Number partitioning via quantum adiabatic computation

V. N. Smelyanskiy[1,*] and U.V. Toussaint[2]
[1]*NASA Ames research Center, MS 269-2, Moffet Field, Ca 94035-1000 and*
[2]*Max-Planck-Institute for Plasma Physics, Boltzmannstr, 2 D-85748 Garching*
(Dated: April 11, 2002)

A new quantum algorithm has been recently suggested [5, 6] for combinatorial search and optimization problems that is based on the properties of quantum adiabatic evolution. We apply the algorithm to random instances of the NP-complete Set Partition problem and show that its run time grows exponentially with the problem size n. We solve the stationary Schrödinger equation for the instantaneous (adiabatic) eigenstates of the quantum computer and obtained the minimum gap $g_{\min} = \mathcal{O}(n\,2^{-n/2})$ between its ground and excited energy levels during the algorithm execution. Our analysis describes the connection between the exponentially small size of $g_{\min}$ that determines poor performance of the algorithm and statistical properties of the optimization problem in question. Analytical results are in qualitative agreement with the numerical simulation of the algorithm for small instances of the Set Partition problem.

PACS numbers: 03.67.Lx,89.70.+c

I. INTRODUCTION

Since the discovery by Shor [1] nearly a decade ago of a quantum algorithm for efficient integer factorization there has been a rapidly growing interest in the development of new quantum algorithms capable of solving computational problems that are practically intractable on classical computers. Perhaps the most notable example of such problems is that of combinatorial optimization (COP). In the simplest case the task in COP is to minimize the cost function ("energy") $E_{\mathbf{z}}$ defined on a set of 2^n binary strings $\mathbf{z} = \{z_1, \ldots, z_n\}$ $z_j = 0, 1$, each containing n bits. In quantum computation this cost function corresponds to a Hamiltonian H_P

$$H_P = \sum_{\mathbf{z}} E_{\mathbf{z}} |\mathbf{z}\rangle\langle\mathbf{z}| \qquad (1)$$
$$|\mathbf{z}\rangle = |z_1\rangle_1 \otimes |z_2\rangle_2 \otimes \cdots \otimes |z_n\rangle_n.$$

where the indices $z_j = 0, 1$ and the summation is over 2^n states $|\mathbf{z}\rangle$ forming the computational basis of a quantum computer with n qubits. State $|z_j\rangle_j$ of the j-th qubit is an eigenstate of the Pauli matrix $\hat{\sigma}_z$ with eigenvalue $S_j = 1 - 2z_j$ ($S_j = \pm 1$). It is clear from the above that the ground state of H_P encodes the solution to the COP with cost function $E_{\mathbf{z}}$.

COPs have a direct analogy in physics, related to finding ground states of classical spin glass models. In the example above bits z_j correspond to Ising spins S_j. The connection between the properties of frustrated disordered systems and the structure of the solution space of complex COPs has been noted first by Fu and Anderson [2]. It has been recognized [3] that many of the spin glass models are in almost one-to-one correspondence with a number of COPs from theoretical computer science that form a so-called NP-complete class [4]. This class contains hundreds of the most common computationally hard problems encountered in practice, such as constraint satisfaction, traveling salesmen, integer programming, and others. NP-complete problems are characterized in the worst cases by exponential scaling of the running time or memory requirements with the problem size n. A special property of the class is that any NP-complete problem can be converted into any other NP-complete problem in polynomial time on a classical computer; therefore, it is sufficient to find a deterministic algorithm that can be guaranteed to solve all instances of just one of the NP-complete problems within a polynomial time bound. However it is widely believed that such an algorithm does not exist on a classical computer. Weather it exists on a quantum computer is one of the central open questions. Ultimately one can expect that the behavior of the new quantum algorithms for COPs and their complexity will be closely related to the properties of quantum spin glasses.

Farhi and co-workers suggested recently a new quantum algorithm for solving combinatorial optimization problems which is based on the properties of quantum adiabatic evolution [5]. Running of the algorithm for several NP-complete problems has been simulated on a classical computer using a large number of randomly generated problem instances that are believed to be computationally hard for classical algorithms [6–8]. Results of these numerical simulations for relatively small size of the problem instances ($n \leq 20$) suggest a *quadratic* scaling law of the run time of the quantum adiabatic algorithm with n. In [5, 9] special symmetric cases of COP were considered where symmetry of the problem allowed to describe the true asymptotic behavior ($n \to \infty$) of the algorithm. In certain examples considered in [9] quantum adiabatic algorithm finds the solution in time polynomial in n while simulated annealing requires exponential time. This effect occurs due to the special connectivity properties of the optimization problems that lead to

*Electronic address: vadim@email.arc.nasa.gov

the relatively large matrix elements for the spin tunneling in transverse magnetic field between different valleys during the quantum adiabatic algorithm. In the examples considered in [9] the tunneling matrix element scales polynomially with n. On the other hand, in simulating annealing algorithm different valleys are connected via classical activation processes for spins with probabilities that scale exponentially with n.

However, so far there are no analytical results on the asymptotic behavior of the algorithm for the general case of randomly generated hard instances of NP-complete problems.

II. SET PARTITION PROBLEM

In what follows we derive the asymptotic complexity of the quantum adiabatic algorithm for the Set Partition Problem (SPP). It is one of the six basic NP-complete problems that are at the heart of the theory of NP-completeness [4]. It can be formulated as combinatorial optimization problem: Given a sequence of positive numbers $\{a_1, \ldots, a_n)$ find a partition, i.e. two disjoint subsets $\mathcal{A}$ and $\mathcal{A}'$ such that the residue

$$E = \left| \sum_{a_j \in \mathcal{A}} - \sum_{a_j \in \mathcal{A}'} \right| \tag{2}$$

is minimized. In SPP we search for the bit strings $\mathbf{z} = \{z_1, \ldots, z_n\}$ (or corresponding Ising spin configurations $\mathbf{S} = \{S_1, \ldots, S_n\}$) that minimize the energy or cost function $E_{\mathbf{z}}$

$$E_{\mathbf{z}} = |\Omega_{\mathbf{S}}|\,, \quad \Omega_{\mathbf{S}} = \sum_{j=1}^{n} a_j S_j,\ S_j = 1 - 2z_j, \tag{3}$$

Here $S_j = 1$ ($z_j = 0$) if $a_j \in \mathcal{A}$ and $S_j = -1$ ($z_j = 1$) if $a_j \in \mathcal{A}'$. The minimum partition can also be viewed as a ground state of the Ising spin glass, $-\Omega_{\mathbf{S}}^2$, with the Mattis-like (global) antiferromagnetic coupling, $J_{ij} = -a_i\, a_j$.

SPP also has many practical applications including multiprocessor scheduling [10], cryptography [11], and others. The interest in SPP also stems from the remarkable failure of simulated annealing to find good solutions, as compared with the solutions found by deterministic heuristics [12]. The apparent reason for this failure is due to the existence of order 2^n local minima whose energies are of the order of $1/n$ [13] which undermines the usual strategy of exploring the space of configurations $\mathbf{S}$ through single spin flips.

The computational complexity of random instances of SPP depends on the number of bits b needed to encode the numbers a_j. Numerical simulations show [14, 15] that for independent, identically distributed (i.i.d.) random b-bit numbers a_j, the solution time grows exponentially with n for $n < b$ and polynomially for $n > b$. The transition from the "hard" to computationally "easy" phases has features somewhat similar to phase transitions in physical systems [16]. Transitions of this kind were observed in various NP-complete problems [17] and can be analyzed in the framework of statistical mechanics. In what follows we concentrate on the computationally hard regime $n \ll b$.

We now consider the distribution of the partition energies $E_{\mathbf{z}}$. It was derived in [18] using statistical averaging over the assemble of instances of SPP with i.i.d. numbers a_j. Bearing in mind our eventual goal of deriving the complexity of the quantum algorithm for a given random instance of SPP we do not perform such an averaging. Instead we work with a given set of $\{a_j\}$ and introduce a coarse-grained "density of states"

$$\rho(E) = \Big\langle \sum_{\mathbf{z}} \delta(E - E_{\mathbf{z}}) \Big\rangle_E. \tag{4}$$

Here $\delta(x)$ is Dirac delta-function. The sum in (4) is over 2^n bit-strings $\mathbf{z}$; partition energy $E_{\mathbf{z}}$ is defined in (3) and $\langle \cdots \rangle_E$ denotes averaging over the interval of the partition values $(E - \eta/2, E + \eta/2)$ with the window size chosen self-consistently, $\eta \gg 1/\rho(E)$. Using (3) we can rewrite (4) in the form

$$\rho(E) = \frac{2^n}{\pi} \int_0^\infty ds\, f\left(\frac{\eta\, s}{2}\right)\, I(s)\, \cos(Es), \tag{5}$$
$$I(s) = \prod_{j=0}^{n} \cos(a_j s), \quad f(x) = \sin(x)/x.$$

Here $f(x)$ is a window function that imposes a cut-off in the integral (5) at $s \sim 2/\eta \ll \rho(E)$. For large n this integral can be evaluated using the steepest descent method. To find the saddle points we shall assume that the b-bit numbers a_j are distributed inside of the interval $(0, 1)$ and are the integer multiples of 2^{-b}, the smallest number that can be represented with available number of bits. We note that for large n the function $I(s)$ has sharp maxima (minima) with width $\sim n^{-1/2}$ at the points $s_k = k\pi\, 2^b$, $k = 0, 1, \ldots$; $|I(s_k)| = 1$. The sum over these saddle-points was evaluated by Mertens [16] in the context of the partition function in SPP at finite temperature. In our case only one saddle point at $s = 0$ contributes to the integral in (5) due to coarse-graining of the density of states. Indeed, it will be seen below that the window size $2/\eta$ can be chosen to obey the conditions $1 \ll n^{1/2}/\eta \ll 2^n$. Therefore in the high-precision case ($b \gg n$) saddle-points s_k with $k > 0$ lie far outside the window and their contributions can be neglected [19]. On the other hand the window function $f(x)$ can be replaced by unity while computing the contribution from the saddle-point at $s = 0$. Finally we obtain for $E \ll n$ [18]

$$\rho(E) = \frac{2^{n+1}\, \Theta(E)}{\sqrt{2\,\pi\,\sigma^2\, n}} \exp\left(-\frac{E^2}{2\sigma^2\, n}\right) + \mathcal{O}(n^{-3/2})$$
$$\sigma^2 = \frac{1}{n} \sum_{j=1}^{n} a_j^2, \quad E \ll n. \tag{6}$$

Here $\Theta(x)$ denote a step function. $\Theta(x)$=1, for $x \geq 0$ and $\Theta(x)$=0 for $x < 0$. The coarse-grained state density in Eq.(6) depends on the set of $\{a_j\}$ through a single self-averaging quantity σ^2 (cf. [16]). For E that are not too large ($E \lesssim \sqrt{n}$) the average separation between the individual partition energies $E_{\min} \sim \sqrt{n} 2^{-n}$. This justifies the choice of the window η above that corresponds to coarse-graining over many individual level separations. For a typical set of numbers $\{a_j\}$ there are only two scales present in the distribution of partition energies, one is a "microscopic" scale given by $E_{\min}$ and another is given by the mean partition energy $\langle E \rangle = \sigma(2n/\pi)^{1/2}$.

Using the same approach one can introduce the distribution $\tilde{\rho}(\Omega)$ of "signed residues" $\Omega_{\mathbf{S}}$. Due to the obvious symmetry of the SPP cost function $|\Omega_{\mathbf{S}}|$ in (3) does not change after flipping signs of all spins, $S_j \to -S_j$. Therefore

$$\tilde{\rho}(\pm\Omega) \equiv \Big\langle \sum_{\mathbf{S}} \delta(\Omega - \Omega_{\mathbf{S}}) \Big\rangle_{\Omega} = 1/2\rho(|\Omega|). \qquad (7)$$

Distribution $\tilde{\rho}(\Omega)$ is Gaussian for $E \ll n$ and can be understood in terms of a random walk with coordinate Ω (cf. (3)). The walk begins at the origin, $\Omega = 0$, and makes n steps. At the j-th step Ω moves to the right or to the left by "distance" $2\,a_j$ if $S_j = 1$ or $S_j = -1$, respectively. In the asymptotic limit of large n the result (6) corresponds to equal probabilities of right and left moves and the distribution of step lengths coinciding with that in the set of numbers $\{2\,a_j\}$.

We now consider the "conditional" density of the partition energies

$$\rho_r(E'|E) = \frac{\rho_r(E', E)}{\rho(E)}, \qquad (8)$$

where $\rho_r(E'|E)$ is a "joint" density defined as follows

rhoEE, rhoEz

$$\rho_r(E', E) = \Big\langle \sum_{\mathbf{z}} \rho_{r,\mathbf{z}}(E')\, \delta(E - E_{\mathbf{z}}) \Big\rangle_{E}, \qquad (9)$$

$$\rho_{r,\mathbf{z}}(E') = \Big\langle \sum_{\mathbf{z}'} \delta(E' - E_{\mathbf{z}'})\, \delta_{r,D(\mathbf{z}',\mathbf{z})} \Big\rangle_{E'} \qquad (10)$$

Here $\delta_{k,l}$ is a Kronecker delta. Function $D(\mathbf{z}, \mathbf{z}')$ above computes the number of bits that take different values in the bit-strings $\mathbf{z}$ and $\mathbf{z}'$, it is a so-called Hamming distance between the strings

$$D(\mathbf{z}, \mathbf{z}') = \sum_{j=1}^{n} (1 - z_j)\, z'_j + (1 - z'_j)\, z_j. \qquad (11)$$

Hamming distance $D(\mathbf{z}, \mathbf{z}')$ is directly related to the overlap between the corresponding spin configurations $q(\mathbf{S}, \mathbf{S}')$ often used in a theory of spin glasses (cf. [3, 18]),

q

$$q(\mathbf{S}, \mathbf{S}') = \frac{1}{n} \sum_{j=1}^{n} S_j S'_j = 1 - \frac{2}{n} D(\mathbf{z}, \mathbf{z}'). \qquad (12)$$

Conditional density $\rho_{r,\mathbf{z}}(E')$ in (10) determines the distribution of energies $E_{\mathbf{z}'}$ for the strings $\mathbf{z}'$ obtained from $\mathbf{z}$ by flipping r bits. Similar to Eq. (4), $\langle \cdots \rangle$ in (9),(10) denotes averaging over the small energy interval $(E - \eta/2, E + \eta/2)$ that, however, includes many individual partition energies $E_{\mathbf{z}'}$.

For $r = 1$ there are exactly n strings $\mathbf{z}'$ on a Hamming distance r =1 from the string $\mathbf{z}$. Partition energies corresponding to these strings equal $|\Omega_{\mathbf{S}} - 2a_j S_j|$, $1 \leq j \leq n$ (cf. (3)). In what following we assume that numbers $\{a_j\}$ are uniformly distributed in the unit interval. Then one can show that for $E_{\mathbf{z}} < 2$ the energies $|\Omega_{\mathbf{S}} - 2a_j S_j|$ are distributed nearly uniformly in the range $(0, 2 - E_{\mathbf{z}})$. This is due to the fact that spins S_j are nearly equally distributed between ± 1 values for configurations with $|\Omega_{\mathbf{S}}| \ll n$. Similar arguments apply for the case $r = n-1$. Using a coarse-graining window such that $n^{-1} \ll \eta \ll 1$ one can obtain in the range of energies $E', E_{\mathbf{z}} \lesssim 1$ the following result:

$$\rho_r(E'|E_{\mathbf{z}}) \approx \rho_{r,\mathbf{z}}(E') = n/2 + \mathcal{O}(1)$$
$$r = 1, n-1, \quad n \gg 1. \qquad (13)$$

For large $r, n - r \gg 1$ one can calculate the conditional densities (9) for a given set of $\{a_j\}$ by evaluation of the appropriate integrals with the steepest descent method, in a similar manner to the derivation of of $\rho(E)$ in Eqs.(4)-(6). The detailed analysis is presented in Appendix. Here we will skip the derivation and only provide the result that we found to be in a good agreement with the numerical simulations of SPP even for modest values of n (see Fig. 1). State density functions in (9) are given each by a sum of Gaussian functions defined in the region $E, E' \geq 0$ and have a broad maximum at the origin. Near the maximum we have:

$$\rho_r(E'|E_{\mathbf{z}}) \approx \rho_{r,\mathbf{z}}(E') \approx \frac{\zeta(r/n)}{\sigma\sqrt{\pi\, n/2}} \binom{n}{r} \qquad (14)$$
$$\zeta(x) = (4x(1-x))^{-1/2}, \quad r,\, n - r \gg 1.$$

This result applies in a range $E', E_{\mathbf{z}} \ll \sigma r^{1/2}, \sigma(n-r)^{1/2}$. We note that conditional density (10) in (13) and (14) does not depend on E' and $\mathbf{z}$ after the coarse-graining over the small interval η of energies $E_{\mathbf{z}'}$. We shall refer to it as $\bar{\rho}_r$. Window size $\eta \gg 1/\bar{\rho}_r$.

Average spacing between the partition energies in the subset of strings $\mathbf{z}'$ with $D(\mathbf{z}', \mathbf{z}) = r$ equals $1/\bar{\rho}_r \sim \binom{n}{r}^{-1}$ for not too large $E_{\mathbf{z}}, E_{\mathbf{z}'}$ (see above). This spacing decreases exponentially with magnitude of the string overlap factor $|q| = |(n-2r)/n|$. Hierarchy of the subsets corresponding to different values of q form a specific structure of SPP. Distribution of energies within the hierarchy, given by $\rho_{r,\mathbf{z}}(E') \approx \bar{\rho}_r$ is nearly independent on the "ancestor" string $\mathbf{z}$. One can see that in the interval of energies $E_{\mathbf{z}} \leq E$ overlap factors q between the strings are limited by $|q| \lesssim \bar{q}$ where $1/\bar{\rho}_{n(1\pm\bar{q})/2} = E$. Strings with $E_{\mathbf{z}'} \sim E_{\min}$ correspond to $|q| = \mathcal{O}(1/n)$, they can be obtained from each other by simultaneously flipping clusters with $\approx n/2$ spins (critical clusters).

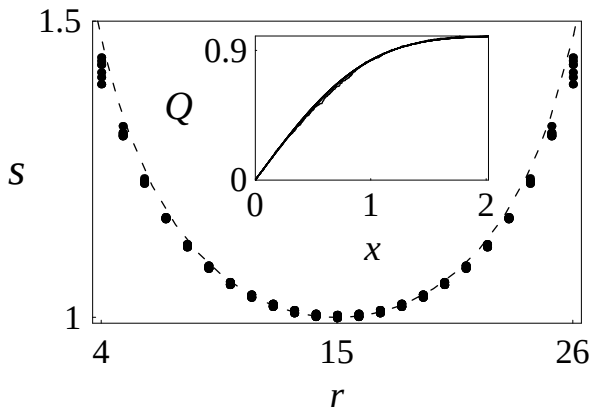

FIG. 1: Plots of (reduced) coarse-grained conditional density of states (9) $s = \sigma(\pi n/2)^{1/2}\binom{n}{r}^{-1}\rho_{r,\mathbf{z}}(0)$ *vs* r are shown with points. The size of the coarse-graining window η=0.3. Different plots correspond to 29 randomly selected bit-strings $\mathbf{z}$ with energies $E_{\mathbf{z}} \in (0, 0.3)$ for one randomly generated instance of SPP with n=30 and $b = 35$. For r close to $n/2$ values of s for different strings $\mathbf{z}$ are visually indistinguishable from each other. Dashed line is a plot of a function $\zeta(r/n)$ *vs* r given in (14). *Insert.* Plots of integrated quantity given in (A.11) $Q = \binom{n}{r}^{-1}\int_0^E d\omega\, \rho_{r,\mathbf{z}}(\omega)$ *vs* $x = E\,\zeta(r/n)/\sigma\sqrt{2n}$ for different values of $r = 2, \ldots, n/2$ and randomly selected bit-string $\mathbf{z}$ with energy $E_{\mathbf{z}}$ close to 0. All plots correspond to the same instance of SPP as the main figure. Plots for different values of r are visually indistinguishable from each other and from the theoretical curve given in (A.12).

We note that one can trivially break the symmetry of the SPP mentioned above by introducing an extra number a_0 and placing it, e.g., in the subset $\mathcal{A}$. In this case different partition energies will still be encoded by spin configurations $\mathbf{S} = \{S_1, \ldots, S_n\}$ (or corresponding bit-strings $\mathbf{z}$) with $\Omega_{\mathbf{S}} = a_0 + \sum_{j=1}^{n} a_j$ and $E_{\mathbf{z}} = |\Omega_{\mathbf{S}}|$ (cf. 3). We shall adopt this approach in the analyses of the performance of the quantum adiabatic evolution algorithm for SPP given below.

III. QUANTUM ADIABATIC EVOLUTION ALGORITHM

In the quantum adiabatic algorithm [5] one specifies the time-dependent Hamiltonian $H(t) = \tilde{H}(t/T)$

$$\tilde{H}(\tau) = (1-\tau)\,V + \tau\,H_P, \qquad (15)$$

where $\tau = t/T$ is dimensionless "time". This Hamiltonian guides the quantum evolution of the state vector $|\psi(t)\rangle$ according to the Schrödinger equation $i\,\partial|\psi(t)\rangle\partial t = H(t)|\psi(t)\rangle$ from $t = 0$ to $t = T$, the *run time* of the algorithm (we let $\hbar = 1$). H_P is the "problem" Hamiltonian given in (1). V is a "driver" Hamiltonian, that is designed to cause the transitions between the eigenstates of H_P. In this algorithm one prepares the initial state of the system $\psi(0)$ to be a ground state of $\tilde{H}(0) = V$. In the simplest case

$$V = -\sum_{j=0}^{n-1}\sigma_x^j, \quad |\psi(0)\rangle = 2^{-n/2}\sum_{\mathbf{z}}|\mathbf{z}\rangle, \qquad (16)$$

where σ_x^j is a Pauli matrix for j-th qubit. Consider instantaneous eigenstates $|\phi_\alpha(\tau)\rangle$ of $\tilde{H}(\tau)$ with energies $\lambda_\alpha(\tau)$ arranged in nondecreasing order at any value of $\tau \in (0,1)$

$$\tilde{H}|\phi_\eta\rangle = \lambda_\eta|\phi_\eta\rangle, \quad \eta = 0, 1, \ldots, 2^n - 1. \qquad (17)$$

Provided the value of T is large enough and there is a finite gap for all $t \in (0,T)$ between the ground and exited state energies, $g(\tau) = \lambda_1(\tau) - \lambda_0(\tau) > 0$, quantum evolution is adiabatic and the state of the system $|\psi(t)\rangle$ stays close to an instantaneous ground state, $|\phi_0(t/T)\rangle$ (up to a phase factor). Because $H(T) = H_P$ the final state $|\psi(T)\rangle$ is close to the ground state $|\phi_0(\tau = 1)\rangle$ of the problem Hamiltonian. Therefore a measurement performed on the quantum computer at $t = T\,(\tau = 1)$ will find one of the solutions of COP with large probability. Quantum transition away from the adiabatic ground state occurs most likely in the vicinity of the point $\tau \approx \tau^*$ where the energy gap $g(\tau)$ reaches its minimum (avoided-crossing region). The probability of the transition, $1 - |\langle\psi(t)|\phi_0(t/T)\rangle|^2_{t=T}$, is small provided that

$$T \gg \frac{|\langle\phi_1|\tilde{H}_\tau|\phi_0\rangle|_{\tau=\tau^*}}{g_{\min}^2}, \quad g_{\min} = \min_{0\le\tau\le1}\left[\lambda_1(\tau) - \lambda_0(\tau)\right], \qquad (18)$$

($\tilde{H}_\tau \equiv d\tilde{H}/d\tau$). The fraction in (18) gives an estimate for the required runtime of the algorithm and the task is to find its asymptotic behavior in the limit of large $n \gg 1$. The numerator in (18) is less than the largest eigenvalue of $\tilde{H}_\tau = H_P - V$, typically polynomial in n [5]. However, $g_{\min}$ can scale down exponentially with n and in such cases the runtime of quantum adiabatic algorithm will grow exponentially fast with the size of COP.

As suggested in [5] the quantum adiabatic algorithm can be recast within the conventional quantum computing paradigm using the technique introduced by Lloyd [20]. Continuous-time quantum evolution can be approximated by a time-ordered product of unitary operators, $e^{-i\,(1-\tau_k)V\delta}\,e^{-i\tau_k H_P\delta}$, corresponding to small time intervals $(t_k, t_k + \delta)$. Operator $e^{-i\,(1-\tau_k)V\delta}$ typically corresponds to a sequence of 1(2)-qubit gates (cf. (16)). Operator $e^{-i\tau_k H_P\delta}$ is diagonal in the computational basis $|\mathbf{z}\rangle$ and corresponds to phase rotations by angles $E_{\mathbf{z}}\delta$. Since in the case $n \ll b$, the average separation between the neighboring values of $E_{\mathbf{z}}$ is $1/\rho(E) = \mathcal{O}(2^{-n})$, the quantum device would need to support a very high precision of physical parameters (like external fields, etc) to control small differences in phases, $\mathcal{O}(2^{-n})$. Since this precision scales with n exponentially it would strongly restrict the size of an instance of SPP that could be solved on such quantum computer (this technical restriction is generic

for COPs that involve a quasi-continuous spectrum of cost-function values). To avoid this restriction we divide an interval of partition energies $(0, B)$, $B = \sum_{j=0}^{j=n} a_j$ into bins which size grows exponentially with the energy. The cost will be an oracle-type function $\mathcal{E}_{\mathbf{z}}$ that takes a set of integer values $\varepsilon_k = -M + k$, $0 \le k \le M$ (one value per bin)

$$\mathcal{E}_{\mathbf{z}} = -k + M, \text{ for } \omega_k \le E_{\mathbf{z}} < \omega_{k+1}, \tag{19}$$

$$\omega_k = (2^k - 1)\,\omega_0, \quad k = 0, \ldots, M. \tag{20}$$

The last bin is $\omega_M \le E_{\mathbf{z}} \le B$ where we have $\mathcal{E}_{\mathbf{z}} = \varepsilon_M = 0$. The Hilbert space of 2^n states $|\mathbf{z}\rangle$ is divided into $M+1$ subspaces $\mathcal{L}_k$, each determined by Eqs. (19) and (20) for a given k

$$H_P = \sum_{k=0}^{M} \epsilon_k \sum_{\mathbf{z}\in\mathcal{L}_k} |\mathbf{z}\rangle\langle\mathbf{z}|. \tag{21}$$

Note that subspace $\mathcal{L}_0$ contains the solution(s) to the SPP. Dimension d_0 of $\mathcal{L}_0$ is controlled by the value of ω_0 in (20) which is another control parameter of the algorithm. We set $\omega_0 = K/\rho(0)$ where the integer $K \approx d_0 \gg 1$ is independent of n and determines how many times in average one needs to repeat the quantum algorithm in order to obtain the solution to SPP with probability close to 1.

Operator H_P projects any state $|\psi\rangle$ onto the states with partition energies in the range $0 \le E_{\mathbf{z}} < \omega_M$. We assume that $1 \lesssim \omega_M \ll \langle E\rangle$ so that the density function (6) is nearly uniform for $E_{\mathbf{z}} \le \omega_M$. Therefore the dimensions of the subspaces $\mathcal{L}_k$ grow exponentially with k: $d_k = d_0\, 2^k$ for $k < M$. This simplification does not affect the complexity of a quantum algorithm that spends most of the time in "annealing" the system to much smaller partition energies, $\omega_M \gg E_{\mathbf{z}} \sim E_{\min} = \mathcal{O}(n^{1/2}\, 2^{-n})$.

A. Stationary Schrödinger equation for adiabatic eigenstates. Minimum gap

We now solve a stationary Schrödinger equation (17) and obtain the minimum gap $g_{\min}$ (18) in the asymptotic limit $n \to \infty$. To proceed we need to introduce a new basis of states $|\mathbf{x}\rangle = |x_1\rangle_1 \otimes |x_2\rangle_2 \otimes \cdots \otimes |x_n\rangle_n$ where state $|x_j\rangle_j$ is an eigenstate of the Pauli matrix $\hat{\sigma}_x$ for the j-th qubit with eigenvalue $1 - 2x_j = \pm 1$. Driver Hamiltonian V can be written in the following form

$$V = \sum_{m=0}^{n} V_m\, \mathcal{I}^m, \quad \mathcal{I}^m = \sum_{x_1+\cdots+x_n=m} |\mathbf{x}\rangle\langle\mathbf{x}|. \tag{22}$$

For a particular case given in Eq. (16) we have $V_m = 2m - n$. Matrix elements of $\mathcal{I}^m$ in a basis of states $|\mathbf{z}\rangle$ depend only on the Hamming distance $D(\mathbf{z}, \mathbf{z}')$ between the strings $\mathbf{z}$ and $\mathbf{z}'$

$$\langle\mathbf{z}|\mathcal{I}^m|\mathbf{z}'\rangle = I^m_{D(\mathbf{z},\mathbf{z}')} \tag{23}$$

$$I^m_r = 2^{-n} \sum_{q=0}^{n-r} \sum_{p=0}^{r} \binom{n-r}{q} \binom{r}{p} (-1)^p\, \Delta_{m,\,q+p} \tag{24}$$

We now rewrite Eq. (17) in the form

$$|\phi\rangle = \frac{\tau}{\lambda - \alpha V}\, H_P\, |\phi\rangle, \quad \alpha \equiv \alpha(\tau) = 1 - \tau. \tag{25}$$

(we drop the subscript η indicating the number of a quantum state and also the argument τ in ϕ and λ). From (19)-(25) we obtain the equation for the amplitudes $\phi_{\mathbf{z}} = \langle\mathbf{z}|\phi\rangle$ in terms of the coefficients I^m_r

$$\Lambda_k \phi_{\mathbf{z}} = \frac{\tau\Phi\, 2^{-n}}{\lambda - \alpha V_0} + \tau \sum_{\mathbf{z}'\ne\mathbf{z}} G_{D(\mathbf{z},\mathbf{z}')} \phi_{\mathbf{z}'} \mathcal{E}_{\mathbf{z}'}, \quad \mathbf{z} \in \mathcal{L}_k \tag{26}$$

$$\Lambda_k \equiv \Lambda_k(\lambda) = 1 - \tau\, G_0(\lambda)\, \varepsilon_k, \quad \Phi = \sum_{\mathbf{z}'} \mathcal{E}_{\mathbf{z}'} \phi_{\mathbf{z}'}.$$

$$G_r \equiv G_r(\lambda) = \sum_{m=1}^{n} \frac{I^m_r}{\lambda - \alpha V_m}, \quad 0 \le r \le n.$$

Here we separated out a "symmetric" term $\propto 2^{-n}\Phi$ corresponding to the coupling between the states $|\mathbf{z}\rangle$ via the projection operator $\mathcal{I}^0$ (22).

We now make a key observation that $\phi_{\mathbf{z}}$ in (26) can be determined based on the properties of conditional density of states $\rho_{r,\mathbf{z}}(E)$ (9) and the form of $G_r(\lambda)$. We compute a cumulative quantity

$$\sum_{\mathbf{z}\in\mathcal{L}_k,\, \mathbf{z}\ne\mathbf{z}'} G_{D(\mathbf{z},\mathbf{z}')}(\lambda) \approx F_k(\lambda) + f_{\mathbf{z}',k}(\lambda) \tag{27}$$

$$F_k(\lambda) = \frac{\mu\, s(\lambda)}{2^{M-k}}, \quad s(\lambda) = \int_0^n dr\, \zeta(r/n) \binom{n}{r} G_r(\lambda) \tag{28}$$

where $\mu = 2\Omega_M/\pi\langle E\rangle$, function $\zeta(x)$ is defined in (14) and $f_{\mathbf{z}',k}(\lambda)$ is a small correction described below. In function $s(\lambda)$ we replaced summation over the integer values of r by an integral. It can be evaluated using the explicit form of $G_r(\lambda)$ that decays rapidly with r. In what follows we will be interested in the region $|\lambda - \alpha V_0| \ll 1$ where

$$G_r(\lambda) = \binom{n}{r}^{-1} \sum_{m=1}^{n-r} \frac{2^{-n}\binom{n}{m+r}}{m} - 2^{-n}\,(\ln r + \gamma)\,. \tag{29}$$

(γ is an Euler's constant) and $s(\lambda) \approx -\ln 2/(2\alpha)$. We note that $G_r \approx (n/2-r)^{-1}\binom{n}{r}^{-1}$ for $n/2 - r \gg 1$. Therefore the integrand in $s(\lambda)$ is a smooth function of r for $r \lesssim n/2$ and quickly decays to zero for $r \gtrsim n/2$. The contribution to the integral in $s(\lambda)$ from the range of $r \ll n$ is small ($\mathcal{O}((r/n)^{1/2})$).

We note that term F_k in (27) provides an "entropic" contribution to the sum in (27). It comes from the large number of states $\mathbf{z} \in \mathcal{L}_k$ corresponding to large Hamming distances r from the state $\mathbf{z}'$, $1 \ll r \lesssim n/2$. Each state contributes a small weight, $G_r \propto \binom{n}{r}^{-1}$, and number of

states for a given r is large, $(\omega_{k+1}-\omega_k)\bar{\rho}_r \gg 1$. Here $(\omega_{k+1}-\omega_k)$ is an energy bin for the subspace $\mathcal{L}_k$ and $\bar{\rho}_r$ is a conditional density of states described in Sec. II. The size of the bin scales down exponentially with k (cf. (20)) and so does the entropic term F_k. Below a certain cross-over value of k one has $|F_k| \ll |f_{\mathbf{z}',k}(\lambda)|$. In this case the dominant contribution to the sum (27) comes from the states $\mathbf{z}$ with small $r = D(\mathbf{z},\mathbf{z}') \sim 1$. In particular for $k=0$ one can obtain

$$f_{\mathbf{z}',0}(\lambda) \approx G_1(\lambda) \sum_{\mathbf{w}\in\mathcal{L}_0} \delta_{1,D(\mathbf{z}',\mathbf{w})} + \mathcal{O}(n^{-3}), \qquad (30)$$

where the higher-order terms corresponds to $D(\mathbf{z}',\mathbf{w}) \geq 2$. According to (29), $|G_1(\lambda)| \sim n^{-2}$ and therefore $|f_{\mathbf{z},0}|$ is exponentially larger then the entropic term, $|F_0| \sim \omega_0 \sim d_0\, 2^{-n}$. We note that, unlike the entropic term $f_{\mathbf{z}',0}$ strongly depends on $\mathbf{z}'$ due to the discreteness of the partition energy spectrum ($\omega_0\,\bar{\rho}_1 \ll 1$). E.g., depending on a state $\mathbf{z}'$, in this case there could be either one or *none* of the states $\mathbf{w} \in \mathcal{L}_0$ in the sum (30) satisfying $D(\mathbf{z}',\mathbf{w}) = 1$.

It follows from the discussion above that one can look for solution of Eq. (26) in the following form:

$$\phi_{\mathbf{z}} = v_k + u_{\mathbf{z}}, \quad \mathbf{z}\in\mathcal{L}_k, \quad 1 \leq k \leq M, \qquad (31)$$

where the components v_k and $u_{\mathbf{z}}$ satisfy the equations

$$\Lambda_k\, v_k = 2^{-n}\tau \left[\Phi\,(\lambda-\alpha V_0)^{-1} + s(\lambda)\overline{\Phi}\right], \qquad (32)$$

$$\Lambda_k\, u_{\mathbf{z}} = \tau \sum_{k=1}^{M} \varepsilon_k \sum_{\mathbf{z}'\in\mathcal{L}_k} G_{D(\mathbf{z},\mathbf{z}')}\, u_{\mathbf{z}'} + \tau\varepsilon_0 \sum_{\mathbf{w}\in\mathcal{L}_0} G_{D(\mathbf{z},\mathbf{w})}\phi_{\mathbf{w}}. \qquad (33)$$

Here Φ and Λ_k are given in (26), and

$$\overline{\Phi} = \sum_{k=1}^{M} \varepsilon_k d_k v_k. \qquad (34)$$

Decomposition (31) is only applied to amplitudes $\phi_{\mathbf{z}}$ with $\mathbf{z}\notin\mathcal{L}_0$. The system of equations for the components v_k and $u_{\mathbf{z}}$ is closed by adding Eq. (26) for the amplitudes $\phi_{\mathbf{w}}$ with $\mathbf{w}\in\mathcal{L}_0$ (ground states of the final Hamiltonian H_P) and taking (31) into account.

We note that Eq.(32) for v_k is coupled to the rest of the equations via the symmetric term Φ

$$\Phi = \overline{\Phi} + \widetilde{\Phi} + \Phi_0 \qquad (35)$$
$$\widetilde{\Phi} = \sum_{k=1}^{M} \varepsilon_k \sum_{\mathbf{z}\in\mathcal{L}_k} \widetilde{u}_{\mathbf{z}}, \quad \Phi_0 = \varepsilon_0 \sum_{\mathbf{w}\in\mathcal{L}_0} \phi_{\mathbf{w}},$$

One can compute $\widetilde{\Phi}$ using equations for $u_{\mathbf{z}}$ in (33) and also the relations in (27), (28)

$$\widetilde{\Phi} = -\kappa\left(\tau\mu s(\lambda)\right)\Phi_0, \qquad (36)$$

here $\kappa(x) = x/(1+x)$. In the initial stage of the algorithm the amplitudes $\phi_{\mathbf{w}}$ of the "solution" states are small and $|\Phi_0| \sim |\widetilde{\Phi}| \sim 2^{-n/2}$. Neglecting these terms we have $\Phi \approx \overline{\Phi}$, and (32) gives a closed-form algebraic equation for λ which solution

$$\lambda_0^i(\tau) \approx \alpha(\tau)V_0 - 2\mu\tau + \mathcal{O}(\mu^2), \qquad (37)$$

accurately tracks the adiabatic ground state energy, $\lambda_0(\tau)$, from $\tau = 0$, up until small vicinity of the avoided-crossing, $\tau \approx \tau^*$ (see below) where $|\Phi_0| \sim 1$.

In the avoided-crossing region branch $\lambda_0^i(\tau)$ intersects with another branch, $\lambda_0^f(\tau)$, that tracks $\lambda_0(\tau)$ in the interval of time following the avoided-crossing, $\tau^* < \tau \leq 1$. This branch can be obtained from simultaneous solution of equations for $u_{\mathbf{z}}$ (33) and $\phi_{\mathbf{w}}$ that are approximately decoupled from (32) after $\bar{\Phi}$ is neglected. Keeping this term gives rise to repulsion between branches $\lambda_0^{i,\,f}(\tau)$ at $\tau = \tau^*$ that determines minimum gap $g_{\min}$.

To proceed, we obtain equation for Φ_0 by adding equations for amplitudes $\phi_{\mathbf{w}}$ that correspond to different states $\mathbf{w} \in \mathcal{L}_0$ and neglecting the coupling between these states separated by large Hamming distances, $D(\mathbf{w},\mathbf{w}') \sim n/2$. It can be shown using Eqs. (26) and (30)-(33) that $u_{\mathbf{z}}$ enters equation for Φ_0 through the term

$$\tau^2\varepsilon_0 \sum_{\mathbf{z}\notin\mathcal{L}_0} \mathcal{E}_{\mathbf{z}} f_{\mathbf{z},0}(\lambda) u_{\mathbf{z}}, \qquad (38)$$

which is is a self-energy term corresponding to elementary bit-flip processes with initial and final states belonging to the subspace $\mathcal{L}_0$ (loop diagrams).

To express $u_{\mathbf{z}}$ in (38) through $\phi_{\mathbf{w}}$ we solve Eq. (33) using order-by-order expansion in a small parameter n^{-1} (cf. Eqs. (27)-(30) and discussion there). In particular, one can show that to the leading order in n^{-1} self-energy term (38) is determined by lowest-order loops with two bit flips that begin and end at $\mathcal{L}_0$. Then after some transformations equation for Φ_0 takes a form

$$\Phi_0\left(\lambda - \tau\varepsilon_0 - \frac{\tau\alpha^2\varepsilon_0}{\lambda}\sum_{\mathbf{z}'\notin\mathcal{L}_0}\frac{\delta_{1,D(\mathbf{z}',\mathbf{w})}}{\lambda-\tau\mathcal{E}_{\mathbf{z}'}}\right)$$
$$= \lambda\varepsilon_0\tau d_0 2^{-n}\left(\frac{\Phi}{\lambda-\alpha V_0)} + \bar{\Phi}\, s(\lambda)\right). \qquad (39)$$

Here $\alpha = 1-\tau$ (cf. (25) and $\bar{\Phi}$ is defined above. We now solve Eq. (39) jointly with (32) and obtain a closed-form equation for λ. We give it below in the region of interest $|\tau - 1/2| \ll 1$

$$\left(\lambda - \lambda_0^{\rm i}(\tau)\right)\left(\lambda - \lambda_0^{\rm f}(\tau)\right) = -n^2 2^{-n}\Delta^2/4 \qquad (40)$$
$$\Delta \approx d_0^{1/2}\left(1 + \mu\tau^*\ln 2 + \mathcal{O}(\mu^2)\right),$$

where the branch $\lambda_0^{\rm i}(\tau)$ is given above and the branch $\lambda_0^{\rm f}(\tau)$ satisfies Eq. (39) with r.h.s. there set to zero,

$$\lambda_0^{\rm f}(\tau) \approx \tau\varepsilon_0 - 1/2, \quad |\tau - 1/2| \ll 1. \qquad (41)$$

Avoided-crossing in (40) takes place at $\tau = \tau^*$

$$\lambda_0^{\rm i}(\tau^*) = \lambda_0^{\rm f}(\tau^*), \quad \tau^* \approx 1/2 + \log_2(d_0/\mu)/(4n). \qquad (42)$$

The value of minimum gap between the two roots of (40) equals

$$g_{\min} = n\,\Delta\,2^{-n/2}. \tag{43}$$

Based on the above analysis one can estimate the matrix element $|\langle\phi_1|\tilde{H}_\tau|\phi_0\rangle|_{\tau=\tau^*} \sim n$. Then from Eq. (18) (see also discussion after Eq. (21)) one can obtain the complexity of the quantum adiabatic algorithm

$$d_0\,H^*_{\tau 01}/g^2_{\min} \sim (n\,d_0)^{-1}2^n. \tag{44}$$

It follows from the above that eigenvalue branch $\lambda^{\rm i}_0(\tau)$ corresponds to a state,

$$|\phi_0\rangle \approx \sum_{k=1}^{M} v_k \sum_{\mathbf{z}\in\mathcal{L}_k} |\mathbf{z}\rangle$$

which is *extended* in the space of the bit configurations $|\mathbf{z}\rangle$: according to (32) it contains large number ($\mathcal{O}(2^n)$) of exponentially small ($\mathcal{O}(2^{-n/2})$) individual amplitudes. This state originates at $\tau = 0$ from the totally symmetric initial state $|\psi(0)\rangle$ (16). In the small region $|\tau - \tau^*| \sim g_{\min}$ it is transformed into the state that corresponds to the eigenvalue branch $\lambda^{\rm f}_0(\tau)$ and is *localized* in Hamming distances near the subspace $\mathcal{L}_0$ containing the solution to SPP

$$|\phi_0\rangle \approx \sum_{\mathbf{w}\in\mathcal{L}_0} |\mathbf{w}\rangle$$

(this state merges with $\mathcal{L}_0$ at τ=1).

We note that at later times $\tau > \tau^*$ similar picture applies to the avoided crossing of the extended-state energy $\lambda^{\rm i}_0(\tau)$ with energies of localized states $\lambda^{\rm f}_k(\tau)$ corresponding to $\mathbf{z} \in \mathcal{L}_k$ with $1 \le k \ll n$ (exited levels of the final Hamiltonian H_P (21)). The existence of the extended eigenstate of $\tilde{H}(\tau)$ whos properties do not depend on a particular instance of SPP can be explained as follows. According to (22)-(26), matrix elements of the Green function associated with the driver Hamiltonian $\langle\mathbf{z}'|(\lambda - \alpha V)^{-1}|\mathbf{z}\rangle$ depend only on a Hamming distance $r = d(\mathbf{z},\mathbf{z}')$; on the other hand, the conditional distribution $\rho_r(E', E_{\mathbf{z}}) \approx \bar{\rho}_r$ does not depend on energies in a broad range $1 \lesssim E', E_{\mathbf{z}} \ll \langle E\rangle$. This gives rise to an eigenstate with probability amplitude of individual states $|\mathbf{z}\rangle$ that depends very smoothly on energy in this range but does *not* depend on the Hamming distance to the solution.

B. Numerical results

We also study the complexity of the algorithm by numerical integration of the time-dependent Schrödinger equation with Hamiltonian $H(t)$ and initial state $|\psi(0)\rangle$ defined in Eqs. (15),(16),(19)-(21). Here we relax the condition $\omega_M \ll \langle E\rangle$ used above in the analytical treatment of the problem; in simulations the value of M is set automatically to be an integer closest to $\log_2 \sum_{j=0}^{n} a_j$ (cf. (20)). We introduce a complexity metric for the algorithm, $C(T) = (1+T)d_0/p_0(T)$ where $p_0(t) = \sum_{\mathbf{w}\in\mathcal{L}_0} |\psi_{\mathbf{w}}(t)|^2$. A typical plot of $C(T)$ for an instance of the problem with n=15 numbers is shown in the insert of Fig. 1. At very small T the wavefunction is close to the symmetric initial state and the complexity is $\sim 2^n$. The extremely sharp decrease in $C(T)$ with T is due to the buildup of the population $p_0(T)$ in the ground level, $\mathcal{E}_{\mathbf{z}} = \varepsilon_0$, as quantum evolution approaches the adiabatic limit. At certain $T = T_{\min}$ the function $C(T)$ goes through the minimum: for $T > T_{\min}$ the decrease in the number of trials $d_0/p_0(T)$ does not compensate anymore for the overall increase in the runtime T for each trial. For a given problem instance the "minimum" complexity $C_{\min} = C(T_{\min})$ is obtained via one dimensional minimization over T. Plot of the complexity $C_{\min}$ for different values of n in Fig. 1 appears to indicate the exponential scaling law, $C_{\min} \sim 2^{0.8n}$ for not too small values of $n \gtrsim 11$.

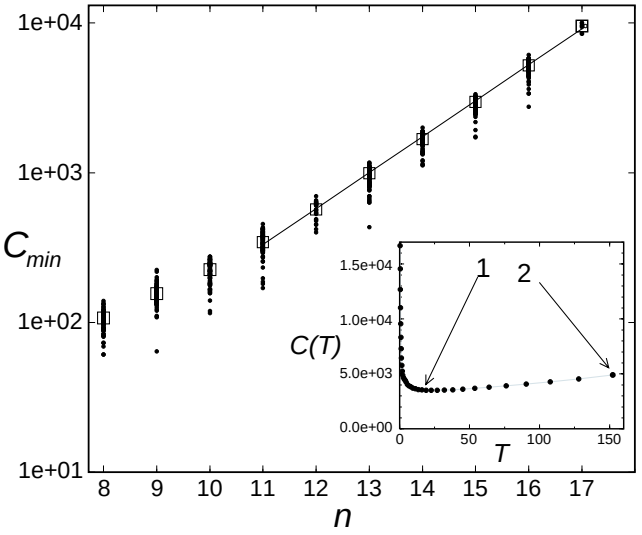

FIG. 2: Logarithmic plot of $C_{\min}$ *vs* n for randomly generated instances of SPP with 25-bit precision numbers. Vertical sets of points indicate results of different trials ($\sim$ 100 trials for each n, except n=17 with 10 trials). Median values of $C_{\min}$ are shown with rectangles. Linear fit to the logarithmic plot of median values for n between 11 and 17 is shown by the line and gives $\ln C_{\min} \approx 0.55$n ($C_{\min} \sim 2^{0.8n}$) . Very close result is obtained for the linear fit if all data points are used instead of the median values. *Insert*: plot of $C(T)$ *vs* T for n=15, precision b=25 bits, d_0=22. Point 1 indicated with the arrow refers to the minimum value of complexity at $T = T_{\min} = 22.67$ where the total population of a ground level $p_0(T_{\min}) = 0.15$. Point 2 refers to the value of T where $p_0(T) = 0.7$.

IV. CONCLUSION

In conclusion, we have developed a general method for the analysis of avoided-crossing phenomenon in quantum

spin-glass problems and used it to study the performance of quantum adiabatic evolution algorithm on random instances of Set Partition problem. We described the onset of avoiding-crossing during the algorithm where adiabatic ground state changes from the extended in the energy space to mostly localized near the minimum energy of the optimization problem. Because the extended and localized state amplitudes are nearly orthogonal to each other the repulsion between the corresponding branches of eigenvalues (the minimum gap) is exponentially small, $g_{\min} \sim n\, 2^{-n/2}$, and the run time of the algorithm scales exponentially with n. Analytical results are in qualitative agreement with numerical results for small-to-moderate instances of Set Partition problem.

This method can be applied to study the performance of continuous-time quantum algorithms for different random combinatorial optimization problems. Among the other possible applications is the analysis of tunneling phenomenon in the low-temperature dynamics of random magnets.

The authors benefited from stimulating discussions with D. A. Timucin, and R.D. Morris. This research was supported by NASA Intelligent Systems Revolutionary Computing Algorithms program (project No: 749-40), and also by NASA Ames NAS Center.

APPENDIX: CONDITIONAL DENSITY OF STATES

Using the symmetry of the SPP we write $\rho_r(E', E)$ from Eqs. (9),(10) in the following form:

$$\rho_r(E', E) = \sum_{s=\pm 1} \sum_{s'=\pm 1} \tilde{\rho}_r(s\,E, s'E'). \qquad \text{(A.1)}$$

Here $\tilde{\rho}_r(\Omega, \Omega')$ is the joint distribution function of the unsigned partition residues (cf. Eq. (7))

$$\tilde{\rho}_r(\Omega, \Omega') = \frac{1}{\eta\,\eta'} \int_{\Omega-\eta/2}^{\Omega+\eta/2} dx \int_{\Omega'-\eta'/2}^{\Omega'+\eta'/2} dx' \sum_{\mathbf{S}} \sum_{\mathbf{S}'} \delta_{r,\tilde{D}(\mathbf{S},\mathbf{S}')} \delta(\Omega - \Omega_{\mathbf{S}}) \delta(\Omega' - \Omega_{\mathbf{S}'}), \quad \tilde{D}(\mathbf{S}, \mathbf{S}') = \frac{1}{2} \sum_{j=1}^{n} |S_j - S'_j|. \qquad \text{(A.2)}$$

Here $\tilde{D}(\mathbf{S}, \mathbf{S}')$ is a Hamming distance between the spin configurations $\mathbf{S}$,$\mathbf{S}'$ (cf. (11)). Using integral representation for delta function we perform summation of the spin configurations in (A.2) and obtain (cf. Eq.(5))
U

$$\tilde{\rho}_r(\Omega, \Omega') = \frac{2^n}{4\pi^2} \int_{-\infty}^{\infty} ds \int_{-\infty}^{\infty} ds' f\left(\frac{\eta s}{2}\right) f\left(\frac{\eta' s'}{2}\right) \times e^{i(s\Omega + s'\Omega')} U_r(s, s'). \qquad \text{(A.3)}$$

$$U_r(s, s') = \sum_{\mathbf{J}} \prod_{j \in \mathbf{J}} \cos(a_j(s - s')) \prod_{j \notin \mathbf{J}} \cos(a_j(s + s')).$$

Here the sum is over all possible subsets $\mathbf{J} = \{j_1, j_2, \ldots, j_r\}$ of the length r obtained from the set of integers $j = 1, 2, \ldots, n$. Window function $f(x)$ is defined in (5). Similar to the analyses of Eq.(5) integrals in (27) can be evaluated by steepest descent method. With appropriate choice of the coarse-graining windows η, η' (see below) contribution to the integrals comes from the vicinity of the point $(s = 0, s' = 0)$. Near this point we use

$$U_r(s, s') = \sum_{\mathbf{J}} \exp\left(-\frac{r}{2}(s - s')^2 \sigma_1^2(\mathbf{J}) - \frac{n - r}{2}(s + s')^2 \sigma_2^2(\mathbf{J})\right) \qquad \text{(A.5)}$$

where

$$\sigma_1^2(\mathbf{J}) = \frac{1}{r} \sum_{j \in \mathbf{J}} a_j^2, \quad \sigma_2^2(\mathbf{J}) = \frac{1}{n - r} \sum_{j \notin \mathbf{J}} a_j^2.$$

For $r, n - r \gg 1$ and i.i.d. random numbers $\{a_j\}$ one has

$$\sigma_1^2(\mathbf{J}) \approx \sigma_2^2(\mathbf{J}) \approx \sigma^2, \qquad \text{(A.7)}$$

where $\sigma^2 = \langle a^2 \rangle$ is given in (6). Using (A.5),(A.7) and replacing window functions in (A.3) by unity, we compute the Gaussian integrals in (A.3) and obtain

$$\tilde{\rho}_r(\Omega, \Omega') = \frac{2^n \binom{n}{r}}{4\pi\sigma^2 \sqrt{r(n - r)}} \exp\left[-\frac{1}{8\sigma^2}\left(\frac{(\Omega + \Omega')^2}{r} + \frac{(\Omega + \Omega')^2}{n - r}\right)\right]. \qquad \text{(A.8)}$$

The size of coarse-graining windows in (A.3) is chosen self-consistently, $1/\rho_r(\Omega, \Omega') \ll r^{1/2}, n - r^{1/2}$.

Finally, using (A.1) and (A.8) we obtain the joint conditional density of states

$$\rho_r(E, E') = \frac{2^{n+1} \zeta(r/n) \binom{n}{r}}{\pi n \sigma^2} \exp\left[-\frac{(E^2 + E'^2)\zeta^2(r/n)}{2n\sigma^2}\right] \times \cosh\left[\frac{E\,E'\zeta^2(r/n)}{n\sigma^2}\left(1 - \frac{2r}{n}\right)\right]. \qquad \text{(A.9)}$$

From the equation above and Eq. (6) one can directly obtain conditional density of states $\rho_r(E|E')$ (8). Expression for $\rho_r(E|E')$ in the case of relatively small energies E, E' is given in (14).

We note that $\rho_r(E|E')$ is obtained by coarse-graining with respect to both energy arguments (cf. (A.2)). How-

ever our numerical results indicate that the following approximate equality holds:

$$\rho_r(E'|E_{\mathbf{z}}) \approx \rho_{r,\mathbf{z}}(E'), \quad E', E_{\mathbf{z}} \ll n. \tag{A.10}$$

(We were able to derive this relation analytically only with an accuracy to pre-exponential factor which is small compare to $\binom{n}{r} \gg 1$). To illustrate this relation numerically we compute the following quantity

$$Q = \binom{n}{r}^{-1} \int_0^{E'} d\omega \rho_{r,\mathbf{z}}(\omega) \tag{A.11}$$

for different r and strings $\mathbf{z}$ with $E_{\mathbf{z}} \ll 1$. The results are presented in the insert to Fig. 1. Curves corresponding to different r are nearly coincide with each other and with the theoretical curve computed using $\rho_r(E'|E)$

$$\binom{n}{r}^{-1} \int_0^{E'} d\omega \rho_r(\omega|0) = \mathrm{erf}\left(\frac{E'\zeta(r/n)}{\sigma\sqrt{2n}}\right). \tag{A.12}$$

To accurately compare prefactors in (A.10) we compute $\rho_r(0|E_{\mathbf{z}})$ for different r and strings $\mathbf{z}$ with $E_{\mathbf{z}} \ll 1$. We then compare these values with theoretical result for $\rho_r(0|E_{\mathbf{z}})$. The results are plotted in Fig. 1.

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

[2] Y. Fu and P.W. Anderson, J. Phys. A: Math. Gen. **19**, 1605-1620 (1986).

[3] M. Mezard, G. Parizi, and M. Virasoro, *Spin glass theory and beyond* (World Scientific, Singapore, 1987).

[4] M.R. Garey and D.S. Johnson, *Computers and Intractability. A Guide to the Theory of NP-Completeness* (W.H. Freeman, New York, 1997)

[5] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, arXiv:quant-ph/0001106.

[6] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, *Science* **292**, 472 (2001).

[7] E. Farhi, J. Goldstone, and S. Gutmann, arXiv:quant-ph/0007071.

[8] A. M. Childs, E. Farhi, J. Goldstone, and S. Gutmann, arXiv:quant-ph/0012104.

[9] E. Farhi, J. Goldstone, S. Gutmann, arXiv:quant-ph/0201031.

[10] Li-Hui Tsai, SIAM J. Comput., **21**(1) p.59-64 (1992).

[11] A. Shamir, *Proc. of 11th Annual ACM Symposium on Theory of Computing*, p.118 (1979).

[12] D.S. Johnson, et al., Operations Research **39**, p.378 (1991).

[13] F.F. Ferreira and J. F. Fontanari, J. Phys. A **31**, p. 3417 (1998).

[14] I.P. Gent and T. Walsh, in Proc. of the ECAI-96, ed. by W. Wahlster (John-Wiley & Sons, New York, 1996), pp. 170-174.

[15] R.E. Korf, Artificial Intelligence **106**, 181 (1998).

[16] S. Mertens, Phys. Rev.Lett. **81**, 4281–4284 (1998).

[17] Artif. Intel. **81** (1-2) (1996), special issue on Topic, ed. by T. Hogg, B.A. Huberman, and C. Williams.

[18] S. Mertens, Phys. Rev.Lett. **84**, 1347–1350 (2000).

[19] It can be shown that for $n \lesssim b$ function $I(w)$ in (5) has additional sharp resonances in the range $0 < |w| < w_1 = 2^b$. They occur at the multiples of π/q where $q \gg 2^{-b}$ is an *approximate* greatest common divisor (g.c.d.) of the subset of numbers a_j of length $p \sim n$ such that for the numbers in this subset the residues $r(j)$ of the division a_j/q are small: $\sum_{m=1}^{p} r^2(j_m) \lesssim 2q^2/\pi^2$. However for the high-precision case $b \gg n$ one can show that these resonances fall outside the range of the window function in (5) and their contribution to the integral in (5) can be neglected. The transition region $n \sim b$ requires special consideration and will be considered elsewhere.

[20] S. Lloyd, Science **273**, 1073 (1996).