



Implementation of Quantum Computing Algorithms on a Nuclear Magnetic Resonance Quantum Computer Based on Polarized Solid ^{129}Xe .

Edward G. Belaga, Daniel Grucker

► To cite this version:

Edward G. Belaga, Daniel Grucker. Implementation of Quantum Computing Algorithms on a Nuclear Magnetic Resonance Quantum Computer Based on Polarized Solid ^{129}Xe . 2003. <hal-00129697>

HAL Id: hal-00129697

<https://hal.science/hal-00129697v1>

Preprint submitted on 8 Feb 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

*Implementation of Quantum Computing Algorithms
on a Nuclear Magnetic Resonance Quantum Computer
Based on Polarized Solid ^{129}Xe .
Research Project.*

Edward G. Belaga

*Institut de Recherche Mathématique Avancée
Université Louis Pasteur
7, rue René Descartes F-67084
Strasbourg Cedex
belaga@math.u-strasbg.fr*

Daniel Grucker

*Institut de Physique Biologique
Université Louis Pasteur
4, rue Kirschlegers F-67085
Strasbourg Cedex
grucker@ipb.u-strasbg.fr*

September 2003

Abstract. We briefly summarize here the history, conceptual base, as well as challenges and implications of quantum computing. Then, we present the theoretical requirements for viable quantum computation, as well as the state-of-the-art experimental approach and a project of solid ^{129}Xe NMR-based quantum computer.

1991 Mathematical Subject Classification : Primary, 11K31, 11K38, 11K55; Secondary, 11B85.

Key words and phrases : universal algebra, generators, digraph, circuit, straight-line algorithm, or stline, computation mode, stline complexity, discordancy, cohesion, free finitely generated monoid.

1. Preamble.

We briefly summarize here the history, conceptual base, as well as challenges and implications of quantum computing. In the following chapters, we talk about the theoretical requirements for viable quantum computation, then present the state-of-the-art experimental approach, and a project of solid ^{129}Xe Nuclear Magnetic Resonance (NMR-) based quantum computer.

Widespread interest in quantum computation is generally attributed to two Feynman's observations, namely, that classical computers cannot effectively model quantum mechanical systems [Feynman 1982], and that by reducing the size of computers to the

atomic scale, the bit state and dynamics of a computer might be described by quantum mechanics [Feynman 1986], thus creating the possibility of computer simulation of quantum mechanical systems.

In fact, a bit state of such computer would look like:

$$|\psi\rangle = a \cdot |001100101\dots\rangle + b \cdot |101011001\dots\rangle + \dots, \quad (1 : 1)$$

with coefficients a, b, \dots being complex numbers and the probability for the computer to be in one of the specific states given by $|a|^2, |b|^2, \dots$. Quantum mechanics tells us that the computer exists in all of its states simultaneously, so long as that state is not measured (the *superposition principle*). When we do choose to measure it, a particular state will be observed with the prescribed probability : in other words, quantum state *irreversibly collapses* into one of the basic states leaving us with a few bits of *classical information* about it.

Almost simultaneously with Richard Feynman, similar ideas were advanced by Paul Benioff [Benioff 1980,1982], Charles Bennett [Bennett 1982], David Deutsch [Deutsch 1985], and a few others [Manin 1980]. As Feynman, these pioneers began thinking about the implications of combining quantum mechanics with the classical Turing machine, where a quantum physical process becomes a computational enterprise [Landauer 1996b] : an appropriately created quantum state can evolve, guided by *reversible*, properly arranged *unitary* transformations (i. e. unitary operators of the corresponding Hilbert space) which would exploit the *interference* and (related to it) *entanglement* phenomena, with the results extracted by appropriate measurements.

Such a quantum “computer” would exhibit certain classical and non-classical powers : *exponentiality, fast access, branching, complex amplitudes, and universality*. The additional power of quantum computers comes from the possibility of employing a superposition of states, of following many distinct computation paths and of producing a final output that depends on the interference of all of them. This “quantum parallelism” outstrips by far any parallelism that can be thought of in classical computation and is responsible for the “exponential” speed-up of computation.

In this initial conceptual development, Deutsch’s paper [Deutsch 1985] has been especially important : it exhibited both a specific problem with no polynomial-time solution on any classical machine and a very simple, but greatly (in fact, exponentially) parallelized polynomial-time quantum algorithm solving the problem. Later, the algorithms of Peter Shor [Shor 1994], for factorizing “big” integers, of Lov Grover [Grover 1996], for searching “big” databases, and of Seth Lloyd and others [Lloyd 1996], for simulating physical systems (with Feynman’s 1982 conjecture, that quantum computers can be programmed to simulate any local quantum system, shown to be correct), demonstrated the exceptional power of parallel computation on quantum computers, with realistic perspectives of very promising practical breakthroughs in cryptography, information search, physical simulation, etc.

The discovery of *quantum teleportation* [Bennett, *et al.*] and of *quantum error correction codes* [Calderbank, Shor 1996] have become points of departure for a vigorous research in *quantum information processing* which, together with *quantum computing*, form what is now known as *Quantum Information Science*, or **QIS** [Bennett, *et al.* 1999].

These theoretical advances, from general principles and schemes of computing and information transfer to efficient quantum algorithms and to quantum “software” development, stimulated efforts for physical implementation of quantum computers, with their architecture, reliability problems, and “hardware” development. Eight years after the first quantum algorithm of Deutsch, Seth Lloyd [Lloyd 1993] has been able to foresee the common features of many schemes of physical implementation of quantum computers.

2. Algorithmic Framework for Quantum Computing.

Theoretical Quantum Information Science, or *TQIS* was initially conceived as a quantum detour and imitation, - based on theoretical ability to manufacture, manipulate, and measure quantum states (1:1), - of the classical computing paradigm, with its models of computation, partially implemented in modern computers [van Leeuwen 1995], its uncomputability and undecidability pitfalls [Boolos, *et al.* 2002], its computational intractability challenges [Garey, Johnson 1979], its rich library of effective algorithms [van Leeuwen 1990], and its computational complexity analysis [Goldreich 2001].

However, the ensuing explosive growth of *TQIS*, since the early 1990', has tremendously accelerated its independent and original development, with its specific computational problems [Nielsen, Chuang 2000] and physical implementation challenges [Bouwmeester, *et al.* 2000], [Braunstein, Lo 2001], [Awschalom, *et al.* 2002].

Uncomputability, Intractability, Effectiveness. Here are some examples of these phenomena, both classical and quantum, mentioned above.

Uncomputability. Does there exist a universal algorithm for solving Diophantine equations ? (*Diophantine equation* is a polynomial equation with integer coefficients and integer solutions.) The answer to this *tenth Hilbert problem* is *no* [Matiyasevich 1993].

Intractability. Many combinatorial problem is possible but very “hard” to solve algorithmically. In other terms, their only known solutions are exponential or sub-exponential in time or size of the memory needed. Such problems form the non-polynomial (or NP-) class [Garey, Johnson 1979].

Also, many physical systems are computationally irreducible, so that their own evolution is effectively the most efficient procedure for determining their future. As a consequence, many questions about these systems can be answered only by very lengthy or potentially infinite computations. But some questions answerable by simpler computations may still be formulated.

Between Intractability and Effectiveness - Primality Testing. Many (classical) algorithms have been devised for determining the prime factors of a given number. The importance of the problem surpasses its mathematical value : the difficulty of factoring

a product of two big primes underlies the security of the most popular today *public key* cryptoschemes invented in 1970’.

In fact, it is very difficult to build a general-purpose algorithm for this classically ”hard” NP-problem. The fastest-known fully proven classical deterministic algorithm is the sub-exponential Pollard-Strassen method [Pomerance 1987]. Then, Peter Shor has constructed a quantum algorithm factoring integers and finding discrete logarithms (the problem which, too, is generally thought to be hard on a classical computer) which take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored [Shor 1997]. This surprising breakthrough puts in doubt the veracity of the classical *strong Church-Turing thesis*, see below.

Effective Computation. Primality test is an algorithm to determine whether or not a given number is prime, as opposed to actually decomposing the number into its constituent prime factors, which is known as *prime factorization*.

Unlike prime factorization, primality testing was long believed to be a polynomial (P-) problem. This had not been demonstrated, however, until [Agrawal, et al. 2002] unexpectedly discovered a polynomial time algorithm of asymptotic complexity $O(\ln^{12}n)$. Their algorithm has come to be called the *AKS test*.

Theoretical Quantum Computation Models. Building on two most important classical paradigms, David Deutsch has introduced two models of quantum computation :

(1) *Turing machine*, or the model \mathcal{T} [Deutsch 1985] (see also the important update by Paul Benioff [Benioff 1998]) and

(2) *quantum circuits* [Deutsch 1989], or \mathcal{C} (later fully formalized and investigated by [Yao 1993]).

(3) Recently, Michael Freedman, Alexei Kitaev, and their collaborators have defined the third, *topological* model of quantum computation which has no classical predecessor or analog : *modular functors*, or \mathcal{MF} [Freedman, et al. 2002a,b,c]

BQP Complexity Class. As in the classical case, the passage from one of these three models to another one turns out to be *efficient*, i. e., requires at most a polynomial number of additional elementary operations [Yao 1993], . This suggests that a quantum version of the classical *strong Church-Turing thesis* might be true.

Thus, all three quantum models of computation, \mathcal{T} , \mathcal{C} , \mathcal{MF} , define the same class of functions computable with **B**ounded error, given **Q**uantum resources, in **P**olynomial time [Freedman, et al. 2002c].

The Church-Turing Thesis for Quantum Computing. The original classical *Church-Turing thesis* affirms that all possible *universal* models of computations *completely and equally capture* what it means to perform a task by algorithmic means, and so are essentially equivalent. All what we know today about the potential power of quantum computing does not challenge this thesis : we still believe that all quantum-computable problems are classically computable (the other way around has been proved).

The *strong* version of the *quantum Church-Turing thesis* postulates (and this claim has been verified for the above quantum computaiton models) [Yao 1993], [Freedman, et

al. 2002c] that the class of *efficient*, i. e., polynomial-time, quantum algorithms is robust, whatever model is used. However, quantum complexity theory challenges the strong version of the *classical Church-Turing thesis* (e. g., [Svozil 1994], §4.6) : as already [Deutsch 1985] has shown, some classcally intractable computational problems become efficiently solvable on quantum computers.

3. Physical Foundations of Quantum Computing.

The following list of quantum “ingredients” represents a (simplified) basis for any idealized quantum computer network [DiVincenzo 2000], [Bouwmeester, *et al.* 2000], [Braunstein, Lo 2001], [Awschalom, *et al.* 2002].

Quantum Computation Requirements.

3.1. A Scalable Physical System with Well-Characterized Qubits. [DiVincenzo 2000], [Braunstein, Lo 2001]

At the base, is the *qubit* (or quantum bit) which, as in any ordinary computer, has two basic states $|0\rangle$ and $|1\rangle$, but unlike in ordinary computers, a qubit can exist in any superposition of these two states. As an example, the basic state up $|1\rangle$ or down $|0\rangle$ of the spin of an unpaired electron, or of the nucleus of H atom, in a magnetic field.

For efficient quantum computing the physical system has to be *scalable* [Braunstein, Lo 2001], i. e., it needs a well defined extendable qubit array-stable memory, in order to reach 1000 or more qubits.

A qubit could have more than two states, but we will limit our considerations to the two-state case. An alternative model of quantum computation could be based on *local fermionic modes*, or **LFMs** instead of qubits. (An **LFM** is a site which can be either empty or occupied by a fermion) [Kitaev 2000]. We leave the both possibilities out.

3.2. The Ability to Initialize the State of the Qubits to a Simple Fiducial state. [DiVincenzo 2000], [Bouwmeester, *et al.* 2000]

This means that the state of the qubits can be put in a simple *coherent* state, accepted as a fixed reference basis, such as $|0,0,0,0,\dots\rangle$. Moreover, quantum error correction requires a continous, fresh supply of qubits in a low-entropy state, like that of $|0\rangle$.

3.3. The system must have a long decoherence time compared to the gate operation time. [DiVincenzo 2000], [Braunstein, Lo 2001]

If the quantum system is not perfectly isolated, the contact with its environment will make the computer’s evolution non-unitary, due to the quantum dynamics of the surrounding apparatus, and will destroy its *coherence*.

3.4. A “universal” set of quantum gates. [DiVincenzo 2000], [Nielsen, Chuang 2000]

This requirement goes to the very heart of quantum computing. It is modelled on the classical paradigm of the universal set of gates, as follows [Deutsch 1985].

A quantum algorithm is specified as a sequence of unitary transformations

$$U_1, U_2, U_3, \dots,$$

each acting on a small number of qubits, typically one, two or three. A fixed finite (preferably, very “small”) set of quantum gates is *universal* if any unitary operator acting on the corresponding to our computer Hilbert space can be approximated with any desirable precision by “gates” from the set.

Virtually any unitary operation on sets of qubits can be thought of as a “gate” of quantum computation. The one-qubit rotation and the exclusive-or function (named *XOR* or *controlled-NOT*) possess this universal property. Qubit rotation is performed by tipping pulses which couple the two energy levels of a spin $\frac{1}{2}$.

A *XOR* protocol which flips the second of two qubits if and only if the first is 1, can be constructed no matter what the form of the coupling term between the two qubits. As an example the *AND* gate requires at least 3 *XOR* gates and 3 one-qubit rotations, and 6 *XOR* and 8 one-qubit rotations if all the phase factors be unity. The unitary of quantum evolution demands that a superposition of input states evolves to a corresponding superposition of outputs. This superposition of states of coupled qubits is named *entangled state* or *entanglement*.

3.5. A qubit-specific measurement capability. [DiVincenzo 2000], [Awschalom, *et al.* 2002]

To read out the result of a computation, one needs the ability to measure specific qubits (similarly to the classical case, where one reads out the values of output bits). Qubits have to be measured in order to know the result of any gate used in the computation algorithm.

Quantum Communication Requirements.

The last two are requirements for using quantum computation in conjunction with quantum communication. This opens the way of quantum teleportation implicit in the EPR (Einstein-Podolsky-Rosen) paradox [Bell 1989] and explicitly constructed by [Bennett, *et al.* 1993].

3.6. Ability to Interconvert Stationary and Flying Qubits. [DiVincenzo 2000]

Spins are not generally considered as the best carrier for moving qubits, most discussions consider photons as flying qubit. Schemes of converting electron or nuclear spin qubits to photons are necessary.

3.7. Ability to Faithfully Transmit Flying Qubits Between Specific Locations. [DiVincenzo 2000], [Awschalom, *et al.* 2002]

This last requirement is needed for quantum teleportation which can be viewed as a “moving” computational procedure used in quantum cryptography and in quantum communications.

4. Experimental Implementation : State-of-the-Art.

Quantum computation has been tested or proposed in several physical systems (the following list has been compiled by David DiVincenzo) :

- | | |
|--|-------------------------------------|
| (1) Liquid-state NMR. | (7) Nitrogen vacancies in diamond. |
| (2) NMR spin lattices. | (8) Electrons on liquid <i>He</i> . |
| (3) Linear ion-trap spectroscopy. | (9) Small Josephson junctions. |
| (4) Neutral-atom optical lattices. | (10) Spin spectroscopies. |
| (5) Cavity QED + atoms. | (11) Coupled quantum dots. |
| (6) Linear optics with single photons. | |

4.1. Bulk NMR at room temperature.

Bulk NMR in the liquid state illustrates clearly the requirements for quantum computation but suffers from the lack of scalability over some 10 qubits.

4.1.1. Well characterized qubits.

The qubit bulk NMR is characterized by the Larmor frequency of different spins in a molecule :

- **2 qubits.** Dibromothiophene [Gershenfeld, *et al.* 1998], [Chuang, *et al.* 1998].
- **3 qubits.** H-Cl-C=C-Cl₂ [Nielsen, *et al.* 1998].
- **7 qubits.** 4F and 2C Shor's algorithm [Vandersypen *et al.* 2001].

Conclusion : *Scalability* is limited to about 10 qubits due to the low signal to noise ratio of NMR at equilibrium [Warren 1997].

To increase the ratio $\frac{S}{N}$, it has been proposed to use:

- Hyperpolarized Xe [Navon, *et al.* 1996], [Verhulst, *et al.* 2001].
- Parahydrogen (Oxford and Malmö groups).

4.1.2 Initializing the state of the qubits.

For NMR at room temperature the Boltzman equilibrium population of the two-spin states differs only for 10^{-5} , and this even in a 10T magnetic field. In order to use only the slight excess of the ground state as the basis of the quantum computation it has been proposed several methods:

- Logical labeling [Gershenfeld, *et al.* 1997].
- Spatial averaging [Cory, *et al.* 1997].
- Temporal averaging [Knill, *et al.* 1998].

4.1.3 Long relevant decoherence times.

The longitudinal relaxation time of ^{13}C spin is several seconds. Gate operations are performed by RF pulses lasting $10\mu\text{s}$ for hard pulse to 10ms for selective pulses. The ratio between decoherence time and gate operation is about 10^6 .

4.1.4. Universal set of quantum gates.

Qubit rotations and Controlled *NOT* gates are implemented by RF pulses with specific frequency, shape and phase, using all the multinuclear spin manipulation described in liquid NMR spectroscopy. [Gershenfeld, *et al.* 1997], [Ernst, *et al.* 1987].

4.1.5. Qubit-specific measurements.

The measurement of the state of qubit is obtained by its Larmor frequency and its phase. [Gershenfeld *et al.* 1997], [Chuang *et al.* 1998].

4.1.6. Interconversion of stationary and flying qubits.

No experimental proof at present time but optical pumping experiments can be suggested to convert electron qubit of an alkaline vapor to polarized photons.

4.1.7. Transmit flying qubits between specific locations.

Full quantum teleportation over inter-atomis distances in a trichloroethylene molecule. [Nielsen *et al.* 1998].

4.2 Quantum dots.

Semiconductor quantum dots are nanoscopic quantum structures that allow electronic properties to be tailored through quantum confinement. Coherent manipulation of single localized quantum system [Bonadeo, *et al.* 1998].

4.3 Trapped ions.

- Ion trap processor utilises motional and electronic quantum states as qubits [Steane, *et al.* 2003].

- Logic gates [Leibfried, *et al.* 2003].
- Controlled *NOT* gate [Schmidt-Kaller, *et al.* 2003].
- Deutsch-Jozsa algorithm [Gulde, *et al.* 2003].

4.4 Josephson junctions.

In superconductor, charge is carried by pairs of electron pairs of electrons, known as *Cooper pairs*. In this case the qubits are micrometre-size specks of superconductor, each connected to a superconducting reservoir named a *Josephson junction*.

By quantum mechanical tunnelling, a Cooper pair might jump from the reservoir onto a qubit. Then analogous to the spin up and down states, the qubit can be in a state with no excess Cooper pair, or one excess Cooper pair, or a superposed state of both. Superconducting quantum interference devices (SQUID) allow to control the Josephson coupling to its reservoir.

- Coupling of 2 qubits [Averin, *et al.* 2000], [Blatter, *et al.* 2003], [Chiorescu, *et al.* 2003], [Clarke, *et al.* 2003], [Pashkin, *et al.* 2003].

5. Solid polarized ¹²⁹Xe.

NMR, as it has been shown, offers the advantage of being an isolated quantum system, with a long decoherence time and easy quantum gate implementation through adequate RF pulses. The main drawback of NMR at equilibrium is its poor sensitivity, which limits its scalability with respect to quantum computation. Another limitation is that qubits are only characterized by the Larmor frequency, which limits the detectable number of qubits, from a technical point of view.

Discussions about the scalability of bulk NMR have shown that only solid NMR involving polarized states could be useful for quantum computation [Warren, *et al.* 1997].

Silicon-based NMR has been suggested by [Kane, *et al.* 1998] but no experimental realisation has been made at present time.

It would seem interesting to explore the potentials of Polarized ^{129}Xe in the solid state. ^{129}Xe could be polarized by optical pumping method (Kastler). In the laboratory, we are able to produce 0.1 mmole of ^{129}Xe polarized at 38(Oregioni Phd thesis). Such polarization yields an enhancement of the NMR signal of about 10^5 . The solidification temperature of ^{129}Xe is 117K, and therefore solid Xe is easily obtained by putting a Xe sample into a tube surrounded by liquid nitrogen ($T_b = 77K$).

In the solid state, the dipole-dipole coupling between ^{129}Xe spins no longer averages to zero through molecular motion and the degeneracy of the Xe spins is cancelled by the magnetic dipole-dipole interaction between the spins. Briefly, the dipolar interaction between two spins is represented by the Hamiltonian

$$H_D = g_n^2 \beta_n^2 \frac{I_1 I_2}{r^3} - 3 \frac{(I_1 r)(I_2 r)}{r^5},$$

which can be written as

$$H_D = g_n^2 \beta_n^2 \left[A + B + C + D + E + F \right].$$

Only the first two terms provide first-order contribution to the energy levels. These two terms are:

$$A = (1 - 3 \cos^2 \theta) I_{1z} I_{2z}; \quad B = -\frac{1}{4} (1 - 3 \cos^2 \theta) \left[I_1^+ I_2^- + I_1^- I_2^+ \right],$$

where θ is the angle between B_0 and \vec{r} which is the vector between I_1 and I_2 , and where I^+ and I^- are the spin shift operators.

When there are more than two spins, the degeneracy of the spin energies is canceled and there is a great number of different states [Abragam 1961]. Only in rare cases does the crystal structure permit complete resolution of the dipole splitting and second-moment methods could provide indirect structural information.

Regarding quantum computation, we would be interested in two special properties of dipolar coupling. The term B in the dipolar hamiltonian corresponds to "flip-flop" which can couple two spins very far from one another. This property is called spin diffusion. The second interesting property is the possibility of selecting multiple-quantum transitions by using appropriate magnetic field gradients.

We will briefly discuss how solid ^{129}Xe can fulfill the core requirements of quantum computation.

5.1. Well-characterized qubits.

Dipolar coupling spreads the energy states through many levels. The qubits could be characterized by the energy g_{N_i} and their position, if we use a sample in a fine tube.

Typically, in NMR we can selectively irradiate a spectral width of 100 Hz in a 1-mm slice. Therefore, in a 6-cm long coil, about 600 qubits can be characterized. This estimation has to be refined, owing to the 2-kHz linewidth of solid ^{129}Xe and the available gradient intensity.

5.2. Ability to initialize the state of qubits.

Even with polarized ^{129}Xe , not all spins are initialized in a single state, because the polarization is only 38%, but bulk NMR spin manipulations (logical labeling and temporal averaging) should be implemented in order to well initialize the qubits by adapted method from liquid NMR.

5.3. Long relevant decoherence times.

Typically, the longitudinal relaxation time (T_1) of solid ^{129}Xe is about hours, much longer than liquid NMR, where the T_1 of ^{13}C is only several seconds.

5.4. A universal set of quantum gates.

Again the RF pulses used in liquid NMR has to be adapted to the short transversal relaxation of solid NMR but there is no fundamental difference between the two NMR domains.

5.5. Qubit specific measurements.

There seems to be two advantages to use solid NMR, firstly the measured qubit could be identified not only by its NMR frequency but also by its position and secondly one can select specific qubits by selection of multi quanta transitions by the use of adapted gradient fields.

The last two requirements involved in quantum teleportation are not relevant for solid Xe.

Before more thinking about quantum computation with polarized Xe in the solid state we have to measure the distance at which the spin diffusion can be detected by performing a selective pulse in presence of z-gradient in order to irradiate a slice far from the centre of the coil and measure the NMR signal at the centre of the coil in presence of a z-gradient.

Bibliography.

- [Deutsch 1985]
- [DiVincenzo 2000]
- [Ernst, *et al.* 1987]
- [Feynman 1982]
- [Freedman, *et al.* 2002a]
- [Freedman, *et al.* 2002b]
- [Freedman, *et al.* 2002c]
- [Garey, Johnson 1979]
- [Gershenfeld, *et al.* 1998]

[Goldreich 2001]
[Gulde, *et al.* 2003]
[Grover 1996]
[Kane, *et al.* 1998]
[Kitaev 2000]
[Leibfried, *et al.* 2003]
[Lloyd 1993]
[Lloyd 1996]
[Manin 1980]
[Matiyasevich 1993]
[Navon, *et al.* 1996]
[Nielsen, Chuang 2000]
[Nielsen, *et al.* 1998]
[Pashkin, *et al.* 2003]
[Pomerance 1987]
[Schmidt-Kaller, *et al.* 2003]
[Shor 1994]
[Shor 1997]
[Steane, *et al.* 2003]
[Svozil 1994]
[Vandersypen, *et al.* 2001)]
[van Leeuwen 1990]
[van Leeuwen 1995]
[Verhulst, *et al.* 2001]
[Warren 1997]
[Warren, *et al.* 1997]
[Yao 1993]