Quantum computing

Shu-Shen Li*†, Gui-Lu Long‡§¶, Feng-Shan Bai‖, Song-Lin Feng*, and Hou-Zhi Zheng*

*National Laboratory for Superlattices and Microstructures, Institute of Semiconductors, Chinese Academy of Sciences, P.O. Box 912, Beijing 100083, China; Departments of ‡Physics and ‖Mathematics, Tsinghua University, Beijing 100084, China; §Key Laboratory for Quantum Information and Measurements, Ministry of Education, Beijing 100084, China; and ¶Center for Atomic, Molecular, and Nanosciences, Tsinghua University, Beijing 100084, China

Quantum computing is a quickly growing research field. This article introduces the basic concepts of quantum computing, recent developments in quantum searching, and decoherence in a possible quantum dot realization.

Quantum computing combines computer science with quantum mechanics and it is a fast-growing research field (1). In 1982, Feynman (2) pointed out that to simulate a quantum system, the computer has to be working quantum mechanically, or one needs a quantum computer (QC). The first proposal for practical implementation of a QC was presented in 1993. The elementary unit of quantum information in a QC is the quantum bit (qubit). A single qubit can be envisaged as a two-state system such as a spin-half, a two-level atom. The potential power of a QC is based on the ability of quantum systems to be in superposition of its basic states. All of these numbers represented by the basic states can be manipulated simultaneously. Thus, a QC has enormous quantum parallelism.

To perform quantum computations, one should have the following basic conditions: (*i*) a two-level system ($|0>$ and $|1>$) as a qubit, (*ii*) the ability to prepare the qubit in a given state, say $|0>$, (*iii*) the capability of measuring each qubit, (*iv*) construction of basic gate operations such as conditional logic gate (the control-not gate), and (*v*) sufficient long decoherence time. It is very important for a QC to be well isolated from any environmental interaction because they destroy the superposition of states. Furthermore, one has to use quantum error corrections, which have been invented in recent years.

Several schemes, such as trapped ions, quantum optical systems, nuclear and electron spins, and superconductor Josephson junctions, have been proposed for embodying quantum computation in recent years.

Quantum Searching and Phase Matching

For a long time, QC research has been the luxury of just a few academic elite in the world, that is, until 1994 when Shor (3) invented his famous prime factorization algorithm. Shor showed in a concrete example that a QC could do much better than a classical computer. More importantly, the difficulty in factoring a large number is the basis of the Rivest–Shamir–Adleman (RSA) public key encryption scheme that is widely used today. Through Shor's algorithm, the QC has suddenly become a real possible threat, and this algorithm has sparked worldwide interests in the QC. Shor's algorithm is applicable only to a specific problem. Grover's algorithm (4), however, devised in 1996, is another that is applicable to many problems. Grover's quantum search algorithm solves the problem of unsorted database searching. Finding a marked state from an unsorted database requires $N/2$ searches for a classical computer. Grover's algorithm finds a marked item in only $\sqrt{N}$ *steps where* N is the size of the database. Grover's algorithm has many applications such as deciphering the digital encryption scheme (DES) encryption scheme optimization.

The standard Grover algorithm achieves quadratic speedup over classical searching algorithms. This algorithm suffers from one problem: the probability of finding the marked state may never be exactly 1. To overcome this difficulty, one has to generalize the standard Grover algorithm by replacing phase inversions by rotations of smaller angles so that the search step can be made smaller. We uncovered that the generalized algorithm which uses only a smaller phase rotation of the marked state alone was wrong (5). Furthermore, if both phase inversions are modified, then the two-phase rotations must satisfy a phase-matching requirement (6). By using homomorphism between su (2) and so (3) groups, we give a simple picture of the phase-matching requirement and the quantities in the generalized quantum search algorithm (7). We have experimentally implemented the phase-matching requirement in a 2-qubit system by using the NMR quantum computation technique (8, 9).

Dephasing Rate in a Quantum Dot (QD) Qubit

A workable QC should contain thousands of qubits. A QC of such size is probably more likely to be built by solid state technologies such as semiconductor nanostructures or QDs. The ground and first excited states of an electron in a QD may be used as $|0>$ and $|1>$ of a qubit. An electromagnetic pulse can be applied to manipulate the states of an electron qubit. To perform a quantum control-not manipulation, one may apply a static electric field to a gate near the QD.

Two major obstacles have to be overcome, however, before QDs can become the triumphant technology in building a QC. First, one should be able to fabricate high-quality regularly spaced uniform semiconductor QDs. Today, by using the Stranski-Krastanov growth mode, fabricating self-assembled high-quality InAs/GaAs QDs may not be very difficult by various types of modern epitaxy technologies, such as molecular-beam epitaxy. However, the growth of regularly spaced, uniform self-assembled QDs for a QC purpose still remains a severe challenge. The second key issue is how to prolong decoherence time in semiconductor QDs when there exist enormous degrees of freedom that quickly dephase the systems.

In a recent study, we concentrated on the latter point by elucidating that a static electric field may efficiently reduce the dephasing rate or prolong decoherence time in a QD. In our model, we assumed a large energy difference between $|0>$ and $|1>$ so that we could neglect the acoustic- and optic-phonon scatterings. We took into account only the dominant decoherence coming from the vacuum fluctuation. We assumed the InAs

This paper is a summary of a session presented at the third annual Chinese–American Frontiers of Science symposium, held October 20–22, 2000, at the Arnold and Mabel Beckman Center of the National Academies of Science and Engineering in Irvine, CA.

Abbreviations: QC, quantum computer; QD, quantum dot; qubit, quantum bit.

†To whom reprint requests should be addressed. E-mail: sslee@red.semi.ac.cn.

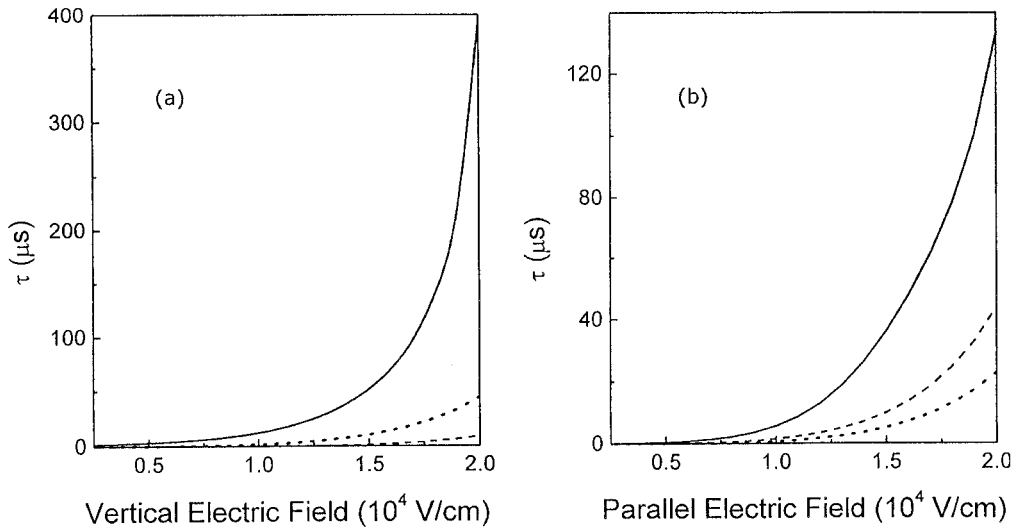

Fig. 1. The decoherence time as a function of the vertical static electric field (*a*) and the parallel static electric field (*b*) with the different QD heights: 4 nm (solid lines), 5 nm (dotted lines), and 6 nm (dashed lines). The radius of the QD is taken as 5 nm.

self-assembled QDs to be a cylinder. We studied the dephasing rate of an InAs single-electron QD embedded in GaAs, used for the solid-state qubit. The effective masses of InAs and GaAs materials were 0.023 m_0 and 0.067 m_0, respectively, and the band gaps of GaAs and InAs were 1.518 eV (1 eV = 1.602×10^{-19} J) and 0.418 eV, respectively. The conduction-band offset was assumed to be 70% of the band gap difference. The material dielectric constant ε is equal to 12.25 ε_0 (10).

Fig. 1 *a* and *b* shows the decoherence times as a function of the vertical and parallel static electric field, respectively, for the same radius (5 nm) and 3 different heights: 4 nm (solid lines), 5 nm (dotted lines), and 6 nm (dashed lines). From this figure, one can find that the decoherence time does not sensitively depend on the electric field until the strength of the electric field is lower than 5 kV/cm. The decoherence time then increases very fast as the electric field goes beyond 5 kV/cm. The decoherence time may reach the order of magnitude of milliseconds under the 20 kV/cm static electric field for the QD with a 5-nm radius and a 4-nm height.

The QC is charming, and the road to building one is long and not straight. Technologies have to be developed further before a realistic QC is built. However, there have been no known insurmountable obstacles blocking the way. The QC of the 21st century will surely unleash its tremendous power.

The National Natural Science Foundation of China is acknowledged for support.

1. Bennett, C. H. & DiVincenzo, D. P. (2000) *Nature (London)* **404,** 247–255.
2. Feynman, R. (1982) *Int. J. Theor. Phys.* **21,** 467–488.
3. Shor, P. W. (1994) *Proc. 36th Annual Symp.* (Santa Fe, NM), Nov. 20–22.
4. Grover, L. (1997) *Phys. Rev. Lett.* **79,** 325–328.
5. Long, G. L., Zhang, W. L., Li, Y. S. & Niu, L. (1999) *Theor. Phys.* **32,** 335–338.
6. Long, G. L., Li, Y. S., Zhang, W. L. & Niu, L. (1999) *Phys. Lett. A* **262,** 27–34.
7. Long, G. L., Li, Y. S., Zhang, W. L. & Tu, C. C. (2000) *Phys. Rev. A* **61,** 42351–42355.
8. Chuang, I. L., Vandersypen, L. M. K., Zhou, X. L., Leung, D. W. & Lloyd, S. (1998) *Nature (London)* **393,** 143–146.
9. Jones, J. A., Mosca, M. & Hansen, R. H. (1998) *Nature (London)* **393,** 344–346.
10. Li, S. S. & Xia, J. B. (1998) *Phys. Rev. B* **58,** 3561–3564.