Physical Models for Quantum Computers

Prog. Theor. Phys. Suppl. 145, ??? - ??? (2002)

H. De Raedt[1*], K. Michielsen[1], S. Miyashita[2] and K. Saito[2]

[1] *Institute for Theoretical Physics and Materials Science Centre*
University of Groningen, Nijenborgh 4
NL-9747 AG Groningen, The Netherlands

[2] *Department of Applied Physics, School of Engineering*
University of Tokyo, Bunkyo-ku, Tokyo 113

(Received May 6, 2002)

We discuss the impact of the physical implementation of a quantum computer on its computational efficiency, using computer simulations of physical models of quantum computer hardware. We address the computational efficiency of practical procedures to extract the results of a quantum computation from the wave function respresenting the final state of the quantum computer.

§1. Introduction

Theoretical work has shown that a quantum computer (QC) has the potential of solving certain computationally hard problems such as factoring integers [1)] and searching databases much faster than a conventional computer [2)]. These two algorithms are concrete examples of quantum algorithms (QAs) that exploit the theoretical power of a QC.

At any point in time, the state of a conventional computer is represented by the two possible states of N two-state systems (bits). A conventional computer can be in only one of the 2^N states simultaneously. Conceptually, operations on these states corresponds to $2^N \times 2^N$ matrices that have no special properties. On the other hand, the state of a QC is represented by the quantum state of N spin-1/2 systems (qubits), which can be in any linear combination of the 2^N basis states, and operations correspond to unitary transformations on vectors in this 2^N-dimensional Hilbert space. In principle, this feature can be exploited to carry out of the order of 2^N arithmetic operations simultaneously. The potential of QCs to perform this super-massive, parallel processing has attracted a lot of interest.

In most theortical work the operation of a QC is described in terms of highly idealized transformations on the qubits [3)-7)]. The impact of the physical implementation of a QC on its computational efficiency is largely unexplored. On a physically realizable, non-ideal QC, operations that manipulate one particular qubit also affect the state of other qubits. This may cause unwanted deviations from the ideal motion of the total system and lead to practical problems of programming QCs:

*) E-mail: deraedt@phys.rug.nl

An implementation of a quantum computation that works well on one QC may fail on others. Furthermore, so far, little attention has been paid to the computational efficiency of the practical (=experimental) procedure to extract the results from the wave function respresenting the final state of the QC. In this paper we discuss both aspects taking the point of view that eventually, a QC will be a real physical system.

§2. Physical models for Quantum Computers

Disregarding relativistic effects (a very good approximation for the case at hand), generic QC hardware can be modeled in terms of quantum spins (qubits) that evolve in time according to the time-dependent Schrödinger equation (TDSE)

$$i\frac{\partial}{\partial t}|\Phi(t)\rangle = H(t)|\Phi(t)\rangle. \tag{1}$$

In this paper we adopt units such that $\hbar = 1$. In the absence of interactions with other degrees of freedom (e.g. with the environment) the spin-1/2 system can be modeled by the time-dependent Hamiltonian

$$H(t) = -\sum_{j,k=1}^{L}\sum_{\alpha=x,y,z} J^{\alpha}_{j,k}(t)S^{\alpha}_{j}S^{\alpha}_{k} - \sum_{j=1}^{L}\sum_{\alpha=x,y,z} h^{\alpha}_{j}(t)S^{\alpha}_{j}, \tag{2}$$

where the first sum runs over all pairs of spins (qubits), S^{α}_{j} denotes the α-th component of the spin-1/2 operator representing the j-th qubit, $J^{\alpha}_{j,k}(t)$ determines the strength of the interaction between the qubits labeled j and k, and $h^{\alpha}_{j}(t)$ is the external field acting on the j-th spin. The number of qubits is L and the dimension of the Hilbert space $D = 2^L$. In terms of spin matrices, the operator Q_j measuring the state of qubit j is given by

$$Q_j = \frac{1}{2} - S^{z}_{j}. \tag{3}$$

The physical system defined by Eq.(2) includes the simplest (Ising) model of a universal QC [8),9)] and is sufficiently general to serve as a physical model for a generic QC at zero temperature without coupling to other degrees of freedom. A QA for QC model (2) consists of a sequence of elementary operations during which the J's and h's take prescribed values. In general, given a QA for an ideal QC, it is a non-trivial problem to express this QA in terms of manipulations of the physical model of the real QC.

Specific candidate hardware realizations of (2) include NMR systems [10)-17)], linear arrays of quantum dots [18)] or Josephson junctions [19)]. An approximate model Hamiltonian for the former reads

$$H(t) = -\sum_{i=1}^{L-1} E_i S^{z}_{i}S^{z}_{i+1} - \sum_{i=1}^{L} h_j(t)S^{x}_{j} + E_0\sum_{i=1}^{L} P_j(t)S^{z}_{j}, \tag{4}$$

where $E_i = E_0$ ($E_i = 2E_0$) when i is odd (even) and $h_i(t)$ and $P_i(t)$ are external controls [18)].

Projection of the Josephson-junction model onto a subspace of two states per qubit yields [20), 21)]

$$H(t) = -2E_L(t)\sum_{i=1}^{L-1} S_i^y S_{i+1}^y - E_J\sum_{i=1}^{L} S_j^x - \sum_{i=1}^{L} h_j(t)S_j^z, \tag{5}$$

where the energy of Josephson tunneling is represented by E_J and $E_L(t)$ denotes the energy associated with the inductive coupling between the qubits [20), 21)]. Here $h_j(t)$ and $E_L(t)$ may be controlled externally.

To study the difference between the ideal and physical realization of a QC, we consider a physical model for NMR-QC experiments [10) - 17)], mainly because other candidate technologies for building QCs are not yet developed to the point that they can execute computationally non-trivial QAs. For simplicity of presentation we confine the discussion to 2-qubit QCs. The model Hamiltonian reads

$$H(t) = -JS_1^zS_2^z - h^z(S_1^z + \gamma S_2^z) - \tilde{h}^x(t)(S_1^x + \gamma S_2^x) - \tilde{h}^y(t)(S_1^y + \gamma S_2^y), \tag{6}$$

where γ denotes the ratio of the gyromagnetic factors of spin 2 and spin 1. In NMR experiments radio frequency fields are used to manupulate individual spins. A simple choice is to put $h^\alpha(t) = \tilde{h}^\alpha \sin(f_j^\alpha t + \varphi_j^\alpha)$ where the frequency and phase of the field are denoted by f_j^α and φ_j^α respectively. The simple choice for the time dependence of the pulses is for pedagogical purposes only. In practice, NMR experiments use much more complicated pulses of electromagnetic radiation [22), 23)] but this is not relevant for the discussion that follows.

The impact of the physical implementation on the performance of a QC is most easily studied through simulation of model (2) on a conventional computer. At the time of writing it is a simple matter to simulate systems of 16 qubits on a PC, using a software emulator for QC hardware [24)]. In this paper we report simulation results for the model of the two nuclear spins of the ^{1}H and ^{13}C atoms in a carbon-13 labeled chloroform, a molecule that has been used in NMR-QC experiments [12), 13)]. In these experiments $h^z/2\pi \approx 500$MHz, $\gamma \approx 1/4$, and $J/2\pi \approx -215$Hz . In the following we will use the model parameters [12)] for the nuclear spins of this molecule rescaled with respect to 500Mhz, i.e we put

$$J = -0.43 \times 10^{-6}, \quad h^z = 1, \quad \gamma = 1/4. \tag{7}$$

With this choice of units, time divided by 2π is measured in units of 2 ns.

§3. Quantum Algorithms

One qubit is a two-state quantum system. The two basis states spanning the Hilbert space are denoted by $|\uparrow\rangle \equiv |0\rangle$ and $|\downarrow\rangle \equiv |1\rangle$. Rotations of spin j about $\pi/2$ around the x and y-axis are basic QC operations. We will denote them by X_j and Y_j respectively, and write $\overline{Z}$ for the inverse of the operation Z. Clearly these operations

can be implemented in terms of the time evolution of model (2) by a proper choice of the model parameters.

Computation necessarily requires some form of communication between the qubits. A basic two-qubit operation is provided by the CNOT gate. The CNOT gate flips the second spin if the first spin is in the down state, i.e. the first qubit acts as a control qubit for the second one. On an ideal QC the CNOT gate can be expressed in terms of single-qubit operations and a two-qubit phase-shift operation. There are many different, logically equivalent sequences that implement the CNOT gate on an NMR QC. Here we limit ourselves to the sequences

$$CNOT_1 = Y_1 X_1' \overline{Y}_1 X_2' \overline{Y}_2 I' Y_2, \tag{8}$$

$$CNOT_2 = Y_1 X_1' X_2' \overline{Y}_1 \overline{Y}_2 I' Y_2, \tag{9}$$

where the symbol I' represents the time evolution $e^{i\tau(JS_1^zS_2^z+h^zS_1^z+\gamma h^zS_2^z)}$ with $\tau = -\pi/J$. The single-spin rotations X_1', Y_1' and X_2' are defined by the identities

$$e^{-i\tau(h^z-h)S_1^z} = Y_1 X_1' \overline{Y}_1 = \overline{X}_1 Y_1' X_1, \tag{10}$$

$$e^{-i\tau(\gamma h^z-h)S_2^z} = Y_2 X_2' \overline{Y}_2, \tag{11}$$

where $h = -J/2$.

As simple examples of QAs, we consider $(QA)_1$ and $(QA)_2$ defined by

$$(QA)_1|b_1b_2\rangle \equiv (CNOT)^5|b_1b_2\rangle \quad , \quad (QA)_2|si\rangle \equiv Y_1(CNOT)^5|si\rangle, \tag{12}$$

where $|b_1b_2\rangle \equiv |b_1\rangle|b_2\rangle$, $b_i = 0, 1$, and $|si\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. On an ideal QC, $CNOT^2$ is the identity operation and hence $(CNOT)^5 = CNOT$. Furthermore we have $\langle si|(CNOT)^5 QA_1 (CNOT)^5|si\rangle = 1/2$. To obtain a clear-cut, zero-one answer in terms of expectation values of the qubits we apply a $\pi/2$ rotation to spin 1: $Y_1(CNOT)^5|si\rangle = |11\rangle$. For this reason the CNOT operations in $(QA)_2$ are followed by a $\pi/2$ rotation of spin 1. Obviously, running $(QA)_1$ and $(QA)_2$ on an ideal QC yields the correct answer but as we will show below, on a physical QC this is not always the case.

It is instructive to inquire about the condition to rotate spin 1 about an angle φ_1 without affecting the state of spin 2. A general analytical, quantitative analysis of this many-body problem is rather difficult but we can easily study the limiting case in which the interaction between the spins has negligible impact on the time evolution of the spins during application of the SF pulse. This is the case that is relevant to the model system considered here (since J is very small) and also to experiments [10)-13)]. For simplicity we consider the case of rotating SF fields, e.g. $\phi_x = 0$ and $\phi_y = \pi/2$. An SF pulse of duration t changes the state of the two-spin system according to

$$|\Phi(t)\rangle = e^{ith_1^z(S_1^z+S_2^z)} e^{it\tilde{h}_1^x S_1^y} e^{it\mathbf{S}_2\cdot\mathbf{v}} |\Phi(0)\rangle, \tag{13}$$

where $\mathbf{v} \equiv (0, \gamma\tilde{h}^x, (\gamma-1)h^z)$.

Without loss of generality we will assume that $0 < \gamma < 1$, in concert with the choice of parameters (7). Then, using representation (13), straightforward algebra

Table I. Model parameters of single-qubit operations on an NMR QC using rotating SFs for the case ($k = 1$, $N = 1$, $M = 4$), see Eq.(16). Parameters of model (2) that do not appear in this table are zero, except for the interaction $J = -0.43 \times 10^{-6}$, $\gamma = 1/4$, $\tilde{h}^y = \tilde{h}^x$ and the constant magnetic fields $h^z = 1$. The TDSE is solved using a time step $\delta/2\pi = 0.01$.

	$\tau/2\pi$	ω	$\tilde{h}_1^x$	ϕ_x	ϕ_y
X_1	8	1.00	-0.0312500	$-\pi/2$	0
X_2	128	0.25	-0.0078125	$-\pi/2$	0
Y_1	8	1.00	0.0312500	0	$\pi/2$
Y_2	128	0.25	0.0078125	0	$\pi/2$
X_1'	8	1.00	0.0559593	$-\pi/2$	0
X_2'	128	0.25	0.0445131	$-\pi/2$	0
Y_1'	8	1.00	-0.0559593	0	$\pi/2$

shows that the condition to rotate spin 1 (2) about an angle φ_1 (φ_2) without affecting the state of spin 2 (1) is given by

$$(1-\gamma)^2 k_1^2 + \frac{\gamma^2}{4}\left(\frac{\varphi_1}{2\pi}\right)^2 = n_1^2 \quad , \quad (1-\frac{1}{\gamma})^2 k_2^2 + \frac{1}{4\gamma^2}\left(\frac{\varphi_2}{2\pi}\right)^2 = n_2^2, \quad (14)$$

where $k_1, k_2, n_1, n_2 \in \mathbb{N}$. The angles of rotation about the y-axis can be chosen such that $0 \leq \varphi_1 \leq 2\pi$ and $0 \leq \varphi_2 \leq 2\pi$. In general, Eqs.(14) have no solution but a good approximate solution may be obtained if γ is a rational number and k_1 and k_2 are large. Let $\gamma = N/M$ (for our choice of parameters, $N = 1$ and $M = 4$) where N and M are integers satisfying $0 < N < M$. It follows that the representation $k_1 = kMN^2$ and $k_2 = kNM^2$ will generate sufficiently accurate solutions of Eqs.(14) if the integer k is chosen such that

$$2kNM(M-N) \gg 1. \quad (15)$$

If k satisfies condition (15) a pulse that rotates spin 1 (2) will hardly affect spin 2 (1). In terms of k, N, and M, the relevant physical quantities are then given by

$$\frac{t_1 h^z}{2\pi} = 2kMN^2, \quad \frac{\tilde{h}^x}{h^z} = \frac{1}{2kMN^2}\frac{\varphi_1}{2\pi}, \quad \frac{t_2 h^z}{2\pi} = 2kM^3, \quad \frac{\gamma\tilde{h}^x}{h^z} = \frac{1}{2kM^3}\frac{\varphi_2}{2\pi}. \quad (16)$$

§4. Simulation of Quantum Computer hardware

The model parameters for the rotating SFs are determined according to the theory outlined above. We use the integer k to compute all free parameters and the subscript $s = 2kMN^2$ to label the results of the QC calculation. For reference we present the set of parameters corresponding to $k = 1$ in Table I. Multiplying s (the duration of the SF pulse) with the unit of time (2 ns) shows that in our simulations, single-qubit operations are implemented by using short SF pulses that are, in NMR terminology, selective and hard.

In Tables II and III we present simulation results for $(QA)_1$ and $(QA)_2$ respectively. The initial states $|10\rangle$, $|01\rangle$, $|11\rangle$ and $|si\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ have been prepared by starting from the state $|00\rangle$ and performing exact rotations of the spins.

It is clear that even the least accurate implementation ($s = 16$) of $(QA)_1$ nicely reproduces the correct answers if the input corresponds to one of the four basis states but it is also clear that it completely fails if the input state is a singlet state. In the regime where systematic phase errors are significant the QAs do not always function correctly. As a further demonstration, we carry out the CNOT operation using $CNOT_1$ and $CNOT_2$. On an ideal QC both sequences yield identical results but on a physical system they may produce different results, as exemplified by comparing Table II ($CNOT_1$) with Table III ($CNOT_2$).

Table II. Expectation values of the two qubits (a_s and b_s) as obtained on a QC that uses rotating SFs to manipulate individual qubits. The results obtained on an ideal QC are given by a and b. The time $s = \tau/2\pi = 2kMN^2$ determines the duration and strength of the SF pulses through relations (16), see Table I for the example of the case $s = 8$.

Operation	a	b	a_{16}	b_{16}	a_{32}	b_{32}	a_{64}	b_{64}
$(CNOT_1)^5\|00\rangle$	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
$(CNOT_1)^5\|10\rangle$	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
$(CNOT_1)^5\|01\rangle$	0.00	1.00	0.00	1.00	0.00	1.00	0.00	1.00
$(CNOT_1)^5\|11\rangle$	1.00	0.00	1.00	0.00	1.00	0.00	1.00	0.00
$Y_1(CNOT_1)^5\|si\rangle$	1.00	1.00	0.03	1.00	0.58	1.00	0.88	1.00

Table III. Same as Table II except that instead of $CNOT_1$ sequence $CNOT_2$ given by (9) was used to perform the quantum computation.

Operation	a	b	a_{16}	b_{16}	a_{32}	b_{32}	a_{64}	b_{64}
$(CNOT_2)^5\|00\rangle$	0.00	0.00	0.50	0.20	0.07	0.02	0.06	0.02
$(CNOT_2)^5\|10\rangle$	1.00	1.00	0.50	0.80	0.93	0.98	0.95	0.98
$(CNOT_2)^5\|01\rangle$	0.00	1.00	0.51	0.20	0.93	0.98	0.06	0.98
$(CNOT_2)^5\|11\rangle$	1.00	0.00	0.50	0.80	0.07	0.02	0.95	0.02
$Y_1(CNOT_2)^5\|si\rangle$	1.00	1.00	0.95	0.98	0.93	0.98	0.99	0.98

Although $(QA)_1$ and $(QA)_2$ are logically identical, the results depend sensitively on the order in which the single-qubit operations are carried out. In agreement with the theoretical analysis of Section 3 the results converge to the exact ones for sufficiently large k, as indicated in Table II. Thus, for sufficiently slow operation this QC will operate correctly.

The following simple example shows the complications that may arise if more than 2 qubits are involved. Consider a QA that performs an ideal operation on the first two qubits while leaving the third and fourth qubits untouched. For simplicity let us assume that the input state factorizes, i.e. $|\Phi\rangle = |\phi(1,2)\rangle \otimes \{a_0|00\rangle + a_1|10\rangle + a_2|01\rangle + a_3|11\rangle\}$. On the ideal QC the output state is $|\widetilde{\Phi}\rangle = |\widetilde{\phi}(1,2)\rangle \otimes \{a_0|00\rangle + a_1|10\rangle + a_2|01\rangle + a_3|11\rangle\}$ but on a physically realizable QC the operation takes some time τ and hence the output state has the form $|\widehat{\Phi}\rangle = |\widetilde{\phi}(1,2)\rangle \otimes \{a_0|00\rangle + a_1 e^{i\tau h_3^z/2}|10\rangle + a_2 e^{i\tau h_4^z/2}|01\rangle + a_3 e^{i\tau(h_3^z+h_4^z)/2}|11\rangle\}$, up to an irrelevant phase factor. It is clear that unless $\tau h_3^z = 4\pi n_3$ and $\tau h_3^z = 4\pi n_4$ ($n_3, n_4 \in \mathbb{Z}$), qubits three and four will acquire a phase and the state $|\widetilde{\Phi}\rangle$ no longer corresponds to the one obtained an ideal QC. The fact that physical qubits evolve in time, i.e. can never be kept still, leads to considerable complications in the design of a QA

for a physical QC [25]. In essence this design becomes a complicated optimization problem, as exemplified by the description of NMR-QC experiments [26), 27]. In general, the solution of this problem may well require computational resources that scale unfavourably with the number of qubits.

Quantum error correction schemes that work well on an ideal QC require many extra qubits and many additional operations to detect and correct errors. The systematic errors discussed above are not included in the current model of quantum error correction and fault tolerant computing [7]. On a physical QC the error-correction qubits will suffer from the same deficiencies.

§5. Computational efficiency of observing a quantum state

We now assume that the QC is operating like an ideal QC and consider aspects related to the readout of the result of a quantum computation. Generally in quantum mechanics, an observation corresponds to a measurement of some physical quantity. For example, let the state be

$$|\Psi\rangle = \sum_i a_i |\phi_i\rangle. \tag{17}$$

If we make a single observation of a quantity A we obtain one of the values

$$A_i = \langle\phi_i|A|\phi_i\rangle. \tag{18}$$

if $|\phi_i\rangle$ is an eigenvector of A with eigenvalue $\{A_i\}$. After repeated observation, we can construct a histogram of the frequencies with which the A_i's occur and estimate the probability $|a_i|^2$ to observe A_i. As a consequence of the observation process, some information about the state $|\Psi\rangle$ is lost: $\{|a_i|^2\}$ does not contain all information about the wave function $|\Psi\rangle$. In order to distinguish between different states we have to observe physical quantities that take different values for each of the states.

Let us consider a system that consists of S=1/2 spins representing the qubits of the QC. We take for the basis states $\{|\phi_i\rangle\}$ the eigenstates of the z components of the Pauli-spin matrices, $|\phi_i\rangle = |\sigma_1^i, \sigma_2^i, \cdots, \sigma_N^i\rangle$, where $\sigma_k^i = \pm 1, k = 1, \cdots, N$, and N is the number of qubits. The most simple quantity that uniquely identifies a basis state is the set of numbers $\{\sigma_1^i, \sigma_2^i, \cdots, \sigma_N^i\}$.

5.1. *Observation of a basis state: Grover's database search algorithm*

In Grover's algorithm [2] the final state of the quantum computation is one of the basis states, e.g.,

$$|\Psi\rangle = |+-++\cdots+\rangle, \tag{19}$$

where the "$-$" representes the position of the item that was to be searched for. In this case, we can first observe spin 1. This gives $\langle\sigma_1\rangle \equiv \langle\Psi|\sigma_1|\Psi\rangle = 1$. We then repeat the calculation (= experiment), yielding the same $|\Psi\rangle$, and measure $\langle\sigma_2\rangle = -1$, and so on. After measuring the N different spins we find the set $\{\langle\sigma_1\rangle, \langle\sigma_2\rangle, \cdots, \langle\sigma_N\rangle\}$. In this case there is no problem of observation: We can identify the final state of the QC with $\mathcal{O}(N)$ measurements, hence the observation process is efficient.

5.2. *Observation of a linear combination of basis states: Shor's algorithm*

In Shor's algorithm [1),6)], the final state of the QC is given by a linear combination of the basis states, see Eq.(17). To complete the factorization, we have to identify the final state of the QC. If we simply measure σ_1, we obtain $+1$ or -1 and the same for the other spins. Accumulating such observations only gives $\langle\Psi|\sigma_i|\Psi\rangle$ but little information on which basis state the QC is in, nor about the distribution of the a_i's. In order to identify the basis states that contribute to the final state of the QC, we have to observe the values of spins $(\sigma_1^i, \sigma_2^i, \cdots, \sigma_N^i)$ simultaneously. This can be done by decomposing the state $|\Psi\rangle$ into N orthogonal projections. Conceptually this can be done by a collection of 2^N Stern-Gerlach beam splitters. Each time a particle enters the device from the left, only one of the detectors on the right will report the arrival of the particle and at the same time identify the basis state. The detector for the basis state $|\sigma_1^i, \sigma_2^i, \cdots, \sigma_N^i\rangle$ will give a signal with probability $\{|a_i|^2\}$.

This procedure seems simple but in practice, in order to detect and identify a basis state, we have to provide 2^N detectors and the potential efficiency of quantum computation is completely lost. Indeed, if we want to factor a large number L and are allowed to use L machines, we let the k-th machine divide L by k and test whether the remainder is zero or not. In this way we can easily find the factors of L in one step but clearly we do not consider this a solution of the factorization problem. If we need $\mathcal{O}(L)$ detectors to process the result of Shor's algorithm, there is no point in using a QC.

We should also consider the case where we measure a single physical quantity that provides detailed information about a final state of the QC. For example, the magnetization

$$M = \sum_{n=1}^{N} \sigma_n, \tag{20}$$

can be measured without observing individual spins. The discrete values of M can be resolved experimentally. Note however that the values of M change from $-N$ to N and the range of M values is only $O(N)$.

In the case of Shor's algorithm, we may consider an operator that directly corresponds to the number of each basis state:

$$X = \sum_{n=1}^{N} 2^{n-1}(\sigma_n - 1). \tag{21}$$

This operator is diagonal in the representation that we use for the basis states $|\phi_i\rangle$. If we observe X we obtain

$$X_i = \langle\phi_i|X|\phi_i\rangle \tag{22}$$

with the probability $|a_i|^2$. Thus, we can uniquely identify the final state of one calculation or, by repeated observation, obtain the distribution of the a_i's.

At first sight using X instead of individual spins seems to solve the detection problem but that is not the case. In contrast to the measurement of the magnetization, the range of X is $\mathcal{O}(2^N)$ and we have to determine all digits of X, which is

essentially the same as using 2^N detectors. This requires measurements with a precision that increases like 2^N and the problem still remains. However, in the case of the number factoring problem where N is a product of two primes, a rough estimate of the value of X may already give a boost in efficiency (compared to a random choice) of searching for candidate factors of N so there may be situations in which the whole procedure may work. Note that in the case of Grover's algorithm it is sufficient to have N instead of 2^N detectors because we know that the results of the calculation are single basis states, not a linear combination.

As another manifestation of the inefficient observation we consider a QA to solve the Number Partitioning Problem, described elsewhere [28]. This QA returns as a result a linear combination of basis states but the relevant information is contained only in the coefficient a_0 of the basis state with zero energy. The partitioning problem has a soloution if a_0 is nonzero, while there is no solution if $a_0 = 0$. In this case we do not need N detectors. One detector for the state $|\phi_0\rangle$ will do. But there is another problem. Effectively this QA computes the ratio of the number of solutions of the partitioning problem to the total number of partitionings (which is $\mathcal{O}(2^{N-1})$). When the number of solutions of partitions is small, e.g. zero or one, and the total number of partitionings is large, $|a_0|^2 = \mathcal{O}(2^{-N})$ which may be too small to be observable in practice. Essentially the problem of observation boils down to a problem of insufficient precision, as in the case of Shor's algorithm.

The observation problem sketched above is generic rather than an exception if the result of the quantum computation is a linear combination of the basis states and the coefficients carry information (we exclude the trivial case of a uniform probability distribution). One way to alleviate this problem is to increase the number of functional units. This is the approach taken in NMR QC experiments where a very large number (orders of magnitude larger than the number of different basis states of the QC) of molecules contribute to the observed signal [26), 27)]. Obviously, in terms of quantum processors, the computational efficiency of this approach is fairly low. If we have additional information about the way the basis states contribute to the linear superposition we may be able to indentify the relevant basis states by measuring the expectation values of the individual spins [26), 27)]. However, in this case, the assessment of the efficiency of the QA should take into account the cost of obtaining this information, in particular scaling of this cost with the problem size.

§6. Summary

For each realization of QC hardware, there is a one-to-one correspondence between the QA and the unitary matrix that transforms the state of the quantum system. A QA will operate correctly under *all* circumstances if the *whole* unitary matrix representing the QA is a good approximation to the ideal one. In other words, the magnitude and the phase of *all* matrix elements should be close to their ideal values. For n qubits there are $2^n(2^n - 1)$ real numbers that specify the unitary matrix corresponding to a QA. All these numbers should be close to their ideal values, otherwise the QA is bound to produce wrong answers. These constraints put considerable demands on technologies to fabricate QCs.

We argued that estimating the efficiency of a quantum computation is more than counting the operations in a quantum algorithm. The cost of quantum state identification, an essential part of potentially powerful QAs, has to be taken into account. It remains a great challenge to show that the theoretical efficiency of a QC can be turned into practically useful computing power.

Acknowledgements

Support from the Dutch "Stichting Nationale Computer Faciliteiten (NCF)" and from the Grant-in-Aid for Research from the Japanese Ministry of Education, Science and Culture is gratefully acknowledged.

References

1) P. Shor, in: *Proc. 35th Annu. Symp. Foundations of Computer Science*, S. Goldwasser ed., (IEEE Computer Soc., Los Alamitos CA, 1994) p. 124
2) L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997)
3) D.P. DiVincenzo, Science **270**, 255 (1995)
4) A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996)
5) V. Vedral and M. Plenio, Progress in Quantum Electronics **22**, 1 (1998)
6) P.W. Shor, SIAM Review **41**, 303 (1999)
7) M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, 2000)
8) S. Lloyd, Science **261**, 1569 (1993)
9) G.P. Berman, G.D. Doolen, D.D. Holm, and V.I. Tsifrinovich, Phys. Lett. **A193**, 444 (1994)
10) J.A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998)
11) J.A. Jones, M. Mosca, and R.H. Hansen, Nature **393**, 344 (1998)
12) I.L. Chuang, L.M.K. Vandersypen, Xinlan Zhou, D.W. Leung, and S. Lloyd, Nature **393**, 143 (1998)
13) I.L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998)
14) R. Marx, A.F. Fahmy, J.M. Meyers, W. Bernel, and S.J. Glaser, Phys. Rev. A **62**, 012310 (2000)
15) E. Knill, R. Laflamme, R. Martinez, and C.-H. Tseng, Nature **404**, 368 (2000)
16) D.G. Cory, R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemariam, Y.S. Weinstein, and W.H. Zurek, Fortschr. Phys. **48**, 875 (2000)
17) J.A. Jones, Fortschr. Phys. **48**, 909 (2000)
18) G. Toth and S. Lent, Phys. Rev. A 63, 052315 (2001)
19) Y. Nakamura, Yu. A. Pashkin, and J.S. Tsai, Nature **398**, 786 (1999)
20) Y. Makhlin, G. Schön, and A. Shnirman, Nature **398**, 305 (1999)
21) R. Fazio, G.M. Palma, and J. Siewert, Phys. Rev. Lett. **83**, 5385 (1999)
22) R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*, (Oxford University Press, New York, 1987)
23) R. Freeman, *Spin Choreography*, (Spektrum, Oxford, 1997)
24) H. De Raedt, A.H. Hams, K. Michielsen, and K. De Raedt, Comp. Phys. Comm. **132**, 1 (2000); QCE can be downloaded from http://rugth30.phys.rug.nl/compphys/qce.htm
25) H. De Raedt, A. Hams, K. Michielsen, S. Miyashita, and K. Saito, J. Phys. Soc. Jpn. (Supp.) **69**, 401 (2000)
26) L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, R. Cleve, I.L. Chuang, Phys. Rev. Lett. **85**, 5452 (2000)
27) L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, I.L. Chuang, Nature **414**, 883 (2001)
28) H. De Raedt, K. Michielsen, K. De Raedt, and S. Miyashita, Physics Letters **A290**, 227 (2001)