum. In DQC1 it is possible to directly observe the spectrum with a resolution inversely related to the effort used. No efficient classical algorithms that accomplish this are known, and neither is there a known DQCp method that can improve on this. There are experimental methods for observing energy transitions of effective Hamiltonians [19]. Here is a method for observing spectra (rather than transitions) of Hamiltonians or unitary operators with network implementations. Let $U(t) = e^{-iHt}$ and assume that an efficient quantum network for applying $U(t)$ with arbitrarily small error is available. Note that the quantum network may increase in complexity if less error is needed. Given the quantum network for $U(t)$, we can derive networks for applying $U(t)$ or $U^\dagger(t)$ to bits $2,\ldots,n+1$, conditionally on the state of the first bit. Let $V(t)$ be the unitary operator that maps $|1\rangle|b\rangle \to |1\rangle U^\dagger(t/2)|b\rangle$ and $|0\rangle|b\rangle \to |0\rangle U(t/2)|b\rangle$. If we first apply a gate to transform the input state $\sigma_z^{(1)}$ to $\sigma_x^{(1)}$, and then apply $V(t)$, the deviation of the state becomes

$$\rho_f = \sum_i [\cos(\lambda_i t)\sigma_x^{(1)} + \sin(\lambda_i t)\sigma_y^{(1)}]\,|i\rangle\langle i|$$

$$= \frac{1}{2^n}\sum_i [\cos(\lambda_i t)\sigma_x^{(1)} + \sin(\lambda_i t)\sigma_y^{(1)}] + \mathrm{rest}, \qquad (6)$$

where the λ_i and $|i\rangle$ are a complete set of eigenvalues and corresponding eigenvectors (with repetition) of H. The second identity gives the expansion of ρ_f in terms of σ_b's, with terms not of interest suppressed (rest). The coefficients of σ_x and σ_y can be measured and the results combined into a single complex number with value $f(t) = \frac{1}{2^{n+1}}\sum_j e^{-i\lambda_j t}$. This can be sampled at as many time points as desired, using repetition to decrease noise, and Fourier transformed to obtain a broadened energy spectrum. The same technique can be used to measure the spectrum of a unitary operator by restricting t to integer multiples (corresponding to powers of the operator). If the evolution $V(t)$ is implemented as a power of $V(\Delta t)$, and the measurement in DQC1 is nondestructive, then the spectrum can in principle be observed directly as is done in Fourier transform NMR spectroscopy.

DQC1 is strictly less powerful than DQCp in the presence of oracles (aka black boxes). Suppose that we are given a black box implementing a unitary operator U on our quantum system and we wish to determine $\langle\mathbf{0}|U^\dagger\sigma_z^{(1)}U|\mathbf{0}\rangle$, whose sign is the one-bit *answer* computed by U on input $|\mathbf{0}\rangle$. One method for obtaining this answer using DQC1 involves preparing a *pseudopure* state from the deviation $\sigma_z^{(1)}$ [3,4]. One kind of pseudopure state has deviation proportional to that of $|\mathbf{0}\rangle\langle\mathbf{0}|$. In this case measurement of $\sigma_z^{(1)}$ after applying U is proportional to the desired answer.

Here is a simple method for making a pseudopure state from $\sigma_z^{(1)}$ using an ancilla bit, labeled 0. This method

compares favorably with those previously described for ensemble quantum computation [3,4,20]. Let T_n be the unitary operator mapping $|b_0\mathbf{0}\rangle \rightarrow |(b_0 + 1)\mathbf{0}\rangle$ and for $b \neq 0$, $|b_0 b\rangle \rightarrow |b_0 b\rangle$ (addition of bits is modulo two). If we first swap bits 0 and 1, then apply T_n, and finally flip bit 0, the deviation is given by $\sigma_z^{(0)}(2|\mathbf{0}\rangle\langle\mathbf{0}| - I)$. If we apply U to bits 1 through n, then the coefficient α of $\sigma_z^{(0)}\sigma_z^{(1)}$ in the state's deviation is the answer we want. As discussed above, this coefficient can be obtained using DQC1, with an intensity of $\alpha/2^{n+1}$. Because of the exponential loss of intensity, it can be difficult to detect α above the noise.

Unfortunately, without the ability to analyze a specification of U (for example, an implementation by a quantum network), we cannot do much better, even if we know that the answer of U is deterministic, that is, $\alpha \in \{-1, 1\}$.

Theorem 4.—To determine the answer of quantum black boxes, exponentially more resources are needed in DQC1 than in DQCp.

Proof.—The most general form of a DQC1 algorithm for determining the answer can be described by k independent DQC1 computations consisting of quantum networks and calls to U and an inference function that attempts to determine α from the k measurements. Consider the first of these measurements. The expectation of the result of the measurement can be written in the form

$$v(U) = \frac{1}{2^m}\,\mathrm{tr}(V_r U \cdots U V_0 \sigma_z^{(1)} V_0^\dagger U^\dagger \cdots U^\dagger V_r^\dagger \sigma_z^{(1)}), \tag{7}$$

where r is the number of invocations of U and the V_i are the quantum networks used in the computation using m bits (of which $m - n$ are ancillas). Since U is deterministic, $U|0\rangle|\mathbf{0}\rangle = |b\rangle|\psi\rangle$. If U is composed with the operator T that, conditionally on the state of bits 2 to n being $|\psi\rangle$, flips the first bit, we get an operator U' that is also deterministic but has the opposite answer. We must be able to distinguish between the two. T can be written in the form $T = I - 2P$, where P is the pure state given by $\frac{1}{2}(I - \sigma_x^1) \otimes |\psi\rangle\langle\psi|$ (the $m - n$ ancillas have been suppressed in this expression). For unitary operators W_1 and W_2 acting on $m \geq n$ bits, we have $|\frac{1}{2^m}\,\mathrm{tr}(W_1 P W_2)| \leq \frac{1}{2^n}$. By expanding $U' = U - 2PU$ in the expression for $v(U')$ we can write

$$\begin{aligned} v(U') &= \frac{1}{2^m}\{\mathrm{tr}[V_r(-2P)UV_{r-1}U'\ldots] + \mathrm{tr}(V_r U V_{r-1} U' \ldots)\} \\ &= \frac{1}{2^m}\{\mathrm{tr}[V_r(-2P)UV_{r-1}U'\ldots] + \mathrm{tr}[V_r U V_{r-1}(-2P)UV_{r-2}U'\ldots] + \mathrm{tr}(V_r U V_{r-1} U V_{r-2} U' \ldots)\} \\ &= \frac{1}{2^m}\{\mathrm{tr}[V_r(-2P)UV_{r-1}U'\ldots] + \mathrm{tr}[V_r U V_{r-1}(-2P)UV_{r-2}U'\ldots] + \cdots + v(U)\}. \end{aligned} \tag{8}$$

Thus, $v(U') = \frac{1}{2^m}(a_1 + \cdots + a_{2r}) + v(U)$, where $|a_i| \leq 2^{m-n+1}$. It follows that $|v(U') - v(U)| \leq 4r/2^n$. Therefore, to confidently distinguish between U' and U requires exponentially many experiments or invocations of the oracle.

We have introduced a new model of computation (DQC1) with power between classical computation and deterministic quantum computation with pure states (DQCp). Since DQC1 requires only one quantum bit of information, the possibility that it adds power to classical computation is surprising. If this is the case, the usual reasons given for why quantum computation appears to be so powerful may have to be revised. On the other hand, a proof that DQC1 can be efficiently simulated by classical computation would be extremely interesting, as this could lead to practical algorithms for simulations of many experimentally interesting physical situations.

We thank David Cory, Tim Havel, and Michael Nielsen for helpful discussions, and the National Security Agency for financial support.

[1] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[3] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).
[4] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
[5] E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).
[6] J. Preskill, Proc. R. Soc. London A **454**, 385 (1998).
[7] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1996), pp. 176–188, quant-ph/9611025.
[8] A. Yu. Kitaev, Usp. Mat. Nauk **52**, 53–112 (1997).
[9] C. H. Papdimitriou, *Computational Complexity*, (Addison-Wesley, Reading, MA, 1994).
[10] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).
[11] S. S. Somaroo, D. G. Cory, and T. F. Havel, Phys. Lett. A **240**, 1 (1998).
[12] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[13] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).
[14] P. J. Huber, *Robust Statistics* (Wiley, New York, 1981).
[15] O. W. Sörensen, Prog. Nucl. Magn. Reson. Spectrosc. **21**, 503 (1989).
[16] D. Aharonov, M. Ben-Or, R. Impagliazzo, and N. Nisan, quant-ph/9611028.
[17] S. Lloyd, Science **273**, 1073 (1996).
[18] W. Zhang and D. G. Cory, Phys. Rev. Lett. **80**, 1324 (1998).
[19] J. S. Waugh, in *Encyclopedia of Nuclear Magnetic Resonance*, edited by D. M. Grant and R. K. Harris (Wiley, New York, 1996), pp. 849–854.
[20] E. Knill, I. Chuang, and R. Laflamme, Phys. Rev. A **57**, 3348 (1998).