Realistic lower bounds for the factorization time of large numbers on a quantum computer

M. B. Plenio and P. L. Knight
Optics Section, Blackett Laboratory, Imperial College, London SW7 2BZ, England

(Received 14 November 1995)

We investigate the time T a quantum computer requires to factorize a given number dependent on the number of bits L required to represent this number. We stress the fact that in most cases one has to take into account that the execution time of a single quantum gate is related to the decoherence time of the quantum bits (qubits) that are involved in the computation. Although exhibited here only for special systems, this interdependence of decoherence and computation time seems to be a restriction in many current models for quantum computers and leads to the result that the computation time T scales much stronger with L than previously expected.

PACS number(s): 03.65.Bz, 89.70.+c

I. INTRODUCTION

Since Shor's discovery [1,2] of an algorithm that allows the factorization of a large number by a quantum computer in polynomial time instead of an exponential time as in classical computing, interest in the practical realization of a quantum computer has been much enhanced. Recent advances in the preparation and manipulation of single ions as well as the engineering of preselected cavity light fields have made quantum optics that field of physics which promises the first experimental realization of a quantum computer. Several proposals for possible experimental implementations have been made relying on nuclear spins, quantum dots [3], cavity QED [4], and ions in linear traps [5].

One can estimate the time T needed for a single run of Shor's algorithm to be equal to the time $\tau_{\rm el}$ required to execute an elementary logical operation multiplied by the required number of elementary operations, which is of the form $\epsilon L^3+O(L^2)$ [6]. It should be noted that, in general, a single run of Shor's algorithm will not be sufficient because it is a stochastic algorithm. In the following we will discuss the time required to perform one run of Shor's algorithm and if not stated explicitly the calculation time is just the time required for this.

The calculation time has to be compared to the decoherence time $\tau_{\rm dec}$ of the quantum computer (e.g., the time in which on average one photon will be emitted by the quantum computer). As spontaneous emissions destroy the coherence in the quantum computer, we need to make sure that practically no spontaneous emission occurs during the whole computation. To ensure this, the inequality

$$\tau_{\rm dec} \gg T = \tau_{\rm el}\epsilon L^3 \qquad (1)$$

has to be satisfied, which then gives rise to an upper limit for the numbers we are able to factorize on the quantum computer. For a given value of $\tau_{\rm el}$ that means that the total computation time scales like L^3. To factorize a number representable by L quantum bits (qubits), one requires $5L+2$ qubits (in what follows we neglect the 2 here) as work space for the necessary calculations [6]. If we assume that each qubit couples to a different bath, the decoherence time of $5L$ qubits is given by [7,8]

$$\tau_{\rm dec} = \frac{\tau_{\rm QB}}{5L}, \qquad (2)$$

where $\tau_{\rm QB}$ denotes the decoherence time of a single qubit. The case of qubits coupling to the same bath leads to smaller decoherence times $\tau_{\rm dec}$ [8]. Combining Eqs. (1) and (2), we obtain

$$\tau_{\rm QB} \gg \tau_{\rm el} 5\epsilon L^4. \qquad (3)$$

Usually $\tau_{\rm el}$ is not assumed to be related to the decoherence time of the quantum computer. As we will see later, this is not true in general. We will show that the dependence of the elementary time step $\tau_{\rm el}$ on the decoherence time $\tau_{\rm dec}$ gives rise to a much stronger dependence of the calculation time on the bit size L. This results in a severe limitation of the maximum size of the numbers to be factorized. In our investigation we focus on the model put forth by Cirac and Zoller [5], but also show briefly that similar restrictions apply for cavity QED implementations. We stress that the results apply to a wide class of possible models as most of them rely on an atom-light interaction similar to that of the models discussed here. Of course, the actual form of $T(L)$ may vary slightly from model to model.

In Sec. II we investigate the model of a quantum computer proposed by Cirac and Zoller for several possible methods to store the qubits as well as a cavity QED implementation. In Sec. III we summarize our results and discuss their implications to the realizability of quantum computers.

II. QUANTUM COMPUTATION IN A LINEAR ION TRAP

In the Introduction we gave a simple estimate of the time T a quantum computer requires to perform Shor's algorithm. From this it is possible to obtain an upper limit for the numbers that we are able to factorize. However, in this estimate it is usually assumed that the execution time for an elementary logical gate does not depend on the decoherence time of the quantum bits on which the operations are performed. This, however, is not generally true. To see this note that all the proposals for the practical implementation of quantum computers mentioned in the Introduction share a common feature. They rely on the interaction of light with atoms where

1050-2947/96/53(5)/2986(5)/$10.00

either the atoms are used as a memory to store the qubits, which are manipulated by light fields, or the light field is used as the memory, which is manipulated by the interaction with atoms. Therefore in all these schemes the atom-light interaction represents the essential building block of all the proposals made so far. In each of these interactions a temporary excitation of the atoms is inevitable (even in adiabatic excitation, given a finite excitation time), which can lead to spontaneous decay. Obviously the interaction strength, proportional to the Rabi frequency Ω, and the spontaneous emission rate, proportional to the Einstein coefficient of the excited level of the transition in question, are related such that

$$\Omega = \rho \Gamma^{1/2}, \tag{4}$$

where Γ is half the Einstein coefficient of the transition and ρ is a constant of proportionality. Certainly, for a given transition frequency ρ cannot be made arbitrarily large. It is limited due to the fact that at high intensities the two-level approximation breaks down, that the rotating-wave approximation becomes invalid, and that for a sufficiently high laser intensity the atom ionizes practically immediately. For optical transitions the latter effect gives rise to an upper limit of the order of

$$\rho_{\max} \cong 10^{10} s^{1/2}. \tag{5}$$

In practice, the limit will be much lower as both detuning and pulse duration have to be controllable quantities and we have not included the other limitations mentioned above in Eq. (5). As the execution time $\tau_{\rm el}$ of a quantum gate depends inversely on the Rabi frequency Ω while the decoherence time of a qubit $\tau_{\rm QB}$ depends inversely on Γ, we immediately observe via Eq. (4) that both quantities are related to each other.

In the following we will investigate how this relationship affects the estimate for the factorization time of a number that can be represented by L qubits. First we discuss the scheme proposed by Cirac and Zoller because it seems to be the most promising proposal. Later we show that for cavity QED implementations similar problems arise. In similar ways one may achieve estimates for other proposed schemes as they mostly rely on atom-light interaction. The exact form of $T(L)$ might be different, but one will always find that the scaling with L is much stronger than expected from Eq. (1).

A. Linear trap with two-level atoms as qubits

We now discuss the model proposed by Cirac and Zoller [5]. Several ions of mass M are stored in a linear trap (see Fig. 1) and it is assumed that all translational degrees of freedom of the ions are cooled to their respective ground state and that especially the center-of-mass (c.m.) motion with frequency ν is in its ground state. This implies that the Lamb-Dicke regime is reached. To implement quantum gates one then applies a sequence of laser pulses of wavelength λ to the ions such that both the internal degrees of freedom as well as the degree of excitation of the c.m. mode may be changed. As the c.m. mode is a collective motion of all ions, its excitation can be used to yield entanglement between different ions. As an approximation it is assumed that only the c.m. mode is excited because the closest lying mode has a frequency $\sqrt{3}\nu$ and is therefore well separated from the c.m. mode frequency. In the model it is assumed that the laser is detuned such that $\Delta = -\nu$, so that the predominant contribution comes from processes where with the excitation of the ion the c.m. mode is deexcited. Processes where the ion and the mode are excited simultaneously include rapidly oscillating phase factors and are neglected in the following (rotating-wave approximation). One then obtains the following Hamilton operator for an ion at the node of a standing light field [5]:

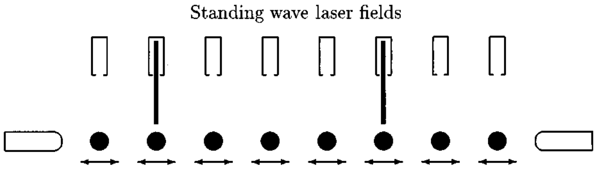

FIG. 1. Schematic picture of the excitation of several ions in a linear ion trap. The translational degrees of freedom of the ions are assumed to be cooled to their respective ground states. To implement quantum gates, standing-wave fields interact with the ions thereby changing the inner state of the ions as well as the state of the center-of-mass mode, which leads to entanglement.

$$H = \frac{\eta}{\sqrt{5L}} \frac{\Omega}{2} [|e\rangle\langle g|a + |g\rangle\langle e|a^{\dagger}], \tag{6}$$

where $\eta = (2\pi/\lambda)\sqrt{\hbar/2M\nu} \ll 1$ is the Lamb-Dicke parameter. The a and $a^{\dagger}$ are the annihilation and creation operators of the c.m. mode. The Hamiltonian Eq. (6) is correct for $(\Omega/2\nu)^2\eta^2 \ll 1$. This system allows the implementation of elementary logical gates such as the controlled-NOT gate [1], which requires in this scheme the equivalent of four π pulses with the Hamiltonian Eq. (6). We use the time required for this as a lower bound for the elementary time step $\tau_{\rm el}$ and find

$$\tau_{\rm el} \cong \frac{4\pi\sqrt{5L}}{\eta\Omega}. \tag{7}$$

Now using the fact that Shor's algorithm requires ϵL^3 elementary steps we find for the total computation time

$$T \cong \frac{4\pi\sqrt{5L}}{\eta\Omega} \epsilon L^3. \tag{8}$$

As we want to minimize T, we insert the maximum value for Ω according to Eq. (4) and obtain

$$T \cong \frac{4\pi\epsilon}{\eta\rho} \sqrt{\frac{5L^7}{\Gamma}}. \tag{9}$$

In this expression not all the parameters are independent, as we have to make sure that T is less than the decoherence time $\tau_{\rm dec}$ of the quantum computer. The decoherence time of the quantum computer is the decoherence time of a single quantum bit $\tau_{\rm QB}$ divided by the number of quantum bits contained in the quantum computer because in the course of the calculation most of the qubits will be partially excited. We find

$$\tau_{\text{dec}} = \frac{\tau_{\text{QB}}}{5L} \cong \frac{1}{5L\Gamma} \tag{10}$$

and obtain the inequality

$$\frac{4\,\pi\epsilon}{\eta\rho}\sqrt{\frac{5L^7}{\Gamma}} \ll \frac{1}{5L\Gamma}. \tag{11}$$

We observe that due to Eq. (4) the decay constant of a single qubit appears on both sides of the equation and we find

$$\frac{\Gamma}{\eta^2} \ll \frac{1}{2000\pi^2}\left(\frac{\rho}{\epsilon}\right)^2 \frac{1}{L^9}, \tag{12}$$

which is far more restrictive than the estimate Eq. (3) obtained when we assume that an elementary time step τ_{el} is independent of τ_{dec}. To be able to perform Shor's algorithm without having spontaneous emissions Eq. (12) has to be satisfied. Using this to eliminate Γ in Eq. (9) then gives a lower bound for the calculation time, which is

$$T \gg 400\pi^2\left(\frac{\epsilon}{\rho\eta}\right)^2 L^8. \tag{13}$$

To obtain explicit values for T we assume $\eta = 0.1$ and $\rho = 10^7\ \text{s}^{-1/2}$. The value of ϵ is of the order of 1000 [6] so that we obtain

L	T_{min} (s)	Γ_{max} (s^{-1})
2	1	10^{-1}
4	259	1.9×10^{-4}

One observes that even with the rather large value of ρ the factorization of a four-bit number (e.g., 15, which is the smallest composite number for which Shor's algorithm applies [2]) seems to be practically impossible when we take into account that, for example, the metastable transition in barium has a lifetime of 45 s and therefore $\Gamma = 0.044\ \text{s}^{-1}$. Note that we have not taken into account the influence of all other possible sources of error such as counterrotating terms in the Hamilton operator, excitations of modes other than the c.m. mode, and errors in the pulse lengths and in the Rabi frequencies of the pulses. One should also realize that although a heroic experimental effort might make the factorization of a four-bit number possible, the factorization of any number of relevant size seems completely out of question as the execution time of Shor's algorithm for a 40 bit number is 10^8 times larger. For a 400-bit number, which represents the upper limit that classical computers can factorize, Shor's algorithm requires 10^{16} times longer than for a four-bit number.

The main problem in the model seems to be that a metastable transition cannot be driven very strongly, which in turn severely limits the execution time of an elementary gate. As a possible way to improve the above model, it was proposed to consider a $j = 1/2 \leftrightarrow j = 1/2$ transition, where the qubit is represented by the two lower levels of the transition [9]. However, in the following we will show that this scheme suffers from similar drawbacks as the previously investigated system.

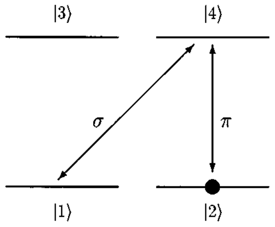

FIG. 2. A $j = 1/2 \leftrightarrow j = 1/2$ transition. The qubit is represented by the two lower levels 1 and 2. Population transfer requires two different lasers. Adiabatic population transfer minimizes unwanted population in the upper level.

B. The $j = 1/2 \leftrightarrow j = 1/2$ transition

The level scheme we now investigate is depicted in Fig. 2. A qubit is represented by the levels 1 and 2, which are assumed to be stable. The transition to the two upper levels, however, may be strong to allow for rapid transitions. As the implementation of quantum gates requires the excitation of one phonon in the c.m. mode, we need to transfer population between the two lower levels with a simultaneous excitation (or deexcitation) of the c.m. mode. To be able to perform this population transfer without appreciable population of the upper levels, which would lead to spontaneous emissions, one has to use the method of adiabatic population transfer [10]. The energy levels shown in Fig. 3 are the most relevant. The vertical axis gives the energy of the bare states $|i;n\rangle$, where i is an atomic level and n is the number of phonons in the c.m. mode. Assume that initially the population is in level $|2;0\rangle$ and we want to transfer it to level $|1;1\rangle$. During the quasiadiabatic population transfer one first applies a σ-polarized laser pulse with a detuning $\Delta = -\nu$; we assume that the ion rests at the node of the light field. The duration of this pulse is a fixed fraction of the total length T_{ad} of the process while the length T_{ad} of the process may be varied. Later, but still overlapping with the σ-polarized laser pulse, a pulse of π-polarized light is applied to the same ion and it is assumed that the ion is situated at the antinode of this field. This pulse, in leading order, preserves the excitation number

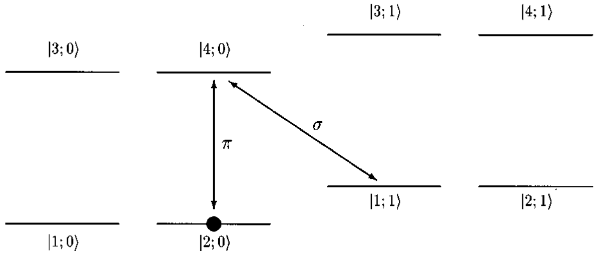

FIG. 3. The $j = 1/2 \leftrightarrow j = 1/2$ transition including the quantized center-of-mass motion. $|i;n\rangle$ denotes an atomic level i and n phonon in the center-of-mass mode. For the implementation of a controlled-NOT gate we need to be able to transfer population from state $|2;0\rangle$ to state $|1;1\rangle$ and vice versa. To minimize population in the excited levels population transfer is performed using adiabatic population transfer with counterintuitive pulse sequence.

of the c.m. mode. Again its length is a certain fraction of the total time T_{ad} and we assume that the σ-polarized laser pulse terminates earlier than the π-polarized pulse. If the time T_{ad} in which this process is performed is sufficiently long then the population in the upper level $|3;0\rangle$ will be small and therefore spontaneous emissions rare. This method certainly has the advantage that the exact pulse shape of the laser is not as important as in the previously discussed scheme. At first glance it also appears to be possible that the population transfer can be made extremely fast as the Rabi frequency is not related to the lifetime of the lower levels. However, there is a limit to the Rabi frequency. To see this we have to realize that an adiabatic process requires infinite time. However, if we want to be able to perform the factorization in finite time we have to take into account small deviations from the adiabatic behavior. In this case some population will end up in the excited levels, which may subsequently lead to spontaneous emissions. We find for the probability p_{em} that at least one spontaneous emission takes place during the quasiadiabatic process

$$p_{\mathrm{em}} \cong \beta\Gamma \frac{5L}{\eta^2\Omega_\sigma^2}\frac{1}{T_{\mathrm{ad}}}, \tag{14}$$

where the constant β depends on the peak value of the Rabi frequency Ω_π of the π-polarized laser, the pulse shapes, and the delay between the pulses. Ω_σ is the peak value of the Rabi frequency of the σ-polarized laser. If Ω_π is larger than $\eta\Omega_\sigma$ and Γ [which we implicitly assume in Eq. (14)] we find for $\sin^4$-pulse shapes $\beta \approx 100$. Analytically as well as numerically one finds that β exhibits a very slow increase with increasing Ω_π. We have assumed that the quasiadiabatic process is sufficiently slow so that the $1/T$ law applies. This is the case when the right-hand side of Eq. (14) is small compared to one. As we do not want to find any spontaneous emission during the whole computation the inequality

$$\frac{\beta}{\eta^2}\frac{\Gamma}{\Omega_\sigma^2}\frac{5\epsilon L^4}{T_{\mathrm{ad}}} = p_{\mathrm{em}}\epsilon L^3 \ll 1 \tag{15}$$

needs to be satisfied. This gives an estimate for the length of an elementary time step τ_{el}, which is

$$\tau_{\mathrm{el}} \approx T_{\mathrm{ad}} \gg \frac{\beta}{\eta^2}\frac{\Gamma}{\Omega_\sigma^2}5\epsilon L^4. \tag{16}$$

Therefore we obtain for the total calculation time the estimate

$$T \gg 5\beta\frac{\epsilon^2}{\eta^2}\frac{\Gamma}{\Omega_\sigma^2}L^7. \tag{17}$$

Again this estimate scales much stronger with the bit size L of the input than expected. To see the orders of magnitude, we give explicit values for T. Assuming $\eta = 0.1$, $\beta = 100$, $\epsilon = 1000$, and $\rho = 10^7\ \mathrm{s}^{-1/2}$ we obtain

L	T_{min} (s)
2	0.05
4	6.5

which indicates that even the factorization of a four-bit number will be extremely difficult to achieve, although the estimate seems to be a little more promising than in the previous scheme. Again we have neglected all other sources of error, such as higher-order contributions in the Lamb-Dicke parameter to the Hamilton operator as well as counterrotating contributions neglected in the rotating-wave approximation. Because the expression Eq. (17) contains the ratio Γ/Ω^2, again we have similar problems as before as this ratio cannot be made arbitrarily small.

C. Cavity QED implementation

Now we would like to show briefly that in cavity QED realizations of quantum computing expressions similar to Eqs. (13) and (17) can be obtained. In cavity QED implementations of quantum gates the atom-light interaction does not involve a classical laser field but a quantized mode of a cavity. Before and after the cavity we may use Ramsey zones to rotate the Bloch vector of the atoms passing the cavity [4]. To perform quantum computations such as Shor's algorithm, many cavities are required and this obviously poses immense experimental difficulties. In the following we neglect the restrictions arising from these problems as well as all difficulties that arise in the realization of exactly one atom passing with a well-defined velocity through the cavity. We will briefly show that again the lower bound for the computation time scales much stronger than L^3 with the bit size L of the number to be factorized. Neglecting decay of the cavity mode, we can estimate that the minimal computation time is of the order of

$$T_{\mathrm{min}} = \frac{\epsilon L^3}{\Omega}, \tag{18}$$

where Ω is the Rabi frequency in the cavity-atom interaction. While traveling in the Ramsey zones and between cavities the atoms may decay. No decay should occur during the quantum computation, which leads to the condition

$$\frac{\alpha\Gamma}{\Omega}\epsilon L^3 \ll 1, \tag{19}$$

where α depends on the ratio between the time the ion spends inside the cavity (where we neglect spontaneous decay) to the time it spends outside the cavity (where it may decay). Using Eq. (4) we then obtain

$$T \gg \frac{\alpha\epsilon^2 L^6}{\rho^2}. \tag{20}$$

Although this estimate seems much more promising than Eqs. (13) and (17), it should be noted that it is certainly an unrealistically low limit because we have neglected major sources of experimental uncertainty mentioned above. We only intend to illustrate that again an expression similar to Eq. (13) and (17) is found, although we have discussed a completely different realization.

These examples show that it seems to be a general feature that the control of population always leads to the appearance of a factor of the form Γ/Ω^2, which, for a given transition frequency, has an upper limit. There seems to be only one way out of this dilemma. Instead of employing optical transitions to represent qubits one could use low-frequency transitions (e.g., microwave transitions), as it was done in the cavity QED implementation of Sleator and Weinfurter [4], because this can considerably decrease the ratio $\Gamma/\Omega^2 = 1/\rho^2$ due to the ω^3 dependence of Γ. However, since in their proposal one would need a tremendous number of cavities it does not seem very promising. To overcome this problem one might use the cavity field in the manner implementation by Cirac and Zoller [5]. Instead of using the c.m. mode to entangle different ions this task could be performed by the cavity mode. This could be done using a linear trap to store the ions inside a microwave cavity. This scheme then resembles that of Sleator and Weinfurter, but differs as we only require one cavity and we do not need atomic beams with all their associated problems. The c.m. mode will not be excited during the calculation as for the long wavelength of the radiation the Lamb-Dicke parameter is extremely small. However, smaller frequencies of the incident fields mean larger wavelengths, which will make it more difficult to address single ions with the microwave radiation. The problem of addressing a single ion, given many are within a wavelength of the incident radiation, may be solved by applying local magnetic or electric fields (or a suitable field gradient) that drive all but one ion out of resonance. However, due to the small spatial separation of the ions this might be difficult to realize experimentally. If it would be possible to implement this idea then the lowest limit for the computation time could become as low as Eq. (20) with a value of ρ that can be much larger than that for an optical transition. However, this idea should serve rather as a basis for discussions than a serious proposal as we still expect the experimental difficulties to be enormous. We are therefore not very optimistic that factorization of nontrivial numbers will be possible in the near future.

III. SUMMARY

In this paper we have investigated how the computation time that a quantum computer needs to factorize an L-bit number depends on several physical parameters. It was shown that T will scale much more strongly with L than previously expected. Instead of an L^3 dependence we find an L^8 or L^7 behavior in the proposal of Cirac and Zoller and L^6 for cavity QED realizations in which, however, this limit is more of theoretical nature than of practical importance due to other experimental problems. In the models that we have investigated explicitly, it also turns out that the computation time is always dependent on the ratio Γ/Ω^2, where Γ and Ω are the decay constant and the Rabi frequency of one of the transitions that are required to transfer population. Although found for special configurations, this seems to be a general result, which limits the length of the elementary time step because the ratio Γ/Ω^2 cannot be made arbitrarily small for an optical transition. As a possible way to circumvent these problems, we briefly discussed the use of microwave transitions to store qubits as in this case the ratio Γ/Ω^2 becomes extremely small. However, practical problems occur that seem to make the experimental realization of this idea difficult, although it might lead at least to the possibility to factorize numbers that are several bits long, a task that seems to be impossible with the present proposals.

Note added in proof. It was brought to our attention, independently by C. Monroe and J. I. Cirac, that Raman pulses have been used in current experiments to transfer population between lower levels in a Λ system. However, an analysis along the lines presented here shows that the conclusions of this paper remain valid with minor modifications.

ACKNOWLEDGMENTS

We would like to thank A. Ekert and A. Barenco for discussions. This work was supported by the Alexander von Humboldt Foundation, the EC Network ''Nonclassical Light,'' and by the United Kingdom Engineering and Physical Sciences Research Council.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos, CA, 1994* (IEEE Computer Society, New York, 1994), p. 124.

[2] A. Ekert and R. Josza, Rev. Mod. Phys. (to be published).

[3] A. Barenco, D. Deutsch, A. Ekert, and R. Josza, Phys. Rev. Lett. **74**, 4083 (1995).

[4] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[5] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[6] V. Vedral, A. Barenco, and A. Ekert (unpublished).

[7] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).

[8] G. M. Palma, K.-A. Suominen, and A. Ekert (unpublished).

[9] P. Zoller, in *Quantum Fluctuations*, Proceedings of the Les Houches Summer School of Theoretical Physics, 1995, edited by S. Reynaud *et al.* (Elsevier, Amsterdam, in press).

[10] B. W. Shore, J. Martin, M. P. Fewell, and K. Bergmann, Phys. Rev. A **52**, 566 (1995); J. Martin, B. W. Shore, and K. Bergmann, *ibid.* **52**, 583 (1995), and references therein.