

## DiVincenzo Criteria and Beyond\*

Martti M. Salomaa

*Materials Physics Laboratory, POB 2200 (Technical Physics),  
Helsinki University of Technology, FIN-02015 HUT, Finland  
and*

*Department of Physics, Kinki University  
Higashi-Osaka, 577-8502, Japan*

Mikio Nakahara

*Department of Physics, Kinki University  
Higashi-Osaka, 577-8502, Japan  
E-mail: nakahara@math.kindai.ac.jp*

Five DiVincenzo criteria and two additional networkability criteria are introduced. Then current status and prospects of the research on physical realization of quantum computing are reviewed following the ARDA QIST roadmap. Finally some proposals for "beyond the DiVincenzo criteria" are outlined.

### 1. Introduction

Quantum information processing is an emerging discipline in which information is encoded and processed in a quantum-mechanical system.<sup>1</sup> It is expected to solve some of problems that are impossible for current digital computers to execute in a practical time scale. Although small scale quantum information processing, such as quantum key distribution, is already available commercially, physical realizations of a large scale quantum information processor are still beyond the current technology.

Benioff proposed in 1982 that a quantum mechanical Turing machine might be reversible and dissipated no energy.<sup>2</sup> Feynman in the same year published a paper in which he first recognized a quantum system as a useful resource for information processing.<sup>3</sup> His idea has been developed since then by a small group of people including Deutsch.<sup>4</sup> A revolution took

---

\*This contribution was presented by MMS at the symposium. His unexpected early death, however, made it impossible for him to submit the manuscript. MN has prepared this contribution following MMS's presentation and powerpoint file.

place when Shor announced an efficient algorithm for integer factorization.<sup>5</sup> The impact his work brought about was tremendous since the security of internet communication depends on the belief that factorization of a large integer is practically impossible.

In classical information theory, information is encoded in a bit, which takes values 0 and 1, while in quantum information theory, 0 and 1 are replaced by orthonormal basis vectors  $|0\rangle$  and  $|1\rangle$  of a two-dimensional complex vector space. Here information is encoded in a qubit (quantum bit) in the form  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , where  $|\alpha|^2 + |\beta|^2 = 1$ . It is estimated that a quantum computer superior to a digital computer today requires at least  $10^2 \sim 10^3$  qubits. Although a quantum computer with a small number of qubits, up to 7, is available in several physical systems, construction of a working quantum computer is still a challenging task. DiVincenzo proposed necessary conditions that any physical system has to fulfill to be a candidate for a viable quantum computer.<sup>6</sup> In the next section, we outline these conditions as well as two additional criteria for networkability.

## 2. DiVincenzo Criteria

In an influential article,<sup>6</sup> DiVincenzo, the keynote speaker of this symposium, proposed five criteria that any physical system must satisfy to be a viable quantum computer. We summarize the relevant parts of these criteria, which may be helpful in reading following contributions in this volume.

### (1) *A scalable physical system with well characterized qubits.*

To begin with, we need a quantum register made of many qubits to store information. The simplest way to realize a qubit physically is to use a two-level quantum system. For example, an electron, a spin 1/2 nucleus and two polarization states (horizontal and vertical) of a single photon may be a qubit. We may equally employ a two-dimensional subspace, such as the ground state and the first excited state, of a multi-dimensional Hilbert space. In the latter case, special care must be taken to avoid leakage of the state to the other part of the Hilbert space. In any case, the two states are identified as the basis vectors,  $|0\rangle$  and  $|1\rangle$ , of the Hilbert space so that a general single qubit state takes the form  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ,  $|\alpha|^2 + |\beta|^2 = 1$ . A multi-qubit state is expanded in terms of tensor products of these basis vectors. Each qubit must be separately addressable. Moreover it should be scalable up to a large number of qubits. The con-

dition of two states may be relaxed to three states (qutrit) or, more generally,  $d$  states (qudit).

A system may be made of several different kinds of qubits. Trapped ions, for instance, may employ (1) hyperfine/Zee-man sublevels in the electronic ground state of ions, (2) a ground and excited states of weakly allowed optical transition, and (3) normal mode of ion oscillation, as qubits. A similar scenario is also proposed for Josephson junction qubits.

- (2) *The ability to initialize the state of the qubits to a simple fiducial state, such as  $|00\dots 0\rangle$ .*

In many realizations, initialization may be done simply by cooling. Let  $\Delta E$  be the difference between energies of the first excited state and the ground state. At low temperatures satisfying  $k_B T \ll \Delta E$ , the system is in the ground state with a good precision. Alternatively, we may use measurement to project the system into a desired state. In some cases, we observe the system to be in an undesired state on measurement. Then we may transform the system to the desired fiducial state by unitary transformation.

For some realizations, such as liquid state NMR, however, it is impossible to cool the system down to extremely low temperatures. In those cases, we are forced to use a thermally populated state as an initial state. This seemingly difficult problem may be amended by several methods if some computational resources are sacrificed. We then obtain an “effective” pure state, so-called the pseudopure state, which works as an initial state for most purposes.

Continuous fresh supply of qubits in a specified state, such as  $|0\rangle$ , is also an important requirement for successful quantum error correction.

- (3) *Long decoherence times, much longer than the gate operation time.*

Decoherence is probably the hardest obstacle to building a viable quantum computer. Decoherence means many aspects of quantum state degradation due to interaction of the system with the environment and sets the maximum time available for quantum computation. Roughly speaking, this is the time required for a pure state

$$\rho_0 = (\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|)$$

to “decay” into a mixed state of the form

$$\rho = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|.$$

The value of the decoherence time itself is not very important. What matters is the ratio “decoherence time/gate operation time”. For some realizations, the decoherence time may be as short as  $\sim \mu$  s. This is not necessarily a big problem provided that the gate operation time, determined by the Rabi oscillation period and the qubit-coupling strength for example, is much shorter than this. If the typical gate operation time is  $\sim$  ps, say, the system may execute  $10^{12-6} = 10^6$  gate operations before the quantum state decays.

There are several ways to effectively elongate the decoherence time. A closed-loop control method is called quantum error correcting codes (QECC) while an open-loop control method is called noiseless subsystem and decoherence free subspace (DFS). Both of these methods require extra qubits to implement. Time-optimal implementation of a quantum algorithm is regarded as a method to fight against decoherence without any extra resource.

(4) A “universal” set of quantum gates.

Let  $H(\gamma(t))$  be the Hamiltonian of an  $n$ -qubit system under consideration, where  $\gamma(t)$  collectively denotes the control parameters in the Hamiltonian. The time-development operator of the system is

$$U[\gamma(t)] = \mathcal{T} \exp \left[ -\frac{i}{\hbar} \int^T H(\gamma(t)) dt \right] \in U(2^n),$$

where  $\mathcal{T}$  is the time-ordering operator. Our task is to find the set of control parameters  $\gamma(t)$  which implements the desired gate  $U_{\text{gate}}$  as  $U[\gamma(t)] = U_{\text{gate}}$ . Although this “inverse problem” seems to be demanding to solve, a well known theorem by Barenco *et al* guarantees that any  $U(2^n)$  gate may be decomposed into single-qubit gates  $\in U(2)$  and CNOT gates.<sup>9</sup> Therefore it suffices to find the control sequences to implement  $U(2)$  gates and a CNOT gate to construct an arbitrary gate. Note that a general unitary gate in  $U(2^n)$  is written as a product of an  $SU(2^n)$  gate and a physically irrelevant  $U(1)$ -phase. Therefore we do not have to worry about the overall phase

and it suffices to concentrate on equivalent  $SU(2^n)$  gates. This observation is noteworthy since the NMR Hamiltonian, for example, is traceless and is able to generate  $SU(2^n)$  matrices only. Single-qubit gates are easily implemented if the one-qubit part of the Hamiltonian assumes two of the  $\mathfrak{su}(2)$  generators by properly choosing the control parameters. Implementation of a CNOT gate in any realization is considered to be a milestone in this respect. Note however that any two-qubit gate, that is neither a tensor product of two one-qubit gates nor a SWAP gate, works as a component of a universal set of gates.

Quantum circuit implementation requires less steps if multi-qubit gates acting on  $n$  ( $\geq 3$ ) qubits are employed as modules.

(5) *A qubit-specific measurement capability.*

The state after an execution of a computation must be measured to extract the result of the computation. Measurement process depends heavily on the physical system under consideration. For most realizations, projective measurements are the primary method to extract the outcome of a computation. In liquid state NMR, in contrast, a projective measurement is impossible and we have to resort to ensemble averaged measurements. This may cause a problem in some cases. Suppose the system is in the state  $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$  for example. The outcome of a projective measurement of  $|\psi\rangle$  is  $|00\rangle$  with the probability  $1/2$ . The ensemble averaged measurement, on the other hand, yields *both*  $|00\rangle$  and  $|11\rangle$  with an equal weight. Measurement in general has no 100% efficiency due to decoherence, gate operation error and many more reasons. If this is the case, we have to repeat the same computation many times to achieve reasonably high reliability.

Moreover, we should be able to send and store quantum information to construct a quantum data processing network. This “networkability” requires following two additional criteria to be satisfied.

(6) *The ability to interconvert stationary and flying qubits.*

Some realizations are excellent in storing quantum information while long distant transmission of quantum information might require different physical resources. It may happen that some system has a Hamiltonian which is easily controllable and is

advantageous in executing quantum algorithms. Compare this with a current digital computer, in which the CPU and the system memory are made of semiconductors while a hard drive is used as a mass storage device. Therefore a working quantum computer may involve several kinds of qubits and we are forced to introduce distributed quantum computing. Interconverting ability is also important in long distant quantum teleportation using quantum repeaters.

- (7) *The ability to faithfully transmit flying qubits between specified locations.*

Needless to say, this is an indispensable requirement for quantum communication such as quantum key distribution. This condition is also important in distributed quantum computing mentioned above.

### 3. Physical Realizations

There are numerous physical systems proposed as a possible candidate for a viable quantum computer. Here is the list of the candidates;

- (1) Liquid-state/Solid-state NMR
- (2) Trapped ions
- (3) Neutral atoms in optical lattice
- (4) Cavity QED with atoms
- (5) Linear optics
- (6) Solid state (spin-based, charge-based)
- (7) Josephson junctions (charge, flux, phase)
- (8) Electrons on liquid helium surface
- (9) Other “unique” realizations.

ARDA QIST roadmap evaluates each of these realizations as outlined in the next section. Subsequent contributions in this volume give detailed accounts on some of these realizations in the light of the DiVincenzo criteria.

### 4. ARDA QIST Roadmap

Most of the content in this section are excerpts from the online article “A Quantum Information Science and Technology (QIST) Roadmap, Part 1: Quantum Computation”<sup>7</sup> compiled by Advanced Research and Development Activity (ARDA), Los Alamos, USA.<sup>7</sup> This article is updated annu-

ally and readers are strongly recommended to visit this webpage for new progress.

The roadmap was compiled by the members of a Technology Experts Panel to help facilitate the progress of quantum computation (QC) research towards the quantum computer-science era. In kick-off QIST Experts Panel Meeting, held in La Jolla, California, USA in January 2002, the panel members decided that the overall purpose of the roadmap should be to set as a desired future objective for QC

to develop by 2012 a suite of viable emerging-QC technologies of sufficient complexity to function as quantum computer-science test-beds in which architectural and algorithmic issues can be explored;

The roadmap has a prescriptive role, namely,

to identify what scientific, technology, skills, organizational, investment, and infrastructure developments will be necessary to achieve the desired goal, while providing options for how to get there;

and a descriptive function

by capturing the status and likely progress of the field while elucidating the role that each aspect of the field is expected to play toward achieving the desired goal.

The roadmap also identifies gaps and opportunities, and places where strategic investments should be beneficial. This will be helpful for both researchers and research managers.

The panel members introduced the four-level structure in the roadmap, namely, “high-level goal”, “mid-level view”, “detailed level summaries”, and “summary with panel’s recommendation”.

#### **4.1. High-Level Goal**

To set a path to realize the desired QC test-bed ear in 2012, the panel provided five- and ten-year technical goals. The five-year (2007) goal is to

- encode a single qubit into the state of a logical qubit formed from several physical qubits,
- perform repetitive error correction of the logical qubit, and
- transfer the state of the logical qubit into the state of another set of physical qubits with high fidelity,

while the ten-year (2012) goal is to

- implement a concatenated quantum error-correcting code.

Meeting the 2007 high-level goal requires the achievement of

- creating deterministic, on-demand quantum entanglement;
- encoding quantum information into a logical qubit;
- extending the lifetime of quantum information; and
- communicating quantum information coherently from one part of a quantum computer to another,

while meeting the 2012 high-level goal requires  $\sim 50$  physical qubits

- to exercise multiple logical qubits through the full range of operations required for fault-tolerant QC in order to perform a simple instance of a relevant quantum algorithm, and
- to approach a natural experimental QC benchmark: the limits of full-scale simulation of a quantum computer by a conventional computer.

The 2012 goal would extend QC into the test-bed regime. It would also enable quantum simulation as originally envisioned by Feynman.

#### 4.2. *Mid-Level View*

The roadmap also presents a “mid-level view” to allow informed decisions about future directions to be made for researchers. The “mid-level view” segments the field into the different scientific approaches in view of the DiVincenzo criteria and metrics to capture the promise and characterize the progress towards the high-level goals within each approach.

Table 1 summarizes the “promise criteria” according to the mid-level view of the roadmap. The panel used three symbols (letters “G, Y, R” here) to indicate the value the panel assigned to these criteria.

The panel also presents status of each approach with a set of metrics that represent relevant steps on the way to the 2007- and 2012-year goals. Table 2 shows the “development status metrics” in which the panel assigned again three symbols. The numbers  $M.$  and  $M.N$  in the table refer to the following criteria:

1. Creation of a qubit
  - 1.1 Demonstrate preparation and readout of both qubit states.
2. Single-qubit operations
  - 2.1 Demonstrate Rabi flops of a qubit.

Table 1  
 The Mid-Level Quantum Computation Roadmap: Promise Criteria.  
 The column number  $k$  corresponds to the  $k$ th DiVincenzo criterion.  
 (Reproduced with permission from <http://qits.lanl.gov/> .)

The DiVincenzo Criteria								
QC Approach	Quantum Computation						QCNetworkability	
	#1	#2	#3	#4	#5		#6	#7
NMR								
Trapped Ion								
Neutral Atom								
Cavity QED								
Optical								
Solid State								
Superconducting								
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							

Legend: = a potentially viable approach has achieved sufficient proof of principle

= a potentially viable approach has been proposed, but there has not been sufficient proof of principle

= no viable approach is known

- 2.2 Demonstrate decoherence times much longer than the Rabi oscillation period.
- 2.3 Demonstrate control of both degrees of freedom on the Bloch sphere
3. Two-qubit operations
  - 3.1 Implement coherent two-qubit quantum logic operations.
  - 3.2 Produce and characterize the Bell entangled states.
  - 3.3 Demonstrate decoherence times much longer than two-qubit gate times.
  - 3.4 Demonstrate quantum state and process tomography for two qubits.
  - 3.5 Demonstrate a two-qubit decoherence-free subspace (DFS).
  - 3.6 Demonstrate a two-qubit quantum algorithm.
4. Operations on 3 – 10 physical qubits
  - 4.1 Produce a Greenberger, Horne, and Zeilinger (GHZ) entangled state of three physical qubits.
  - 4.2 Produce maximally-entangled states of four or more physical qubits.
  - 4.3 Quantum state and process tomography.
  - 4.4 Demonstrate DFSs.

Table 2  
The Mid-Level QC Roadmap - Development Status Metrics. (Reproduced with permission from <http://qits.lanl.gov/>.)

QC Approach	1	1.1	2	2.1	2.2	2.3	3	3.1	3.2	3.3	3.4	3.5	3.6	4	4.1	4.2	4.3	4.4	
NMR		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Trapped Ion		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Neutral Atom				▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Cavity QED		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Optical		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Solid State:																			
Charged or excitonic qubits		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Spin qubits		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
Superconducting		▲▲		▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	
QC Approach	4	4.5	4.6	4.7	4.8	5	5.1	5.2	6	6.1	6.2	6.3	7	7.1	7.2	7.3	7.4	7.5	
NMR		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Trapped Ion		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Neutral Atom		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Cavity QED		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Optical		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Solid State:																			
Charged or excitonic qubits		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Spin qubits		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲
Superconducting		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲		▲▲	▲▲	▲▲	▲▲		▲▲	▲▲	▲▲	▲▲	▲▲

Legend: ▲▲ = sufficient experimental demonstration  
 ▲ = preliminary experimental demonstration, but further experimental work is required  
 □ = no experimental demonstration and □ = a change in the development status between Versions 1.0 and 2.0

- 4.5 Demonstrate the transfer of quantum information (e.g., teleportation, entanglement swapping, multiple SWAP operations etc.) between physical qubits.
- 4.6 Demonstrate quantum error-correcting codes.
- 4.7 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza).
- 4.8 Demonstrate quantum logic operations with fault-tolerant precision.
- 5. Operations on one logical qubit
  - 5.1 Create a single logical qubit and “keep it alive” using repetitive error correction.
  - 5.2 Demonstrate fault-tolerant quantum control of a single logical qubit.
- 6. Operations on two logical qubits
  - 6.1 Implement two-logical-qubit operations.
  - 6.2 Produce two-logical-qubit Bell states.
  - 6.3 Demonstrate fault-tolerant two-logical-qubit operations.
- 7. Operations on 3 – 10 logical qubits
  - 7.1 Produce a GHZ-state of three logical qubits.
  - 7.2 Produce maximally-entangled states of four or more logical qubits.
  - 7.3 Demonstrate the transfer of quantum information between logical qubits.
  - 7.4 Demonstrate simple quantum algorithms (e.g., Deutsch-Josza) with logical qubits.
  - 7.5 Demonstrate fault-tolerant implementation of simple quantum algorithms with logical qubits.

Detailed-level summaries are given for each physical realization. They are intended to provide a description of each of the experimental approaches and a description of the likely developments over the next decade.

## 5. Beyond DiVincenzo Criteria

The DiVincenzo criteria are not necessarily the gospel and some conditions can be relaxed. For example, it is possible to replace unitary gates by irreversible non-unitary gates generated by measurements. This idea is already implemented in linear optics quantum computation.<sup>10</sup> An extreme in this approach must be the “one-way quantum computing”, where conditional measurements send an initial “cluster state” to the final desired state.<sup>11</sup>

There have also been active discussions concerning sufficiency of the criteria and what comes beyond the DiVincenzo criteria. Here is the list of some proposals:

- (1) Implementation of decoherence-free subsystems/subspaces.
- (2) Implementation of quantum error correction.
- (3) Fault-tolerant quantum computing.
- (4) Topologically protected qubits.

Gottesman's article "Requirements and Desiderata for Fault-Tolerant Quantum Computing: Beyond the DiVincenzo Criteria"<sup>12</sup> also discusses requirements for fault-tolerant quantum computing such as

- (1) Low gate error rates.
- (2) Ability to perform operations in parallel.
- (3) A way of remaining in, or returning to, the computational Hilbert space.
- (4) A source of fresh initialized qubits during the computation.
- (5) Benign error scaling: error rates that do not increase as the computer gets larger, and no large-scale correlated errors.

It also lists "additional desiderata" for a practical quantum computer such as

- (1) Ability to perform gates between distant qubits.
- (2) Fast and reliable measurement and classical computation.
- (3) Little or no error correlation (unless the registers are linked by a gate).
- (4) Very low error rates.
- (5) High parallelism.
- (6) An ample supply of extra qubits.
- (7) Even lower error rates.

Many of the above conditions are necessary for quantum error corrections to work reasonably well.

## 6. Summary

- Solid state and superconducting qubits are expected to be scalable with current lithography technology. However few-qubit operations have been hardly demonstrated with these systems to date.
- In contrast, few-qubit operations are demonstrated on liquid-state NMR and ion traps, although they are probably not scalable.
- Is DiVincenzo criteria classification sufficient? Generalizations "beyond" DiVincenzo may be included using memory, program, . . .
- QIST roadmap, based on the DiVincenzo criteria, is extremely valuable for the identification and quantification of progress in this multidisciplinary field.

## Acknowledgment

We would like to thank Japan Society for the Promotion of Science (JSPS) for making MMS's stay at Kinki University possible. One of the authors (MN) would like to thank Dr. Richard J. Hughes for allowing us to use materials from ARDA Quantum Information Science and Technolgoy Roadmap<sup>7</sup> and Dr. Daniel Gottesman for allowing us to use his online material<sup>12</sup> and useful suggestions.

## References

1. M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).
2. Phys. Rev. Lett. **48**, 1581 (1982).
3. R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
4. D. Deutsch, Proc. Royal Soc. Lond.: Ser. A **400**, 97 (1985).
5. P. W. Shor, *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science (FOCS '94)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) 124; quant-ph/9508027.
6. D. P. DiVincenzo, Fortschr. Phys. **48**, 771 (2000). See also the attached CD.
7. <http://qits.lanl.gov/>
8. L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Nature **414**, 883 (2001).
9. A. Barenco *et. al.* Phys. Rev. A **52**, 3457 (1995).
10. E. Knill, R. Laflamme and G. J. Milburn, Nature **409**, 46 (2001).
11. R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
12. D. Gottesman, <http://www.perimeterinstitute.ca/personal/dgottesman/FTreqs.ppt>. See also D. Aharonov and M. Ben-Or, quant-ph/9906129 and J. Preskill, quant-ph/9712048.