Quantum Computation by Adiabatic Evolution

Edward Farhi, Jeffrey Goldstone[*]
Center for Theoretical Physics
Massachusetts Institute of Technology
Cambridge, MA 02139

Sam Gutmann[†]
Department of Mathematics
Northeastern University
Boston, MA 02115

Michael Sipser[‡]
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139

Abstract

We give a quantum algorithm for solving instances of the satisfiability problem, based on adiabatic evolution. The evolution of the quantum state is governed by a time-dependent Hamiltonian that interpolates between an initial Hamiltonian, whose ground state is easy to construct, and a final Hamiltonian, whose ground state encodes the satisfying assignment. To ensure that the system evolves to the desired final ground state, the evolution time must be big enough. The time required depends on the minimum energy difference between the two lowest states of the interpolating Hamiltonian. We are unable to estimate this gap in general. We give some special symmetric cases of the satisfiability problem where the symmetry allows us to estimate the gap and we show that, in these cases, our algorithm runs in polynomial time.

1   Introduction

We present a quantum algorithm for the satisfiability problem (and other combinatorial search problems) that works on the principle of quantum adiabatic evolution.

An n-bit instance of satisfiability is a formula

$$C_1 \wedge C_2 \wedge \cdots \wedge C_M \tag{1.1}$$

where each clause C_a is True or False depending on the values of some subset of the bits. For a single clause, involving only a few bits, it is easy to imagine constructing a quantum device that evolves to a state that encodes the satisfying assignments of the clause. The real difficulty, of course, lies in constructing a device that produces an assignment that satisfies all M clauses.

Our algorithm is specified by an initial state in an n-qubit Hilbert space and a time-dependent Hamiltonian $H(t)$ that governs the state's evolution according to the Schrödinger equation. The Hamiltonian takes the form

$$H(t) = H_{C_1}(t) + H_{C_2}(t) + \cdots + H_{C_M}(t) \tag{1.2}$$

where each H_{C_a} depends only on clause C_a and acts only on the bits in C_a. $H(t)$ is defined for t between 0 and T and is slowly varying. The initial state, which is always the same and easy to construct, is the ground state of $H(0)$. For each a, the ground state of $H_{C_a}(T)$ encodes the satisfying assignments of clause C_a. The ground state of $H(T)$ encodes the satisfying assignments of the intersection of all the clauses. According to the adiabatic theorem, if the evolution time T is big enough, the state of the system at time T will be very close to the ground state of $H(T)$, thus producing the desired solution. For this algorithm to be considered successful we require that T grow only polynomially in n, the number of bits. In this paper we analyze three examples where T grows only polynomially in n. We are unable to estimate the required running time T in general.

The quantum adiabatic evolution that we are using should not be confused with cooling. For example, simulated annealing is a classical algorithm that attempts to find the lowest energy configuration of what we have called $H(T)$ by generating the stochastic distribution proportional to $e^{-\beta H(T)}$, where β is the inverse temperature, and gradually lowering the temperature to zero. In contrast, quantum adiabatic evolution forces the state of the system to remain in the ground state of the slowly varying $H(t)$.

In Section 2 we present the building blocks of our algorithm in detail. This includes some discussion of the adiabatic theorem and level crossings. In Section 3 we illustrate the method on a small example that has three clauses, each acting on 2 bits. Each 2-bit clause has more than one satisfying assignment but adiabatic evolution using $H(t)$ of the form (1.2) produces the unique common satisfying assignment. In Section 4 we look at examples that grow with the number of bits in order to study the dependence of the required running time on the number of bits. We give three examples of 2-SAT problems, each of which has a regular structure, which allows us to analyze the quantum evolution. In these three cases the required evolution time T is only polynomially big in the number of bits. We also look at a version of the Grover problem that can be viewed as a relativized satisfiability problem. In this case our algorithm requires exponential time to produce a solution. This had to be so, as explained in Section 4.2.

In Section 5 we show that our algorithm can be recast within the conventional paradigm of quantum computing, involving sequences of few-bit unitary operators.

2   Adiabatic Evolution for Solving Satisfiability

In this section we present a quantum algorithm for solving satisfiability problems.

2.1   The Adiabatic Theorem

A quantum system evolves according to the Schrödinger equation

$$i\frac{\mathrm{d}}{\mathrm{d}t}\left|\psi(t)\right\rangle = H(t)\left|\psi(t)\right\rangle \tag{2.1}$$

and the adiabatic theorem [1] tells us how to follow this evolution in the case that $H(t)$ is slowly varying. Consider a smooth one-parameter family of Hamiltonians $\widetilde{H}(s), 0 \leq s \leq 1$, and take

$$H(t) = \widetilde{H}(t/T) \tag{2.2}$$

so that T controls the rate at which $H(t)$ varies. Define the instantaneous eigenstates and eigenvalues of $\widetilde{H}(s)$ by

$$H(s)\left|\ell; s\right\rangle = E_\ell(s)\left|\ell; s\right\rangle \tag{2.3}$$

with

$$E_0(s) \leq E_1(s) \leq \cdots \leq E_{N-1}(s) \tag{2.4}$$

where N is the dimension of the Hilbert space. Suppose $|\psi(0)\rangle$ is the ground state of $\widetilde{H}(0)$, that is,

$$|\psi(0)\rangle = |\ell = 0; s = 0\rangle . \tag{2.5}$$

According to the adiabatic theorem, if the gap between the two lowest levels, $E_1(s) - E_0(s)$, is strictly greater than zero for all $0 \leq s \leq 1$, then

$$\lim_{T \to \infty} |\langle \ell = 0; s = 1 | \psi(T)\rangle| = 1 . \tag{2.6}$$

This means that the existence of a nonzero gap guarantees that $|\psi(t)\rangle$ obeying (2.1) remains very close to the instantaneous ground state of $H(t)$ of the form (2.2) for all t from 0 to T if T is big enough. Let us define the minimum gap by

$$g_{\min} = \min_{0 \leq s \leq 1} \left(E_1(s) - E_0(s) \right) . \tag{2.7}$$

A closer look at the adiabatic theorem tells us that taking

$$T \gg \frac{\mathcal{E}}{g_{\min}^2} \tag{2.8}$$

where

$$\mathcal{E} = \max_{0 \leq s \leq 1} \left| \left\langle \ell = 1; s \left| \frac{\mathrm{d}\widetilde{H}}{\mathrm{d}s} \right| \ell = 0; s \right\rangle \right| \tag{2.9}$$

can make

$$\left| \langle \ell = 0; s = 1 | \psi(T)\rangle \right| \tag{2.10}$$

arbitrarily close to 1. For all of the problems that we study $\mathcal{E}$ is of order a typical eigenvalue of H and is not too big, so the size of T is governed by $g_{\min}^{-2}$.

2.2 The Satisfiability Problem

Many computationally interesting problems can be recast into an equivalent problem of finding a variable assignment that minimizes an "energy" function. As a specific example, consider 3-SAT. An n-bit instance of 3-SAT is a Boolean formula, (1.1), that is specified by a collection of Boolean clauses, each of which involves (at most) 3 of the n bits. Each bit z_i can take the value 0 or 1 and the i label runs from 1 to n. Clause C is associated with the 3 bits labeled i_C, j_C, and k_C. For each clause C we define an energy function

$$h_C(z_{i_C}, z_{j_C}, z_{k_C}) = \begin{cases} 0 , & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ satisfies clause } C \\ 1 , & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ violates clause } C. \end{cases} \tag{2.11}$$

We then define the total energy h as the sum of the individual h_C's,

$$h = \sum_C h_C . \tag{2.12}$$

Clearly $h \geq 0$ and $h(z_1, z_2, \ldots, z_n) = 0$ if and only if $(z_1, z_2, \ldots, z_n)$ satisfies all of the clauses. Thus finding the minimum energy configuration of h tells us if the formula has a satisfying assignment.

We will not distinguish between conventional clauses, which compute the OR function of each constituent variable or negated variable, and generalized clauses, which are permitted to compute an arbitrary Boolean function of the constituent variables. In some of our examples it will be more convenient to consider generalized clauses.

2.3   The Problem Hamiltonian H_{P}

If we go from classical to quantum computation we replace the bit z_i by a spin-$\frac{1}{2}$ qubit labeled by $|z_i\rangle$ where $z_i = 0, 1$. The states $|z_i\rangle$ are eigenstates of the z component of the i-th spin,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.13}$$

so

$$\tfrac{1}{2}(1 - \sigma_z^{(i)})\,|z_i\rangle = z_i\,|z_i\rangle \quad \text{where} \quad \sigma_z^{(i)} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.14}$$

The Hilbert space is spanned by the $N = 2^n$ basis vectors $|z_1\rangle\,|z_2\rangle\cdots|z_n\rangle$. Clause C is now associated with the operator $H_{\mathrm{P},C}$,

$$H_{\mathrm{P},C}(|z_1\rangle\,|z_2\rangle\cdots|z_n\rangle) = h_C(z_{i_C}, z_{j_C}, z_{k_C})\,|z_1\rangle\,|z_2\rangle\cdots|z_n\rangle \ . \tag{2.15}$$

The Hamiltonian associated with all of the clauses, which we call H_{P},

$$H_{\mathrm{P}} = \sum_C H_{\mathrm{P},C} \tag{2.16}$$

is the sum of Hamiltonians each of which acts on a fixed number of bits. By construction, H_{P} is nonnegative, that is, $\langle \psi |\, H_{\mathrm{P}}\, |\psi\rangle \geq 0$ for all $|\psi\rangle$ and $H_{\mathrm{P}}\,|\psi\rangle = 0$ if and only if $|\psi\rangle$ is a superposition of states of the form $|z_1\rangle\,|z_2\rangle\cdots|z_n\rangle$ where $z_1, z_2, \ldots, z_n$ satisfy all of the clauses. In this context, solving a 3-SAT problem is equivalent to finding the ground state of a Hamiltonian. Clearly many other computationally interesting problems can be recast in this form.

2.4   The Initial Hamiltonian H_{B}

For a given problem, specifying H_{P} is straightforward but finding its ground state may be difficult. We now consider an n-bit Hamiltonian H_{B} that is also straightforward to construct but whose ground state is simple to find. Let $H_{\mathrm{B}}^{(i)}$ be the 1-bit Hamiltonian acting on the i-th bit

$$H_{\mathrm{B}}^{(i)} = \tfrac{1}{2}(1 - \sigma_x^{(i)}) \quad \text{with} \quad \sigma_x^{(i)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.17}$$

so

$$H_{\mathrm{B}}^{(i)}\,|x_i = x\rangle = x\,|x_i = x\rangle$$

where

$$|x_i = 0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and} \quad |x_i = 1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{2.18}$$

Continuing to take 3-SAT as our working example, clause C is associated with the bits i_C, j_C, and k_C. Now define

$$H_{\mathrm{B},C} = H_{\mathrm{B}}^{(i_C)} + H_{\mathrm{B}}^{(j_C)} + H_{\mathrm{B}}^{(k_C)} \tag{2.19}$$

and

$$H_{\mathrm{B}} = \sum_C H_{\mathrm{B},C} \ . \tag{2.20}$$

The ground state of H_B is $|x_1 = 0\rangle |x_2 = 0\rangle \cdots |x_n = 0\rangle$. This state, written in the z basis, is a superposition of all 2^n basis vectors $|z_1\rangle |z_2\rangle \cdots |z_n\rangle$,

$$|x_1 = 0\rangle |x_2 = 0\rangle \cdots |x_n = 0\rangle = \frac{1}{2^{n/2}} \sum_{z_1} \sum_{z_2} \cdots \sum_{z_n} |z_1\rangle |z_2\rangle \cdots |z_n\rangle \ . \tag{2.21}$$

Note that we can also write

$$H_B = \sum_{i=1}^{n} d_i H_B^{(i)} \tag{2.22}$$

where d_i is the number of clauses in which bit i appears in the instance of 3-SAT being considered.

The key feature of H_B is that its ground state is easy to construct. The choice we made here will lead to an $H(t)$ that is of the form (1.2), that is, a sum of Hamiltonians associated with each clause.

2.5 Adiabatic Evolution

We will now use adiabatic evolution to go from the known ground state of H_B to the unknown ground state of H_P. Assume for now that the ground state of H_P is unique. Consider

$$H(t) = (1 - t/T)H_B + (t/T)H_P \tag{2.23}$$

so from (2.2),

$$\widetilde{H}(s) = (1 - s)H_B + sH_P \ . \tag{2.24}$$

Prepare the system so that it begins at $t = 0$ in the ground state of $H(0) = H_B$. According to the adiabatic theorem, if g_{min} is not zero and the system evolves according to (2.1), then for T big enough $|\psi(T)\rangle$ will be very close to the ground state of H_P, that is, the solution to the computational problem.

Using the explicit form of (2.16) and (2.20) we see that $H(t)$ and $\widetilde{H}(s)$ are sums of individual terms associated with each clause. For each clause C let

$$H_C(t) = (1 - t/T)H_{B,C} + (t/T)H_{P,C} \tag{2.25}$$

and accordingly

$$\widetilde{H}_C(s) = (1 - s)H_{B,C} + sH_{P,C} \ . \tag{2.26}$$

Then we have

$$H(t) = \sum_{C} H_C(t) \tag{2.27}$$

and

$$\widetilde{H}(s) = \sum_{C} \widetilde{H}_C(s) \ . \tag{2.28}$$

This gives the explicit form of $H(t)$ described in the Introduction as a sum of Hamiltonians associated with individual clauses.

2.6   The Size of the Minimum Gap and the Required Evolution Time

Typically $g_{\min}$ is not zero. To see this, note from (2.7) that vanishing $g_{\min}$ is equivalent to there being some value of s for which $E_1(s) = E_0(s)$. Consider a general 2×2 Hamiltonian whose coefficients are functions of s

$$\begin{pmatrix} a(s) & c(s) + id(s) \\ c(s) - id(s) & b(s) \end{pmatrix} \tag{2.29}$$

where a, b, c, and d are all real. The two eigenvalues of this matrix are equal for some s if and only if $a(s) = b(s)$, $c(s) = 0$, and $d(s) = 0$. The curve $\big(a(s), b(s), c(s), d(s)\big)$ in $\mathbb{R}^4$ will typically not intersect the line $(y, y, 0, 0)$ unless the Hamiltonian has special symmetry properties. For example, suppose the Hamiltonian (2.29) commutes with some operator, say for concreteness σ_x. This implies that $a(s) = b(s)$ and $d(s) = 0$. Now for the two eigenvalues to be equal at some s we only require c to vanish at some s. As s varies from 0 to 1 it would not be surprising to find $c(s)$ cross zero so we see that the existence of a symmetry, that is, an operator which commutes with the Hamiltonian makes level crossing more commonplace. These arguments can be generalized to $N \times N$ Hamiltonians and we conclude that in the absence of symmetry, levels typically do not cross. We will expand on this point after we do some examples.

In order for our method to be conceivably useful, it is not enough for $g_{\min}$ to be nonzero. We must be sure that $g_{\min}$ is not so small that the evolution time T is impractically large; see (2.8). For an n-bit problem we would say that adiabatic evolution can be used to solve the problem if T is less than n^p for some fixed p whereas the method does not work if T is of order a^n for some $a > 1$. Returning to (2.8) we see that the required running time T also depends on $\mathcal{E}$ given in (2.9). Using (2.24) we have $\mathrm{d}\widetilde{H}/\mathrm{d}s = H_{\mathrm{P}} - H_{\mathrm{B}}$. Therefore $\mathcal{E}$ can be no larger than the maximum eigenvalue of $H_{\mathrm{P}} - H_{\mathrm{B}}$. From (2.16) we see that the spectrum of H_{P} is contained in $\{0, 1, 2, \ldots, M\}$ where M is the number of terms in (2.16), that is, the number of clauses in the problem. From (2.22) we see that the spectrum of H_{B} is contained in $\{0, 1, 2, \ldots, d\}$ where $d = \sum d_i$. For 3-SAT, d is no bigger than $3M$. We are interested in problems for which the number of clauses grows only as a polynomial in n, the number of bits. Thus $\mathcal{E}$ grows at most like a polynomial in n and the distinction between polynomial and exponential running time depends entirely on $g_{\min}$.

We make no claims about the size of $g_{\min}$ for any problems other than the examples given in Section 4. We will give three examples where $g_{\min}$ is of order $1/n^p$ so the evolution time T is polynomial in n. Each of these problems has a regular structure that made calculating $g_{\min}$ possible. However, the regularity of these problems also makes them classically computationally simple. The question of whether there are computationally difficult problems that could be solved by quantum adiabatic evolution we must leave to future investigation.

2.7   The Quantum Algorithm

We have presented a general quantum algorithm for solving SAT problems. It consists of:

1. An easily constructible initial state (2.21), which is the ground state of H_{B} in (2.20).

2. A time-dependent Hamiltonian, $H(t)$, given by (2.23) that is easily constructible from the given instance of the problem; see (2.16) and (2.20).

3. An evolution time T that also appears in (2.23).

4. Schrödinger evolution according to (2.1) for time T.

5. The final state $|\psi(T)\rangle$ that for T big enough will be (very nearly) the ground state of H_{P}.

6. A measurement of $z_1, z_2, \ldots, z_n$ in the state $|\psi(T)\rangle$. The result of this measurement will be a satisfying assignment of formula (1.1), if it has one (or more). If the formula (1.1) has no satisfying assignment, the result will still minimize the number of violated clauses.

Again, the crucial question about this quantum algorithm is how big must T be in order to solve an interesting problem. It is not clear what the relationship is, if any, between the required size of T and the classical complexity of the underlying problem. The best we have been able to do is explore examples, which is the main subject of the rest of this paper.

3   One-, Two-, and Three-Qubit Examples

Here we give some one-, two-, and three-qubit examples that illustrate some of the ideas of the introduction. The two-qubit examples have clauses with more than one satisfying assignment and serve as building blocks for the three-qubit example and for the more complicated examples of the next section.

3.1   One Qubit

Consider a one-bit problem where the single clause is satisfied if and only if $z_1 = 1$. We then take

$$H_{\mathrm{P}} = \tfrac{1}{2} + \tfrac{1}{2}\sigma_z^{(1)} \tag{3.1}$$

which has $|z_1 = 1\rangle$ as its ground state. For the beginning Hamiltonian we take (2.22) with $n = 1$ and $d_1 = 1$,

$$H_{\mathrm{B}} = H_{\mathrm{B}}^{(1)} = \tfrac{1}{2} - \tfrac{1}{2}\sigma_x^{(1)} \ . \tag{3.2}$$

The smooth interpolating Hamiltonian $\widetilde{H}(s)$ given by (2.24) has eigenvalues $\tfrac{1}{2}(1 \pm \sqrt{1 - 2s + 2s^2})$, which are plotted in Fig. 1. We see that $g_{\min}$ is not small and we could adiabatically evolve from $|x_1 = 0\rangle$ to $|z_1 = 1\rangle$ with a modest value of T.

At this point we can illustrate why we picked the beginning Hamiltonian, H_{B}, to be diagonal in a basis that is *not* the basis that diagonalizes the final problem Hamiltonian H_{P}. Suppose we replace H_{B} by H_{B}'

$$H_{\mathrm{B}}' = \tfrac{1}{2} - \tfrac{1}{2}\sigma_z^{(1)} \tag{3.3}$$

keeping H_{P} as in (3.1). Now $\widetilde{H}(s)$ is diagonal in the z-basis for all values of s. The two eigenvalues are s and $(1 - s)$, which are plotted in Fig. 2. The levels cross so $g_{\min}$ is zero. In fact there is a symmetry, $\widetilde{H}(s)$ commutes with σ_z for all s, so the appearance of the level cross is not surprising. Adiabatically evolving, starting at $|z_1 = 0\rangle$, we would end up at $|z_1 = 0\rangle$, which is *not* the ground state of H_{P}. However, if we add to H_{B} any small term that is not diagonal in the z basis, we break the symmetry, and $\widetilde{H}(s)$ will have a nonzero gap for all s. For example, the Hamiltonian

$$\begin{bmatrix} s & \varepsilon(1-s) \\ \varepsilon(1-s) & 1-s \end{bmatrix} \tag{3.4}$$

has $g_{\min} = \varepsilon$ for ε small and the eigenvalues are plotted in Fig. 3 for a small value of ε. This "level repulsion" is typically seen in more complicated systems whereas level crossing is not.
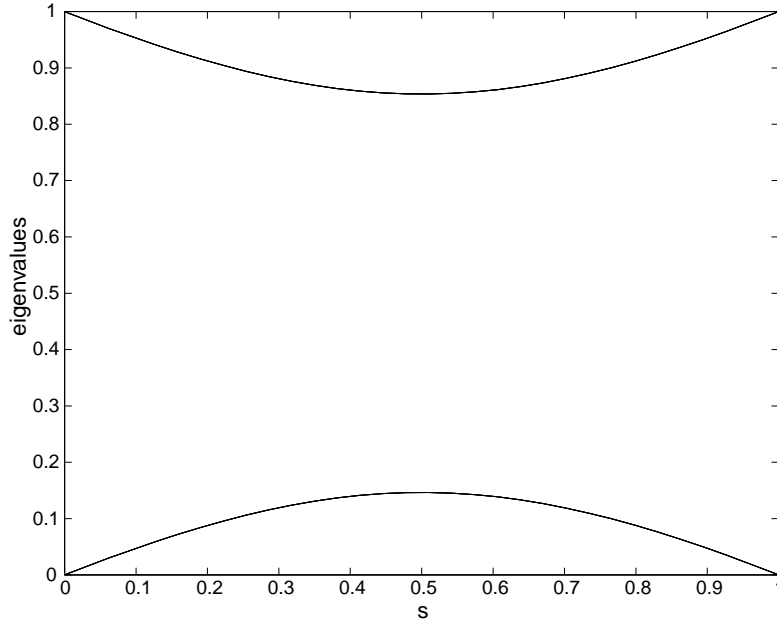
Figure 1: *The two eigenvalues of $\widetilde{H}(s)$ for a one-qubit example.*

3.2   Two Qubits

A simple two-qubit example has a single two-bit clause that allows the bit values 01 and 10 but not 00 and 11. We call this clause "2-bit disagree." We take H_{B} of the form (2.22) with $n = 2$ and $d_1 = d_2 = 1$, and we take H_{P} of the form (2.16) with the single 2-bit disagree clause. The instantaneous eigenvalues of $\widetilde{H}(s)$ of the form (2.24) are shown in Fig. 4. There are two ground states of H_{P}, $|z_1 = 0\rangle |z_2 = 1\rangle$ and $|z_1 = 1\rangle |z_2 = 0\rangle$. The starting state $|\psi(0)\rangle$, which is the ground state of H_{B}, is (2.21) with $n = 2$. There is a bit-exchange operation $|z_1\rangle |z_2\rangle \rightarrow |z_2\rangle |z_1\rangle$ that commutes with $\widetilde{H}(s)$. Since the starting state $|\psi(0)\rangle$ is invariant under the bit-exchange operation, the state corresponding to the $s = 1$ end of the lowest level in Fig. 4 is the symmetric state $\frac{1}{\sqrt{2}}\big(|z_1 = 0\rangle |z_2 = 1\rangle + |z_1 = 1\rangle |z_2 = 0\rangle\big)$. The next level, $E_1(s)$, begins at the antisymmetric state $\frac{1}{\sqrt{2}}\big(|x_1 = 0\rangle |x_2 = 1\rangle - |x_1 = 1\rangle |x_2 = 0\rangle\big)$ and ends at the antisymmetric state $\frac{1}{\sqrt{2}}\big(|z_1 = 0\rangle |z_2 = 1\rangle - |z_1 = 1\rangle |z_2 = 0\rangle\big)$. Because $\widetilde{H}(s)$ commutes with the bit-exchange operation there can be no transitions from the symmetric to the antisymmetric states. Therefore the $E_1(s)$ curve in Fig. 4 is irrelevant to the adiabatic evolution of the ground state and the relevant gap is $E_2(s) - E_0(s)$.

Closely related to 2-bit disagree is the "2-bit agree clause," which has 00 and 11 as satisfying assignments. We can obtain H_{P} for this problem by taking H_{P} for 2-bit disagree and acting with the operator that takes $|z_1\rangle |z_2\rangle \rightarrow |\bar{z}_1\rangle |z_2\rangle$. Note that $H_{\mathrm{B}} = H_{\mathrm{B}}^{(1)} + H_{\mathrm{B}}^{(2)}$ is invariant under this transformation as is the starting state $|\psi(0)\rangle$ given in (2.21). This implies that the levels of $\widetilde{H}(s)$ corresponding to 2-bit agree are the same as those for 2-bit disagree and that beginning with the ground state of H_{B}, adiabatic evolution brings you to $\frac{1}{\sqrt{2}}\big(|z_1 = 0\rangle |z_2 = 0\rangle + |z_1 = 1\rangle |z_2 = 1\rangle\big)$.

Another two-bit example that we will use later is the clause "imply". Here the satisfying assignments are 00, 01, and 11. The relevant level diagram is shown in Fig. 5.
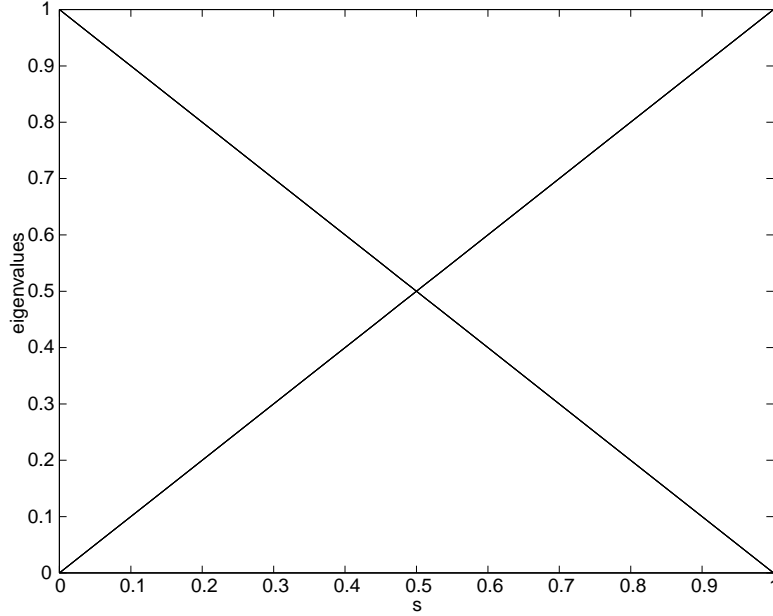
Figure 2: *The two eigenvalues of $\widetilde{H}(s)$ for a one-qubit example where H_{B} and H_{P} are diagonal in the same basis. The levels cross so $g_{\min} = 0$.*

3.3   Three Qubits

Next we present a three-bit example that is built up from two-bit clauses so we have an instance of 2-SAT with three bits. We take the 2-bit imply clause acting on bits 1 and 2, the 2-bit disagree clause acting on bits 1 and 3, and the 2-bit agree clause acting on bits 2 and 3. Although each two-bit clause has more than one satisfying assignment, the full problem has the unique satisfying assignment 011.

The corresponding quantum Hamiltonian, $\widetilde{H}(s) = (1-s)H_{\mathrm{B}} + sH_{\mathrm{P}}$, we write as the sum of Hamiltonians each of which acts on two bits,

$$H_{\mathrm{P}} = H_{\mathrm{imply}}^{12} + H_{\mathrm{disagree}}^{13} + H_{\mathrm{agree}}^{23}$$
$$H_{\mathrm{B}} = (H_{\mathrm{B}}^{(1)} + H_{\mathrm{B}}^{(2)}) + (H_{\mathrm{B}}^{(1)} + H_{\mathrm{B}}^{(3)}) + (H_{\mathrm{B}}^{(2)} + H_{\mathrm{B}}^{(3)}) \ . \tag{3.5}$$

The eigenvalues of $\widetilde{H}(s)$ are shown in Fig. 6. We see that $g_{\min}$ is not zero. Starting in the ground state of H_{B}, and evolving according to (2.1) with $H(t) = \widetilde{H}(t/T)$ the system will end up in the ground state of H_{P} for $T \gg 1/g_{\min}^2$. This example illustrates how our algorithm evolves to the unique satisfying assignment of several overlapping clauses even when each separate clause has more than one satisfying assignment.

The alert reader may have noticed that two of the levels in Fig. 6 cross. This can be understood in terms of a symmetry. The Hamiltonian H_{P} of (3.5) is invariant under the unitary transformation $V(|z_1\rangle |z_2\rangle |z_3\rangle) = |\overline{z}_2\rangle |\overline{z}_1\rangle |z_3\rangle$, as is H_{B}. Now the three states with energy equal to 4 at $s = 0$ are $|x_1 = 1\rangle |x_2 = 1\rangle |x_3 = 0\rangle$, $|x_1 = 0\rangle |x_2 = 1\rangle |x_3 = 1\rangle$, and $|x_1 = 1\rangle |x_2 = 0\rangle |x_3 = 1\rangle$. The transformation $|z\rangle \to |\overline{z}\rangle$ in the $|x\rangle$ basis is $|x\rangle \to (-1)^x |x\rangle$, so the states

$$|x_1 = 1\rangle |x_2 = 1\rangle |x_3 = 0\rangle \ \text{ and } \ |x_1 = 0\rangle |x_2 = 1\rangle |x_3 = 1\rangle - |x_1 = 1\rangle |x_2 = 0\rangle |x_3 = 1\rangle$$

are invariant under V, whereas

$$|x_1 = 0\rangle |x_2 = 1\rangle |x_3 = 1\rangle + |x_1 = 1\rangle |x_2 = 0\rangle |x_3 = 1\rangle$$
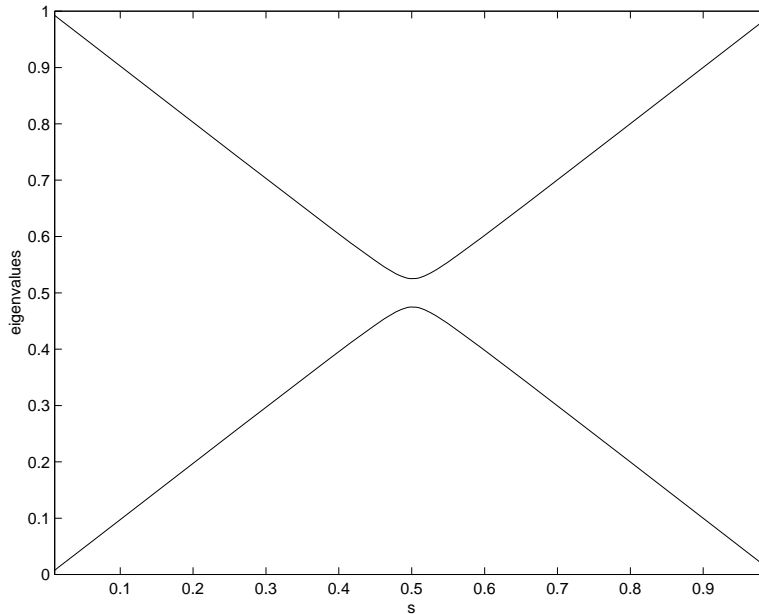
Figure 3: *A small perturbation is added to the Hamiltonian associated with Fig. 2 and we see that the levels no longer cross.*

goes to minus itself. We call these two different transformation properties "invariant" and "odd". Thus at $s = 0$ there are two invariant states and one odd state with energy 4. We see from Fig. 6 that one combination of these states ends up at energy 2 when $s = 1$. The energy-2 state at $s = 1$ is $|z_1 = 0\rangle |z_2 = 1\rangle |z_3 = 0\rangle$, which is invariant so the level moving across from energy 4 to energy 2 is invariant. This means that one of the two levels that start at energy 4 and end at energy 1 is invariant and the other is odd. Since the Hilbert space can be decomposed into a direct sum of the invariant and odd subspaces and accordingly $H(t)$ is block diagonal, the invariant and odd states are decoupled, and their crossing is not an unlikely occurrence.

Since, in this simple 3-bit example, we do see levels cross you may wonder if we should expect to sometimes see the two lowest levels cross in more complicated examples. We now argue that we do not expect this to happen and even if it does occur it will not effect the evolution of the ground state. First note that the transformation which is a symmetry of (3.5) is not a symmetry of the individual terms in the sum. Thus it is unlikely that such symmetries will typically be present in more complicated n-bit examples. However, it is inevitable that certain instances of problems will give rise to Hamiltonians that are invariant under some transformation. Imagine that the transformation consists of bit interchange and negation (in the z basis) as in the example just discussed. Then the starting state $|x = 0\rangle$ given by (2.21) is invariant. Assume that H_P has a unique ground state $|z_1 = w_1\rangle |z_2 = w_2\rangle \cdots |z_n = w_n\rangle$. Since H_P is invariant this state must transform into itself, up to a phase. However, from the explicit form of the ground state we see that it transforms without a phase, that is, it is invariant. Thus, following the evolution of the ground state we can restrict our attention to invariant states. The gap that matters is the smallest energy difference between the two lowest invariant states.
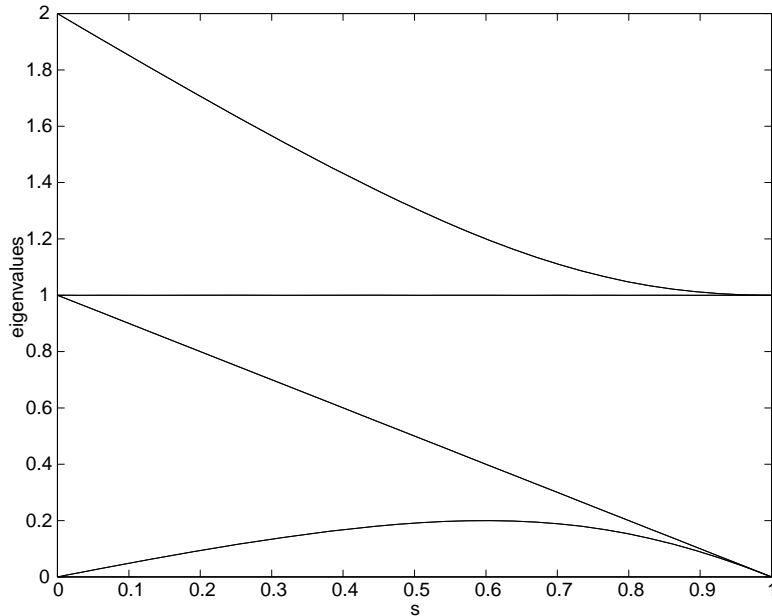
Figure 4: *The four eigenvalues of $\widetilde{H}(s)$ associated with "2-bit disagree". The same levels are associated with "2-bit agree".*

4   Examples with an Arbitrary Number of Bits

Here we discuss four examples of n-bit instances of satisfiability. In three of the examples the problems are classically computationally simple to solve. These problems also have structure that we exploit to calculate $g_{\min}$ in the corresponding quantum version. In each case $g_{\min}$ goes like $1/n^p$, so these problems can be solved in polynomial time by adiabatic quantum evolution. The other example is the "Grover problem" [2], which has a single (generalized) n-bit clause with a unique satisfying assignment. If we assume that we treat the clause as an oracle, which may be queried but not analyzed, it takes 2^n classical queries to find the satisfying assignment. Our quantum version has $g_{\min}$ of order $2^{-n/2}$, so the time required for quantum adiabatic evolution scales like 2^n, which means that there is no quantum speedup. Nonetheless, it is instructive to see how it is possible to evaluate $g_{\min}$ for the Grover problem.

4.1   2-SAT on a Ring: Agree and Disagree

Consider an n-bit problem with n clauses, each of which acts only on adjacent bits, that is, clause C_j acts on bits j and $j+1$ where j runs from 1 to n and bit $n+1$ is identified with bit 1. Furthermore we restrict each clause to be either "agree", which means that 00 and 11 are satisfying assignments or "disagree", which means that 01 and 10 are satisfying assignments. Suppose there are an even number of disagree clauses so that a satisfying assignment on the ring exists. Clearly given the list of clauses it is trivial to construct the satisfying assignment. Also, if $w_1, w_2, \ldots, w_n$ is a satisfying assignment, so is $\overline{w}_1, \overline{w}_2, \ldots, \overline{w}_n$, so there are always exactly two satisfying assignments.

    The quantum version of the problem has

$$H_{\mathrm{P}} = H_{C_1}^{12} + H_{C_2}^{23} + \cdots + H_{C_n}^{nn+1} \tag{4.1}$$

where each C_j is either agree or disagree. The ground states of H_{P} are $|w_1\rangle |w_2\rangle \cdots |w_n\rangle$ and $|\overline{w}_1\rangle \times$
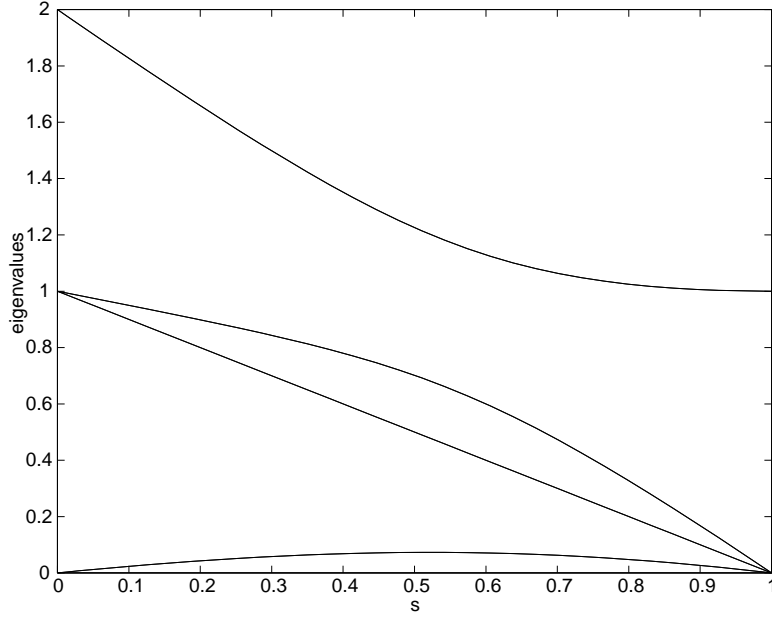
Figure 5: *The four eigenvalues of $\widetilde{H}(s)$ associated with the 2-bit imply clause.*

$|\overline{w}_2\rangle \cdots |\overline{w}_n\rangle$ all in the z basis. Define the unitary transformation

$$|z_1\rangle |z_2\rangle \cdots |z_n\rangle \rightarrow |z_1'\rangle |z_2'\rangle \cdots |z_n'\rangle \qquad \begin{cases} z_j' = \overline{z}_j \ , & \text{if } w_j = 1 \\ z_j' = z_j \ , & \text{if } w_j = 0 \ . \end{cases} \tag{4.2}$$

Under this transformation H_{P} becomes

$$H_{\mathrm{P}} = H_{\text{agree}}^{12} + H_{\text{agree}}^{23} + \cdots + H_{\text{agree}}^{nn+1} \tag{4.3}$$

and the symmetric ground state of H_{P} is

$$|w\rangle = \frac{1}{\sqrt{2}}\big(|z_1 = 0\rangle |z_2 = 0\rangle \cdots |z_n = 0\rangle + |z_1 = 1\rangle |z_2 = 1\rangle \cdots |z_n = 1\rangle\big) \ . \tag{4.4}$$

We take H_{B} to be (2.22) with n bits and each $d_i = 2$. H_{B} is invariant under the transformation just given. This implies that the spectrum of $\widetilde{H}(s) = (1-s)H_{\mathrm{B}} + sH_{\mathrm{P}}$, with H_{P} given by (4.1), is identical to the spectrum of $\widetilde{H}(s)$ with H_{P} given by (4.3). Thus when we find $g_{\min}$ using (4.3) we will have found $g_{\min}$ for all of the n-bit agree-disagree problems initially described.

We can write $\widetilde{H}(s)$ using (4.3) for H_{P} as

$$\widetilde{H}(s) = (1 - s)\sum_{j=1}^{n}(1 - \sigma_x^{(j)}) + s\sum_{j=1}^{n} \tfrac{1}{2}(1 - \sigma_z^{(j)}\sigma_z^{(j+1)}) \ . \tag{4.5}$$

We denote the $s = 0$ ground state given by (2.21) as $|x = 0\rangle$. Define the operator G that negates the value of each bit in the z basis, that is, $G |z_1\rangle |z_2\rangle \cdots |z_n\rangle = |\overline{z}_1\rangle |\overline{z}_2\rangle \cdots |\overline{z}_n\rangle$. This can be written as

$$G = \prod_{j=1}^{n} \sigma_x^{(j)} \ . \tag{4.6}$$
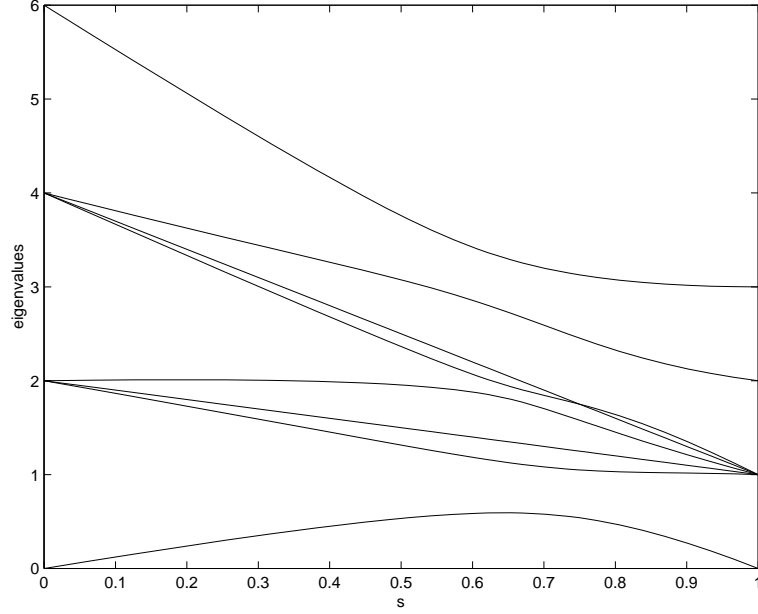
Figure 6: *The eight levels of $\widetilde{H}(s)$ for the 3-bit problem with H_{P} and H_{B} given by (3.5).*

Since $G\,|x=0\rangle = |x=0\rangle$ and $\left[G, \widetilde{H}(s)\right] = 0$, we can restrict our attention to states that are invariant under G such as (4.4).

We now write (4.5) in the invariant sector as a sum of $n/2$ commuting 2×2 Hamiltonians that we can diagonalize. First we make a standard transformation to fermion operators. To this end we define for $j = 1, \ldots, n$,

$$b_j = \sigma_x^{(1)} \sigma_x^{(2)} \cdots \sigma_x^{(j-1)} \sigma_-^{(j)} 1^{(j+1)} \cdots 1^{(n)}$$

$$b_j^\dagger = \sigma_x^{(1)} \sigma_x^{(2)} \cdots \sigma_x^{(j-1)} \sigma_+^{(j)} 1^{(j+1)} \cdots 1^{(n)} \tag{4.7}$$

where

$$\sigma_- = \tfrac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \sigma_+ = \tfrac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}.$$

It is straightforward to verify that

$$\{b_j, b_k\} = 0$$

$$\{b_j, b_k^\dagger\} = \delta_{jk} \tag{4.8}$$

where $\{A, B\} = AB + BA$. Furthermore

$$b_j^\dagger b_j = \tfrac{1}{2}(1 - \sigma_x^{(j)}) \tag{4.9}$$

for $j = 1, \ldots, n$ and

$$(b_j^\dagger - b_j)(b_{j+1}^\dagger + b_{j+1}) = \sigma_z^{(j)} \sigma_z^{(j+1)} \tag{4.10}$$

for $j = 1, \ldots, n-1$. We need a bit more care to make sense of (4.10) for $j = n$. An explicit calculation shows that

$$(b_n^\dagger - b_n)(b_1^\dagger + b_1) = -G \sigma_z^{(n)} \sigma_z^{(1)} \tag{4.11}$$

where G is given by (4.6). Since we will restrict ourselves to the $G = 1$ sector, (4.10) and (4.11) are only consistent if $b_{n+1} = -b_1$, so we take this as the definition of b_{n+1}.

We can now reexpress $\widetilde{H}(s)$ of (4.5) in terms of the b's:

$$\widetilde{H}(s) = \sum_{j=1}^{n} \left\{ 2(1-s)b_j^\dagger b_j + \frac{s}{2}\big(1 - (b_j^\dagger - b_j)(b_{j+1}^\dagger + b_{j+1})\big) \right\} . \tag{4.12}$$

Because this is invariant under the translation, $b_j \to b_{j+1}$, and is quadratic in the b_j and $b_j^\dagger$, a transformation to fermion operators associated with waves running round the ring will achieve the desired reduction of $\widetilde{H}(s)$. Let

$$\beta_p = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} e^{i\pi pj/n} b_j \quad \text{for } p = \pm 1, \pm 3, \ldots, \pm(n-1) \tag{4.13}$$

which is equivalent to

$$b_j = \frac{1}{\sqrt{n}} \sum_{p=\pm 1, \pm 3, \ldots, \pm(n-1)} e^{-i\pi pj/n} \beta_p \tag{4.14}$$

and is consistent with $b_{n+1} = -b_1$. (We assume for simplicity that n is even.) Furthermore

$$\{\beta_p, \beta_q\} = 0$$

and

$$\{\beta_p, \beta_q^\dagger\} = \delta_{pq} \tag{4.15}$$

which follows from (4.8). Substituting (4.14) into (4.12) gives

$$\widetilde{H}(s) = \sum_{p=1,3,\ldots,(n-1)} A_p(s) \tag{4.16}$$

where

$$\begin{aligned}
A_p(s) = {}& 2(1-s)\big[\beta_p^\dagger \beta_p + \beta_{-p}^\dagger \beta_{-p}\big] \\
& + s\Big\{ 1 - \cos\frac{\pi p}{n}\big[\beta_p^\dagger \beta_p - \beta_{-p}\beta_{-p}^\dagger\big] + i\sin\frac{\pi p}{n}\big[\beta_{-p}^\dagger \beta_p^\dagger - \beta_p \beta_{-p}\big] \Big\} .
\end{aligned} \tag{4.17}$$

The A_p's commute for different values of p so we can diagonalize each A_p separately.

For each $p > 0$ let $|\Omega_p\rangle$ be the state annihilated by both β_p and β_{-p}, that is, $\beta_p |\Omega_p\rangle = \beta_{-p} |\Omega_p\rangle = 0$. When $s = 0$, $|\Omega_p\rangle$ is the ground state of A_p. Now $A_p(s)$ only connects $|\Omega_p\rangle$ to $|\Sigma_p\rangle = \beta_{-p}^\dagger \beta_p^\dagger |\Omega_p\rangle$. In the $|\Omega_p\rangle$, $|\Sigma_p\rangle$ basis $A_p(s)$ is

$$A_p(s) = \begin{bmatrix} s + s\cos\pi p/n & is(\sin\pi p/n) \\ -is(\sin\pi p/n) & 4 - 3s - s\cos\pi p/n \end{bmatrix} . \tag{4.18}$$

For each p the two eigenvalues of $A_p(s)$ are

$$E_p^\pm(s) = 2 - s \pm \big\{ (2 - 3s)^2 + 4s(1-s)(1 - \cos\pi p/n) \big\}^{\frac{1}{2}} . \tag{4.19}$$

The ground state energy of (4.16) is $\sum_p E_p^-(s)$. The next highest energy level is $E_1^+(s) + \sum_{p=3...} E_p^-(s)$.
The minimum gap occurs very close to $s = \frac{2}{3}$ and is

$$g_{\min} \approx E_1^+(\tfrac{2}{3}) - E_1^-(\tfrac{2}{3}) \approx \frac{4\pi}{3n} \tag{4.20}$$

for n large.

Referring back to (2.8) we see that the required evolution time T must be much greater than $\mathcal{E}/g_{\min}^2$ where for this problem $\mathcal{E}$ scales like n so $T \gg cn^3$ where c is a constant. We have shown that for any set of agree and disagree clauses on an n-bit ring, quantum adiabatic evolution will find the satisfying assignment in a time which grows as a fixed power of n.

4.2   The Grover Problem

Here we consider the Grover problem [2], which we recast for the present context. We have a single (generalized) clause, h_G, which depends on all n bits with a unique (but unknown) satisfying assignment $w = w_1, w_2, \ldots, w_n$. Corresponding to h_G is a problem Hamiltonian

$$H_{\mathrm{P}} \, |z\rangle = \left\{ \begin{array}{ll} |z\rangle\,, & z \neq w \\ 0\,, & z = w \end{array} \right.$$

$$= 1 - |z = w\rangle\,\langle z = w| \tag{4.21}$$

where we use the shorthand $|z\rangle = |z_1\rangle\,|z_2\rangle\ldots,|z_n\rangle$. We imagine that we can construct $H(t) = \widetilde{H}(t/T)$ of the form (2.23) with H_{B} given by (2.22) with $d_i = 1$ for all i from 1 to n. Since we are evolving using $H(t)$ the problem is "oracular," that is, we use no knowledge about the structure of H_{P} which could aid us in finding w other than (4.21).

We can write $\widetilde{H}(s)$ explicitly as

$$\widetilde{H}(s) = (1-s)\sum_{j=1}^n \tfrac{1}{2}\big(1-\sigma_x^{(j)}\big) + s\big(1 - |z=w\rangle\,\langle z=w|\big)\,. \tag{4.22}$$

Consider the transformation given by (4.2). Under this transformation $\widetilde{H}(s)$ becomes

$$\widetilde{H}(s) = (1-s)\sum_{j=1}^n \tfrac{1}{2}\big(1-\sigma_x^{(j)}\big) + s\big(1 - |z=0\rangle\,\langle z=0|\big)\,. \tag{4.23}$$

Because the two Hamiltonians (4.22) and (4.23) are unitarily equivalent they have the same spectra and accordingly the same $g_{\min}$. Thus it suffices to study (4.23).

The ground state of $\widetilde{H}(0)$ is $|x=0\rangle$, which is symmetric under the interchange of any two bits. Also the operator (4.23) is symmetric under the interchange of any two bits. Instead of working in the 2^n-dimensional space we can work in the $(n+1)$-dimensional subspace of symmetrized states. It is convenient (and perhaps more familiar to physicists) to define these states in terms of the total spin. Define $\vec{S} = (S_x, S_y, S_z)$ by

$$S_a = \tfrac{1}{2}\sum_{j=1}^n \sigma_a^{(j)} \tag{4.24}$$

for $a = x, y, z$. The symmetrical states have $\vec{S}^{\,2}$ equal to $\frac{n}{2}(\frac{n}{2}+1)$, where $\vec{S}^{\,2} = S_x^2 + S_y^2 + S_z^2$. We can characterize these states as either eigenstates of S_x or S_z

$$S_x\,|m_x = m\rangle = m\,|m_x = m\rangle \qquad m = -\tfrac{n}{2}, -\tfrac{n}{2}+1, \ldots, \tfrac{n}{2}$$

$$S_z\,|m_z = m\rangle = m\,|m_z = m\rangle \qquad m = -\tfrac{n}{2}, -\tfrac{n}{2}+1, \ldots, \tfrac{n}{2} \tag{4.25}$$

where we have suppressed the total spin label since it never changes. In terms of the z basis states previously introduced,

$$\left|m_z = \tfrac{n}{2} - k\right\rangle = \binom{n}{k}^{-\frac{1}{2}} \sum_{z_1+z_2+\cdots+z_n=k} |z_1\rangle |z_2\rangle \cdots |z_n\rangle \tag{4.26}$$

for $k = 0, 1, \ldots, n$. In particular

$$\left|m_z = \tfrac{n}{2}\right\rangle = |z = 0\rangle \ . \tag{4.27}$$

Now we can write $\widetilde{H}(s)$ in (4.23) as

$$\widetilde{H}(s) = (1 - s)\left[\tfrac{n}{2} - S_x\right] + s\left[1 - \left|m_z = \tfrac{n}{2}\right\rangle \left\langle m_z = \tfrac{n}{2}\right|\right] \ . \tag{4.28}$$

We have reduced the problem, since $\widetilde{H}(s)$ is now an $(n + 1)$-dimensional matrix whose elements we can simply evaluate.

We wish to solve

$$\widetilde{H}(s) |\psi\rangle = E |\psi\rangle \tag{4.29}$$

for the lowest two eigenvalues at the value of s at which they are closest. Hitting (4.29) with $\left\langle m_x = \tfrac{n}{2} - r\right|$ we get

$$[s + (1 - s)r]\left\langle m_x = \tfrac{n}{2} - r \,\middle|\, \psi\right\rangle - s\left\langle m_x = \tfrac{n}{2} - r \,\middle|\, m_z = \tfrac{n}{2}\right\rangle \left\langle m_z = \tfrac{n}{2} \,\middle|\, \psi\right\rangle$$
$$= E\left\langle m_x = \tfrac{n}{2} - r \,\middle|\, \psi\right\rangle . \tag{4.30}$$

We replace E by the variable λ where $E = s + (1 - s)\lambda$ and obtain

$$\frac{(1 - s)}{s}\left\langle m_x = \frac{n}{2} - r \,\middle|\, \psi\right\rangle = \frac{1}{r - \lambda}\left\langle m_x = \frac{n}{2} - r \,\middle|\, m_z = \frac{n}{2}\right\rangle \left\langle m_z = \frac{n}{2} \,\middle|\, \psi\right\rangle . \tag{4.31}$$

Multiply by $\left\langle m_z = \tfrac{n}{2} \,\middle|\, m_x = \tfrac{n}{2} - r\right\rangle$ and sum over r to get

$$\frac{(1 - s)}{s} = \sum_{r=0}^{n} \frac{1}{r - \lambda} P_r \tag{4.32}$$

where

$$P_r = \left|\left\langle m_z = \frac{n}{2} \,\middle|\, m_x = \frac{n}{2} - r\right\rangle\right|^2 . \tag{4.33}$$

Using (4.26) with $k = 0$ and also the identical formula with z replaced by x we have

$$P_r = \frac{1}{2^n}\binom{n}{r} . \tag{4.34}$$

The eigenvalue equation (4.32) has $n + 1$ roots. By graphing the right-hand side of (4.32) and keeping $0 < s < 1$ we see that there is one root for $\lambda < 0$, one root between 0 and 1, one root between 1 and 2, $\ldots$, and one root between $n - 1$ and n. The two lowest eigenvalues of $E = s + (1 - s)\lambda$ correspond to the root with $\lambda < 0$ and the root with $0 < \lambda < 1$. We will now show that there is a value of s for which these two roots are both very close to zero.

The left-hand side of (4.32) ranges over all positive values as s varies from 0 to 1. Pick $s = s^*$ such that

$$\frac{(1 - s^*)}{s^*} = \sum_{r=1}^{n} \frac{P_r}{r} \ . \tag{4.35}$$

At $s = s^*$ the eigenvalue equation (4.32) becomes

$$\frac{P_0}{\lambda} = \sum_{r=1}^{n} P_r \frac{\lambda}{r(r - \lambda)} \ . \tag{4.36}$$

From (4.34) we know that $P_0 = 2^{-n}$. Define u by $\lambda = 2^{-n/2}u$. Then (4.36) becomes

$$\frac{1}{u} = \sum_{r=1}^{n} P_r \frac{u}{r(r - 2^{-n/2}u)} \ . \tag{4.37}$$

Because of the $2^{-n/2}$ we can neglect the u piece in the denominator and we get

$$\frac{1}{u^2} \approx \sum_{r=1}^{n} \frac{P_r}{r^2} \tag{4.38}$$

which gives

$$\lambda \approx \pm \Big(\sum_{r=1}^{n} \frac{P_r}{r^2} \Big)^{-\frac{1}{2}} 2^{-n/2} \tag{4.39}$$

and we have

$$g_{\min} \approx 2(1 - s^*) \Big(\sum_{r=1}^{n} \frac{P_r}{r^2} \Big)^{-\frac{1}{2}} 2^{-n/2} \ . \tag{4.40}$$

Now

$$\sum_{r=1}^{n} \frac{P_r}{r} = \frac{2}{n} + O\Big(\frac{1}{n^2}\Big) \tag{4.41}$$

and

$$\sum_{r=1}^{n} \frac{P_r}{r^2} = \frac{4}{n^2} + O\Big(\frac{1}{n^3}\Big) \ . \tag{4.42}$$

So using (4.35) and (4.40) we have

$$g_{\min} \simeq 2 \cdot 2^{-\frac{n}{2}} \tag{4.43}$$

which is exponentially small.

In Fig. 7 we show the two lowest eigenvalues of $\widetilde{H}(s)$ for the case of 12 bits. If you evolve too quickly the system jumps across the gap and you do not end up in the ground state of $\widetilde{H}(1)$.

That $g_{\min}$ goes like $2^{-n/2}$ means that the required time for finding the satisfying assignment grows like 2^n and quantum adiabatic evolution is doing no better than the classical algorithm which checks all 2^n variable assignments. In reference [3] a Hamiltonian version of the Grover problem was studied with a time dependent Hamiltonian of the form
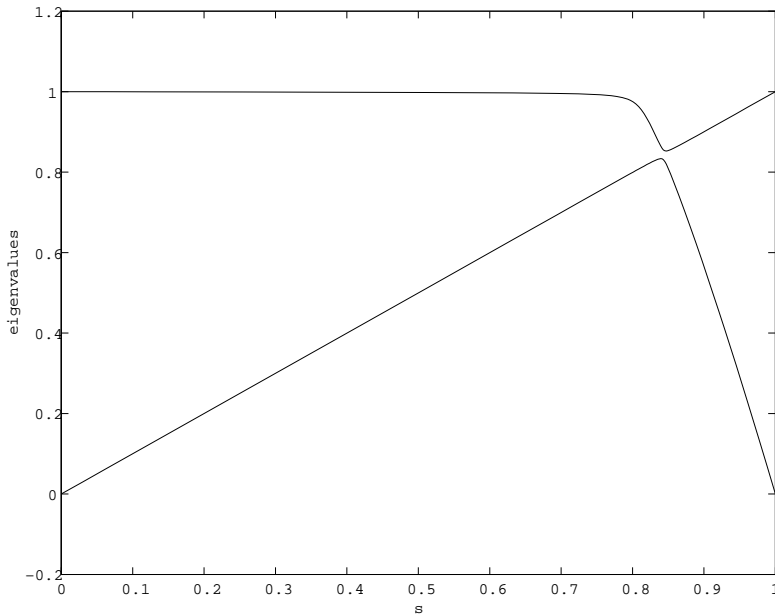
$$H(t) = H_D(t) + (1 - |z = w\rangle \langle z = w|) \ . \tag{4.44}$$

Figure 7: *The two lowest eigenvalues of $\widetilde{H}(s)$ for the Grover problem with 12 bits.*

The goal was to choose $H_D(t)$ without knowing w so that Schrödinger evolution from a w-independent initial state would bring the system to $|z = w\rangle$ in time T. There it was shown how to choose H_D so that the required running time T grows as $2^{\frac{n}{2}}$, which is then interpreted as the square-root speedup found by Grover. It was also shown that for any $H_D(t)$, T must be at least of order $2^{\frac{n}{2}}$ for the quantum evolution to succeed for all w. (The continuous time bound found in [3] is closely related to the query bound found first in [4].) A slight modification of the argument which gives this lower bound can be made for quantum evolution with

$$H(t) = H_D(t) + \frac{t}{T}(1 - |z = w\rangle \langle z = w|) \tag{4.45}$$

and again T must be at least of order $2^{\frac{n}{2}}$. The adiabatic evolution we studied in this section corresponds to $H_D(t) = (1 - t/T)H_B$ with H_B as described above. The lower bound just discussed shows that no choice of H_B can achieve better than square-root speedup.

4.3   The Bush of Implications

Ultimately we would like to know if there are general (and identifiable) features of problems which can tell us about the size of $g_{\min}$. For the 2-SAT example of Section 4.1, $g_{\min}$ is of order $1/n$ whereas for the Grover problem it is of order $2^{-n/2}$. In the Grover case H_P has the property that $2^n - 1$ states have energy 1, that is, there are an exponential number of states just above the ground state. For the ring problem this is not so. With H_P of the form (4.3) there are no states with energy 1 and (roughly) n^2 states with energy 2. Here we present an example with an exponential number of states with energy 1 but for which the gap is of order $1/n^p$. This tells us that we cannot judge the size of the minimum gap just from knowledge of the degeneracy of the first level above the ground state of H_P.

   The example we consider has $n + 1$ bits labeled $0, 1, 2 \ldots, n$. There are n 2-bit imply clauses, each of which involves bit 0 and one of the other n bits. Recall that the imply clause is satisfied by the bit

values $00, 01$ and 11 but not by 10. Furthermore we have a one-bit clause that is satisfied only if bit 0 has the value 1. The unique satisfying assignment of all clauses is $z_0 = 1, z_1 = 1, z_2 = 1, \ldots, z_n = 1$.
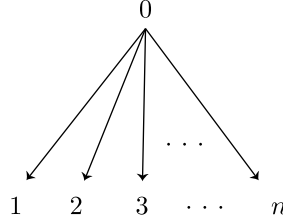

Figure 8: *The bush of implications. There is a one-bit clause that is satisfied if bit 0 has a value of 1. There are n imply clauses. The jth imply clause is satisfied unless bit 0 has the value 1 and bit j has the value 0.*

Suppose that $z_0 = 0$. Any of the 2^n values of $z_1, z_2, \ldots, z_n$ satisfy all of the imply clauses. Only the one bit clause is not satisfied, so these 2^n variable assignments violate only one clause. There are n other variable assignments that violate only one clause. These have all bits set to 1 except for the kth bit where $1 \leq k \leq n$. In total there are $2^n + n$ assignments that violate only one clause and accordingly there are an exponential number of states with energy 1.

We can write H_{P} explicitly as

$$H_{\mathrm{P}} = \tfrac{1}{2}(1 + \sigma_z^{(0)}) + \tfrac{1}{4} \sum_{j=1}^{n} (1 - \sigma_z^{(0)})(1 + \sigma_z^{(j)}) . \tag{4.46}$$

To evaluate H_{B} from (2.22) note that bit 0 is involved in $n+1$ clauses whereas bits 1 through n are each involved in only one clause, so

$$H_{\mathrm{B}} = (n+1)\tfrac{1}{2}(1 - \sigma_x^{(0)}) + \sum_{i=1}^{n} \tfrac{1}{2}(1 - \sigma_x^{(i)}) . \tag{4.47}$$

Then $\widetilde{H}(s)$ in terms of the spin operators (4.24) is

$$\widetilde{H}(s) = (1-s)\left[\frac{n+1}{2}(1 - \sigma_x^{(0)}) + \frac{n}{2} - S_x\right] + s\left[\tfrac{1}{2}(1 + \sigma_z^{(0)}) + \tfrac{1}{2}(1 - \sigma_z^{(0)})\left(\frac{n}{2} + S_z\right)\right] . \tag{4.48}$$

We need only consider states that are symmetrized in the bits 1 to n. We can label the relevant states as $|z_0\rangle \, |m_z\rangle$ where z_0 gives the value of bit 0 and m_z labels the z component of the total spin as in (4.25). We need to know the matrix elements of S_x in the $|m_z\rangle$ basis. These are

$$\langle m_z' \mid S_x \mid m_z \rangle = \tfrac{1}{2}\left[\left(\frac{n}{2}\left(\frac{n}{2} + 1\right) - m_z^2 - m_z\right)^{\frac{1}{2}} \delta_{m_z, m_z' - 1}\right.$$
$$\left. + \left(\frac{n}{2}\left(\frac{n}{2} + 1\right) - m_z'^2 - m_z'\right)^{\frac{1}{2}} \delta_{m_z', m_z - 1}\right] . \tag{4.49}$$

Given (4.49) we have numerically evaluated the eigenvalues of the $2(n+1)$-dimensional matrix with elements

$$\left(\langle z_0' | \, \langle m_z' | \right) \widetilde{H}(s) \left(|z_0\rangle \, |m_z\rangle\right) \tag{4.50}$$

for values of n in the range from 20 to 120. The two lowest eigenvalues are shown in Fig. 9 for $n = 50$. The gap is clearly visible. In Fig. 10 we plot $\log(g_{\min})$ versus $\log(n)$ and a power law dependence is
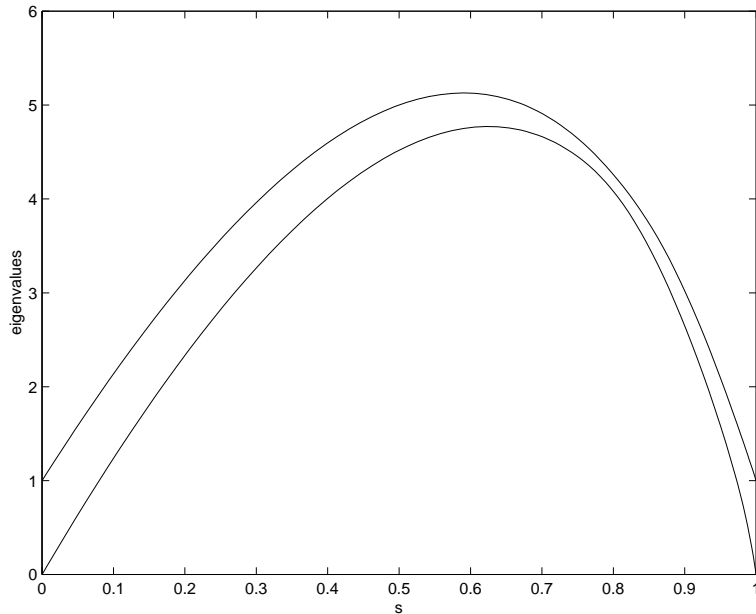
Figure 9: *The two lowest eigenvalues of $\widetilde{H}(s)$ for the bush of implications with $n = 50$. The visible gap indicates that $g_{\min}$ is not exponentially small.*

clearly visible. We conclude that $g_{\min} \sim n^{-p}$ with $p \simeq \frac{3}{8}$. For this problem the maximum eigenvalue of H_B is $2n + 1$ and the maximum eigenvalue of H_P is $n + 1$, so $\mathcal{E}$, which appears in (2.8), at most grows linearly with n. Therefore we have that with T of order $n^{(1+2p)}$ adiabatic evolution is assured.

We also analyzed adiabatic evolution for the bush of implications using a different prescription for the initial Hamiltonian. We tried

$$H'_B = \sum_{i=1}^{n} H_B^{(i)} \tag{4.51}$$

as opposed to (2.22). This has the effect of replacing the factor of $(n+1)$ in (4.47) with a 1. The effect on $g_{\min}$ is dramatic. It now appears to be exponentially small as a function of n. This means that with the choice of H'_B above, quantum adiabatic evolution fails to solve the bush of implications in polynomial time. This sensitivity to the distinction between H_B and H'_B presumably arises because bit 0 is involved in $(n+1)$ clauses. This suggests to us that if we restrict attention to problems where no bit is involved in more than, say, 3 clauses, there will be no such dramatic difference between using H_B or H'_B.

4.4 Overconstrained 2-SAT

In this section we present another 2-SAT problem consisting entirely of agree and disagree clauses. This time every pair of bits is involved in a clause. We suppose the clauses are consistent, so there are exactly 2 satisfying assignments, as in Section 4.1. In an n-bit instance of this problem, there are $\binom{n}{2}$ clauses, and obviously the collection of clauses is highly redundant in determining the satisfying assignments. We chose this example to explore whether this redundancy could lead to an extremely small $g_{\min}$. In fact, we will give numerical evidence that $g_{\min}$ goes like $1/n^p$ for this problem, whose symmetry simplifies the analysis.
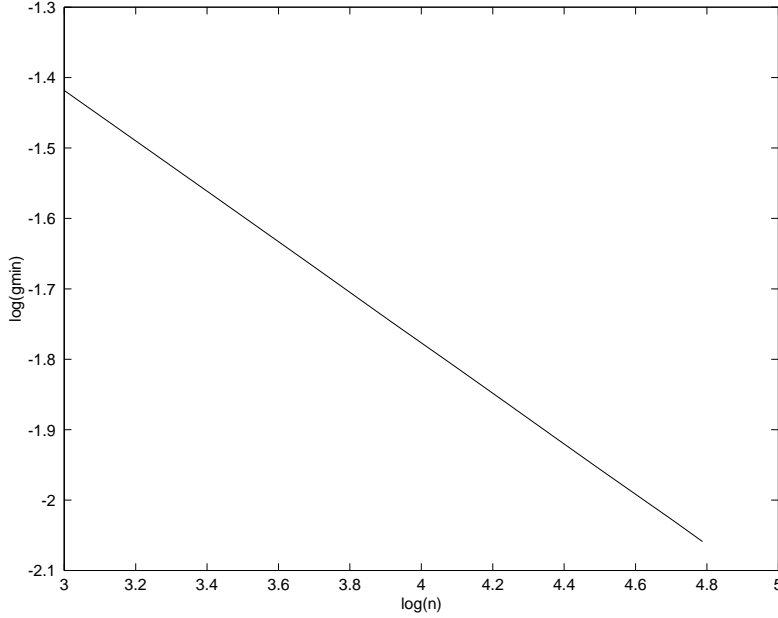
Figure 10: *The bush of implications;* $\log(g_{\min})$ *versus* $\log(n)$ *with* n *ranging from 20 to 120. The straight line indicates that* $g_{\min} \sim n^{-p}$.

As with the problem discussed in Section 4.1, at the quantum level we can restrict our attention to the case of all agree clauses, and we have

$$H_{\mathrm{P}} = \sum_{j<k} H^{jk}_{\mathrm{agree}} \ . \tag{4.52}$$

Each bit participates in $(n-1)$ clauses, so when constructing H_{B} using (2.22) we take $d_i = n - 1$ for all i. We can write $\widetilde{H}(s)$ explicitly for this problem

$$\widetilde{H}(s) = (1-s)(n-1) \sum_{j=1}^{n} \tfrac{1}{2}(1 - \sigma_x^{(j)}) + s \sum_{j<k} \tfrac{1}{2}(1 - \sigma_z^{(j)}\sigma_z^{(k)}) \tag{4.53}$$

which in terms of the total spin operators S_x and S_z is

$$\widetilde{H}(s) = (1-s)(n-1)\left[\frac{n}{2} - S_x\right] + s\left[\frac{n^2}{4} - S_z S_z\right] \ . \tag{4.54}$$

As in Section 4.3, it is enough to consider the symmetric states $|m_z\rangle$. Using (4.49), we can find the matrix elements

$$\langle m'_z | \, \widetilde{H}(s) \, | m_z \rangle \tag{4.55}$$

and numerically find the eigenvalues of this $(n+1) \times (n+1)$-dimensional matrix.

Actually there are two ground states of $\widetilde{H}(1)$, $\left| m_z = \frac{n}{2} \right\rangle$ and $\left| m_z = -\frac{n}{2} \right\rangle$, corresponding to all bits having the value 0 or all bits having the value 1. The Hamiltonian $\widetilde{H}(s)$ is invariant under the operation of negating all bits (in the z basis) as is the initial state given by (2.21). Therefore we can restrict our attention to invariant states. In Fig. 11 we show the two lowest invariant states for 33 bits. The gap is clearly visible. ($E_1(0) = 64 = 2(33 - 1)$ because the invariant states all have an even
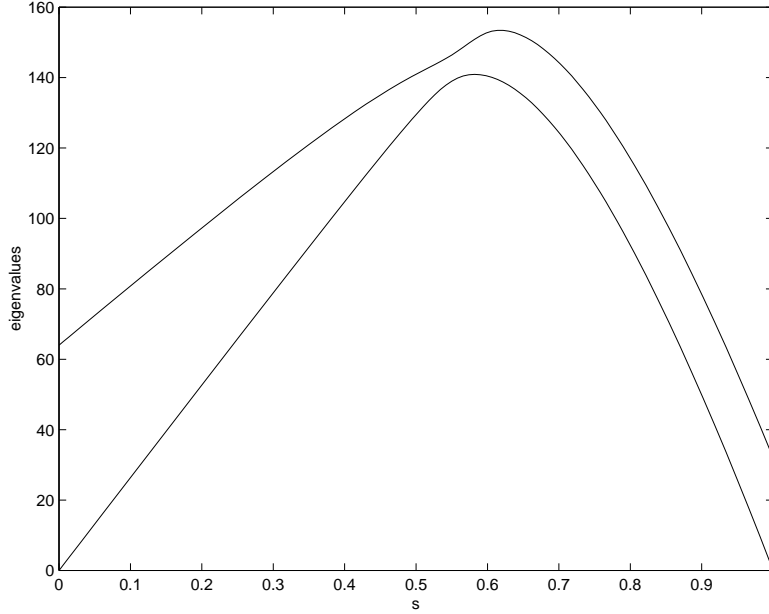
Figure 11: *The two lowest eigenvalues of $\widetilde{H}(s)$, restricted to the invariant subspace, for overconstrained 2-SAT with $n = 33$. The visible gap indicates that $g_{\min}$ is not exponentially small.*

number of 1's in the x-basis.) In Fig. 12 we plot $\log(g_{\min})$ against $\log(n)$. The straight line shows that $g_{\min} \sim n^p$ with $p \simeq 0.7$. For this problem the maximum eigenvalues of H_B and H_P are both of order n^2 so $\mathcal{E}$ appearing in (2.8) is no larger than n^2. Adiabatic evolution with T only as big as $n^{(2-2p)}$ will succeed in finding the satisfying assignment for this set of problems.

5   The Conventional Quantum Computing Paradigm

The algorithm described in this paper envisages continuous-time evolution of a quantum system, governed by a smoothly-varying time-dependent Hamiltonian. Without further development of quantum computing hardware, it is not clear whether this is more or less realistic than conventional quantum algorithms, which are described as sequences of unitary operators each acting on a small number of qubits. In any case, our algorithm can be recast within the conventional quantum computing paradigm using the technique introduced by Lloyd [5].

The Schrödinger equation (2.1) can be rewritten for the unitary time evolution operator $U(t, t_0)$,

$$i\frac{\mathrm{d}}{\mathrm{d}t}U(t, t_0) = H(t)U(t, t_0) \tag{5.1}$$

and then

$$|\psi(T)\rangle = U(T, 0)|\psi(0)\rangle \ . \tag{5.2}$$

To bring our algorithm within the conventional quantum computing paradigm we need to approximate $U(T, 0)$ by a product of few-qubit unitary operators. We do this by first discretizing the interval $[0, T]$ and then applying the Trotter formula at each discrete time.

The unitary operator $U(T, 0)$ can be written as a product of M factors

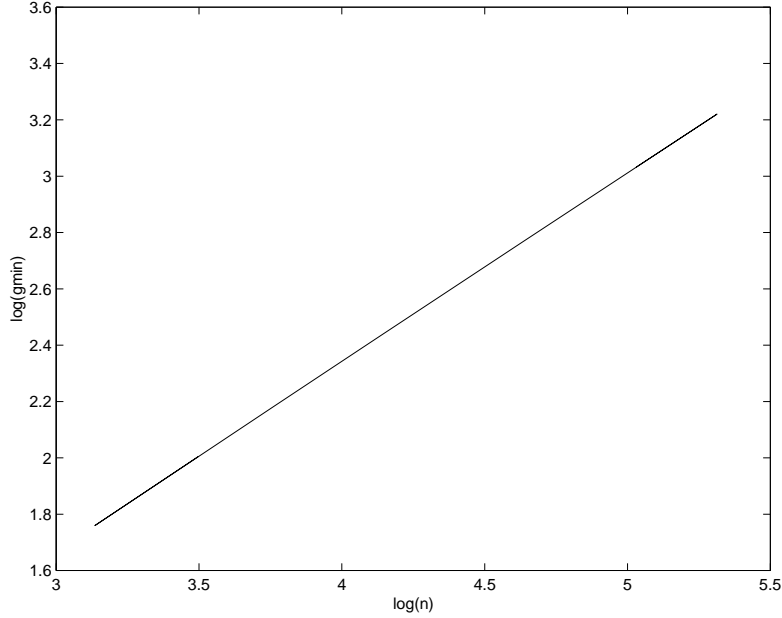$$U(T, 0) = U(T, T - \Delta)U(T - \Delta, T - 2\Delta) \cdots U(\Delta, 0) \tag{5.3}$$

Figure 12: *Overconstrained 2-SAT;* $\log(g_{\min})$ *versus* $\log(n)$ *with* n *ranging from 33 to 203. The straight line indicates that* $g_{\min} \sim n^p$.

where $\Delta = T/M$. We use the approximation

$$U((\ell + 1)\Delta, \ell\Delta) \simeq e^{-i\Delta H(\ell\Delta)} \tag{5.4}$$

which is valid in (5.3) if

$$\left\|\Delta H(t_1) - \Delta H(t_2)\right\| \ll \frac{1}{M} \quad \text{for all} \quad t_1, t_2 \in [\ell\Delta, (\ell + 1)\Delta] . \tag{5.5}$$

Using (2.23) this becomes

$$\Delta\left\|H_{\mathrm{P}} - H_{\mathrm{B}}\right\| \ll 1 . \tag{5.6}$$

We previously showed (in the paragraph after Eq. (2.29)) that $\|H_{\mathrm{P}} - H_{\mathrm{B}}\|$ grows no faster than the number of clauses, which we always take to be at most polynomial in n. Thus we conclude that the number of factors $M = T/\Delta$ must be of order T times a polynomial in n.

Each of the M terms in (5.3) we approximate as in (5.4). Now $H(\ell\Delta) = uH_{\mathrm{B}} + vH_{\mathrm{P}}$ where $u = 1 - (\ell\Delta/T)$ and $v = \ell\Delta/T$ are numerical coefficients each of which is between 0 and 1. To use the Trotter formula

$$e^{-i\Delta H(\ell\Delta)} \simeq \left(e^{-i\Delta u H_{\mathrm{B}}/K} e^{-i\Delta v H_{\mathrm{P}}/K}\right)^K \tag{5.7}$$

for each ℓ, $\ell = 0, 1, \ldots, M - 1$, we need $K \gg M\left(1 + \Delta\|H_{\mathrm{B}}\| + \Delta\|H_{\mathrm{P}}\|\right)^2$. Since $\|H_{\mathrm{B}}\|$ and $\|H_{\mathrm{P}}\|$ are at most a small multiple of the number of clauses, we see that K need not be larger than M times a polynomial in n.

Now (5.7) is a product of $2K$ terms each of which is $e^{-i\Delta u H_{\mathrm{B}}/K}$ or $e^{-i\Delta v H_{\mathrm{P}}/K}$. From (2.22) we see that H_{B} is a sum of n commuting one-bit operators. Therefore $e^{-i\Delta u H_{\mathrm{B}}/K}$ can be written (exactly) as a product of n one-qubit unitary operators. The operator H_{P} is a sum of commuting operators,

one for each clause. Therefore $e^{-i\Delta v H_{\mathrm{P}}/K}$ can be written (exactly) as a product of unitary operators, one for each clause acting only on the qubits involved in the clause.

All together $U(T,0)$ can be well approximated as a product of unitary operators each of which acts on a few qubits. The number of factors in the product is proportional to T^2 times a polynomial in n. Thus if the required T for adiabatic evolution is polynomial in n, so is the number of few-qubit unitary operators in the associated conventional quantum computing version of the algorithm.

6 Outlook

We have presented a continuous-time quantum algorithm for solving satisfiability problems, though we are unable to determine, in general, the required running time. The Hamiltonian that governs the system's evolution is constructed directly from the clauses of the formula. Each clause corresponds to a single term in the operator sum that is $H(t)$. We have given several examples of special cases of the satisfiability problem where our algorithm runs in polynomial time. Even though these cases are easily seen to be classically solvable in polynomial time, our algorithm operates in an entirely different way from the classical one, and these examples may provide a small bit of evidence that our algorithm may run quickly on other, more interesting cases.

References

[1] A. Messiah, *Quantum Mechanics*, Vol. II, Amsterdam: North Holland; New York: Wiley (1976).

[2] L.K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search", quant-ph/9605043; Phys. Rev. Lett. **78**, 325 (1997).

[3] E. Farhi, S. Gutmann, "An Analog Analogue of a Digital Quantum Computation", quant-ph/9612026; Phys. Rev. A **57**, 2403 (1998).

[4] C.H. Bennett, E. Bernstein, G. Brassard and U.V. Vazirani, "Strengths and Weaknesses of Quantum Computing", quant-ph/9701001.

[5] S. Lloyd, "Universal Quantum Simulators", Science **273**, 1073 (1996).