Quantum Adiabatic Algorithm for Factorization and Its Experimental Implementation

Xinhua Peng,[1] Zeyang Liao,[1] Nanyang Xu,[1] Gan Qin,[1] Xianyi Zhou,[1] Dieter Suter,[2] and Jiangfeng Du[1,*]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[2]*Fakultät Physik, Technische Universität Dortmund, 44221 Dortmund, Germany*

(Received 10 August 2008; published 26 November 2008)

We propose an adiabatic quantum algorithm capable of factorizing numbers, using fewer qubits than Shor's algorithm. We implement the algorithm in a NMR quantum information processor and experimentally factorize the number 21. In the range that our classical computer could simulate, the quantum adiabatic algorithm works well, providing evidence that the running time of this algorithm scales polynomially with the problem size.

DOI: 10.1103/PhysRevLett.101.220405 PACS numbers: 03.65.Ud, 05.50.+q, 87.23.Cc

Using quantum mechanical systems as computational devices may be a possible way to build computers that are qualitatively more powerful than classical computers [1]. The algorithms that are adapted to the special capabilities of these devices are called quantum algorithms. One of the best known quantum algorithms is Shor's algorithm for integer factorization [2]. Since no efficient factorization algorithm is known for classical computers [3], various cryptographic techniques rely on the difficulty of finding the prime factors of large numbers [4]. However, in 1994, Peter Shor developed a quantum algorithm that can factorize large numbers in polynomial time [2]. This discovery was one of the main reasons for the subsequent strong interest in quantum computation. An experimental implementation of Shor's algorithm was demonstrated by Vandersypen *et al.* [5], using nuclear spins as qubits to find the prime factors of 15. More recent experiments by Lu *et al.* [6] and Lanyon *et al.* [7] used photons as qubits and found the same factors.

While Shor's algorithm and its experimental implementation are based on the circuit (or network) model of quantum computation, an alternative computational model has been proposed by Farhi *et al.* [8]. This model is based on the quantum adiabatic theorem: a quantum system remains in its instantaneous eigenstate if the system Hamiltonian varies slowly enough and if there is a gap between this eigenvalue and the rest of the Hamiltonian's spectrum [9]. It has been proved that this adiabatic model of quantum computing is equivalent to the conventional circuit model [10]. Several adiabatic quantum algorithms have been discussed theoretically and experimentally, such as 3SAT [8,11,12] and search of unstructured databases [13]. Moreover, since the adiabatic scheme only involves the ground state, (as long as the system is kept at low temperature), it appears to offer lower sensitivity to some perturbations and thus improved robustness against errors due to dephasing, environmental noise and some unitary control errors [14]. Therefore, adiabatic quantum computation has recently attracted extensive interest. Here we first apply the adiabatic method to the problem of integer factorization.

A large number of the computationally hard problems can be formulated as optimization problems. The quantum adiabatic evolution provides an attractive approach to solve this kind of problems. It requires a problem Hamiltonian H_P to describe the problem, whose ground state encodes the answer. Classically, finding the ground state of a Hamiltonian is a computationally hard problem. Adiabatic evolution gives a natural method to find the ground states. Suppose a quantum system starts with an initial Hamiltonian H_0, whose ground state $\psi_g(0)$ is known. Then if a time-dependent Hamiltonian $H(t)$ of the system varies slowly enough to fulfill the adiabatic condition, the evolving quantum state $\psi(t)$ will remain close to the instantaneous ground state $\psi_g(t)$ of $H(t)$. We take $H(T) = H_P$ at a time T, which means the ground state $\psi_g(T)$ encodes the solution of the optimization problem. The change of the Hamiltonian is realized by an interpolation scheme

$$H(t) = [1 - s(t)]H_0 + s(t)H_P, \tag{1}$$

where the function $s(t)$ varies from 0 to 1 to parametrize the interpolation. The solution of the optimization problem is then determined by measuring the final ground state $\psi_g(T)$ of H_P.

We now apply this approach to find nontrivial prime factors of an ℓ-bit integer $N = p \times q$ where p and q are prime numbers. We can write the factorization problem as an optimization problem by using the function $f(x, y) = (N - xy)^2$, in which the variables x and y are positive integers. Clearly, the minimum of this function is reached when x and y are the factors of N.

To solve this optimization problem by the adiabatic quantum algorithm, we must construct a problem Hamiltonian for the function $f(x, y)$, whose ground state is the solution. Generally, the eigenvalues of the problem Hamiltonian are $f(x, y)$, and the corresponding eigenvec-

tors $|x\rangle$ and $|y\rangle$ represent the variables x and y. These conditions are satisfied by $H_P = \sum_{x,y} f(x,y)|x,y\rangle\langle x,y|$.

To determine the Hilbert space that we need for implementing this scheme, we first consider the range of the variables x and y. Without loss of generality, we assume that N is odd (in case of even N, we could repeatedly divide N by 2 until an odd integer is obtained). Since N is odd, its factors x and y must also be odd; i.e., its last bit is always 1 and can therefore be omitted from the computation. Without loss of generality, we choose $x < y$ and $3 \le x \le \sqrt{N}$, $\sqrt{N} \le y \le \frac{N}{3}$. It is then easy to prove that $n_x = m(\lfloor\sqrt{N}\rfloor_o) - 1 \le \lfloor\frac{\ell+1}{2}\rfloor - 1$ bits are sufficient to represent x and $n_y = m(\lfloor\frac{N}{3}\rfloor) - 1 \le \ell - 2$ bits to represent y, where $\lfloor a\rfloor$ ($\lfloor a\rfloor_o$) denotes the largest (odd) integer not larger than a, while $m(b)$ denotes the smallest number of bits required for representing b. The total number of qubits required is then $n = n_x + n_y \le \lfloor\frac{\ell+1}{2}\rfloor + \ell - 3 \sim O(3l/2)$, which is less than the number of qubits used in Shor's algorithm, $2\ell + 1 + \lceil\log(2 + \frac{1}{2\varepsilon})\rceil \sim O(2l)$, where ε is the failure probability and $\lceil c\rceil$ denotes the smallest integer not less than c [2]. Obviously, at least 25% of qubits are saved in our present adiabatic algorithm.

Using the conventional computational basis $\{|0\rangle, |1\rangle\} = \{|\uparrow\rangle, |\downarrow\rangle\}$, it is straightforward to construct the problem Hamiltonian:

$$H_P = \left[NI - \left(2^{n_x-1}\frac{I-\sigma_z^1}{2} + \cdots + 2^1\frac{I-\sigma_z^{n_x-1}}{2} + I\right) \times \left(2^{n_y-1}\frac{I-\sigma_z^{n_x}}{2} + \cdots + 2^1\frac{I-\sigma_z^{n}}{2} + I\right)\right]^2, \quad (2)$$

where I represents the unit operator and σ_z^i is the Pauli matrix of qubit i.

All computational basis states $|z_1 z_2 \ldots z_n\rangle$, with $z_i = 0$ or 1, are eigenstates of H_P and the corresponding eigenvalues are $(N - xy)^2$, in which x and y are represented by the bits $z_1 \ldots z_{n_x}$ and $z_{n_x+1} \ldots z_n$, respectively. The lowest eigenvalue of H_P is 0, and the corresponding eigenstate (i.e., the ground state) $|p'\rangle|q'\rangle$ encodes the factors $p = 2p' + 1$ and $q = 2q' + 1$.

As the initial Hamiltonian, we choose

$$H(0) = g(\sigma_x^1 + \sigma_x^2 + \cdots + \sigma_x^n). \quad (3)$$

This Hamiltonian describes a system, in which all the spins interact with the same magnetic field with strength g, oriented along the x axis. Its ground state is

$$|\psi_g(0)\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}(-1)^{b(j)}|j\rangle, \quad (4)$$

where $b(j)$ is the parity of j [i.e., the number of 1 s in the binary representation mod 2]. The initial state is thus an equal superposition of all computational basis states, each representing a combination of trial factors x and y.

In the adiabatic process, the system evolves under the time-dependent Hamiltonian (1) according to the Schrödinger equation:

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \quad (5)$$

with the initial condition $|\psi(0)\rangle = |\psi_g(0)\rangle$. The adiabatic theorem [9] ensures that, if the evolution time T is long enough, the quantum system will always be close to the ground state of $H(t)$, and the final state will be the solution of the problem.

As an example, we apply this algorithm to the factorization of 21. The number of qubits required to represent the two registers x and y is $n_x = m(\lfloor\sqrt{21}\rfloor_o) - 1 = 1$, $n_y = m(\lfloor\frac{21}{3}\rfloor) - 1 = 2$. Hence, the total number of qubits needed is $n = 3$. According to Eq. (2), the problem Hamiltonian is:

$$H_P = 210I + 84\sigma_z^1 + 88\sigma_z^2 + 44\sigma_z^3 - 20\sigma_z^1\sigma_z^2 - 10\sigma_z^1\sigma_z^3 + 20\sigma_z^2\sigma_z^3 - 16\sigma_z^1\sigma_z^2\sigma_z^3. \quad (6)$$

Its energy-level diagram is shown in Fig. 1(a) where we used $s(t) = (t/T)^2$ to interpolate the Hamiltonian (1), a total evolution time $T = 0.168$ and $g = 30$. Under these conditions, the adiabatic condition is satisfied as the system evolves towards the desired final state at $t = T$. The blue

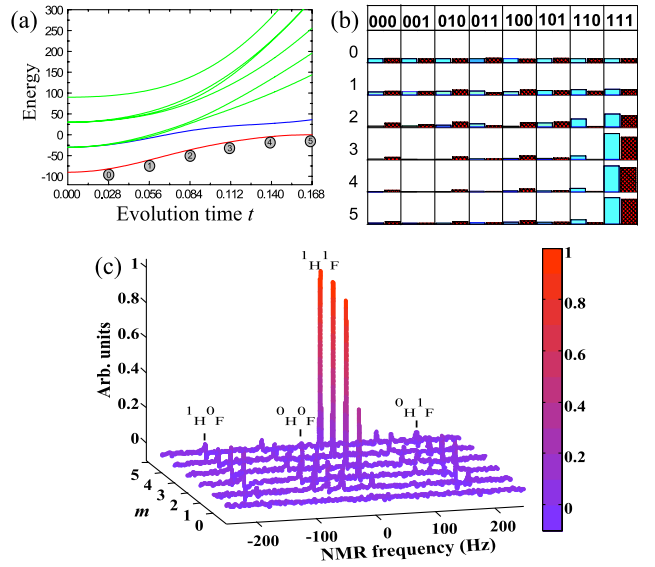

FIG. 1 (color online). (a) Energy-level diagram for the adiabatic factorization of $N = 21$ when $s(t) = (t/T)^2$ and $T = 0.168$. (b) Occupation probabilities for the computational basis states $|z_1 z_2 z_3\rangle$ for the theoretical simulation [denoted by blue (light gray) bars] and experimentally reconstructed populations of the computational basis states after m evolution steps [denoted by red (dark gray) bars]. (c) Measured spectra of ^{13}C for each adiabatic step. The four resonance lines of ^{13}C are labeled by the corresponding states of the two other qubits. The spectra were adjusted as absorption spectra by 180° phase correction, which leads to positive amplitude indicating the $|1\rangle$ subspace of the ^{13}C qubit. A color scale indicates peak intensities, which are in arbitrary units. The system starts in an equal weight superposition and evolves to the desired final state $|111\rangle$, which encodes the solution $p = 3$, $q = 7$.

(light gray) bars in Fig. 1(b) show the numerical simulation for the evolution of the occupation probabilities of the computational basis states $|z_1 z_2 z_3\rangle$ when the whole adiabatic evolution is divided into 6 equidistant steps. The ground state of the problem Hamiltonian, $|111\rangle$ encodes the value of x in the first bit, so $p = 2z_1 + 1 = 3$, and the value of y in the second and third bits, $q = 4z_2 + 2z_3 + 1 = 7$.

Now we turn to the real physical system (a three-qubit NMR quantum processor) to demonstrate this algorithm. The three qubits are represented by the ^{1}H, ^{13}C, and ^{19}F nuclear spins of Diethyl-fluoromalonate. The molecular structure is shown in Fig. 2(a), where the three nuclei used as qubits are marked by the oval. The natural Hamiltonian of the three-qubit system in the rotating frame is

$$\mathcal{H}_{\mathrm{NMR}} = \sum_{i=1}^{3} \frac{\omega_i}{2} \sigma_z^i + \sum_{i<j,=1}^{3} \frac{\pi J_{ij}}{2} \sigma_z^i \sigma_z^j, \qquad (9)$$

where ω_i represent the field strengths and J_{ij} the coupling

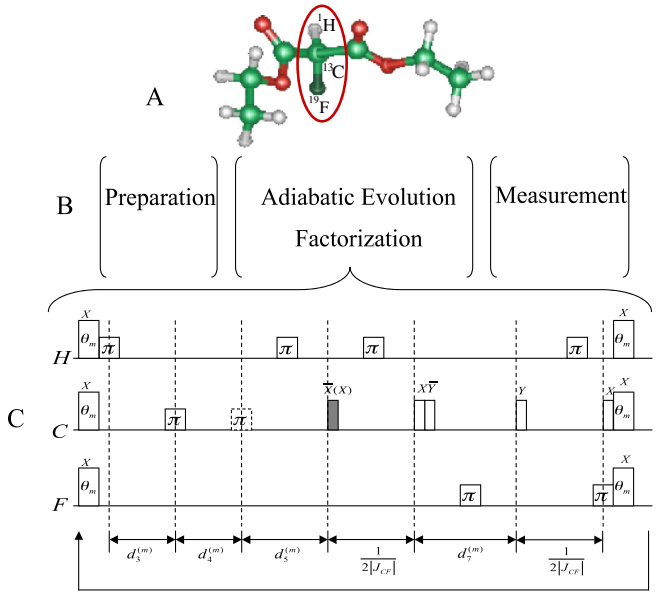

FIG. 2 (color online). (a) Molecular structure of Diethyl-fluoromalonate, (b) schematic representation of the experiment and (c) the pulse sequence that implements the adiabatic evolution for factorizing 21. The oval in (a) marks the three spins used as qubits. The rectangles in (c) labeled with θ_m represent rotations by an angle $g[1 - (\frac{m}{M})^r]\tau$, while the narrow empty rectangles denote 90° rotations and the wide ones (labeled by π) denote the refocusing 180° pulses. The delays are $d_3^{(m)} = 10(\frac{m}{M})^r\tau(\frac{1}{\pi J_{\mathrm{HF}}} + \frac{2}{\pi J_{\mathrm{HC}}})$, $d_4^{(m)} = 10(\frac{m}{M})^r\tau(\frac{1}{\pi J_{\mathrm{HF}}} - \frac{2}{\pi J_{\mathrm{HC}}})$, $d_5^{(m)} = \frac{1}{2|J_{\mathrm{CF}}|} - 20(\frac{m}{M})^r\tau(\frac{1}{\pi J_{\mathrm{HC}}} + \frac{1}{\pi |J_{\mathrm{CF}}|})$, and $d_7^{(m)} = 32(\frac{m}{M})^r\tau\frac{1}{\pi J_{\mathrm{HC}}}$. Negative durations $d_5^{(m)} < 0$ according to this formula were implemented as positive ones, by omitting the dashed π pulse preceding $d_5^{(m)}$ and replacing the gray $-x$ pulse immediately after the period by an x pulse.

constants $J_{\mathrm{HC}} = 161.3$ Hz, $J_{\mathrm{CF}} = -192.2$ Hz and $J_{\mathrm{HC}} = 47.6$ Hz. The experiments were carried out at room temperature, using a Bruker Avance II 500 MHz (11.7 Tesla) spectrometer equipped with a QXI probe with pulsed field gradient.

The experiment was divided into three steps [Fig. 2(b)]: initial state preparation into the ground state of $H(0)$, adiabatic passage for the time-dependent $H(t)$, and measurement of the final ground state of $H(T)$. Starting from thermal equilibrium, we first created a pseudopure state [15] $\rho_{000} = \frac{1-\epsilon}{8}\mathbf{1} + \epsilon|000\rangle\langle 000|$, with $\mathbf{1}$ representing the 8×8 unity operator and $\epsilon \approx 10^{-5}$ the polarization. The ground state of $H(0)$ [Eq. (4)] was prepared from ρ_{000} by applying $\pi/2$ pulses along the $-y$ axis to each qubit.

The adiabatic evolution of $H(t)$ was approximated by $M + 1$ discrete steps [11,16]. Instead of the usual linear interpolation $s(t) = t/T$, we used a polynomial interpolation, $s_m = (m/M)^r$, with r integer and $0 \le m \le M$. The unitary evolution for the discrete adiabatic passage is then $U = \prod_{m=0}^{M} U_m = \prod_{m=0}^{M} e^{-iH_m\tau}$, where the duration of each step is $\tau = T/(M + 1)$. The adiabatic limit is achieved when both T, $M \to \infty$ and $\tau \to 0$. Using Trotter's formula, we can approximately generate the unitary operators

$$U_m \approx e^{-iH_0(1-s_m)(\tau/2)} e^{-iH_P s_m \tau} e^{-iH_0(1-s_m)(\tau/2)} + O(\tau^3).$$

The pulse sequence for the implementation of the adiabatic evolution is shown in Fig. 2(c). As a suitable set of parameters, we chose the values $g = 30$, $r = 2$, $M = 5$ and $\tau = 0.028$. This parameter set yields an adiabatic evolution that finds the solution in a relatively efficient way. The theoretical fidelity is around 0.91. This means that the final state has more than 90% overlap with the true solution state corresponding to the factors.

To read out the final state, only the occupation numbers of the different computational basis states are required. To measure the populations, we first applied a pulsed field gradient to dephase transverse magnetization, and then a $[\pi/2]^i_{-y}$ readout pulse to qubit i and measured the resulting free induction decay signal. The readout procedure was applied to each of the three qubits in subsequent experiments. In the experiment, we used a sample in natural abundance; i.e., only $\approx 1\%$ of the molecules had a ^{13}C nuclear spin. To distinguish those molecules against the large background, we read out all three qubits via the ^{13}C channel, by applying SWAP gates and measuring the ^{13}C qubit.

Figure 1(c) shows experimental spectra obtained by reading out the ^{13}C qubit, at different instances during the adiabatic transfer. The spectrum consists of four resonance lines; in the figure, they are labeled by the corresponding logical states of the ^{1}H and ^{19}F qubits. While these four resonance lines have initially comparable amplitude, the last 2 measurements find almost all the amplitude in the line at 15.5 Hz, which corresponds to the $|11\rangle$ state of the ^{1}H and ^{19}F qubits. Since the amplitude is

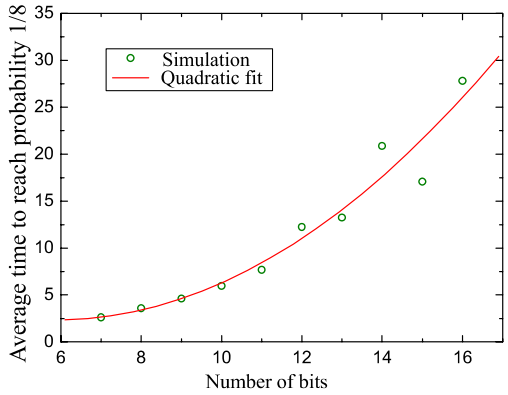

FIG. 3 (color online). Average evolution time for achieving the probability $1/8$ for 50 instances as a function of the number of input bits n. The circles represent the simulation data for the bit length $7 \leq n \leq 16$, while the solid line shows the quadratic fit to the data.

positive, the ^{13}C qubit must also be in the $|1\rangle$ state. The red (dark gray) bars in Fig. 1(b) show the populations of the eight computational ground states. They were obtained from a least-squares fit to the spectra measured after reading out the three different qubits. The results confirm that the final state has a high occupation probability on the $|111\rangle$ state, which encodes the two factors $p = 3$ and $q = 7$.

Obviously, there is only the relatively small deviation from the theoretical expectation in our experiment, which mainly results from the experimental imperfections such as the inhomogeneity of the radio frequency field and the static magnetic field, and the imperfect calibration of the radio frequency pulses. The decoherence from spin relaxation was small, since the total experimental time of $\sim$50 ms was short compared to the shortest relaxation time of $\sim$1.0 s. As a comparison, the NMR demonstration of Shor's algorithm based on the circuit model took a long time ($\sim$720 ms) which results in the severe decoherence effects [5]. Therefore, the experimental results exhibit the advantage of our adiabatic approach.

To assess its usefulness, the time complexity is another important aspect of the algorithm. While a decisive mathematical analysis of this quantum adiabatic algorithm has not been possible, we performed numerical simulations to assess its efficiency [8]. For each possible problem size, we randomly chose 50 different integers with nontrivial prime factors. Then we numerically integrated the Schrödinger equation (6) by a fourth-order Runge-Kutta technique. For each run, we determined the evolution time required to reach a success probability between 0.12 and 0.13 [8]. In Fig. 3, we plot the average of these evolution times against the problem size up to the range of 16 bits. The circles represent simulated data, while the solid curve is a quadratic fit. The good agreement between data points and fit provides clear evidence that our algorithm scales quadratically in the range we could simulate, roughly the same as Shor's algorithm.

In conclusion, based on the adiabatic theorem, we propose a new quantum algorithm for factorizing integers with fewer qubits than Shor's algorithm. At the same time, we have experimentally demonstrated the factorization of 21 in a NMR quantum simulator. This is, to our knowledge, the first experimental demonstration of a quantum algorithm that factorizes an integer larger than 15. Furthermore, we have seen evidence from numerical simulations that the required running time exhibits a polynomial behavior with the problem size in the range of the capabilities of our classical computer. Although the proof for the complexity of quantum adiabatic algorithm is still an open and timely issue, the encouraging results presented here as well as its inherent robustness [14] show that it certainly deserves further study.

This work was supported by National Nature Science Foundation of China, the CAS, Ministry of Education of PRC, the National Fundamental Research Program, and the DFG through Su 192/19-1.

*djf@ustc.edu.cn

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, New York, 1994), p. 124.
[3] D. E. Knuth, *The Art of Computer Programming Vol. 2, Seminumerical Algorithms* (Addison-Wesley, Reading, Massachusetts, 1998).
[4] N. Koblitz, *A Course in Number Theory and Cryptography* (Springer-Verlag, Berlin, 1994), 2nd ed..
[5] L. M. K. Vandersypen *et al.*, Nature (London) **414**, 883 (2001).
[6] C.-Y. Lu *et al.*, Phys. Rev. Lett. **99**, 250504 (2007).
[7] B. P. Lanyon *et al.*, Phys. Rev. Lett. **99**, 250505 (2007).
[8] E. Farhi *et al.*, Science **292**, 472 (2001).
[9] A. Messiah, *Quantum Mechanics* (Wiley, New York, 1976); T. Kato, J. Phys. Soc. Jpn. **5**, 435 (1936).
[10] A. Mizel, D. A. Lidar, and M. Mitchell, Phys. Rev. Lett. **99**, 070502 (2007).
[11] M. Steffen *et al.*, Phys. Rev. Lett. **90**, 067903 (2003).
[12] M. H. S. Amin, Phys. Rev. Lett. **100**, 130503 (2008).
[13] J. Roland and N. J. Cerf, Phys. Rev. A **65**, 042308 (2002); A. Mitra *et al.*, J. Magn. Reson. **177**, 285 (2005).
[14] A. M. Childs, E. Farhi, and J. Preskill, Phys. Rev. A **65**, 012322 (2001); J. Roland and N. J. Cerf, *ibid.* **71**, 032330 (2005).
[15] I. L. Chuang *et al.*, Proc. R. Soc. A **454**, 447 (1998); D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).
[16] X. Peng, J. Du, and D. Suter, Phys. Rev. A **71**, 012307 (2005).