Exponential complexity of an adiabatic algorithm for an NP-complete problem

Marko Žnidarič[1,2] and Martin Horvat[2]
[1]*Department of Quantum Physics, University of Ulm, D-89069 Ulm, Germany*
[2]*Physics Department, Faculty of Mathematics Physics, University of Ljubljana, Ljubljana, Slovenia*

(Received 4 August 2005; published 17 February 2006)

We prove an analytical expression for the size of the gap between the ground and the first excited state of quantum adiabatic algorithm for the 3-satisfiability, where the initial Hamiltonian is a projector on the subspace complementary to the ground state. For large problem sizes the gap decreases exponentially and as a consequence the required running time is also exponential.

DOI: 10.1103/PhysRevA.73.022329 PACS number(s): 03.67.Lx, 89.70.+c

I. INTRODUCTION

Quantum computation has attracted a lot of attention after the discovery of Shor's quantum algorithm for factoring [1]. It requires polynomial number of steps while the best known classical algorithm is slower than polynomial. Another important quantum algorithm is Grover's search algorithm [2] which offers square-root improvement over classical search [3]. Quantum algorithms therefore seem to be qualitatively better than the classical ones. The obvious question is how much better are they? Classically problems can be split roughly into two groups, those whose solution requires polynomial number of steps and the so-called nondeterministic polynomial (NP) for which no polynomial classical algorithms are known. Especially fine subclass of NP problems are NP-complete (NPC) ones. They have the property that solving a single NPC problem in polynomial time would immediately provide a polynomial algorithm for all NP problems. There are literally thousands of problems known to be NPC [4], a paradigmatic example being the 3-satisfiability (3-SAT). The question of whether there exist polynomial algorithms for NPC problems is one of the great unsolved problems in mathematics [5]. It is not known whether quantum algorithms can solve NPC problems in polynomial time.

For quantum adiabatic computation, suggested by Farhi *et al.* [6,7], the initial numerical simulations for small problems suggested polynomial complexity for the NPC problem. If proved to be a generic behavior this would be a major breakthrough. But even if the worst case scaling turns out to be exponential one could still have a significant improvement in the average case performance compared to classical algorithms. Subsequent numerical studies did not fully clarify the issue, some indicated exponential complexity [8], some polynomial [9]. It seems that the worst case performance is exponential [10] but it might be nontrivial to identify this "hardest" instances. On the theoretical side there are no rigorous results about the complexity of quantum adiabatic algorithm for NPC problems. There are few exact calculations of complexity for tailored problems [11] like, e.g., 2-SAT instances [6,12] (but note that 2-SAT is not NPC). Exact results are available though for adiabatic Grover's algorithm [6,11,13,14]. Recently a random matrix theory has been used to describe adiabatic algorithm [15] even though it is not clear whether it applies to low energy eigenstates [16]. For the discussion of the relation between the minimal gap Δ and the necessary running time see also [17].

In the present paper we are going to prove an analytical formula for the size of the gap, thereby also of the complexity, for a particular implementation of the quantum adiabatic algorithm for 3-SAT, where the initial Hamiltonian is a simple projector. Section II is the core of the paper and gives a derivation of the gap.

II. ANALYTICAL CALCULATION OF THE GAP

We will choose a linear interpolation between the initial and the final Hamiltonian

$$H(t) = (1-t)H(0) + tH(1). \tag{1}$$

The initial Hamiltonian will be a projector to the space complementary to the single ground state $|\psi\rangle$

$$H(0) = b(\mathbb{1} - |\psi\rangle\langle\psi|), \quad |\psi\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle, \tag{2}$$

where $b=(n/2)[N/(N-1)]$ and $N=2^n$ is the dimension of the Hilbert space. We choose this "strange" value of b in order to have $\mathrm{tr}[H(0)]=Nn/2$. The final Hamiltonian is a sum of m three qubit projectors, one for each clause C_i

$$H(1) = a\sum_{i=1}^{m}|C_i\rangle\langle C_i|, \tag{3}$$

with $a=4/\alpha$, $\alpha=m/n$, and m and n are number of clauses and variables, respectively. The final Hamiltonian counts the number of violated clauses and can be realized using three-local Hamiltonian. Despite two parameters the Hamiltonian $H(t)$ depends essentially on a single parameter $1/\gamma := a/b \approx 8/(n\alpha) = 8/m$.

Our goal is to calculate the minimal energy gap Δ between the ground and the first excited state of $H(t)$. First, we are going to use the symmetry of the system to reduce the eigenvalue problem for an exponentially large matrix $H(t)$ to the eigenvalue problem of a matrix whose dimension will grow only linearly with n.

Let us consider a fixed 3-SAT instance, i.e., having a certain $H(1)$. Let D be the largest number of violated clauses by that instance. The final Hamiltonian has therefore eigenenergies $E_j(t=1)=ja$ with degeneracies $d_j, j=0,\ldots,D$. First, note that the Hamiltonian $H(t)$ is symmetric to any permutation of states that have the same final energy $E_i(1)$. Let us denote the state that is a symmetric combination of all d_j states with final energy ja by $|j\rangle_{\mathrm{s}}$, $|j\rangle_{\mathrm{s}}=(1/\sqrt{d_j})\Sigma_{E_k(1)=ja}|k\rangle$. We split N dimensional Hilbert space into $D+1$ totally symmetric states $|j\rangle_{\mathrm{s}}$ and $N-D-1$ antisymmetric states orthogonal to $D+1$ totally symmetric ones. Because the initial ground state $|\psi\rangle$ is totally symmetric we immediately see that all matrix elements of $H(t)$ between totally symmetric and antisymmetric subspaces are zero. What is more, the eigenvalues of the antisymmetric states are readily written down, $E_j^{\mathrm{anti}}=(1-t)b+jat=:\varepsilon_j$, and are (d_j-1) times degenerate, $j=0,\ldots,D$. To determine the minimal gap Δ we therefore have to solve the eigenvalue problem only for a $D+1$ dimensional submatrix on the space of totally symmetric states $|j\rangle_{\mathrm{s}}$ instead of on the full exponentially large Hilbert space. On the totally symmetric subspace the matrix $H_{\mathrm{s}}(t)$ $[H(t)$ limited to the totally symmetric subspace] of the Hamiltonian has a simple form

$$H_{\mathrm{s}}(t)=\mathrm{diag}(\varepsilon)-(1-t)b\mathbf{x}\mathbf{x}^T, \tag{4}$$

with a normalized $D+1$ dimensional column vector $\mathbf{x}=(\sqrt{d_0/N},\sqrt{d_1/N},\ldots,\sqrt{d_D/N})^T$ occurring in a projector $\mathbf{x}\mathbf{x}^T$ and $\varepsilon_j=(1-t)b+jat$ are the elements of the diagonal matrix $\mathrm{diag}(\varepsilon)$. We are now going to determine the gap for matrix H_{s} (4).

The characteristic polynomial $p(\lambda)=\det[H_{\mathrm{s}}(t)-\lambda\mathbb{1}]$ can be explicitly evaluated [18]

$$p(\lambda,t)=\prod_{j=0}^{D}(\varepsilon_j-\lambda)-(1-t)b\sum_{j=0}^{D}\frac{d_j}{N}\prod_{k\neq j}^{D}(\varepsilon_k-\lambda). \tag{5}$$

The calculation of the minimal gap Δ will now proceed in two steps. First we will prove that the region around the minimal gap is empty of other close eigenlevel encounters, meaning that sufficiently close to the minimal gap the geometry is that of a two-level avoided crossing. The characteristic polynomial $p(\lambda,t)$ has therefore parabolic shape around $t_{\min}$, the location of the minimal gap. In the second step we will determine Δ by simply calculating derivatives of $p(\lambda,t)$ at $t_{\min}$, fitting a parabola, and thereby obtain the gap with exponentially small relative error. We will always assume that the degeneracy d_0 of the ground state is small, $d_0 \ll N$, so that we will be able to neglect exponentially small terms of the form $\sim d_0/N$.

Let us show that the avoided crossing is really isolated. First observe that the value of the characteristic polynomial along lines ε_j is always nonzero, $p(\varepsilon_j,t)=-(1-t)b(at)^D(D-j)!j!(-1)^j d_j/N$. Therefore, due to the continuity of eigenvalues $E(t)$ of $H_{\mathrm{s}}(t)$ no eigenvalue can cross any of the lines $\varepsilon_j=(1-t)b+jat$. At time $t=1$ we know that the eigenvalues are $E_j(1)=ja$. Furthermore, because the derivative $\partial p(\varepsilon_j,1)/\partial\lambda=-a^D(D-j)!j!(-1)^j$ has the same sign as $p(\varepsilon_j,t\to 1)$ the eigenvalues approach ja from below as $t\to 1$. Therefore, jth eigenvalue of $H_{\mathrm{s}}(t)$ is bounded by ε_{j-1} and ε_j, i.e., $(1-t)b+(j-1)at<E_j(t)<(1-t)b+jat$. This has two consequences: (i) if the gap $\Delta \ll a$ the ground state avoided crossing will be isolated from $E_2(t)$, and (ii) the line $\varepsilon_0=(1-t)b$ passes through the gap Δ, i.e., between $E_0(t)$ and $E_1(t)$. From our result we will see that we indeed have $\Delta \ll a$, meaning that the avoided crossing is isolated. The second point above will be used in the following to determine the location $t_{\min}$ of the minimal gap. This will be obtained by remembering that in the two-level crossing the first derivative of the characteristic polynomial changes sign at the crossing. Demanding a zero of $\partial p/\partial\lambda$ on the line $\lambda=\varepsilon_0$ will give us an equation for $t_{\min}$ while the second derivative $\partial^2 p/\partial\lambda^2$ will be used to calculate Δ.

Using (5) we can calculate the determinant, $p(\varepsilon_0,t)/[(at)^D D!]=-(1-t)bd_0/N$, and its first and second derivatives, all evaluated along the line $\lambda=\varepsilon_0=(1-t)b$

$$\frac{\partial p(\varepsilon_0,t)/\partial\lambda}{(at)^{D-1}D!}=-at+(1-t)b\left[\gamma_{-1}+\frac{d_0}{N}h_D\right],$$

$$\frac{\partial^2 p(\varepsilon_0,t)/\partial\lambda^2}{(at)^{D-2}D!}=2ath_D-(1-t)b\left[2\gamma_{-1}h_D+2\gamma_{-2}-\frac{d_0}{N}(h_D^2-g_D)\right], \tag{6}$$

where $h_D:=\Sigma_{i=1}^{D}1/i$ and $g_D:=\Sigma_{i=1}^{D}1/i^2$. Two other important coefficients that are functions of size n and depend on the 3-SAT instance in question are

$$\gamma_{-1}:=\sum_{i=1}^{D}\frac{d_i}{N}\frac{1}{i},\quad \gamma_{-2}:=\sum_{i=1}^{D}\frac{d_i}{N}\frac{1}{i^2}. \tag{7}$$

The sum $\Sigma d_i i$ is given by the trace of $H(1)$, $\Sigma_{i=0}^{D}(d_i/N)i=(1/aN)\mathrm{tr}[H(1)]=\gamma\approx n\alpha/8$. Enforcing that the first derivative of $p(\lambda,t)$ vanishes at $t_{\min}$ and neglecting exponentially small term involving d_0/N we obtain

$$t_{\min}\approx\frac{\gamma\gamma_{-1}}{1+\gamma\gamma_{-1}}. \tag{8}$$

Note that because the gap Δ will turn out to be exponentially small, the error of so calculated $t_{\min}$ is also exponentially small. We now determine the two lowest levels E_0 and E_1 at $t_{\min}$ by parabolic fit to the values of determinant and its first two derivatives (6), obtaining $\Delta=E_1(t_{\min})-E_0(t_{\min})$

$$\Delta\approx\frac{n\sqrt{d_0}}{2\sqrt{N}}f(n),\quad f(n)=\frac{2}{1+\gamma\gamma_{-1}}\sqrt{\frac{\gamma_{-1}^2}{\gamma_{-2}}}, \tag{9}$$

where we used the asymptotic value $b\approx n/2$ and we neglected all terms of relative size $O(1/N)$ (i.e., involving d_0). This is the main result of the present paper. It gives an explicit expression for the gap Δ in terms of two coefficients γ_{-1} and γ_{-2} (7). By evaluating the values of the determinant and its first derivative at the so obtained $\lambda=E_{0,1}$ one can verify that the error in $f(n)$ is $O(d_0/N)$. Relative precision of Δ (9) is therefore exponential. To preserve this accuracy we have to demand that the ground state degeneracy d_0 does not increase by increasing n, i.e., the number of solutions is kept constant.

How do γ_{-1} and γ_{-2} behave as n increases? The coefficients d_i/N can be viewed as a discrete probability distribution, γ_{-1} and γ_{-2} as negative moments and γ as the first moment. Let us denote by σ the standard deviation of this distribution, $\sigma := \sqrt{\gamma_2 - \gamma^2}$, with $\gamma_2 = \Sigma d_i i^2/N$. Then, if with increasing n the ratio σ/γ goes to zero sufficiently fast (i.e., the distribution becomes narrow), the inverse moments will be in the leading order given just by the inverse powers of the first moment

$$\gamma_{-1} = \frac{1}{\gamma} + O(1/n^2), \quad \gamma_{-2} = \frac{1}{\gamma^2} + O(1/n^3). \tag{10}$$

For random 3-SAT with constant α one can show [19] that one indeed has $\sigma/\gamma \sim 1/\sqrt{n}$. We can therefore see that the function $f(n)$ will for large n behave as $f(n) = 1 + O(1/n)$ for arbitrary random 3-SAT. Note though that this does not mean that the gap is exponentially small for arbitrary random 3-SAT. For Δ to be small we also have to keep the number of solutions constant. For instance, below the transition point $\alpha_c \approx 4.25$ the number of solutions for random 3-SAT grows exponentially with n (see, e.g., Ref. [20]) and therefore our formula for gap (9) cannot be used to predict the scaling for $n \to \infty$.

In the next section we are going to demonstrate the validity of Eq. (9) by numerical calculations. We are going to consider two ensembles of 3-SAT instances having a single solution, $d_0 = 1$. The first one will be the so-called single-solution random 3-SAT ensemble whose members seem to be hard also for classical algorithms [21]. The second ensemble of 3-SAT instances, called binomial 3-SAT, is generated in such a way that the degeneracies d_i are explicitly known, enabling analytical calculation of γ_{-1} and γ_{-2}.

III. NUMERICAL DEMONSTRATION

To illustrate the theory we numerically calculated Δ for single-solution random 3-SAT instances with $\alpha = 4.5$ and compared this with the theoretical prediction for Δ, Eq. (9). Because the accuracy of Eq. (9) is exponential in n one can hardly see any difference between the theory and numerics in Fig. 1 (e.g., for $n = 20$ the two agree to 3 decimal places). Note that for random 3-SAT we do not know explicit form of degeneracies d_j so we had to calculate γ_{-1} and γ_{-2} numerically. For instance, for $n = 30$ we have $\gamma_{-1}\gamma \approx 1.05$ and $\gamma_{-2}\gamma^2 \approx 1.17$, resulting in $f(30) \approx 0.95$, see also data in Fig. 2. To remedy this drawback of having to numerically calculate γ_{-1} and γ_{-2} we have constructed another set of 3-SAT instances, shortly binomial 3-SAT, for which d_j are given by the binomial distribution and therefore we can explicitly calculate γ_{-1} and γ_{-2}.

The prescription to construct binomial 3-SAT is the following. Assume that n is divisible by 3 and denote $r = n/3$. We split n qubits into r triples and for each triple we add 7 different clauses involving this three qubits (out of 8 possible). In total we therefore have $m = 7r$ clauses, so the clause density is $\alpha = 7/3$. The degeneracies of such binomial 3-SAT are $d_i = 7^i \binom{r}{i}$, $i = 0, \ldots, r$. For binomial degeneracies one can express γ_{-1} and γ_{-2} in term of a generalized hypergeometric function

$$\gamma_{-1} = \frac{7r}{8^r} {}_2F_3\left(\begin{matrix} 1,1,1-r \\ 2,2 \end{matrix}; -7\right),$$

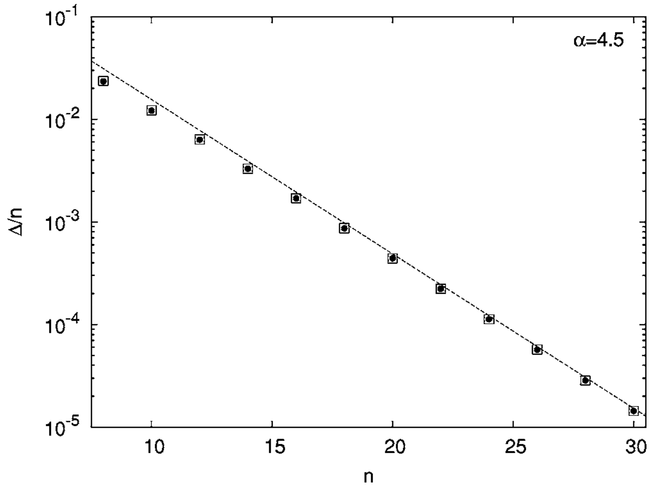

FIG. 1. Single-solution random 3-SAT with $\alpha = 4.5$. Empty squares are numerically calculated gaps, full circles (overlapping with squares) is the theoretical formula (9) (with numerically calculated γ_{-1} and γ_{-2}). Dashed line is $1/(2\sqrt{N})$.

$$\gamma_{-2} = \frac{7r}{8^r} {}_3F_4\left(\begin{matrix} 1,1,1,1-r \\ 2,2,2 \end{matrix}; -7\right). \tag{11}$$

While these expressions are exact they are not very illuminating. We are particularly interested in large n behavior. Using asymptotic expansion [22] one gets $\gamma_{-1} \asymp 1/\gamma(1 + 1/8\gamma + \cdots)$ and $\gamma_{-2} \asymp 1/\gamma^2(1 + 3/8\gamma + \cdots)$, resulting in $f(n) \asymp 1 - 1/8\gamma$, where $\asymp$ denotes asymptotically equal. To demonstrate our explicit result (9) in the case of binomial 3-SAT (11) we again performed numerical calculations. The results are shown in Fig. 2. This time we rather show $f(n)$ as

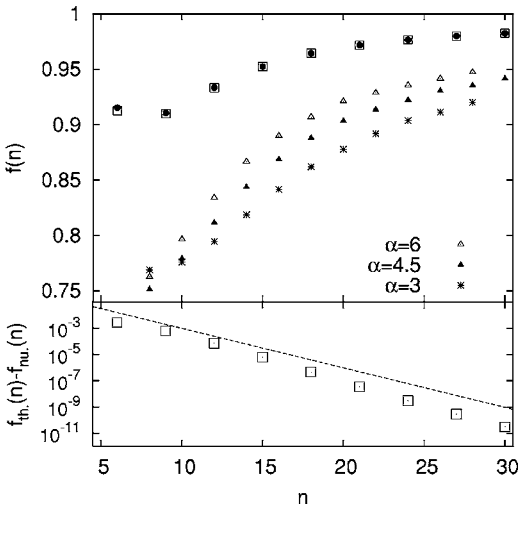

FIG. 2. Binomial 3-SAT. Full circles are theoretical prediction for $f(n)$ using Eq. (11), empty squares (overlapping with full circles) are numerical result for full diagonalization. In the bottom figure we show for the same data the difference between the theory and the numerics. Dashed line is $1/2^n$. For comparison we also show in the top frame $f(n)$ (obtained by numerically calculating γ_{-1} and γ_{-2}) for three different single-solution random 3-SAT ensembles (stars and triangles).

the plot for Δ would look very similar to the one for single-solution random 3-SAT in Fig. 1. In the lower frame we can see that the accuracy of theoretical $f(n)$ (9) is indeed exponential. Note that binomial 3-SAT is rather artificial and easy to solve classically, we use it just to demonstrate our theory. The same expression for the minimal gap as here for the binomial 3-SAT has been obtained also for the adiabatic Grover's algorithm in [6] where a similar symmetry as here has been exploited.

IV. DISCUSSIONS

Our result shows that asymptotically the gap scales as $\Delta \asymp n/(2\sqrt{N})$ for an arbitrary random 3-SAT (with constant d_0). This means that the running time grows as $\sim\sqrt{N}$, the same as for Grover's algorithm. In Ref. [12] it is proved that the running time of any Grover's algorithm of the form $H=|w\rangle\langle w|+H_D(t)$, for an arbitrary $H_D(t)$, must be larger than $\sim\sqrt{N}$. Farhi *et al.* have pointed out [23] that the proof can be straightforwardly extended to Hamiltonians of the form $H(t)=(1-t/T)(1-|w\rangle\langle w|)+(t/T)H(1)$ (i.e., of the form we use) to show that: demanding that after time T we reach the ground state of $H(1)$ from any of the basis states $|w\rangle$ (i.e., averaging over a complete basis is used in the proof), the running time T must be larger than $\sim\sqrt{N}$. What does this tell us about the running time for a single specific choice of $|w\rangle=|\psi\rangle$ that we use? Provided one is able to show that there exists a basis, a member of which is our $|\psi\rangle$, for which the running time is the same for all members $|w\rangle$ of that basis (or at least scales the same), would mean that the running time must necessarily be larger than $\sim\sqrt{N}$ also for specific $|w\rangle=|\psi\rangle$, i.e., the gap must be smaller than $\sim 1/\sqrt{N}$. Without showing this nothing can be concluded about the running time for a particular $H(t)$, not even about the average running time. But fortunately, such a basis can be found. It consists of eigenvectors of σ_x operator. In z eigenbasis that we use, all such basis states are sums of all computational states with the signs in front of them depending on the eigenvalue of σ_x, $|w\rangle=(1/\sqrt{N})\Sigma_i\,\mathrm{sgn}_i|i\rangle$, with $\mathrm{sgn}_i=\pm 1$. For instance, for our $|\psi\rangle$ (2) we have $\mathrm{sgn}_i\equiv 1$. One can now quickly see that the same symmetry arguments used in the derivation of Eq. (4) for state $|\psi\rangle$ can be used also for other $|w\rangle$'s of the above form. In particular, the eigenvalue problem can be reduced to the very same matrix $H_s(t)$ (4) for each of $|w\rangle$'s. This then shows that if one uses for $|w\rangle$'s the eigenstates of σ_x operator the running time is the same for all. Using the above mentioned proof one can then conclude that the running time must be larger than $\sim\sqrt{N}$ also for our choice of $|w\rangle=|\psi\rangle$ which is in accordance with our explicit result (9).

It is interesting to note that one can obtain the asymptotic dependence of $\Delta \asymp n/(2\sqrt{N})$ already by projecting the Hamiltonian $H_s(t)$ to a two-dimensional subspace spanned by state $|\psi\rangle$ and the solution state $|0\rangle_s$. The reason for the Grover-like scaling of Δ for large n is that the lowest two levels become effectively decoupled from the rest of the spectrum. This "decoupling" arises because the couplings d_j/N (for fixed j) go toward zero by increasing n. Note though that our result for Δ (9) is nonperturbative, i.e., one cannot obtain function $f(n)$ by perturbative corrections to the asymptotic result, e.g, by perturbatively including higher levels.

Is this asymptotic square-root behavior of quantum adiabatic algorithm for 3-SAT general, i.e., independent of our choice of $H(0)$ or of the interpolating path? Here we will discuss only the effect of different choices of $H(0)$ although the choice of optimal path is also important, for an example when the choice of the path matters see [24]. It is important to distinguish between the average-case and the worst-case performance. For the average-case performance numerics clearly shows that our choice of $H(0)$ is less than optimal. For instance, taking for $H(0)$ a sum of terms σ_x, one for each qubit, the average gap is usually much larger than $\sim 1/\sqrt{N}$. The situation is on the other hand different if one considers the worst-case performance. Numerical calculations of Δ for $H(0)=\Sigma_i(1-\sigma_x)$, see Refs. [10,16], indicate that the gap for single-solution random 3-SAT instances with small α (e.g, $\alpha=3$) shows dependence similar to the square-root asymptotic formula derived in the present paper. In Ref. [16] where exactly the same normalization of the Hamiltonian as here is used, the asymptotic dependence of Δ is exactly $\Delta \asymp n/(2\sqrt{N})$, i.e., without any fitting prefactor. Therefore, there are numerical indications that the worst-case performance could be the same $\sim 1/\sqrt{N}$ also for other choices of $H(0)$ while on the other hand the average-case performance might be significantly better [25]. A distinctive feature of single-solution 3-SAT instances with small α that seems to play a role in this square-root behavior of the gap is that the number of statements (states) that violate only one clause is exponentially large (though still exponentially smaller than N). That is, $H(1)$ has a single ground state and at the same time exponentially degenerate first excited state just above it. Adiabatic algorithm therefore has to "find" the right ground state among exponentially many that are "almost" ground states. Shor also presented an informal mathematical argument why one can expects the worst-case performance for NPC problems to be the same as that for searching in an unstructured database [26].

In conclusion, we have provided an analytical expression for the minimal gap of a particular implementation of the quantum adiabatic algorithm for 3-SAT. The derivation shows that such adiabatic algorithm is asymptotically equivalent to searching in an unstructured database. Numerical calculations hint that the same asymptotic worst-case performance might be obtained also for other choices of initial Hamiltonian.

Note added in proof. Recently a paper by Farhi *et al.* has appeared [27], explaining in detail a general proof briefly mentioned in the discussions.

ACKNOWLEDGMENTS

We would like to thank E. Farhi, J. Goldstone, and S. Gutmann for discussions and for pointing out the relevance of the proof in Ref. [12]. M.Ž. would like to thank the Alexander von Humboldt Foundation for financial support.

[1] P. W. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by Shafi Goldwasser (IEEE Computer Society Press, Los Alamitos, 1994), 124–134.

[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] Classical algorithms with square-root performance are possible but require exponential memory overhead, see S. Lloyd, Phys. Rev. A **61** 010301 (2000); L. K. Grover and A. M. Sengupta, Phys. Rev. A **65**, 032319 (2002).

[4] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979).

[5] S. A. Cook, *Millennium Problems* (Clay Mathematics Institute, 2000), http://www.claymath.org/millennium; C. Seife, Science **309**, 96 (2005).

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

[7] E. Farhi, J. Goldstone, S. Gutman, J. Lapan, A. Lundgren, and D. Preda, Science **292**, 472–476 (2001).

[8] V. N. Smelyanskiy, U. V. Toussaint, and D. A. Timucin, e-print quant-ph/0112143.

[9] T. Hogg, Phys. Rev. A **67**, 022314 (2003).

[10] M. Žnidarič, Phys. Rev. A **71**, 062305 (2005).

[11] W. van Dam, M. Mosca, and U. Vazirani, *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science* (IEEE, New York, 2001), pp. 279–287.

[12] B. W. Reichardt, *Proceedings of the 36th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2004), pp. 502–510.

[13] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403 (1998).

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

[15] A. Boulatov and V. N. Smelyanskiy, Phys. Rev. A **71**, 052309 (2005); D. R. Mitchell, C. Adami, W. Lue, and C. P. Williams, Phys. Rev. A **71**, 052324 (2005).

[16] M. Žnidarič, Phys. Rev. A **72**, 052336 (2005).

[17] G. Schaller, S. Mostame, and R. Schützhold, e-print quant-ph/0510183.

[18] We use $\det(D-\mathbf{y}\mathbf{y}^T)=\det\{D^{1/2}(\mathbb{1}-D^{-1/2}\mathbf{y}\mathbf{y}^T D^{-1/2})D^{1/2}\}$ which is equal to $\det D \det(\mathbb{1}-\mathbf{v}\mathbf{v}^T)$ for diagonal D and $\mathbf{v}:=D^{-1/2}\mathbf{y}$.

[19] $\gamma_2=\mathrm{tr}[H^2(1)]/Na^2=\Sigma_{i,j}\mathrm{tr}[|C_i\rangle\langle C_i||C_j\rangle\langle C_j|]/N$. Denoting by $p=\binom{n-3}{3}/\binom{n}{3}\asymp 1-3/n$ the probability that two random clauses involve six different qubits, we can estimate $\gamma_2\approx pm^2/2^6+(1-p)m^2k/2^6+O(m)$, where the term involving k ($k>1$) takes into account clause pairs that involve less than six different qubits. From this we get $\gamma_2-\gamma^2\sim m^2/n$ and $\sigma/\gamma\sim 1/\sqrt{n}$. With increasing n the mean of unimodal distribution d_i/N scales as $\gamma\propto n$ and the width as $\sigma\propto\sqrt{n}$. The number of d_i's also grows as $D\propto n$.

[20] R. Monasson and R. Zecchina, Phys. Rev. Lett. **76**, 3881 (1996).

[21] M. Žnidarič, e-print cs.AI/0504101.

[22] M. Žnidarič, e-print math.ST/0511226.

[23] E. Farhi, J. Goldstone, and S. Gutmann (private communication).

[24] E. Farhi, J. Goldstone, and S. Gutmann, e-print quant-ph/0208135.

[25] For our artificial binomial 3-SAT and $H(0)$ that is a sum of 1–qubit terms, the gap is even independent of n.

[26] P. W. Shor, Quantum Inf. Process. **3**, 5 (2004).

[27] E. Farhi, J. Goldstone, S. Gutmann, and D. Nagaj, e-print quant-ph/0512159.