Universality of entanglement and quantum-computation complexity

Román Orús and José I. Latorre

Departament d'Estructura i Constituents de la Matèria, Universidad Barcelona, 08028, Barcelona, Spain

(Received 14 November 2003; published 12 May 2004)

We study the universality of scaling of entanglement in Shor's factoring algorithm and in adiabatic quantum algorithms across a quantum phase transition for both the *NP*-complete exact cover problem as well as Grover's problem. The analytic result for Shor's algorithm shows a linear scaling of the entropy in terms of the number of qubits, therefore making it hard to generate an efficient classical simulation protocol. A similar result is obtained numerically for the quantum adiabatic evolution exact cover algorithm, which also shows universality of the quantum phase transition near which the system evolves. On the other hand, entanglement in Grover's adiabatic algorithm remains a bounded quantity even at the critical point. The classification of scaling of entanglement appears as a natural grading of the computational complexity of simulating quantum phase transitions.

I. INTRODUCTION

One of the main theoretical challenges in quantum-computation theory is quantum-algorithm design. Some attempts to uncover underlying principles common to all known efficient quantum algorithms have already been explored although no definite and satisfactory answer has been found yet. On the one hand, it has been seen that majorization theory seems to play an important role in the efficiency of quantum algorithms [1–3]. All known efficient quantum algorithms show a step by step majorization of the probability distribution associated to the quantum register in the measurement basis. Therefore, efficient quantum algorithms drive the system toward the final solution by carefully reordering the probability amplitudes in such a way that a majorization arrow is always present. On the other hand, the most relevant ingredient is likely the role entanglement plays in quantum-computational speedup. Regarding this topic, several results have recently been found [4–9] which suggest that entanglement is at the heart of the power of quantum computers.

An important result was obtained by Vidal [8], who proved that large entanglement of the quantum register is a necessary condition for exponential speed-up in quantum computation. To be concrete, a quantum register such that the maximum Schmidt number of any bipartition is bounded at most by a polynomial in the size of the system can be simulated efficiently by classical means. The figure of merit χ proposed in [8] is the maximum Schmidt number of any bipartitioning of the quantum state or, in other words, the maximum rank of the reduced density matrices for any possible splitting. It can be proved that $\chi \geq 2^{E(\rho)}$, where the von Neumann entropy $E(\rho)$ refers to the reduced density matrix of either of the two partitions. If $\chi = O(\text{poly}(n))$ at every step of the computation in a quantum algorithm, then it can be efficiently classically simulated. Exponential speedup over classical computation is possible only if at some step in the computation $\chi \sim \exp(n^a)$, or $E(\rho) \sim n^b$, a and b being positive constants. In order to exponentially accelerate the performance of classical computers, any quantum algorithm

must necessarily create an exponentially large amount of χ at some point.

Another topic of intense research concerns the behavior of entanglement in systems undergoing a quantum phase transition [10]. Quantum correlations in critical systems have been analyzed in many situations and using a wide range of entanglement measurements [9,11–18]. In particular, it has been noted [13,14,16,17] that some of these measurements have important connections to well-known results arising from conformal field theory [19–22]. More generally, when a splitting of a d-dimensional spin system is made, the von Neumann entropy for the reduced density matrix of one of the subsystems $E(\rho) = -\text{tr}(\rho \log_2 \rho)$ at the critical point should display a universal leading scaling behavior determined by the *area* of the region partitioning the whole system. This result depends on the connectivity of the Hamiltonian and applies as is to theories with a Gaussian continuum limit. For example, when separating the system into the interior and the exterior of a sphere of radius R and assuming an ultraviolet cutoff x_0, the entropy of, e.g., the interior is

$$E = c_1 \left(\frac{R}{x_0} \right)^{d-1}, \tag{1}$$

where c_1 corresponds to a known heat-kernel coefficient [21]. In terms of the number of spins present in the system, this leading universal scaling behavior can be written as

$$E \sim n^{(d-1)/d} \tag{2}$$

(which reduces to a logarithmic law for $d=1$). This explicit dependence of entanglement on dimensionality throws additional light on some well-established results from quantum computation.

A similar situation is present in quantum adiabatic algorithms, initially introduced by Farhi *et al.* [23], where the Hamiltonian of the system depends on a control parameter s which in turn has a given time dependence. The Hamiltonians related to adiabatic quantum computation for solving some *NP*-complete problems [such as three-variable satisfi-

69 052308-1

ability (3-SAT) or exact cover] can be directly mapped to interactive nonlocal spin systems, and therefore we can extend the study of entanglement to include this kind of Hamiltonian. This point of view has the additional interest of being directly connected to the possibility of efficient classical simulations of the quantum algorithm, by means of the protocol proposed in Ref. [8].

In this paper we analyze the scaling of the entropy of entanglement in several quantum algorithms. More concretely, we focus on Shor's quantum factoring algorithm [24] and on a quantum algorithm solving by adiabatic evolution the *NP*-complete exact cover problem [25], finding for both of them evidence of a quantum exponential speedup with linear scaling of quantum correlations, which makes difficult the design of an efficient classical simulation. We study furthermore the adiabatic implementation of Grover's quantum search algorithm [26–28], in which entanglement is a bounded quantity even at the critical point, regardless of the size of the system.

We have structured the paper as follows. In Sec. II we analytically address the study of quantum entanglement present in Shor's factoring algorithm. We consider the problem of universal scaling of entanglement at the critical point of an adiabatic quantum algorithm solving the *NP*-complete exact cover problem in Sec. III, where we present numerical results for systems up to 20 qubits. In Sec. IV we focus on the adiabatic implementation of Grover's quantum search algorithm, and derive analytical expressions for the study of entanglement in the system. Finally, in Sec. V we collect the conclusions of our work.

II. SCALING OF ENTANGLEMENT IN SHOR'S FACTORING ALGORITHM

It is believed that the reason why Shor's quantum algorithm for factorization [24] so clearly beats its classical rivals is rooted in the clever use it makes of quantum entanglement. Several attempts have been made to understand the behavior of the quantum correlations present throughout the computation [6,7]. In our case, we will concentrate on the study of the scaling behavior for the entanglement entropy of the system. We shall first remember both Shor's original [24] and the phase-estimation [29] proposals for the factoring algorithm and afterward we shall move to the analytical analysis of their quantum correlations.

A. The factoring algorithm

The interested reader is addressed to [24,29–31] for precise details. Given an odd integer N to factorize, we pick up a random number $a \in [1, N]$. We make the assumption that a and N are co-primes (otherwise the greatest common divisor of a and N would already be a nontrivial factor of N). There exists a smaller integer $r \in [1, N]$, called the *order* of the modular exponentiation $a^x \mod N$, such that $a^r \mod N = 1$. Let us assume that the a we have chosen is such that r is even and $a^{r/2} \mod N \neq -1$, which happens with very high probability [bigger than or equal to $1/(2 \log_2 N)$]. This is the case of interest because then the greatest common divisor of
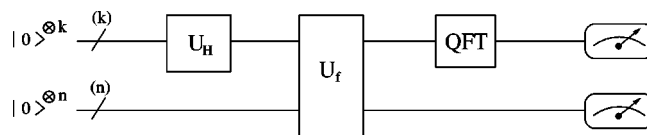

FIG. 1. Quantum circuit for the order-finding algorithm for the modular exponentiation function.

N and $a^{r/2} \pm 1$ is a nontrivial factor of N. Therefore, the factoring problem has been reduced to the order-finding problem of the modular exponentiation function $a^x \mod N$, and it is at this point where quantum mechanics comes into play. The procedure can be cast in two different ways.

1. Shor's proposal for order finding

We make use of two quantum registers: a source register of k qubits (such that $2^k \in [N^2, 2N^2]$) and a target register of $n = \lceil \log_2 N \rceil$ qubits (where the brackets indicated the closest bigger integer). The performance of the quantum algorithm is shown in Fig. 1, where we are making use of the Hadamard gate initially acting over the k qubits of the source, the unitary implementation of the modular exponentiation function

$$U_f|q\rangle|x\rangle = |q\rangle|(x + a^q) \mod N\rangle \tag{3}$$

(where $|q\rangle$ and $|x\rangle$ respectively belong to the source and target registers), and the quantum Fourier transform operator

$$\mathcal{F}|q\rangle = \frac{1}{2^{k/2}} \sum_{m=0}^{2^k-1} e^{2\pi i q m/2^k} |m\rangle. \tag{4}$$

All these operations can be efficiently implemented by means of one- and two-qubit gates. Finally, a suitable classical treatment of the final measurement of this quantum algorithm provides us with r in a few steps, and therefore the prime factorization of N in a time $O((\log_2 N)^3)$.

2. Phase-estimation proposal for order finding

We refer the interested reader to [29] for more details. The quantum circuit is similar to the one shown in the previous section but slightly modified, as is shown in Fig. 2. The unitary operator V_f to which the phase-estimation procedure is applied is defined as

$$V_f|x\rangle = |(a\,x) \mod N\rangle \tag{5}$$

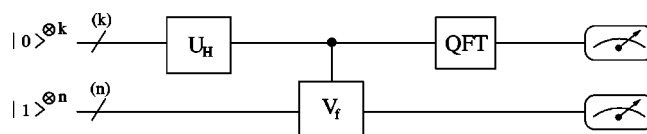[notice the difference between expressions (5) and (3)], being diagonalized by the eigenvectors

FIG. 2. Phase-estimation version of the quantum circuit for the order-finding algorithm. The controlled operation is $\Lambda(V_f)$.

$$|v_s\rangle = \frac{1}{r^{1/2}} \sum_{p=0}^{r-1} e^{-2\pi isp/r} |a^p \bmod N\rangle \qquad (6)$$

such that

$$V_f |v_s\rangle = e^{2\pi is/r} |v_s\rangle, \qquad (7)$$

and satisfying the relation $(1/r^{1/2})\Sigma_{s=0}^{r-1}|v_s\rangle = |1\rangle$. The operator is applied over the target register, being controlled on the qubits of the source in such a way that

$$\Lambda(V_f)|j\rangle|x\rangle = |j\rangle V_f^j |x\rangle, \qquad (8)$$

where by $\Lambda(V_f)$ we understand the full controlled operation acting over the whole system, which can be efficiently implemented in terms of one- and two-qubit gates. As in the previous case, the information provided by a final measurement of the quantum computer enables us to get the factors of N in a time $O((\log_2 N)^3)$.

B. Analytical results

We choose to study the amount of entanglement between the source and the target register in the two proposed quantum circuits, right after the modular exponentiation operation U_f (Fig. 1) or the controlled V_f operation (Fig. 2), and before the quantum Fourier transform in both cases. At this step of the computation, the pure quantum state of the quantum computer is easily seen to be exactly the same for both quantum circuits, and is given by

$$|\psi\rangle = \frac{1}{2^{k/2}} \sum_{q=0}^{2^k-1} |q\rangle |a^q \bmod N\rangle, \qquad (9)$$

and therefore the density matrix of the whole system is

$$|\psi\rangle\langle\psi| = \frac{1}{2^k} \sum_{q,q'=0}^{2^k-1} (|q\rangle\langle q'|)(|a^q \bmod N\rangle\langle a^{q'} \bmod N|). \qquad (10)$$

Tracing out the quantum bits corresponding to the source, we get the density matrix of the target register, which reads

$$\rho_{\text{target}} = \text{tr}_{\text{source}}(|\psi\rangle\langle\psi|)$$
$$= \frac{1}{2^k} \sum_{p,q,q'=0}^{2^k-1} (\langle p|q\rangle\langle q'|p\rangle)(|a^q \bmod N\rangle\langle a^{q'} \bmod N|), \qquad (11)$$

that is,

$$\rho_{\text{target}} = \frac{1}{2^k} \sum_{p=0}^{2^k-1} |a^p \bmod N\rangle\langle a^p \bmod N|$$
$$\sim \frac{1}{r} \sum_{p=0}^{r-1} |a^p \bmod N\rangle\langle a^p \bmod N|. \qquad (12)$$

The last step comes from the fact that $a^r \bmod N = 1$, where $r \in [1,N]$ is the order of the modular exponentiation. If 2^k were a multiple of r there would not be any approximation

and the last equation would be exact. This is not necessarily the case, but the corrections to this expression vary as $O(1/2^k)$, thus being exponentially small in the size of the system.

It follows from expression (12) that the rank of the reduced density matrix of the target register at this point of the computation is

$$\text{rank}(\rho_{\text{target}}) = r. \qquad (13)$$

Because $r \in [1,N]$, this rank is usually $O(N)$. If this were not the case, for example, if r were $O(\log_2 N)$, then the order-finding problem could be efficiently solved by a classical naive algorithm and it would not be considered as classically hard. Because N is exponentially big in the number of qubits, we have found a particular bipartition of the system (namely, the bipartition between the source register and the target register) and a step in the quantum algorithm in which the entanglement, as measured by the rank of the reduced density matrix of one of the subsystems, is exponentially big. This implies in turn that Shor's quantum factoring algorithm cannot be efficiently classically simulated by any protocol in Ref. [8], owing to the fact that at this step $\chi = O(N)$, therefore constituting an inherent exponential quantum speedup based on an exponentially big amount of entanglement. It is worth noticing that the purpose of the entanglement between the two registers consists in leaving the source in the right periodic state to be processed by the quantum Fourier transform. Measuring the register right after the entangling gate disentangles the two registers while leaving the source in a periodic state, and this effect can be accomplished only by previously entangling the source and target. These conclusions apply both to Shor's original proposal (circuit of Fig. 1) and to the phase-estimation version (circuit of Fig. 2).

The behavior of the rank of the system involves the fact that the entropy of entanglement of the reduced density matrix at this point will mainly scale linearly with the number of qubits, $E \sim \log_2 r \sim \log_2 N \sim n$, which is the hardest of all the possible scaling laws. We will again find this strong behavior for the entropy in Sec. III.

III. SCALING OF ENTANGLEMENT IN AN *NP*-COMPLETE PROBLEM

We now turn to analyzing how entanglement scales for a quantum algorithm based on adiabatic evolution [23], designed to solve the *NP*-complete exact cover problem [25]. We first briefly review the proposal and then we consider the study of the properties of the system, in particular the behavior of the entanglement entropy for a given bipartition of the ground state.

A. Adiabatic quantum computation

The adiabatic model of quantum computation deals with the problem of finding the ground state of a given system represented by its Hamiltonian. Many relevant computational problems (such as 3-SAT) can be mapped to this situation.
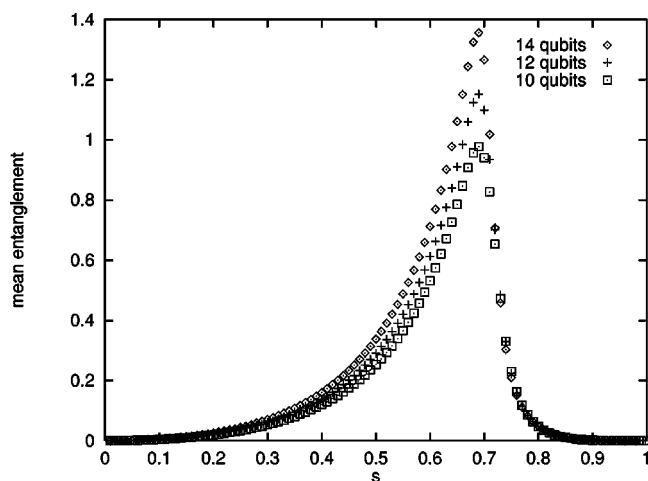
FIG. 3. Evolution of the entanglement entropy between the two blocks of size $n/2$ when a bipartition of the system is made, on average over 300 different instances with one satisfying assignment. A peak in the correlations appears for $s_c \sim 0.7$ in the three cases.
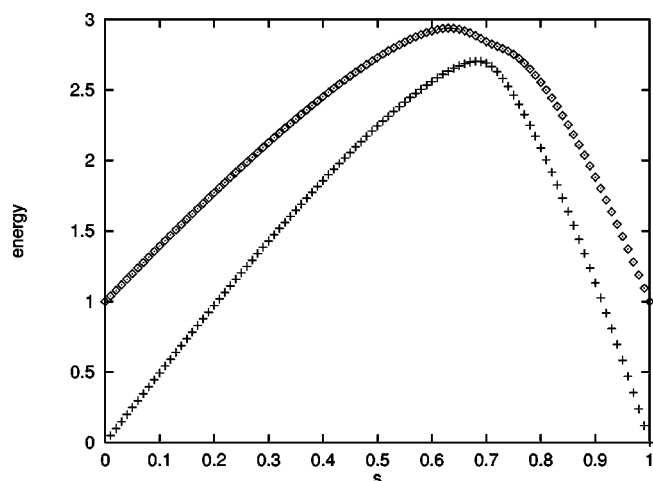

FIG. 4. Energies of the ground state and first excited state for a typical instance with one satisfying assignment of exact cover in the case of ten qubits (in dimensionless units). The energy gap approaches its minimum at $s_c \sim 0.7$.

The method is briefly summarized as follows. We start from a time-dependent Hamiltonian of the form

$$H(s(t)) = [1 - s(t)]H_0 + s(t)H_p, \qquad (14)$$

where H_0 and H_p are the initial and problem Hamiltonians, respectively, and $s(t)$ is a time-dependent function satisfying the boundary conditions $s(0)=0$ and $s(T)=1$ for a given T. The desired solution to a certain problem is codified in the ground state of H_p. The gap between the ground and the first excited states of the instantaneous Hamiltonian at time t will be called $g(t)$. Let us define $g_{\min}$ as the global minimum of $g(t)$ for t in the interval $[0, T]$. If at time T the ground state is given by the state $|E_0; T\rangle$, the adiabatic theorem states that if we prepare the system in its ground state at $t=0$ (which is assumed to be easy to prepare) and let it evolve under this Hamiltonian, then

$$|\langle E_0; T | \psi(T) \rangle|^2 \geq 1 - \epsilon^2, \qquad (15)$$

provided that

$$\frac{\max|dH_{1,0}/dt|}{g_{\min}^2} \leq \epsilon, \qquad (16)$$

where $H_{1,0}$ is the Hamiltonian matrix element between the ground and first excited states, $\epsilon \ll 1$, and the maximization is taken over the whole time interval $[0, T]$. Because the problem Hamiltonian codifies the solution to the problem in its ground state, we get the desired solution with high probability after a time T. A closer look at the adiabatic theorem tells us that T dramatically depends on the scaling of the inverse of $g_{\min}^2$ with the size of the system. More concretely, if the gap is only polynomially small in the number of qubits, that is to say, it scales as $O(1/\text{poly}(n))$, the computational

time is $O(\text{poly}(n))$, whereas if the gap is exponentially small $[O(2^{-n})]$ the algorithm takes an exponentially large time to reach the solution.

The explicit functional dependence of the parameter $s(t)$ on time can be very diverse. The point of view we adopt in the present paper is such that this time dependence is not taken into account, as we study the properties of the system as a function of s, which will be understood as the Hamiltonian parameter. We will in particular analyze the entanglement properties of the ground state of $H(s)$, as adiabatic quantum computation assumes that the quantum state always remains close to the instantaneous ground state of the Hamiltonian throughout the computation. Note that we are dealing with a system which is suitable to undergo a quantum phase transition at some critical value of the Hamiltonian parameter, and therefore we expect to achieve the biggest quantum correlations at this point. The question is how these big quantum correlations scale with the size of the system when dealing with interesting problems. This is the starting point for the next two sections.

B. Exact cover

The *NP*-complete exact cover problem is a particular case of the 3-SAT problem, and is defined as follows. Given the n Boolean variables $\{x_i\}_{i=1,\dots,n}$, $x_i=0, 1 \; \forall \; i$, where i is regarded as the bit index, we define a *clause* of the exact cover involving the three qubits i, j, and k (say, clause C) by the equation $x_i + x_j + x_k = 1$. There are only three assignments of the set of variables $\{x_i, x_j, x_k\}$ that satisfy this equation, namely, $\{1,0,0\}$, $\{0,1,0\}$, and $\{0,0,1\}$. The clause can be more specifically expressed in terms of a Boolean function in conjunctive normal form (CNF) as

$$\phi_C(x_i, x_j, x_k) = (x_i \vee x_j \vee x_k) \wedge (\neg x_i \vee \neg x_j \vee \neg x_k) \wedge (\neg x_i \vee \neg x_j \vee x_k) \wedge (\neg x_i \vee x_j \vee \neg x_k) \wedge (x_i \vee \neg x_j \vee \neg x_k), \qquad (17)$$

so $\phi_C(x_i, x_j, x_k) = 1$ as long as the clause is properly satisfied. An *instance* of exact cover is a collection of clauses which involves different groups of three qubits. The problem is to find a string of bits $\{x_1, x_2, \ldots, x_n\}$ that satisfies all the clauses.

This problem can be mapped into finding the ground state of a Hamiltonian H_p in the following way. Given a clause C, define the Hamiltonian associated with this clause as

$$H_C = \frac{1}{2}(1 + \sigma_i^z)\frac{1}{2}(1 + \sigma_j^z)\frac{1}{2}(1 + \sigma_k^z)$$
$$+ \frac{1}{2}(1 - \sigma_i^z)\frac{1}{2}(1 - \sigma_j^z)\frac{1}{2}(1 - \sigma_k^z)$$
$$+ \frac{1}{2}(1 - \sigma_i^z)\frac{1}{2}(1 - \sigma_j^z)\frac{1}{2}(1 + \sigma_k^z)$$
$$+ \frac{1}{2}(1 - \sigma_i^z)\frac{1}{2}(1 + \sigma_j^z)\frac{1}{2}(1 - \sigma_k^z)$$
$$+ \frac{1}{2}(1 + \sigma_i^z)\frac{1}{2}(1 - \sigma_j^z)\frac{1}{2}(1 - \sigma_k^z), \quad (18)$$

where we have defined $\sigma^z|0\rangle = |0\rangle$, $\sigma^z|1\rangle = -|1\rangle$. Note the parallelism between Eqs. (17) and (18). The quantum states of the computational basis that are eigenstates of H_C with zero eigenvalue (ground states) are the ones that correspond to the bit string which satisfies C, whereas the remainder of the computational states are penalized with an energy equal to 1. Now we construct the problem Hamiltonian as the sum of all the Hamiltonians corresponding to all the clauses in our particular instance, that is to say,

$$H_p = \sum_{C \in \text{instance}} H_C, \quad (19)$$

so the ground state of this Hamiltonian corresponds to the quantum state whose bit string satisfies *all* the clauses. We have reduced the original problem stated in terms of Boolean logic to the hard task of finding the ground state of a two- and three-body interactive spin Hamiltonian with local magnetic fields. Observe that the couplings depend on the particular instance we are dealing with, and that the spin system has neither an *a priori* well-defined dimensionality nor a well-defined lattice topology, in contrast with some more usual simple spin models.

We now define our s-dependent Hamiltonian $H(s)$ as a linear interpolation between an initial Hamiltonian H_0 and H_p:

$$H(s) = (1 - s)H_0 + sH_p, \quad (20)$$

where we take the initial Hamiltonian H_0 to be basically a magnetic field in the x direction; more concretely,

$$H_0 = \sum_{i=1}^{n} \frac{d_i}{2}(1 - \sigma_i^x), \quad (21)$$

where d_i is the number of clauses in which qubit i appears, and $\sigma^x|+\rangle = |+\rangle$, with $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$, so the ground state of H_0 is an equal superposition of all the possible

computational states. Observe that $H(s)$ is, apart from a constant factor, a sum of terms involving local magnetic fields in the x and z directions, together with two- and three-body interaction coupling terms in the z component. This system is suitable to undergo a quantum phase transition (in the limit of infinite n) as s is shifted from 0 to 1. The study of this phenomenon is the aim of the following section.

C. Numerical results up to 20 qubits

We have randomly generated instances for exact cover with only one possible satisfying assignment and have constructed the corresponding problem Hamiltonians. Instances are produced by adding clauses at random until there is exactly one satisfying assignment, starting over if we end up with no satisfying assignments. According to [25], these are believed to be the most difficult instances for the adiabatic algorithm. Our analysis proceeds as follows.

1. Appearance of a quantum phase transition

We have generated 300 exact cover instances (300 random Hamiltonians with a nondegenerate ground state) and have calculated the ground state for 10, 12, and 14 qubits for different values of the parameter s in steps of 0.01. We then consider a particular bipartition of the system into two blocks of $n/2$ qubits, namely, the first $n/2$ qubits versus the rest, and have calculated the entanglement entropy between the two blocks. For each of the randomly generated Hamiltonians we observe a peak in the entanglement entropy around a critical value of the parameter $s_c \sim 0.7$. We have averaged the curves obtained over the 300 instances and have obtained the plot from Fig. 3.

The point at which the entropy of entanglement reaches its maximum value is identified as the one corresponding to the critical point of a quantum phase transition in the system (in the limit of infinite size). This interpretation is reinforced by the observation of the typical energy eigenvalues of the system. For a typical instance of ten qubits we observe that the energy gap between the ground state and the first excited state reaches a minimum precisely for a value of the parameter $s_c \sim 0.7$ (see Fig. 4).

We observe from Fig. 3 that the peak in the entropy is highly asymmetric with respect to the parameter s. A detailed study of the way this peak diverges near the critical region seems to indicate that the growth of entanglement is slower at the beginning of the evolution and fits remarkably well a curve of the type $E \sim \log|\log(s - s_c)|$, whereas the decrease of the peak is better parametrized by a power law $E \sim |s - s_c|^{-\alpha}$ with $\alpha \sim 2.3$, α being a certain critical exponent. These laws governing the critical region fit the data better and better as the number of qubits is increased.

2. Analysis of different bipartitions of the system

Explicit numerical analysis for ten qubits tells us that all possible bipartitions for each one of the instances produce entropies at the critical point of the same order of magnitude—as expected from the nonlocality of the interac-
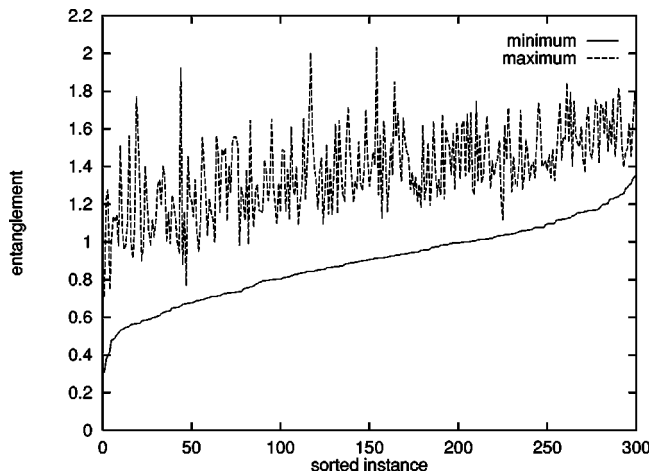
FIG. 5. Minimum and maximum entropy over all possible bipartitions of a ten-qubit system for each of the 300 randomly generated instances of exact cover. Instances are sorted such that the minimum entanglement increases monotonically.

tions. This is represented in Fig. 5, where we plot the minimum and maximum entanglement obtained from all the possible partitions of the system for each one of the generated instances (points are sorted such that the minimum entropy monotonically increases).

Similar conclusions derive from the data plotted in Fig. 6, where we have considered the same quantities again but looking at 64 partitions of the ground state for 10 different instances of 16 qubits. According to these results we restrict ourselves in what follows to the analysis of a particular bipartition of the system, namely, the first $n/2$ qubits versus the rest.

It is worth emphasizing that the existence of a single partition with exponentially large entanglement makes the algorithm not amenable to classical simulation. The above result is stronger and shows that essentially all partitions are highly entangled. The system is definitely hard to simulate by classical means.
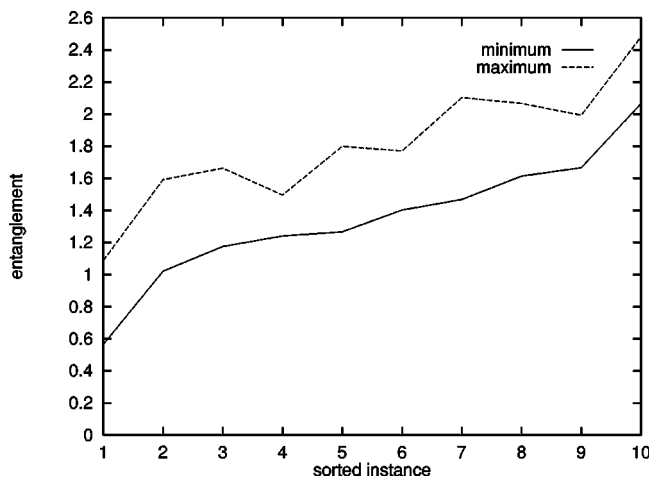

FIG. 6. Minimum and maximum entropy over 64 bipartitions of a 16-qubit system for ten randomly generated instances of exact cover. Instances are sorted such that the minimum entanglement increases monotonically.
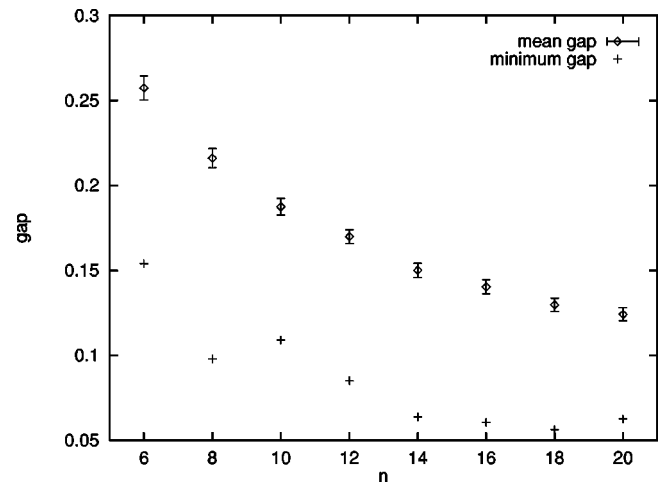

FIG. 7. Scaling of the minimum energy gap (in dimensionless units) with the size of the system, both in the worst case and in the mean case over all the randomly generated instances. Error bars give 95% confidence level for the mean.

3. Scaling laws for the minimum energy gap and the entanglement entropy

To characterize the finite-size behavior of the quantum phase transition, we have generated 300 random instances of exact cover with only one satisfying assignment from six to 20 qubits, and studied the maximum von Neumann entropy for a bipartition of the system as well as the minimum gap, both in the worst case and in the mean case over all the randomly generated instances. We must point out that the scaling laws found in this section are limited to the small systems we can handle with our computers. Increasing the number of qubits may lead to corrections in the numerical results, which would be of particular importance for a more precise time-complexity analysis of the adiabatic algorithm. Figure 7 represents the behavior of the gap in the worst and mean cases. From Fig. 8 it is noticed that the gap seems to
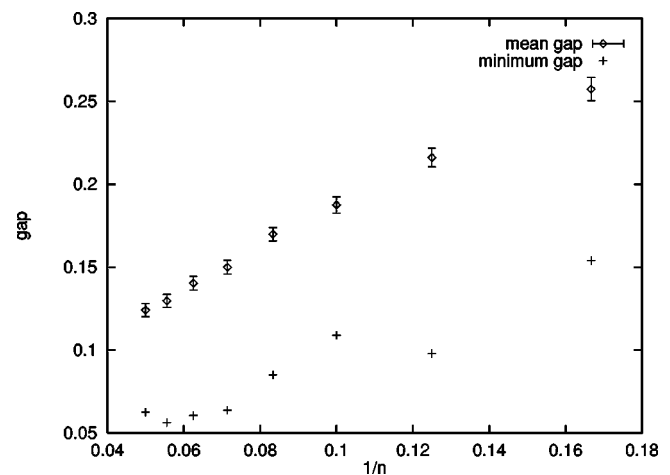

FIG. 8. Minimum energy gap (in dimensionless units) versus the inverse size of the system, both in the worst case and in the mean case over all the randomly generated instances. Error bars give 95% confidence level for the mean. The behavior is apparently linear.
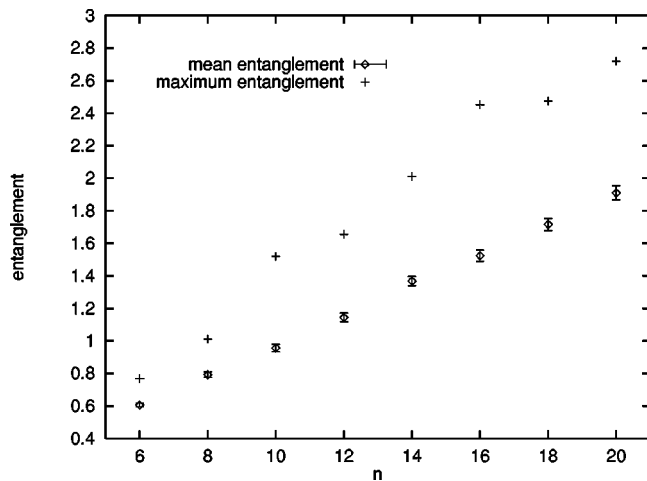
FIG. 9. Scaling of the entanglement entropy for an equally sized bipartition of the system, both in the worst case and in the mean case over all the randomly generated instances. Error bars give 95% confidence level for the mean. The data are consistent with a linear scaling.

obey a scaling law of the style $O(1/n)$, n being the number of qubits, which would assure a polynomial-time quantum computation. This law is in agreement with the results in [25] and in concordance with the idea that the energy gap typically vanishes as the inverse of the volume in condensed matter systems (here the volume is the number of qubits). Error bars in the two plots give the 95% confidence level in the numerically calculated mean.

We have considered as well the scaling behavior of the entanglement entropy for an equally sized bipartition of the system, also in the worst and in the mean cases. The data obtained from our simulations are plotted in Fig. 9, where the error bars give the 95% confidence level in the mean, and seem to be in agreement with a strongly linear scaling of entanglement as a function of the size of the number of qubits. More concretely, a numerical linear fit for the mean entanglement entropy gives us the law $E \sim 0.1n$. Observe that the entropy of entanglement does not become saturated at its maximum allowed value (which would be $E = n/2$ for n qubits), so we can say that only 20% of all the possible potential available entanglement appears in the quantum algorithm. Linearity in the scaling law would imply that this quantum computation by adiabatic evolution, after a suitable discretization of the continuous time dependence, could not be classically simulated by the protocol of Ref. [8]. Given that the scaling of the gap seems to indicate that the quantum computation runs for a time polynomial in the size of the system, our conclusion is that apparently we are confronted with an exponentially fast quantum computation that seems extremely difficult (if not impossible) to simulate efficiently by classical means. This could be an inherent quantum mechanical exponential speedup that can be understood in terms of the linear scaling of the entropy of entanglement. Note also the parallelism with the behavior of the entanglement found in Shor's algorithm in Sec. II. As a remark, our numerical analysis shows that the quantum algorithm is difficult to simulate classically in an efficient way, which does

not necessarily imply that the quantum computer runs exponentially faster than the classical one, as our time-complexity analysis is limited to 20 qubits.

The linear behavior for the entropy with respect to the size of the system could in principle be expected according to the following qualitative reasoning. Naively, the entropy was expected to scale as the area of the boundary of the splitting, according to some considerations taken from conformal field theory (see [13,14,19–21]). This area law is in some sense natural: because the entropy value is the same for both density matrices arising from the two subsystems, it can only be a function of their shared properties, and these are geometrically encoded in the area of the common boundary. For a system of n qubits, this implies a scaling law for the entropy like $E \sim n^{(d-1)/d}$ (which reduces to a logarithm for $d=1$). Our system does not have a well-defined dimensionality, but, owing to the fact that there are many random two- and three-body interactions, the effective (fractal) dimensionality of the system should be very large. Therefore, we expect a linear (or almost linear) scaling, which is what we obtained numerically. The data seem to indicate that such an effective dimensionality is around $d \sim n$, thus diverging as n goes to infinity.

It is possible to compare our apparently linear scaling of the mean entropy of entanglement with the known results obtained by averaging this quantity over the entire manifold of n-qubit pure states, with respect to the natural Fubini-Study measure. According to the results conjectured by Page [32] and later proved in [33], the average entropy for an equally sized bipartition of a random n-qubit pure state in the large n limit can be approximated by $E \sim (n/2) - 1/(2 \ln 2)$ (in our notation), therefore also displaying a linear scaling law (but different from ours). In fact, this is an indicator that most of the n-qubit pure states are highly entangled, and that adiabatic quantum computation naturally brings the system close to these highly entangled regions of the pure state manifold (more information about the average entanglement of an n-qubit system can be found in [34]).

4. The entanglement-gap plane

The plots in Fig. 10 and Fig. 11 show the behavior of the peak in the entanglement versus the gap, both again in the average and in the worst case for all the generated instances. Clearly, as the gap becomes smaller the production of entanglement in the algorithm increases. A compression of the energy levels correlates with high quantum correlations in the system.

5. Convergence of the critical points

The critical point s_c seems to be bounded by the values of s associated with the minimum gap and with the maximum entropy. Actually, the critical point corresponding to the minimum size of the energy gap is systematically slightly bigger than the critical point corresponding to the peak in the entropy. On increasing the size of the system, these two points converge toward the same value, which would correspond to the true critical point of a system of infinite size. This effect is neatly observed in Fig. 12, which displays the
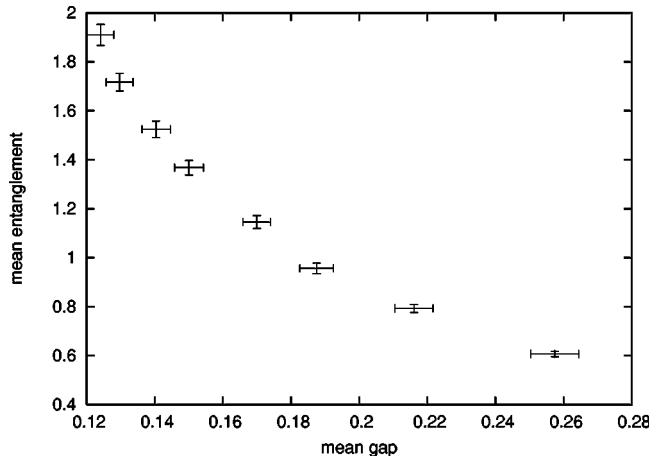
FIG. 10. Mean entropy of entanglement versus mean size of the energy gap (in dimensionless units). Error bars give 95% confidence level for the means. Each point corresponds to a fixed number of qubits.

values of s associated with the mean critical points both for the gap and for the entropy as a function of n.

6. Universality

All the above results suggest that the system comes close to a quantum phase transition. The characterization we have presented based on the study of averages over instances reconstructs its universal behavior. The results do not depend on particular microscopic details of the Hamiltonian, such as the interactions shared by the spins or the strength of local magnetic fields. Any adiabatic algorithm solving a k-SAT problem and built in the same way we have done for exact cover should display on average exactly the same properties we have found regardless of the value of k, which follows from universality (the case $k=2$, though not being *NP* complete [37], should also display this property as its Hamiltonian would also consist of local interactions in a high-dimensional lattice; $k=1$ is a particular case, as its

FIG. 12. Mean critical point for the energy gap and for the entropy. Error bars give 95% confidence level for the means. Note that they tend to approach as the size of the system is increased.

Hamiltonian is noninteracting). Linear scaling of entanglement should therefore be a universal law for these kinds of quantum algorithms. The specific coefficients of the scaling law for the entropy should be a function only of the connectivity of the system, that is, of the type of clauses defining the instances.

We have explicitly checked this assertion by numerical simulations for clauses of exact cover but involving four qubits ($x_i+x_j+x_k+x_l=1$), which is a particular case of 4-SAT. In Fig. 13 we plot the behavior of the entropy of entanglement for a ten-qubit system for these types of clauses and compare it to the same quantity calculated previously for the clauses involving three qubits (the usual exact cover Hamiltonian). We observe again the appearance of a peak in the entropy, which means that the system is evolving close to a quantum phase transition.

Figures 14 and 15, respectively, show the scaling of the energy gap in the mean and worst cases and the scaling of
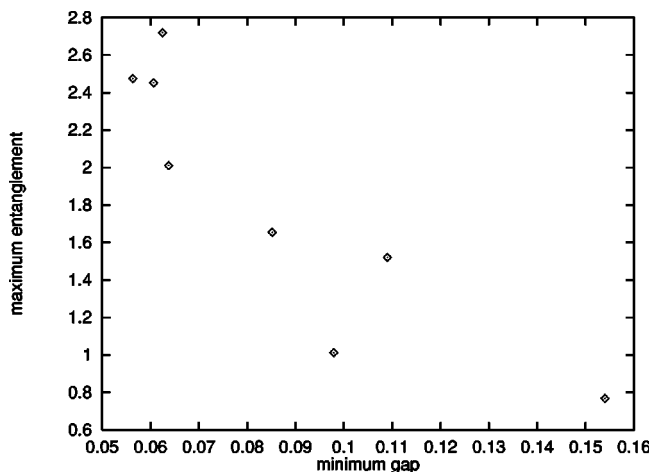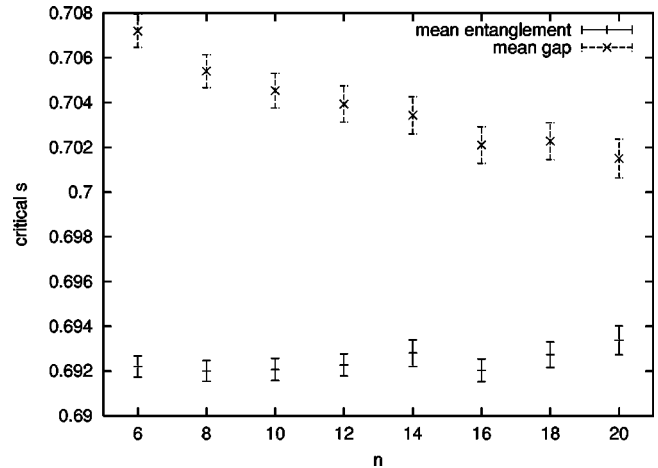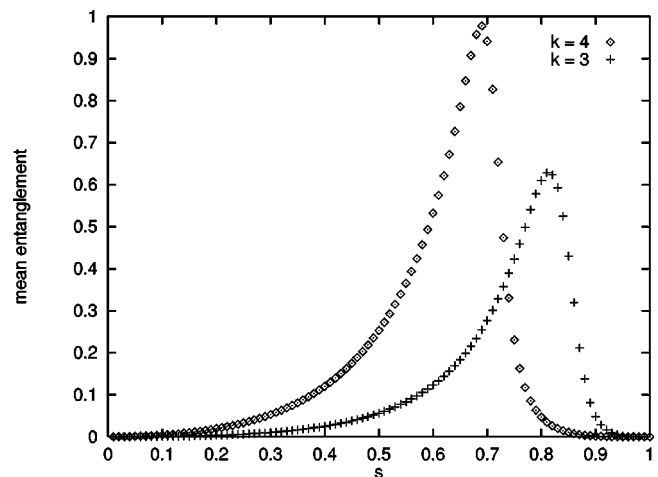

FIG. 11. Maximum entropy of entanglement versus minimum size of the energy gap (in dimensionless units). Each point corresponds to a fixed number of qubits.

FIG. 13. Entanglement as a function of the Hamiltonian parameter for clauses of exact cover involving three ($k=3$) and four ($k=4$) qubits, for a ten-qubit system, averaged over all the randomly generated instances.
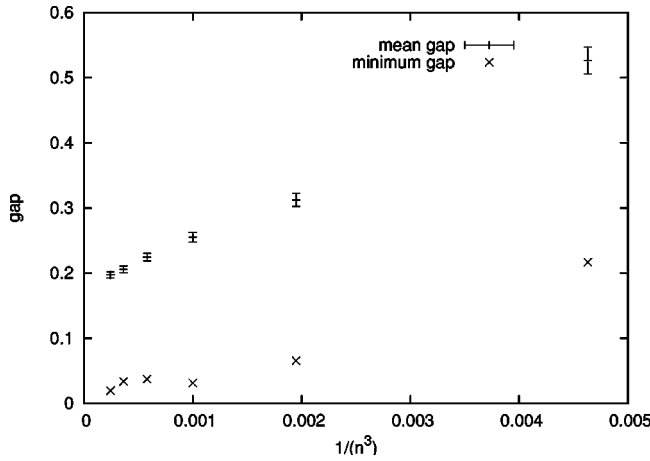
FIG. 14. Minimum energy gap (in dimensionless units) versus $1/(n^3)$, both in the worst and in the mean cases over all the randomly generated instances of clauses involving four qubits, up to $n=16$. Error bars give 95% confidence level for the mean. The behavior seems to be linear.

the peak in the entropy in the mean and worst cases as well, up to 16 qubits. Error bars again give 95% confidence levels for the means. The behavior is similar to the one already found for the instances of exact cover involving three qubits (Figs. 8 and 9), which supports the idea of the universality of the results. The minimum energy gap seems to scale in this case as $\sim 1/n^3$ (n being the number of qubits), which would again guarantee a polynomial-time quantum adiabatic evolution.

IV. SCALING OF ENTANGLEMENT IN ADIABATIC GROVER'S ALGORITHM

Let us now consider the adiabatic implementation of Grover's quantum searching algorithm in terms of a Hamil-
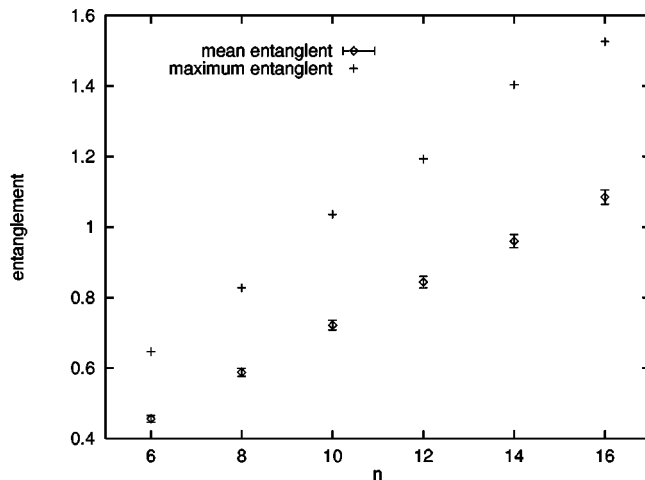

FIG. 15. Scaling of the entanglement entropy for an equally sized bipartition of the system, both in the worst and in the mean cases over all the randomly generated instances of clauses involving four qubits, up to $n=16$. Error bars give 95% confidence level for the mean. The data are consistent with a linear scaling.

tonian evolution [26–28] and study its properties as a function of the number of qubits and the parameter s. For this problem, it is possible to compute all the results analytically, so we shall get a closed expression for the scaling of entanglement. As a side remark, it is worth noting that the treatment in [8] is not valid for oracular problems as it is assumed that all quantum gates are known in advanced. Independently of this issue, we shall see that the system remains little entangled between calls to the oracle.

A. Implementation of Grover's searching algorithm with adiabatic quantum computation

Grover's searching algorithm [26] can be implemented in adiabatic quantum computation by means of the s-dependent Hamiltonian

$$H(s) = (1-s)(I - |s\rangle\langle s|) + s(I - |x_0\rangle\langle x_0|), \qquad (22)$$

where $|s\rangle \equiv (1/2^{n/2})\Sigma_{x=0}^{2^n-1}|x\rangle$, n is the number of qubits, and $|x_0\rangle$ is the marked state. The computation takes the quantum state from an equal superposition of all computational states directly to the state $|x_0\rangle$, as long as the evolution remains adiabatic. The time the algorithm takes to succeed depends on how we choose the parametrization of s in terms of time. Our aim is to compute the amount of entanglement present in the register, and we need not deal with the explicit dependence of the parameter s on time and its consequences (see [27,28] for further information about this topic).

It is straightforward to check that the Hamiltonian (22) has its minimum gap between the ground and first excited states at $s=0.5$, which goes to zero exponentially fast as the number of qubits in the system is increased. Therefore, this Hamiltonian apparently undergoes a quantum phase transition in the limit of infinite size at $s=0.5$. Quantum correlations approach their maximum for this value of s (for more on Grover's problem as a quantum phase transition, see [35]).

B. Analytical results

It can be seen (see, for example, [36]) that the ground state energy of the Hamiltonian given in Eq. (22) corresponds to the expression

$$E_-(s) = \frac{1}{2}\left(1 - \sqrt{(1-2s)^2 + \frac{4}{2^n}s(1-s)}\right), \qquad (23)$$

where s is the Hamiltonian parameter. The corresponding normalized ground state eigenvector is given by

$$|E_-(s)\rangle = a|x_0\rangle + b\sum_{x\neq x_0}|x\rangle, \qquad (24)$$

where we have defined the quantities

$$a \equiv \alpha b,$$

$$b^2 \equiv \frac{1}{2^n - 1 + \alpha^2},$$

$$\alpha \equiv \frac{2^n - 1}{2^n - 1 - [2^n/(1-s)]E_-(s)}. \tag{25}$$

In all the forthcoming analysis we will assume that the marked state corresponds to $|x_0\rangle = |0\rangle$, which will not alter our results. The corresponding density matrix for the ground state of the whole system of n qubits is then given by

$$\rho_n = b^2(\alpha^2 - 2\alpha + 1)|0\rangle\langle 0| + b^2|\phi\rangle\langle\phi| + b^2(\alpha - 1)(|\phi\rangle\langle 0| + |0\rangle \times \langle\phi|), \tag{26}$$

where we have defined $|\phi\rangle$ as the the unnormalized sum of all the computational quantum states (including the marked one), $|\phi\rangle \equiv \Sigma_{x=0}^{2^n-1}|x\rangle$. Taking the partial trace over half the qubits, regardless of which $n/2$ qubits we choose, we find the reduced density matrix

$$\rho_{n/2} = b^2(\alpha^2 - 2\alpha + 1)|0'\rangle\langle 0'| + 2^{n/2}b^2|\phi'\rangle\langle\phi'| + b^2(\alpha - 1)(|\phi'\rangle\langle 0'| + |0'\rangle\langle\phi'|), \tag{27}$$

where we understand that $|0'\rangle$ is the remaining marked state for the subsystem of $n/2$ qubits and $|\phi'\rangle \equiv \Sigma_{x=0}^{2^{n/2}-1}|x\rangle$ is the remaining unnormalized equal superposition of all the possible computational states for the subsystem. Defining the quantities

$$A \equiv \frac{\alpha^2 + 2^{n/2} - 1}{\alpha^2 + 2^n - 1},$$

$$B \equiv \frac{\alpha + 2^{n/2} - 1}{\alpha^2 + 2^n - 1},$$

$$C \equiv \frac{2^{n/2}}{\alpha^2 + 2^n - 1} \tag{28}$$

[note that $A + (2^{n/2} - 1)C = 1$], the density operator for the reduced system of $n/2$ qubits can be expressed in matrix notation as

$$\rho_{n/2} = \begin{pmatrix} A & B & \cdots & B \\ B & C & \cdots & C \\ \vdots & \vdots & \ddots & \vdots \\ B & C & \cdots & C \end{pmatrix}, \tag{29}$$

where its dimensions are $2^{n/2} \times 2^{n/2}$. We clearly see that the density matrix has rank equal to 2. Therefore, because $\text{rank}(\rho) \geq 2^{E(\rho)} \ \forall \rho$ [where $E(\rho)$ is the von Neumann entropy of the density matrix ρ], we conclude that $E(\rho_{n/2})$, which corresponds to our entanglement measure between the two blocks of qubits, is always ≤ 1. This holds true even for nonsymmetric bipartitions of the complete system. Regardless of the number of qubits, entanglement in Grover's adiabatic algorithm is always a *bounded* quantity for any s, in contrast with the results obtained in the previous sections for Shor's factoring algorithm and for the exact cover problem. Grover's adiabatic quantum algorithm essentially makes use of very little entanglement, but even this

bounded quantity of quantum correlations is enough to give a square root speedup.

We have explicitly calculated the von Neumann entropy for $\rho_{n/2}$. Because the rank of the reduced density matrix is 2, there are only two nonvanishing eigenvalues that contribute in the calculation, which are

$$\lambda_\pm = \frac{1}{2}[1 \pm \sqrt{1 - 4(2^{n/2} - 1)(AC - B^2)}]. \tag{30}$$

We analyze the limit $n \to \infty$ for $s \neq 0.5$ and $s = 0.5$ separately.

(a) $s \neq 0.5$. In the limit of very high n we can approximate the ground state energy given in Eq. (23) by

$$E_-(s) \sim \frac{1}{2}[1 - \sqrt{1 - 4s(1-s)}]. \tag{31}$$

Therefore, the quantity

$$\alpha \sim \frac{1}{1 - [E_-(s)]/(1-s)} \tag{32}$$

diverges at $s = 0.5$, which implies that this limit cannot be correct for that value of the parameter. The closer we are to $s = 0.5$, the bigger is α. In this limit we find that

$$A \sim \frac{\alpha^2 + 2^{n/2}}{\alpha^2 + 2^n}, \tag{33}$$

$$B \sim \frac{\alpha + 2^{n/2}}{\alpha^2 + 2^n}, \tag{34}$$

$$C \sim \frac{2^{n/2}}{\alpha^2 + 2^n}, \tag{35}$$

where all these quantities tend to zero as $n \to \infty$. It is important to note that the convergence of the limit depends on the value of α or, in other words, how close to $s = 0.5$ we are. The closer we are to $s = 0.5$, the slower is the convergence, and therefore any quantity depending on these parameters (such as the entropy) will converge more slowly to its asymptotic value. For the eigenvalues of the reduced density matrix we then find that when $n \to \infty$

$$\lambda_\pm \to \frac{1}{2}(1 \pm 1), \tag{36}$$

so $\lambda_+ \sim 1$ and $\lambda_- \sim 0$, and therefore the asymptotic entropy is

$$E(s \neq 0.5, n \to \infty) = -\lambda_+ \log_2 \lambda_+ - \lambda_- \log_2 \lambda_- = 0. \tag{37}$$

The convergence of this quantity is slower as we move toward $s = 0.5$.

(b) $s = 0.5$. We begin our analysis by evaluating the quantities at $s = 0.5$ and then taking the limit of large size of the system. We have that $\alpha(s = 0.5) = (2^n - 1)/(2^{n/2} - 1) \sim 2^{n/2}$. From here it is easy to get the approximations
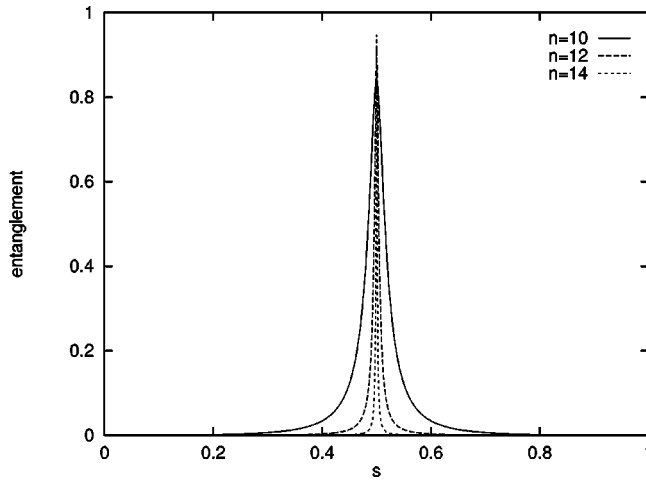
$$A \sim \frac{1}{2},$$

FIG. 16. Von Neumann entropy for the reduced system as a function of s for 10, 12, and 14 qubits. As the size of the system increases the entropy tends to zero at all points, except at $s=0.5$ where it tends to 1.

$$B \sim \frac{1}{2^{n/2}},$$

$$C \sim \frac{1}{2^{n/2+1}}, \tag{38}$$

and therefore

$$\lambda_{\pm} \sim \frac{1}{2}\left[1 \pm \sqrt{1 - 4\,2^{n/2}\left(\frac{1}{4}\frac{1}{2^{n/2}} - \frac{1}{2^{n}}\right)}\right] = \frac{1}{2} \pm \frac{1}{2^{n/4}}, \tag{39}$$

so $\lambda_{\pm} \to \frac{1}{2}$ and $E(s=0.5, n \to \infty)=1$. According to Eq. (39) we can evaluate the finite-size corrections to this behavior and find the scaling of the entropy with the size of the system for very large n. The final result for the entropy at the critical point reads

$$E(s=0.5, n \gg 1) \sim 1 - \frac{4}{\ln 2} 2^{-n/2}. \tag{40}$$

Note that the entropy remains bounded and tends to 1 for $s=0.5$ as a square root in the exponential of the size of the system, which is the typical factor in Grover's quantum algorithm.

We have represented the evolution of the entanglement entropy as a function of s for different sizes of the system in Fig. 16 and have plotted in Fig. 17 the maximum value of the entropy along the computation as a function of the size of the system according to the expression given in Eq. (40). We can now compare the two plots with Fig. 3 and Fig. 9 in the previous section. The behavior for the entropy in Grover's adiabatic algorithm is dramatically different from the one observed in the NP-complete problem. Entanglement gets saturated in Grover's adiabatic algorithm *even at the critical*
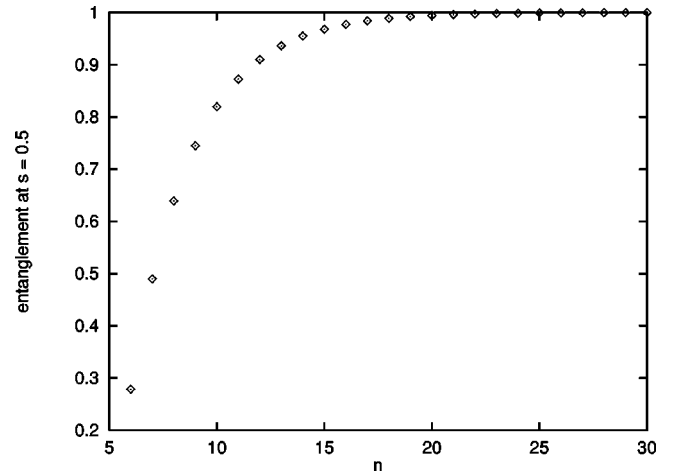

FIG. 17. Von Neumann entropy for the reduced system at $s=0.5$ as a function of n. For infinite size of the system there is saturation at 1.

point, which is reminiscent of short ranged quantum correlations in quantum spin chains.[1]

Let us note that, in the limit of infinite size, the quantum state in Grover's algorithm is separable with respect to any bipartition of the system (and therefore not entangled, as it is a pure state) for any s except for $s=0.5$. All the entanglement throughout the algorithm is concentrated at this point, but this entanglement is still a bounded quantity and actually equal to 1. Consequently, a small amount of entanglement appears essentially only at one point when the size of the system is big, whereas the rest of the algorithm needs to handle just separable states. We point out that these results apply as well to the traditional discrete-time implementation of Grover's searching algorithm, as the states between iterations are the same as in the adiabatic version for discrete s values.

V. CONCLUSIONS

In this paper we have studied the scaling of the entanglement entropy in several quantum algorithms. In particular, we have proved analytically that Shor's factoring algorithm makes use of an exponentially large amount of entanglement between the target register and the source register after the modular exponentiation operation, which in turn implies the impossibility of an efficient classical simulation by means of the protocol of Ref. [8]. Furthermore, we have provided numerical evidence for a universal linear scaling of the entropy with the size of the system together with a polynomially small gap in a quantum algorithm by adiabatic evolution devised to solve the NP-complete exact cover problem, therefore obtaining a polynomial-time quantum algorithm

---

[1]A somewhat similar situation is present in one-dimensional quantum spin chains outside the critical region, where the entanglement entropy also reaches saturation when the size of the system is increased [14]. Saturation does not appear in higher dimensional systems.

TABLE I. Entanglement scaling laws in different problems, in order of decreasing complexity.

Problem	Entanglement scaling
Adiabatic exact cover quantum algorithm	$E = O(n)$
Shor's quantum factoring algorithm	$E = O(\log_2 r) \sim O(n)$
Critical d-dimensional spin networks	$E = O(n^{(d-1)/d})$
Critical one-dimensional spin chains	$E = O(\log_2 n)$
Noncritical one-dimensional spin chains	$E = O(1)$
Adiabatic Grover's quantum algorithm	$E = O(1)$

which would involve exponential resources if simulated classically, in analogy with Shor's algorithm. The universality of this result follows from the fact that the quantum adiabatic algorithm evolves close to a quantum phase transition and the properties at the critical region do not depend on particular details of the microscopic Hamiltonian (instance) such as interactions among the spins or local magnetic fields. We have also proved that the von Neumann entropy remains a bounded quantity in Grover's adiabatic algorithm regardless of the size of the system even at the critical point. More concretely, the maximum entropy approaches 1 as a square root in the size of the system, which is the typical Grover scaling factor.

Our results show that studying the scaling of the entropy is a useful way of analyzing entanglement production in quantum computers. Results from other fields of physics [19–21] can be directly applied to bring further insight into the analysis of quantum correlations. Different entanglement scaling laws follow from different situations according to the amount of correlations involved, as can be seen in Table I. A quantum algorithm can be understood as the simulation of a system evolving close to a quantum phase transition. The amount of entanglement involved depends on the effective dimensionality of the system, which in turn governs the possibilities of certain efficient classical simulation protocols.

These scaling laws provide a different way of understanding some aspects from one-way quantum computation. It is known that the so-called cluster state of the one-way quantum computer can be generated by using Ising-like interactions on a planar two-dimensional lattice [38–40]. This fact can be related to the linear (in the size of the box) behavior of entropy for spin systems in two dimensions. One-dimensional models seem not to be able to efficiently create the highly entangled cluster state [41]. Again, this fact can be traced to the logarithmic scaling law of the entropy in spin chains, which is insufficient to handle the large amount of entanglement needed to carry out, e.g., Shor's algorithm. Note also that $(d \geq 3)$-dimensional systems bring unnecessarily large entanglement.

Quantum phase transitions remain as the more demanding systems in terms of entanglement. They are very hard to simulate classically. It is then reasonable to try to bring *NP*-complete problems into a quantum phase transition setup, which quantum mechanics handles naturally.

[1] J. I. Latorre and M. A. Martín-Delgado, Phys. Rev. A **66**, 022305 (2002).

[2] R. Orús, J. I. Latorre, and M. A. Martín-Delgado, Quantum Inf. Process. **4**, 283 (2003).

[3] R. Orús, J. I. Latorre, and M. A. Martín-Delgado, e-print quant-ph/0212094.

[4] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum, Science **287**, 463 (2000).

[5] P. Knight, Science **287**, 441 (2000).

[6] R. Jozsa and N. Linden, e-print quant-ph/0201143.

[7] S. Parker and M. B. Plenio, J. Mod. Opt. **49**, 1325 (2002).

[8] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).

[9] G. Vidal, e-print quant-ph/0310089.

[10] S. Sachdev, *Quantum Phase Transitions* (Cambridge University Press, Cambridge, England, 1999).

[11] T. J. Osborne and M. A. Nielsen, e-print quant-ph/0202162.

[12] A. Osterloh, L. Amico, G. Falci, and R. Fazio, Nature (London) **416**, 608 (2002).

[13] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev, Phys. Rev. Lett. **90**, 227902 (2003).

[14] J. I. Latorre, E. Rico, and G. Vidal, e-print quant-ph/0304098.

[15] F. Verstraete, M. Popp, and J. I. Cirac, e-print quant-ph/0307009.

[16] N. Lambert, C. Emary, and T. Brandes, e-print quant-ph/0309027.

[17] J. I. Latorre and R. Orús, e-print quant-ph/0308042.

[18] V. Murg and J. I. Cirac, e-print quant-ph/0309026.

[19] C. G. Callan and F. Wilczek, Phys. Lett. B **333**, 55 (1994).

[20] T. M. Fiola, J. Preskill, A. Strominger, and S. P. Trivedi, Phys. Rev. D **50**, 3987 (1994); M. Srednicki, Phys. Rev. Lett. **71**, 666 (1993).

[21] D. Kabat and M. J. Strassler, Phys. Lett. B **329**, 46 (1994); D.

Kabat, Nucl. Phys. B **453**, 281 (1995).

[22] V. E. Korepin, e-print cond-mat/0311056.

[23] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, e-print quant-ph/0001106.

[24] Peter W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, 1994*, edited by S. Goldwasser (IEEE, Los Alamitos, CA, 1994), p. 352.

[25] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, e-print quant-ph/0104129.

[26] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (Association for Computer Machinery, New York, 1996), p. 212.

[27] J. Roland and N. J. Cerf, Phys. Rev. A **65**, 042308 (2002).

[28] W. van Dam, M. Mosca, and U. Vazirani, in *Proceedings of the 42nd Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, CA, 2001), p. 279.

[29] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. London, Ser. A **454**, 339 (1998).

[30] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[31] A. Galindo and M. A. Martín-Delgado, Rev. Mod. Phys. **74**, 347 (2002).

[32] D. N. Page, Phys. Rev. Lett. **71**, 1291 (1993).

[33] S. Sen, Phys. Rev. Lett. **77**, 1 (1996).

[34] V. M. Kendon, K. Nemoto, and W. J. Munro, J. Mod. Opt. **49**, 1709 (2002).

[35] A. M. Childs and J. Goldstone, e-print quant-ph/0306054.

[36] S. Das, R. Kobes, G. Kunstatter, J. Phys. A **36**, 1 (2003).

[37] S. A. Cook, in *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1971), pp. 151–158.

[38] R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[39] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[40] R. Raussendorf and H.-J. Briegel, e-print quant-ph/0207183.

[41] H.-J. Briegel (private communication).