Fortschr. Phys. **46** (1998) 6–8, 759–769

Prospects for Quantum Computation with Trapped Ions

R. J. HUGHES and D. F. V. JAMES

Los Alamos National Laboratory
Los Alamos, NM 87545, USA

Abstract

A brief survey of the requirements for quantum computational hardware, and an overview of the ion trap quantum computation project at Los Alamos are presented. The physical limitations to quantum computation with trapped ions are discussed.

1. Introduction

Over the past decade information theory has been generalized to allow binary data to be represented by two-state quantum mechanical systems. (A single two-level system has come to be known as a qubit in this context.) The additional freedom introduced into information physics with quantum systems has opened up a variety of capabilities that go well beyond those of conventional information. For example, quantum cryptography [1, 2] allows two parties to generate a secret key even in the presence of eavesdropping. But perhaps the most remarkable capabilities have been predicted in the field of quantum computation [3, 4].

BENIOFF [5] and subsequently FEYNMAN [5] explored the uses of quantum systems for (conventional) computation, but it was DEUTSCH [6] who first suggested that the quantum superposition principle could be exploited to achieve greater computational power quantum mechanically than with conventional computation. He coined the term "quantum parallelism" to describe the ability of a quantum computer to perform computations in superposition. However, it was not until the work of SHOR [7] in 1994 that quantum parallelism was shown to offer an efficient solution of an interesting computational problem. Specifically, building on earlier work of SIMON [8], SHOR invented polynomial-time quantum algorithms for solving the integer factorization and discrete logarithm problems [7]. The computational difficulty of solving these two problems with conventional computers underlies the security of much of modern public key cryptography [9]. Shor's algorithms are sufficiently compelling that the daunting scientific and technological challenges involved in practical quantum computation are now worthy of serious experimental study.

Every integer can be decomposed into a unique product of prime numbers. Most integers are easy to factor because they are products of small (prime) factors, but large integers (hundreds of digits) that are a product of two, comparably-sized primes can be very difficult to factor with conventional computers [10]. For example, in 1994 the 129-digit number known as RSA129 [11] required 5,000 MIPS-years of computer time over an 8-month period to determine its 64-digit and 65-digit prime factors [12]. In contrast a quantum computer (QC) using Shor's algorithm at a clock speed of 100 MHz would have factored this number in a few seconds. Furthermore, the growth in complexity of the quantum factoring algorithm is sufficiently slow that much larger numbers (1,024 bits, say) would require only tens of seconds for their factorization on such a QC, whereas the best conventional factoring algorithm would take $\sim 10^7$ years, extrapolating from the recent factorization of RSA130 [13].

Although experimental quantum computation is in its infancy, there is a very promising hardware concept using the quantum states of ions in an electromagnetic trap [14]. Several groups, including our own, [15] are now investigating quantum computation with such systems. Cirac and Zoller showed that laser-cooled ions in an electromagnetic trap have the necessary characteristics to perform quantum computation. The relevant coherence times can be adequately long; mechanisms for performing the quantum logic gate operations exist; and a high-probability readout method is possible. (For a detailed description see Reference [16].) A single logic operation using a trapped beryllium ion has been demonstrated [17]. However, even algorithmically small computations will require the creation and controlled evolution of entangled quantum states that are far more complex than have so far been achieved experimentally. It is therefore important to quantify the extent to which trapped ions could allow the quantum engineering of the complex states required for quantum computation [18]. Furthermore, by characterizing the way in which the precision of quantum operations depends on experimental parameters, it will be possible to determine how quantum error correction schemes and fault-tolerant methods can best be applied. These concepts hold out the prospect of indefinite quantum computation, even with imperfect physical implementations, if certain precision thresholds can be attained [19].

The rest of this paper is organized as follows. In Section 2 we review the Cirac-Zoller scheme for ion trap quantum computation, and Section 3 is devoted to a description of the different qubit schemes possible with trapped ions. Sections 4 and 5 contain estimates of the limits to quantum computation with the two classes of qubits. In Section 6 we compare the bounds obtained in sections 4 and 5 with the requirements of quantum factoring, and in Section 7 we investigate whether there is an upper bound to ion trap computational capacity in terms of fundamental constants. Finally in Section 8 we present some conclusions.

2. Quantum Computation with Trapped Ions

There are three essential requirements for quantum computation hardware. Firstly, it must be possible to prepare multiple qubits, adequately isolated from interactions with their environment for the duration of computation, in an addressable form. Secondly, there must be an external drive mechanism for performing the requisite quantum logic operations. And thirdly, there must be a readout mechanism for measuring the state of each qubit at the end of the computation. These conditions can be satisfied with trapped ions.

In an ion trap quantum computer a qubit would comprise two long-lived internal states, which we shall denote $|0\rangle$ and $|1\rangle$, of an ion isolated from the environment by the electromagnetic fields of a linear radio-frequency quadrupole (RFQ) ion trap. Many different ion species are suitable for quantum computation, and several different qubit schemes are possible, as we shall see below. For example, at Los Alamos we are developing an ion-trap quantum-computer experiment using calcium ions, with the ultimate objective of performing multiple gate operations on a register of several qubits (and possibly small computations) in order to determine the potential and physical limitations of this technology [15]. We have chosen calcium ions for the convenience of the wavelengths required. The heart of our experiment is a linear radio-frequency quadrupole (RFQ) ion trap with cylindrical geometry in which strong radial confinement is provided by radio-frequency potentials applied to four "rod" electrodes and axial confinement is produced by a harmonic electrostatic potential applied by two "end caps". After Doppler cooling on their 397-nm *S-P* transition, several calcium ions will become localized along the ion trap's axis because their recoil energy (from photon emission) is less than the spacing of the ion's quantum vibrational energy levels in the axial confining potential. Although localized to distances much smaller than the wavelength of the cooling radiation, the ions nevertheless undergo small amplitude oscillations. Their lowest frequency mode is the axial center of mass (CM) motion in which

all the ions oscillate in phase along the trap axis. The frequency of this mode, whose quantum states will provide a computational "bus", is set by the axial potential. The inter-ion spacing is determined by the equilibrium between this axial potential, which tends to push the ions together, and the ions' mutual Coulomb repulsion. For example, with a 200-kHz axial CM frequency, the inter-ion spacing is on the order of 30 μm. After this first stage of cooling, the ions form a "quantum register" in which one qubit can be addressed (with a suitable laser beam) in isolation from its neighbors. We have determined that more than 20 ions can be held in an optically addressable configuration. However, before quantum computation can take place, the quantum state of the ion's CM mode must be prepared in its quantum ground state.

Because of the long radiative lifetime of the metastable $3D$-states ($\sim$1 s), the S-D electric quadrupole transition in calcium ions has such a narrow width that it displays upper and lower sidebands separated from the central frequency by the CM frequency. With a laser that has a suitably narrow linewidth, tuned to the lower sideband, an additional stage of laser cooling (beyond Doppler cooling) can be used to prepare the "bus" qubit (CM vibrational mode) in its lowest quantum state ("sideband cooling"). On completion of this stage, the QC would have all qubits in the $|0\rangle$ state, ready for quantum computation. (This second stage of cooling could also be performed with Raman transitions.)

The quantum state of the register of ions will then be manipulated by performing quantum logical-gate operations that will be effected by directing a laser beam at individual ions for a prescribed time. The laser-ion interaction will coherently change the state of the qubit through the phenomenon of Rabi oscillations. (Several different types of transition are possible.) An arbitrary logical operation can be constructed from a small set of elementary quantum gates, such as the so-called "controlled-NOT" operation ("CNOT"), in which the state of one qubit (the "target") is flipped if a second qubit (the "control") is in the "1" state but left unchanged if the second qubit is in the "0" state,

$$\mathrm{CNOT}_{ct}\colon \begin{array}{l} |0\rangle_c\,|0\rangle_t \to |0\rangle_c\,|0\rangle_t \\ |0\rangle_c\,|1\rangle_t \to |0\rangle_c\,|1\rangle_t \\ |1\rangle_c\,|0\rangle_t \to |1\rangle_c\,|1\rangle_t \\ |1\rangle_c\,|1\rangle_t \to |1\rangle_c\,|0\rangle_t \end{array}, \tag{1}$$

where the subscripts c and t denote control and target, respectively. As we will see below, the CNOT operation can be effected with the help of the quantum states of the ions' CM motion to convey quantum information from one ion to the other.

On completion of the quantum logic operations the result of the quantum computation can be read out by turning on a laser connecting the $|0\rangle$ state with another ionic level that decays rapidly back to $|0\rangle$. An ion in the $|0\rangle$ state will then fluoresce, whereas an ion in the $|1\rangle$ state will remain dark. So, by observing which ions fluoresce and which are dark, a bit value can be obtained. We have recently succeeded in trapping calcium ions in our ion trap and imaging them with a charge-coupled device (CCD) camera. This is the first step toward creation of a quantum register [15].

3. Trapped Ion Qubits

In an ion trap QC, each qubit is comprised of two states, $|0\rangle$ and $|1\rangle$. There is also a computational "bus" qubit formed by the ground, $|g\rangle$, and first excited state, $|e\rangle$, of the ion's CM axial vibrational motion that is used to perform logic operations between qubits. By virtue of energy conservation (and possibly other selection rules) it is possible to perform two types of coherent operations on a qubit, using laser pulses directed at an ion: on-

resonance transitions that change only an ion's internal state ("V" pulses); and red-sideband transitions (detuned from resonance by the CM frequency) that change both the qubit's internal state and the CM quantum state ("U" pulses). The V-pulse Hamiltonian for a particular ion is,

$$H_V = \frac{\hbar\Omega}{2}\left[e^{-i\varphi}|1\rangle\langle 0| + e^{-i\varphi}|0\rangle\langle 1|\right], \tag{2}$$

and the U-pulse Hamiltonian is,

$$H_U = \frac{\hbar\eta\Omega}{2\sqrt{L}}\left[e^{-i\varphi}|1\rangle\langle 0|\, a + e^{-i\varphi}|0\rangle\langle 1|\, a^\dagger\right]. \tag{3}$$

Here Ω is the Rabi frequency, φ is the phase of laser drive, η is the Lamb-Dicke parameter (characterizing the strength of the interaction between the laser and the ions' oscillations), L is the number of ions, and a ($a^\dagger$) is the destruction (creation) operator for quanta of the CM motion, satisfying

$$a|g\rangle = 0\,, \qquad a^\dagger|g\rangle = |e\rangle\,, \qquad [a,\, a^\dagger] = 1\,. \tag{4}$$

The unitary operations effected by applying these Hamiltonians to the m-th qubit for a duration given by a parameter θ and phase φ are:

$$V_m(\theta,\,\varphi)\colon \quad \begin{array}{l} |0\rangle_m \to \cos(\theta/2)\,|0\rangle_m - ie^{i\varphi}\sin(\theta/2)\,|1\rangle_m \\ |1\rangle_m \to \cos(\theta/2)\,|1\rangle_m - ie^{-i\varphi}\sin(\theta/2)\,|0\rangle_m \end{array}, \tag{5}$$

and

$$U_m(\theta,\,\varphi)\colon \quad \begin{array}{l} |0\rangle_m|e\rangle \to \cos(\theta/2)\,|0\rangle_m|e\rangle - ie^{i\varphi}\sin(\theta/2)\,|1\rangle_m|g\rangle \\ |1\rangle_m|g\rangle \to \cos(\theta/2)\,|1\rangle_m|g\rangle - ie^{-i\varphi}\sin(\theta/2)\,|0\rangle_m|e\rangle \end{array}. \tag{6}$$

To perform logic operations on the qubits an additional red-detuned operation involving an auxiliary level, $|aux\rangle$, in each qubit is required, with Hamiltonian

$$H_U^{aux} = \frac{\hbar\eta\Omega}{2\sqrt{L}}\left[e^{i\varphi}|aux\rangle\langle 0|\, a + e^{-i\varphi}|0\rangle\langle aux|\, a^\dagger\right], \tag{7}$$

with associated unitary operation $U_m^{aux}(\theta,\,\varphi)$. For example, the controlled-sign-flip (CSF) operation between two qubits, c and t

$$\mathrm{CSF}_{ct}\colon \quad \begin{array}{l} |0\rangle_c|0\rangle_t \to |0\rangle_c|0\rangle_t \\ |0\rangle_c|1\rangle_t \to |0\rangle_c|1\rangle_t \\ |1\rangle_c|0\rangle_t \to |1\rangle_c|0\rangle_t \\ |1\rangle_c|1\rangle_t \to |1\rangle_c|1\rangle_t \end{array}, \tag{8}$$

can be accomplished with the sequence of three U-pulses of appropriate duration:

$$\mathrm{CSF}_{ct} = U_c(\pi,\,0)\; U_t^{aux}(2\pi,\,0)\; U_c(\pi,\,0)\,. \tag{9}$$

From this operation a CNOT gate can be produced as

$$\mathrm{CNOT}_{ct} = V_t(\pi/2,\,\pi/2)\;\mathrm{CSF}_{ct}\;V_t(\pi/2,\,\pi/2)\,. \tag{10}$$

The U-pulse Hamiltonian drives transitions much more slowly than the V-pulse for a given Rabi frequency, which is proportional to the square root of the laser intensity. This is because it is necessary to put the ions' center of mass into motion, which is a slower process with more ions, and moreover the Lamb-Dicke parameter, η, is less than one. Because of their slowness (smallness of the coupling) the U-operations are the rate-limiting quantities to quantum logic operations. It is therefore desirable to drive these transitions as quickly as possible. However, the laser intensity cannot by made arbitrarily large, in order to avoid driving a V-transition, for instance. In the following we shall only count the duration of the U-pulses to the computational time.

There are two classes of candidates for the qubit levels. The first category occurs in ions such as Hg^+, Sr^+, Ca^+, Ba^+ and Yb^+ with first excited states that are metastable, with lifetimes ranging from 0.1 s (Hg^+), 0.4 s (Sr^+), 1 s (Ca^+); 1 min (Ba^+) and even 10 years (Yb^+). A qubit is comprised of an ion's electronic ground (S) state ($|0\rangle$), and a sublevel ($|1\rangle$) of the metastable excited state (a D-state in Hg, Ca or Ba; an F-state in Yb). The advantage of this scheme is that it requires only a single laser beam to drive the qubit transitions, which greatly simplifies the optics of ion addressing. However, the disadvantage of this scheme is that it requires optical frequency stability of the laser drive that effects coherent transitions between the qubit levels.

Alternative qubit schemes use hyperfine sublevels of an ion's ground state, or even Zeeman sublevels in a small magnetic field for ions with zero nuclear spin, with transitions between the qubit levels driven by Raman transitions. The advantages of this type of scheme are that the qubit states can be much longer-lived than the metastable state qubits; only radio frequency stability is required (corresponding to the frequency difference between the sublevels); and there are many more possible choices of ion (Be^+, Ca^+, Ba^+ and Mg^+ for example). Disadvantages are that addressing of the qubits is more complex owing to the requirement for two laser beams; and the readout is more involved than with metastable state qubits.

During quantum computation it is essential that a QC evolves through a sequence of pure quantum states, prescribed by some quantum algorithm. In general there will be some time scale required for a particular computation, and other time scales characterizing the processes that lead to the loss of quantum coherence. By estimating these time scales we can determine if ion trap QCs have the necessary preconditions to allow quantum computation to be performed, and which systems are most favorable. Furthermore, certain decoherence mechanisms become more pronounced with larger numbers of qubits, and there are technological limits to the number of qubits that can be held and addressed. Therefore, there are also memory (space) limitations to quantum computation, as well as time limitations, and it will be important to determine how to optimize quantum algorithms to make best use of the available resources.

The various decoherence mechanisms can be separated into two classes: fundamental or technical. The former are limitations imposed by laws of Nature, such as the spontaneous emission of a photon from a qubit level, or the breakdown of the two-level approximation if a qubit transition is driven excessive laser power. The technical limits are those imposed by existing experimental techniques, such as the "heating" of the ions' CM vibrational mode, or the phase stability of the laser driving the qubit transitions. One might expect that these limitations would become less restrictive as technology advances.

It is useful to have benchmarks against which computational capacity can be characterized. We will use two: factoring capacity and error probability per quantum logic gate. The former is algorithm dependent, but illustrative, whereas the latter allows us to contrast the physical systems with the error correction threshold estimates for continuous quantum computation. (However, the threshold numbers have been obtained under assumptions that may not be applicable to trapped ions, e.g. an error probability per gate that is independent of the number of qubits.)

4. Metastable State Qubits

We shall consider a quantum algorithm that requires L qubits (ions), and N laser pulses (we count only the slow, U-pulses), each of duration t (a π-pulse, $\theta = \pi$, for definiteness). Spontaneous emission of just one photon from one of the qubits' $|1\rangle$ states will destroy the quantum coherence required to complete this computation, so we may set an upper limit on the computational time, Nt, in terms of the spontaneous emission lifetime of this level, τ_0. The specific form of the bound depends on the "average" number of qubits that will occupy the $|1\rangle$ state during the computation: we choose this proportion to be $2/3$; giving a bound:

$$Nt < 6\tau_0/L\,. \tag{11}$$

So we see that "more" computation can be performed if the logic gate time, t, can be reduced. The duration, t, of a π-pulse is determined by the intensity, I, of the laser field: $t \sim I^{-1/2}$. However, t, cannot be made arbitrarily small. In an earlier paper we showed that t cannot be smaller than the period of the CM motion, and shorter periods require stronger axial potentials that push the ions closer together. The shortest possible gate time then corresponds to a minimum ion spacing of one wavelength of the interrogating laser light. In this paper we will consider a different mechanism that gives comparable limits: the breakdown of the two level approximation in intense laser fields, first considered in Reference [20].

In addition to the two states comprising each qubit, there are other ionic levels with higher energies than the $|1\rangle$ state that have rapid electric dipole transitions (lifetime τ_{ex}) to the ground state, and so if some population is transferred to such states during computation their rapid decay will destroy quantum coherence. Although the driving laser frequency is far off-resonance (detuning Δ) from the transition frequency between $|0\rangle$ and a higher lying ("extraneous") level, in intense laser fields there will be some probability, P, of occupying this level, given by

$$P \sim \frac{\Omega_{\mathrm{ex}}^2}{8\Delta^2}\,, \tag{12}$$

where Ω_{ex} is the Rabi frequency for the transition from the ground state, $|0\rangle$, to the higher lying, extraneous level. Therefore, the probability of decoherence through this two-level breakdown is proportional to the laser intensity, I. By requiring that the probability of photon emission from a third level should be less than one during the computation, we obtain the following inequality

$$Nt\,\frac{\Omega_{\mathrm{ex}}^2}{8\Delta^2\tau_{\mathrm{ex}}} < 1\,. \tag{13}$$

This inequality sets an upper bound on the laser intensity. From the two inequalities (11) and (13) we obtain the bound

$$NL < \eta \left(\frac{20}{\pi}\right)^{1/2} \left(\frac{\lambda_0}{\lambda_{\mathrm{ex}}}\right)^{3/2} \tau_{\mathrm{ex}}\Delta\,, \tag{14}$$

between an algorithmic quantity (left-hand side) and a physics parameter (right-hand side), where λ_0 is the wavelength of the $|0\rangle - |1\rangle$ transition, and λ_{ex} is the wavelength of the transition from the extraneous level to the $|0\rangle$ state. Using "typical" values of $\tau_{\mathrm{ex}} \sim 10^{-8}$ s and $\Delta \sim 10^{15}$ Hz we see that the value of the right-hand-side of this inequality is $\sim\eta \cdot 10^7$, translating into enough time to perform a very large number ($10^5 - 10^6$) of logic operations on tens of qubits. (The Lamb-Dicke parameter for these ions will be $\sim 0.01 - 0.1$.)

The inequality (14) suggests that longer wavelength qubit transitions allow more computation. Indeed, for specific ions we obtain the bounds:

$$\begin{aligned} &Hg^+: \; NL < \eta \cdot 3 \cdot 10^7 \,, \\ &Sr^+: \; NL < \eta \cdot 7 \cdot 10^7 \,, \\ &Ca^+: \; NL < \eta \cdot 1 \cdot 10^8 \,, \\ &Ba^+: \; NL < \eta \cdot 5 \cdot 10^8 \,, \end{aligned}$$

suggesting that Ba^+ ions may offer greater computational potential than Hg^+ or Ca^+. However, with $L \sim 60$ qubits the bound (14) in Ba^+ corresponds to a computational time $6\tau_0/L \sim 6$ s, whereas technical sources of decoherence such as ion heating and laser phase stability are likely to limit the computation before this limit is reached. Therefore, Ba^+ ions are not likely to offer any significant computational advantage over Ca^+ at present. We note that when translated into an error probability per gate, the above bounds fail to meet the threshold precision that has been suggested for quantum error correction to allow indefinite quantum computation by one to two orders of magnitude [15].

5. Raman Qubits

When qubits are represented by Zeeman or hyperfine sublevels of an ion's ground state, Raman transitions would be used to drive the computational operations, detuned by an amount Δ below some third level (lifetime τ_1). the Rabi frequency for Raman transitions is proportional to the laser field intensity,

$$\Omega \sim I/\Delta \,, \tag{15}$$

as is the decoherence process of spontaneous emission from the third level,

$$P \sim I/\Delta^2 \,. \tag{16}$$

Hence, the probability of a successful computational result is independent of how quickly the computation is performed (at least from the perspective of this decoherence mechanism). Therefore, Raman transitions offer the possibility of completing a computation before technical decoherence mechanisms, such as ion heating, become significant. Using similar arguments as in the last section, we can derive the following inequality for quantum algorithm parameters in terms of the physics parameters for Raman qubits:

$$NL^{1/2} < 8\eta\tau_1\Delta \,. \tag{17}$$

The right-hand side of this inequality has a typical value $\sim \eta \cdot 5 \cdot 10^5$ which is adequate for a large number of gate operations ($\sim 10^6$) on tens of qubits. Also, with the same number of qubits, the error probability per gate is lower for the Raman transitions than with metastable qubits. Therefore, Raman qubits come closer to the error correction thresholds than metastable qubits [15].

6. Quantum Factoring with Trapped Ions

To translate the above physics bounds on algorithmic quantities into limits on the size of integer that could be factored, it is necessary to determine the computational space and time

requirements of quantum factoring. To factor an l-bit integer, N, Shor's factoring algorithm requires a classical integer, x, that shares no factors with N, and the computation of the period of the function [21]

$$f(a) = x^a \bmod N\,, \qquad a = 0,\, 1, \ldots,\, N^2 - 1\,. \tag{18}$$

From the period of this function the order, r, of x can be determined. The order is the smallest integer, r, for which

$$x^r = 1 \bmod N\,. \tag{19}$$

If this order is even, the factors of N are then distributed between the parentheses of congruence

$$(x^{r/2} - 1)\,(x^{r/2} + 1) = 0 \bmod N\,. \tag{20}$$

Therefore, the integers

$$\text{g.c.d.}\,[(x^{r/2} \pm 1),\, N] \tag{21}$$

are factors of N.

Shor's algorithm therefore requires one $2l$-bit register to hold the argument of the function; an l-bit register to hold the function values, and some additional register space to allow reversible computation of the function. (The computation of the Fourier transform to determine the order, r, involves an insignificant number of quantum gate operations in comparison with the computation of the function.)

The amount of scratch space and number of gates is somewhat dependent on the specific implementation of the algorithm [22], but a total number of $(5l + 4)$ qubits and $\sim 96l^3 + \mathrm{O}(l^2)$ U-pulses are required in our recent improved version [23]. The l^3-dependence can be understood as arising from the (conditional) multiplication of $2l$ classical l-bit integers to build the function, f. Each of the multiplications requires $\mathrm{O}(l^2)$ bit-additions (using "elementary school" multiplication) that can be reduced to CNOT and similar elementary gate operations. Using the values

$$L = 5l + 4\,,$$
$$N = 96l^3 + \mathrm{O}(l^3)$$

in the decoherence bounds above, we obtain the factoring limits ($\eta = 0.01$):

$$\mathrm{Hg}^+\text{:}\ l < 5 \text{ bits}\,,$$
$$\mathrm{Sr}^+\text{:}\ \ l < 6 \text{ bits}\,,$$
$$\mathrm{Ca}^+\text{:}\ l < 6 \text{ bits}\,,$$
$$\mathrm{Ba}^+\text{:}\ l < 10 \text{ bits}\,,$$
$$\mathrm{Yb}^+\text{:}\ l < 5 \text{ bits}\,,$$

with metastable qubits. Even larger values may be possible with Raman qubits provided a careful optimization of the parameters is made. These limits correspond roughly to the size of computation at which the probability of success has fallen to $1/e$. Larger integers could be factored but with a lower success probability.

We note that the total computational time with metastable qubits is $\sim 6\tau_0/L$, so that it might be possible to reduce the computation time by using an algorithm with additional

qubits but less gate operations. Such a space-time trade-off could then allow a factoring time that was smaller than the technical decoherence times. We also note that the above limits to integer factoring do not take into account any possible gains from the use of quantum error correction.

7. Computational Bounds and Fundamental Constants

In the estimates made above of the computational capacity of trapped ion OCs we used measured values of atomic parameters for specific ions. It would be of great interest if one could determine an absolute upper bound on the algorithmic quantities that was independent of these details of specific ionic systems. For instance, we could use "typical" values of the relevant parameters in terms of fundamental constants:

$$\text{unit of wavelength} = R_\infty^{-1} = ch^3/2\pi^2 m_e e^4 ,$$
$$\text{unit of electric dipole moment} = ea_0 ,$$
$$\text{unit of electric quadrupole moment} = ea_0^2 ,$$

where h is Planck's constant, e is the unit of electric charge, m_e is the electron mass, and $a_0 = h^2/4\pi^2 m_e e^2$ is the Bohr radius. Using these values we obtain the bounds

$$NL < \frac{8\sqrt{30}}{16\pi^2}\,\eta\alpha^{-3} \tag{22}$$

for metastable qubits, and

$$NL^{1/2} < \eta\alpha^{-3} , \tag{23}$$

for Raman qubits, as first noted by HAROCHE and RAIMOND [24], where $\alpha = e^2/\hbar c \approx 1/137$ is the fine structure constant.

These bounds are considerably more pessimistic than the ones we above, and so do not serve the purpose of providing an absolute upper bound on computational capacity. (One of the reasons that this approach fails is that real ions have much longer lived metastable levels than is suggested by the atomic unit of electric quadrupole moment.)

8. Summary and Conclusions

In this paper we have surveyed the prospects for and limitations to quantum computation with trapped ions. It is apparent that with existing technology adequate time scales and capacity to hold multiple qubits are available to explore quantum computation beyond the current state-of-the-art: a single logic operation involving two qubits. These intrinsic limits (without quantum error correction) only correspond to the factoring of small integers. However, the numbers of qubits and logic operations involved are huge, and the gate precision with Raman qubits is close to the correction thresholds for indefinite computation. Ion traps will therefore be a potent method for exploring whether superpositions and entangled states of large numbers of qubits can be created. Investigations of the type studied here identify the relevant physics issues that must be addressed to achieve computational gains. In particular, we note that there has yet to be a demonstration that more than one ion can be sideband cooled to the vibrational ground state. Furthermore, the heating mechanisms for this vibrational mode are poorly understood [25, 26]. Studies of sideband cooling and re-

heating of multiple ions will therefore be crucial to the development of ion trap QCs. Once entangled states of three or more qubits can be constructed it will also be possible to determine whether multiparticle decoherence mechanisms are consistent with the model that we have used.

Finally, we note that ion trap quantum computation offers many advantages to the recently proposed NMR quantum computation model [27], as summarized in Reference 28. Ion trap qubit coherence is limited by spontaneous emission processes whereas NMR qubit decoherence is thermally dominated ($kT \gg h\nu$). Ion trap quantum information is consequently much more robust. Furthermore, gate times in an ion trap QC could be as short as 1 μs (set by achievable laser intensities, and two-level breakdown), whereas NMR gate times will typically be $\sim 0.1-1$ s (set by the strength of spin-spin interactions and the need to avoid crosstalk with unintended qubits). Readout in an NMR QC is problematic, with an exponential reduction in magnetization signal with additional qubits, whereas ion trap QC readout is a robust process independent of the number of qubits involved. Moreover, an ion trap QC has the advantage that logic operations can be performed between arbitrary qubits in the register, whereas in NMR only nearest-neighbor operations are possible. Therefore, computation in an NMR QC would use much of the available coherence time in moving qubits around the register until they are adjacent to each other. We estimate that a realistic bound to the computation possible in NMR QC is about 10 qubits and 100 logic operations. Of these 100 operations many would be used in a typical computation by moving qubits until they are adjacent. A more detailed comparison of ion trap QCs and NMR will be the subject of a forthcoming paper [29].

Acknowledgements

It is a pleasure to thank W. Warren for helpful discussions. RJH thanks the ISI Foundation, Torino, Italy for hospitality. This research was funded by the National Security Agency.

References

[1] C. H. BENNETT and G. BRASSARD, "Quantum Cryptography: public Key Distribution and Coin Tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore (New York, IEEE, 1984).
[2] R. J. HUGHES et al., *Countemporary Physics* **36**, 149 (1995); R. Hughes et al., *Lecture Notes in Computer Science* **1109**, 329 (1996).
[3] R. P. FEYNMAN, *Found. Phys.* **16**, 507 (1986); and "The Feynman Lecture on Computation", A. J. G. Hey and R. W. Allen eds., (Addison-Wesley, New York, 1996).
[4] S. LLOYD, *Sci. Am.* **273***, 140 (October 1995).*
[5] P. BENIOFF, *Phys. Rev. Lett.* **48**, 1581 (1982).
[6] D. DEUTSCH, *Proc. Roy. Soc.,* **A400**, 97 (1985).
[7] P. W. SHOR, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring", in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, S. Goldwasser ed., (IEEE, Los Alamitos, CA) pp. 124 (1994).
[8] D. SIMON, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, S. Goldwasser ed., (IEEE, Los Alamitos, CA), pp. 124 (1994).
[9] B. SCHNEIER, "Applied Cryptography" (Wiley, New York, 1996).
[10] C. POMERANCE, *Notices of the AMS* **43**, 1473 (1996).
[11] M. GARDNER, *Sci. Am.* **237** (August), 120 (1977).
[12] D. ATKINS et al., Advances in Cryptology – ASIACRYPT '94 pp. 263 (Springer-Verlag, New York, 1994).
[13] J. COWIE et al., Advances in Cryptology – ASIACRYPT '96, pp. 382, K. Kim and T. Matsumoto eds. (Springer, New York, 1996).

[14] J. I. CIRAC and P. ZOLLER, *Phys. Rev. Lett.* **74**, 4094 (1995).
[15] R. J. HUGHES et al., Fortschr. Phys. **46**, 329 (1998). see also http://p23.lanl.gov./Quantum/quantum.html.
[16] D. F. V. JAMES, *Appl. Phys. B* **66**, 181 (1998).
[17] C. MONROE et al., *Phys. Rev. Lett.* **75**, 4714 (1995).
[18] R. J. HUGHES et al., *Phys. Rev. Lett.* **77**, 3240 (1996); D. F. V. James et al., *Proc. SPIE* **3076**, 42 (1997).
[19] J. PRESKILL, "Reliable quantum computers", quant-ph/9705031.
[20] M. B. PLENIO and P. L. KNIGHT, *Phys. Rev.* **A53**, 2986 (1996); "Decoherence limits to quantum computation using trapped ions", quant-ph 9610015.
[21] A. K. EKERT and R. JOSZA, *Rev. Mod. Phys.* **68**, 733–753 (1996).
[22] D. BECKMAN et al., *Phys. Rev.* **A54**, 1034 (1996).
[23] R. J. HUGHES and M. S. NEERGAARD, in preparation.
[24] S. HAROCHE and J.-M. RAIMOND, *Physics Today* (August 1996) 51.
[25] D. J. WINELAND et al., *Phys. Rev.* **A50**, 67 (1994); D. J. WINELAND and H. G. DEHMELT, *J. Appl. Phys.* **46**, 919 (1975).
[26] S. K. LAMOREAUX, "Thermal heating of trapped ions: a quantum perturbation approach", to be published in *Phys. RevA.*
[27] N. A. GERSHENFELD and I. L. CHUANG, *Science* **275**, 350 (1997).
[28] W. S. WARREN, *Science* **277**, 1688 (1997).
[29] R. J. HUGHES, D. F. V. JAMES and S. K. LAMOREAUX, in preparation.