Solving a hidden subgroup problem using the adiabatic quantum-computing paradigm

M. V. Panduranga Rao*
Department of Computer Science and Automation, Indian Institute of Science, Bangalore 560 012, India

We present and solve a restricted Abelian hidden subgroup problem using the adiabatic quantum-computing paradigm. The time step complexity is shown to be a polynomial in the number of input qubits. This paper is a step towards looking at the Abelian hidden subgroup problem from a quantum adiabatic standpoint.

I. INTRODUCTION

Models of quantum computing in the continuous time domain have evoked a lot of interest in recent times. Adiabatic quantum computing is one such model. It has been applied to problems such as restricted versions of Boolean formula satisfiability [1] and the Deutsch-Jozsa problem [2]. This model has also been shown to be ''truly quantum in nature'' in Ref. [3], where a quadratic speedup in searching an unordered list is achieved. It may be recalled that a classic result in ''discrete'' quantum computing, Grover's algorithm [4], achieves the same. Another interesting problem that has been closely examined in the discrete setting is the following [5].

The hidden subgroup problem (HSP). Given an efficiently computable function $\phi: G \rightarrow S$ from a finite group G to a set S, which is constant on the (left) cosets of some hidden subgroup H and takes distinct values for distinct cosets, find the generating set for H.

Polynomial time solutions have been proposed for Abelian groups, including those with immense practical applications such as Shor's algorithm [6] for prime factorization.

In this paper, we take a step towards studying the HSP ''quantum adiabatically.'' Simon's problem [7] seems to be an appropriate starting point in that direction, as it was for the discrete paradigm. This problem is defined over the group $\mathcal{Z}_2^n$ with ''bitwise exclusive OR'' ($\otimes$) as the group operation. The problem considered in this paper is a restriction of Simon's problem in that we disallow the trivial hidden subgroup (consisting of only the identity element 0^n).

Modified Simon's problem (MSP). Given a function $\phi: \{0,1\}^n \rightarrow \{0,1\}^{n-1}$ such that $\phi(x) = \phi(x')$ if and only if $x' = x \oplus h$, for $h \in \{0^n, c\}$, where $c \in \{0,1\}^n \setminus 0^n$.

Problem. Find c.

Note that $\{0^n, c\}$ is the hidden subgroup in this case. The original problem of Simon has the range $\{0,1\}^m$, $m \geqslant n$. Reducing this range to $\{0,1\}^{n-1}$ does not significantly reduce the toughness of the problem.

II. THE ADIABATIC QUANTUM-COMPUTING PARADIGM

The adiabatic quantum-computing paradigm is based on the adiabatic theorem of quantum mechanics. The rest of this section describes the theorem and the computing technique. For a more comprehensive treatment, the reader is referred to Ref. [8] and Refs. [1–3], respectively.

Let $H(s)$ $(0 \leqslant s = t/T \leqslant 1)$ be a time-dependent Hamiltonian $\hat{H}(t)$ acting on a system having an N-dimensional Hilbert space, scaled linearly in time by a delay factor T. At any instant s, let the eigenstates of $H(s)$ be given by $|l;s\rangle$ and the eigenvalues by $\lambda_l(s)$, with $\lambda_0(s) \leqslant \lambda_1(s) \leqslant \cdots \leqslant \lambda_{N-1}(s)$. Suppose we start with the initial state of the system $|\psi(0)\rangle$ as $|0;0\rangle$ [the ground state of $H(0)$] and apply the Hamiltonian $H(s)$, $0 \leqslant s \leqslant 1$, to evolve it to $|\psi(1)\rangle$ at $s = 1$. Then the quantum adiabatic theorem states that for a ''large enough'' delay factor T, the final state of the system $|\psi(1)\rangle$ will be arbitrarily close to the ground state $|0;1\rangle$ of $H(1)$. In addition, for the purpose of efficient computation, we also require T to be small. Let $g_{min} = \min_{0 \leqslant s \leqslant 1}[\lambda_1(s) - \lambda_0(s)]$. Then the delay required for such an evolution to take place is given by

$$T \gg \frac{\max_{0 \leqslant s \leqslant 1} \left\| \left\| \frac{d}{ds} H(s) \right\| \right\|_2}{g_{min}^2}. \tag{1}$$

The interpolating Hamiltonian

In this section, we present an overview of the general technique. Adiabatic quantum computing is useful when a problem can be reformulated as a minimization problem—given a function $f: \{0,1\}^n \rightarrow \mathcal{R}$ (computable in time polynomial in n), find those inputs $\{x_i\}_{i=1}^k$ for which f is minimum.

We construct the final Hamiltonian $H(1)$ in such a way that its ground state encodes the required solution set $\{x_i\}_{i=1}^k$. An obvious way is to associate the eigenvalues of $H(1)$ with the function values so that

$$H(1) = \sum_{z \in \{0,1\}^n} f(z) |z\rangle\langle z|,$$

where $\{|z\rangle\}$ form the ''computational basis'' of the Hilbert space of the system.

The initial Hamiltonian is independent of the problem, with the restriction that it should *not* be diagonal in the computational basis [1]. It is easy to see that the following Hamiltonian satisfies the above condition:

*Electronic address: pandurang@csa.iisc.ernet.in

$$H(0)=\sum_{z\in\{0,1\}^n\setminus 0^n}|\hat{z}\rangle\langle\hat{z}|, \tag{2}$$

where each $|\hat{z}\rangle$ is a basis vector in the ''Hadamard'' basis given by

$$|\hat{z}\rangle=\frac{1}{\sqrt{2^n}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}^{\otimes n}|z\rangle$$

and the ground state is $(1/\sqrt{2^n})\Sigma_{z\in\{0,1\}^n}|z\rangle$, which is easy to construct. Given the initial and final Hamiltonians, define the interpolating Hamiltonian as

$$H(s)=(1-s)H(0)+sH(1). \tag{3}$$

We start in the ground state of $H(0)$ and evolve to $H(1)$ slowly enough and end up in its ground state. However, since the eigenvalues have been associated with function values, the ground state is a superposition of all solutions. If $f(x)$ is bounded by a polynomial in n then so is the numerator of Eq. (1), $|||(d/ds)H(s)|||_2$. The deciding factor then is the denominator g_{min}^2.

III. SOLUTION TO MSP

Choose $x\in\{0,1\}^n\setminus 0^n$ uniformly at random. With a very high probability $[1-1/(2^n-1)]$, $x\neq c$. Let the final Hamiltonian be

$$H(1)=\sum_{z\in\{0,1\}^n}\left(\frac{|\phi(x)-\phi(x\oplus z)|}{N}+(1-\delta_{\phi(x),\phi(x\oplus z)})n\right)|z\rangle\langle z|, \tag{4}$$

where $\delta_{i,j}$ is the delta function (having value 1 if $i=j$ and 0 otherwise) and $N=2^n$. Clearly, f, the function to be minimized, is bounded by a polynomial in n. Therefore, the crucial factor in determining the time delay is g_{min}. We take the initial Hamiltonian as given by Eq. (2) and use Eq. (3) to obtain $H(s)$.

Lemma 1. The characteristic equation of $H(s)$ is

$$c(\lambda)=(1-s-\lambda)\Bigg[(1-s-\lambda)\prod_{k=1}^{N/2-2}\left[1-s+\left(\frac{k}{N}+n\right)s-\lambda\right]^2\left\{1-s+\left[\left(\frac{N}{2}-1\right)\frac{1}{N}+n\right]s-\lambda\right\}\left\{\frac{(N-1)}{N}(1-s)+\left[\left(\frac{N}{2}-1\right)\frac{1}{N}+n\right]s-\lambda\right\}-\frac{1-s}{N}\Bigg\{\prod_{k=1}^{N/2-1}\left[1-s+\left(\frac{k}{N}+n\right)s-\lambda\right]^2+2(1-s-\lambda)\sum_{j=1}^{N/2-2}\prod_{k=1}^{N/2-1}\frac{\left[1-s+\left(\frac{k}{N}+n\right)s-\lambda\right]^2}{1-s+\left(\frac{j}{N}+n\right)s-\lambda}+(1-s-\lambda)\prod_{k=1}^{N/2-1}\frac{\left[1-s+\left(\frac{k}{N}+n\right)s-\lambda\right]^2}{1-s+\left[\left(\frac{N}{2}-1\right)\frac{1}{N}+n\right]s-\lambda}\Bigg\}\Bigg]-\frac{1-s}{N}(1-s-\lambda)\prod_{k=1}^{N/2-1}\left[1-s+\left(\frac{k}{N}+n\right)s-\lambda\right]^2=0.$$

Proof. To evaluate the eigenvalues $\lambda(s)$'s[1] of $H(s)$, we evaluate the determinant

$$|H(s)-\lambda I|=0.$$

Subtracting the last column of this determinant from all other columns and using x_0 for $1-s-\lambda$, x_1 for $1-s+(1/N+n)s-\lambda$ and so on up to $x_{N/2-1}$ for $1-s+[(N/2-1)(1/N)+n]s-\lambda$, we have

$$\begin{vmatrix} x_0 & 0 & 0 & \cdots & \cdots & -\frac{(1-s)}{N}\\ 0 & x_0 & 0 & \cdots & \cdots & -\frac{(1-s)}{N}\\ \vdots & 0 & \ddots & \vdots & x_{N/2-1} & \vdots\\ -x_{N/2-1} & -x_{N/2-1} & \cdots & & -x_{N/2-1} & \left(x_{N/2-1}-\frac{(1-s)}{N}\right)\end{vmatrix}_{N\times N}=0.$$

[1]We use λ and $\lambda(s)$ interchangeably.

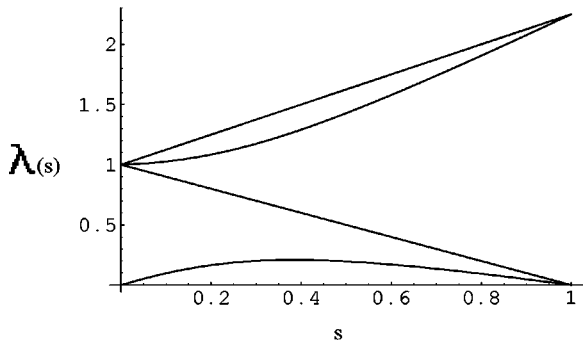

FIG. 1. $N=4$.

Expanding this determinant gives the required characteristic equation.

Remark. In the above characteristic equation, $N/2$ of the N eigenvalue curves are immediately identifiable (as factors).[2] (See Figs. 1–3.) They are (in increasing order at $s=1$) $\lambda_1(s)=1-s$, $\lambda_3(s)=1-s+(1/N+n)s, \ldots, \lambda_{N-1}=1-s+[(N/2-1)(1/N)+n]s$.

We now state a classic result from the theory of equations.

Theorem 1. If a real polynomial $f(x)$ for $x=a$ and $x=b$ takes values $f(a)$ and $f(b)$ of opposite signs, so that, for instance, $f(a)<0$ and $f(b)>0$, then there is a root of the equation $f(x)=0$ in the interval (a,b).

The above theorem will be used extensively to prove our result.

Lemma 2. There exists exactly one root (i.e., an eigenvalue curve) of the characteristic equation (Lemma 1) in the intervals $(0,1-s)$, $(1-s,1-s+(1/N+n)s), \ldots, (1-s+[(N/2-2)(1/N)+n]s, 1-s+[(N/2-1)(1/N)+n]s)$; $s\in(0,1)$.

Proof. Consider the interval $(0,\lambda_1(s)=1-s)$. Let $\lambda(s)=\delta$ and $\lambda(s)=1-(1+\epsilon)s$ be two lines, where δ and ϵ are positive reals tending to 0. Substituting for λ in $c(\lambda)$, we see that $c(\delta)>0$ and $c[1-(1+\epsilon)s]<0$ for $s\in(0,1)$. Therefore, by Theorem 1, there exists a root of $c(\lambda)=0$ in the interval $(0,1-s)$ for $s\in(0,1)$. Similarly, in the interval $(1-s,1-s+(1/N+n)s)$, $c(1-s+\delta s)>0$ and $c[1-s+(1/N+n-\epsilon)s]<0$. For $(1-s+(k/N+n)s, 1-s+[(k+1)/N+n]s)$, $1\leqslant k\leqslant N/2-2$, we have $c[1-s+(k/N+n+\delta)s]>0$ and $c(1-s+[(k+1)/N+n-\epsilon]s)<0$ for $s\in(0,1)$.

Therefore there is a root in each interval. Given that (i) there are $N/2$ open intervals bounded by $N/2$ straight line eigenvalue curves; (ii) there is at least one root in each interval; and (iii) there are N roots in all, the lemma follows.

The eigenvalue curves $\lambda_0(s)$ and $\lambda_1(s)$ intersect at $s=1$ because there is more than one solution (0 and c). Note that $H(s)$ commutes with the operations $|0^n\rangle\leftrightarrow|c\rangle$, which rules out transitions between the eigenstates $(1/\sqrt{2})(|0^n\rangle+|c\rangle)$ and $(1/\sqrt{2})(|0^n\rangle-|c\rangle)$ corresponding to the eigenvalues $\lambda_0(1)$ and $\lambda_1(1)$, respectively. By the same argument as

[2]See, example, eigenvalue curves in the Appendix.

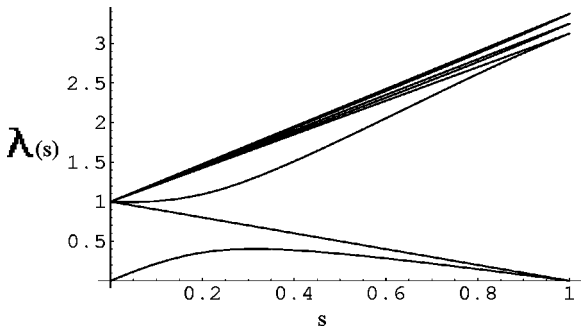

FIG. 2. $N=8$.

given in Sec. 3.2 of Ref. [1], we consider the gap between $\lambda_0(s)$ and $\lambda_2(s)$.

We will try to estimate the minimum gap between $\lambda_0(s)$ and $\lambda_2(s)$ by studying their slopes. The Wielandt-Hoffman theorem [9] is a useful tool for obtaining an upper bound on their instantaneous slopes.

Theorem 2. Wielandt-Hoffman Theorem (WHT): Let A and E be real symmetric matrices and let $\hat{A}=A+E$. Let the eigenvalues of A be $\lambda_0\leqslant\lambda_1\leqslant\cdots\leqslant\lambda_{N-1}$ and those of $\hat{A}$ be $\hat{\lambda}_0\leqslant\hat{\lambda}_1\leqslant\cdots\leqslant\hat{\lambda}_{N-1}$. Then

$$\left[\sum_{j=0}^{N-1}(\lambda_j-\hat{\lambda}_j)^2\right]^{1/2}\leqslant\left[\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}|E_{ij}|^2\right]^{1/2}. \tag{5}$$

Let E of the WHT be the "perturbation matrix" $H(s+ds)-H(s)$. This completely specifies the right-hand side (rhs) of Eq. (5). In the collection of $N/2$ straight-line eigenvalues, consider the following set: $\{\lambda_3(s)=1-s+(1/N+n)s, \ldots, \lambda_{N-1}(s)=1-s+[(N/2-1)(1/N)+n]s\}$. Their slopes $d\lambda/ds$ are known. These lines are closely spaced in the sense that they start at $\lambda(0)=1$ and the gap between "consecutive" lines is just $1/N$ at $s=1$. Consider any interval $(1-s+(k/N+n)s, 1-s+[(k+1)/N+n]s)$, $1\leqslant k\leqslant N/2-2$. There lies an eigenvalue curve $\lambda^k(s)$ in it with $\lambda^k(0)=1$ and $\lambda^k(1)=n+(k+1)/N$, so that its average slope is $n+(k+1)/N-1$. Since the WHT deals with only squared terms, both positive and negative slopes of equal magnitude can be treated at par. Due to such a small gap between $1-s+(k/N+n)s$ and $1-s+[(k+1)/N+n]s$, any significant deviation (in magnitude) of the slope from the

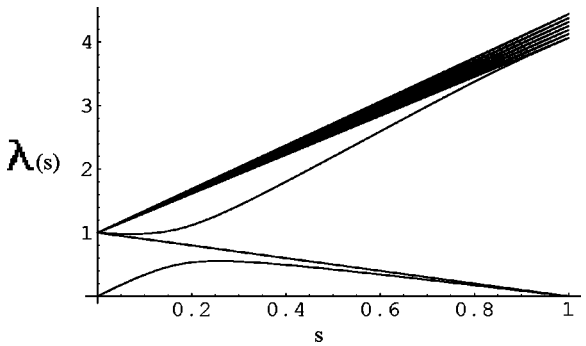

FIG. 3. $N=16$.

average is short lived. Moreover, it has to be compensated later to maintain the average. For example, $\lambda^k(s)$ having a slope zero at a stretch is possible for a duration of only

$$\frac{p}{N\left(n+\frac{k+1}{N}-1\right)}, \quad 0\leqslant p\leqslant 1 \quad \text{(by simple trigonometry)}.$$

The maximum can be attained only towards the end ($p=1$). Therefore, we can approximate the slope of $\lambda^k(s)$ by $n+(k+1)/N-1$, $1\leqslant k\leqslant N/2-2$ for use in the WHT with negligible error. But the same cannot be said about the slopes $d\lambda_0(s)/ds$ and $d\lambda_2(s)/ds$ as $\lambda_0(s)$ and $\lambda_2(s)$ are not bounded by closely spaced lines.

Lemma 3. $[d\lambda_0(s)/ds]^2+[d\lambda_2(s)/ds]^2\leqslant n^2+\frac{3}{2}$.

Proof. Substitute the values of the $d\lambda$'s and the matrix elements of the perturbation matrix E in the WHT to obtain

$$\begin{aligned}
&2\sum_{k=2}^{N/2-1}\left(n+\frac{k}{N}-1\right)^2(ds)^2+\left(n+\frac{1}{N}-1\right)^2(ds)^2+(ds)^2\\
&\quad+(d\lambda_0)^2+(d\lambda_2)^2\\
&\leqslant 2\left(\frac{N-1}{N}\right)^2(ds)^2+N\frac{(N-1)}{N^2}(ds)^2\\
&\quad+2\sum_{k=1}^{N/2-1}\left(n+\frac{k}{N}-\frac{N-1}{N}\right)^2(ds)^2. \qquad (6)
\end{aligned}$$

Rearranging some terms, we have

$$\begin{aligned}
&\left(\frac{d\lambda_0(s)}{ds}\right)^2+\left(\frac{d\lambda_2(s)}{ds}\right)^2\\
&\quad\leqslant\left[2\left(\frac{N-1}{N}\right)^2+\frac{N-1}{N}-1\right]+\left[2\left(n+\frac{1}{N}-\frac{N-1}{N}\right)^2\right.\\
&\qquad\left.-\left(n+\frac{1}{N}-1\right)^2\right]+\left[2\left(\sum_{k=2}^{N/2-1}\left(n+\frac{k}{N}-\frac{N-1}{N}\right)^2\right.\right.\\
&\qquad\left.\left.-\sum_{k=2}^{N/2-1}\left(n+\frac{k}{N}-1\right)^2\right)\right].
\end{aligned}$$

Let us evaluate the expressions in square brackets of the rhs individually for the sake of clarity.

$$2\left(\frac{N-1}{N}\right)^2+\frac{N-1}{N}-1=3-\frac{5}{N}+\frac{2}{N^2}-1\approx 2,$$

$$\begin{aligned}
&2\left(n+\frac{1}{N}-\frac{N-1}{N}\right)^2-\left(n+\frac{1}{N}-1\right)^2\\
&\quad\approx\left(n+\frac{1}{N}-1\right)^2\approx(n-1)^2,
\end{aligned}$$

$$\begin{aligned}
&2\left[\sum_{k=2}^{N/2-1}\left(n+\frac{k}{N}-\frac{N-1}{N}\right)^2-\sum_{k=2}^{N/2-1}\left(n+\frac{k}{N}-1\right)^2\right]\\
&\quad=2\left[\sum_{k=2}^{N/2-1}\left(n+\frac{k}{N}-\frac{N-1}{N}+n+\frac{k}{N}-1\right)\right.\\
&\qquad\left.\times\left(n+\frac{k}{N}-\frac{N-1}{N}-n-\frac{k}{N}+1\right)\right]\\
&\quad=\frac{2}{N}\sum_{k=2}^{N/2-1}\left(2n+\frac{2k}{N}-\frac{2N-1}{N}\right)=2n-\frac{3}{2}.
\end{aligned}$$

We have ignored small terms [of $O(n/N)$] because whatever little error that occurs turns out to be on the conservative side. Reassembling the three expressions, we have

$$\left(\frac{d\lambda_0(s)}{ds}\right)^2+\left(\frac{d\lambda_2(s)}{ds}\right)^2\leqslant(n-1)^2+2n-\frac{3}{2}+2=n^2+\frac{3}{2}.$$

Corollary 3.1. From the above lemma, it is easy to see that $\sqrt{n^2+\frac{3}{2}}$ is an upper bound for both $|d\lambda_0/ds|$ and $|d\lambda_2/ds|$.

We are now in a position to state the main results of the paper.

Lemma 4. The minimum time s_1 required for the $\lambda_0(s)$ eigenvalue curve to rise to [within $O(1/N)$ distance of] the $\lambda_1(s)$ curve is $1/(1+\sqrt{n^2+\frac{3}{2}})$.

Proof. The minimum time will be attained when the $\lambda_0(s)$ rises with the maximum available slope. Therefore, $(1-s_1)/s_1=\sqrt{n^2+\frac{3}{2}}$, from which we have $s_1=1/(1+\sqrt{n^2+\frac{3}{2}})$. Using binomial expansion,

$$s_1\approx\frac{1}{1+n+\frac{3}{4n}}. \qquad (7)$$

Theorem 3. The minimum gap between $\lambda_0(s)$ and $\lambda_2(0)$ for $s\in[0,1]$ is $O(1/poly(n))$.

Proof. Consider the interval $(\lambda_1(s)=1-s,\lambda_3(s)=1-s+(1/N+n)s)$. There exists exactly one eigenvalue curve $\lambda_2(s)$ in this interval. Further, $c[1-s+(1/N+n-\delta)s]<0$ for a positive δ tending to 0. Consider a line $\lambda_1'(s)=1-(1-1/m)s$ where $m=\text{poly}(n)$ or a polynomial in n. Since it lies above[3] $\lambda_1(s)=1-s$, the $\lambda_2(s)$ eigenvalue curve may not lie between $\lambda_3(s)$ and $\lambda_1'(s)$ for the entire interval $s\in[0,1]$. To find the interval in which it does lie, we solve[4] $c[1-(1-1/m)s]>0$ for s and invoke Theorem 1.

---

[3]By above we mean $\lambda_1'(s)>\lambda_1(s)$ for $s\in(0,1]$ (or any other interval, if specified).

[4]Note that $(1-s+[(N/2-1)(1/N)+n]s-\lambda)([(N-1)/N](1-s)+[(N/2-1)(1/N)+n]s-\lambda)$, the first term in the square bracket of $c(\lambda)$, has been approximated by $(1-s+[(N/2-1)(1/N)+n]s-\lambda)^2$. The error introduced because of this can be ignored in Eq. (8) and later.

Theorem 1.

$$-\frac{s}{m}\left\{-\frac{s}{m}s^{N-2}\prod_{k=1}^{N/2-1}\left(\frac{k}{N}+n-\frac{1}{m}\right)^2-\frac{1-s}{N}\left[2s^{N-2}\prod_{k=1}^{N/2-1}\left(\frac{k}{N}+n-\frac{1}{m}\right)^2-\frac{2s}{m}s^{N-3}\sum_{j=1}^{N/2-2}\prod_{k=1}^{N/2-1}\frac{\left(\frac{k}{N}+n-\frac{1}{m}\right)^2}{\frac{j}{N}+n-\frac{1}{m}}\right.\right.$$
$$\left.\left.-\frac{s}{m}s^{N-3}\prod_{k=1}^{N/2-1}\frac{\left(\frac{k}{N}+n-\frac{1}{m}\right)^2}{\left(\frac{N}{2}-1\right)\frac{1}{N}+n-\frac{1}{m}}\right]\right\}\geqslant 0,$$

which gives

$$s\geqslant\frac{1}{1+\frac{N}{m\left(\frac{2}{m}\sum_{j=1}^{N/2-2}\frac{1}{\frac{j}{N}+n-\frac{1}{m}}+\frac{1}{m}\frac{1}{\left(\frac{N}{2}-1\right)\frac{1}{N}+n-\frac{1}{m}}-2\right)}}. \tag{8}$$

But,

$$\sum_{j=1}^{N/2-2}\frac{1}{\frac{j}{N}+n-\frac{1}{m}}=N\sum_{j=1}^{N/2-2}\frac{1}{j+N\left(n-\frac{1}{m}\right)}=N\sum_{N(n-1/m)+1\leqslant j\leqslant N/2-2+N(n-1/m)}\frac{1}{j}.$$

Separating into two summations, we have the sum as

$$N\left(\sum_{1\leqslant j\leqslant N/2-2+N(n-1/m)}\frac{1}{j}-\sum_{1\leqslant j\leqslant N(n-1/m)}\frac{1}{j}\right).$$

The two summations above are in the form of harmonic numbers. The sum to p terms of a harmonic series is bounded as $\ln(p)<\Sigma_{k=1}^{p}1/k<\ln(p)+1$. Therefore,

$$N\sum_{j=1}^{N/2-2}\frac{1}{j+N\left(n-\frac{1}{m}\right)}\approx N\ln\frac{\frac{N}{2}-2+N\left(n-\frac{1}{m}\right)}{N\left(n-\frac{1}{m}\right)}\approx N\ln\left(1+\frac{1}{2\left(n-\frac{1}{m}\right)}\right).$$

Expanding the logarithm,

$$\approx N\left(\frac{1}{2\left(n-\frac{1}{m}\right)}-\frac{1}{8\left(n-\frac{1}{m}\right)^2}\right). \tag{9}$$

Substituting in Eq. (8), we get

$$s\geqslant\frac{1}{1+\frac{1}{\frac{1}{n-\frac{1}{m}}-\frac{1}{4\left(n-\frac{1}{m}\right)^2}+\frac{1}{N}\frac{1}{\left(\frac{N}{2}-1\right)\frac{1}{N}+n-\frac{1}{m}}-2\frac{m}{N}}}.$$

Ignoring smaller terms,

$$s \geqslant \frac{1}{1+\frac{4\left(n-\frac{1}{m}\right)^2}{4\left(n-\frac{1}{m}\right)-1}} = \frac{1}{1+n-\frac{1}{m}+\frac{n-\frac{1}{m}}{4\left(n-\frac{1}{m}\right)-1}},$$

which gives

$$s \geqslant \frac{1}{1+n-\frac{1}{m}+\frac{1}{4}}. \tag{10}$$

This implies that the line $\lambda_1'(s)=1-(1-1/m)s$ cuts $\lambda_2(s)$ at

$$s_2 = 1/(1+n-1/m+1/4)$$

[and therefore $\lambda_2(s)>\lambda_1'(s)$ for $s_2<s\leqslant 1$]. This happens at

$$\lambda_1'(s_2)=\lambda_2(s_2)=1-\left(1-\frac{1}{m}\right)\frac{1}{1+n-\frac{1}{m}+\frac{1}{4}},$$

which is above the $\lambda_1(s)$ curve by an inverse polynomial distance. Clearly, the minimum time required by the $\lambda_0(s)$ eigenvalue curve to reach $\lambda_0(s)=1-s$ [given by Eq. (7)], s_1, is greater than s_2. Therefore, by the time $\lambda_0(s)$ nears $\lambda_1(s)=1-s$, there exists an inverse polynomial gap between $\lambda_2(s)$ curve and $\lambda_0(s_1)[\approx\lambda_1(s_1)]$ which only increases for $s_1<s\leqslant 1$. Since the numerator of Eq. (1) is a polynomial in n and the denominator is an inverse polynomial in n, the total time delay for evolution to the solution state is upper bounded by a polynomial.

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

[2] Saurya Das, Randy Kobes, and Gabor Kunstatter, Phys. Rev. A **65**, 062310 (2002); e-print quant-ph/0111032.

[3] W. van Dam, M. Mosca, and U. Vazirani, *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, (IEEE Computer Society Press, Los Alamitos, CA, 2001), pp. 279–287; e-print quant-ph/0206003; Jeremie Roland and Nicolas J. Cerf, Phys. Rev. A **65**, 042308 (2002); e-print quant-ph/0107015.

[4] Lov Grover, *Proceedings of the 28th Annual Symposium on Theory of Computing*, (ACM Press, New York, 1996), pp. 212–219.

[5] Sean Hallgren, Ph.D. thesis, University of California, Berkeley, CA, 2000 (unpublished).

[6] P.W. Shor, SIAM J. Comput. **26**, 1484 (1997); e-print quant-ph/9508027.

[7] Daniel R. Simon, SIAM J. Comput. **26**, 1474 (1997).

[8] Albert Messiah, *Quantum Mechanics* (Wiley, New York, 1958).

[9] A.J. Hoffman and H.W. Wielandt, Duke Math. J. **20**, 37 (1953).