Exponential algorithmic speedup by quantum walk

Yan-Tong Lin

National Chiao Tung University

QIQC 2020fall, 2020/12/22

Outline

1. Introduction

2. The problem

3. Quantum algorithm

4. Classical lower bound

5. Discussion

1. Introduction
2. The problem
3. Quantum algorithm
4. Classical lower bound
5. Discussion

Previous Work

- Quantum analogues to random walks were proposed
- Separation was not "algorithmic"

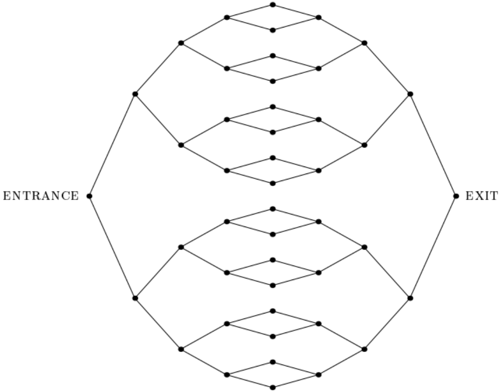


Figure: The graph G_4.

This Paper

Provide a graph where the separation is "algorithmic".

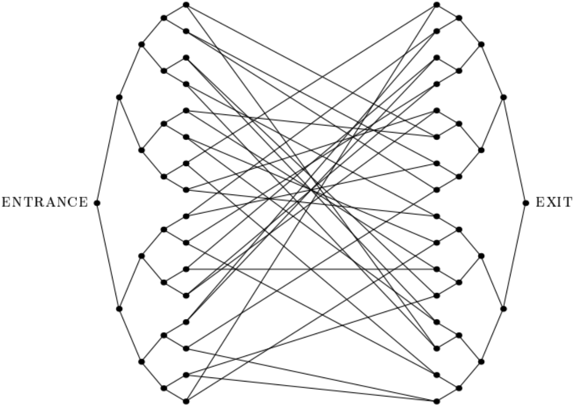


Figure: A typical graph G_4'.

1. Introduction
2. The problem
3. Quantum algorithm
4. Classical lower bound
5. Discussion

The problem

- Input: an oracle for the graph and the name of the ENTRANCE
- Output: find the name of the EXIT

- number of vertex is N and $n = O(\log(n))$
- names are $2n$-bit string

1. Introduction
2. The problem
3. Quantum algorithm
   - Quantum walk
   - Implementing the quantum walk
   - Propagation on a line
   - Upper bound on the hitting time
4. Classical lower bound
5. Discussion

Classical Random Walk

Markov process

$$K_{aa'} = \begin{cases} \gamma & a \neq a',\ aa' \in G \\ 0 & a \neq a',\ aa' \notin G \\ -d(a)\gamma & a = a'\,. \end{cases} \tag{1}$$

$$\frac{\mathrm{d}p_a(t)}{\mathrm{d}t} = \sum_{a'} K_{aa'}\, p_{a'}(t)\,. \tag{2}$$

here γ is the probability to go to an adjacent vertex in a unit time.

Quantum Analogue

the Schrödinger equation

$$i\frac{\mathrm{d}}{\mathrm{d}t}\langle a|\psi(t)\rangle = \sum_{a'}\langle a|H|a'\rangle\langle a'|\psi(t)\rangle \tag{3}$$

- In **[FG98]**, $\langle a|H|a'\rangle = K_{aa'}$
- In this paper,

$$\langle a|H|a'\rangle = \begin{cases} \gamma & a \neq a',\ aa' \in G \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

For norm preserving, a Hamiltonian with Hermiticity is required.

Goal

simulate the unitary evolution e^{-iHt} with H given by (4)

Implementing the quantum walk - the Oracle

To make the oracle, an additional structure is required
a consistent k-edge coloring, here $k = \mathrm{poly}(\log N)$.

Definition

An edge coloring is consistent if no vertex is incident with two edges of the same color.

Remark

We will show that the oracle can provide a consistent coloring for the graph that cannot be used by any classical algorithm to help solve the problem, since a classical algorithm could make up the coloring as it goes.

Implementing the quantum walk - the Oracle (Cont.)

Given a consistent coloring, the graph is presented with the oracle U

$$U|a, b, c\rangle = |a, b \oplus v_c(a), c\rangle \tag{5}$$

- a, b are $2n$-bit strings
- c is a color
- $v_c(a) = a'$, $a' = 11\ldots1$ if vertex a doesn't exist or there is no incident edge of color c
- Note that $v_c(v_c(a)) = a$ for $v_c(a) \neq 11\ldots1$

Implementing the quantum walk - the Oracle (Cont.)

Since no query with a superposition of colors will be used and we want to track whether there is an $11\ldots1$ case, we construct oracle V_c for each color c with U.

the final oracle

$$V_c|a,b,r\rangle = |a, b \oplus v_c(a), r \oplus f_c(a)\rangle\,, \tag{6}$$

where

$$f_c(a) = \begin{cases} 0 & v_c(a) \neq 11\ldots1 \\ 1 & v_c(a) = 11\ldots1 \end{cases} \tag{7}$$

We will use V_cs to simulate the quantum evolution with Hamiltonian H

$$H|a,0,0\rangle = \sum_{c:\, v_c(a)\in G} |v_c(a),0,0\rangle\,. \tag{8}$$

Useful standard tools for simulating Hamiltonians

Useful standard tools for simulating Hamiltonians

1. *Local terms.*
2. *Linear combination.*
3. *Unitary conjugation.*
4. *Tensor product.*

Simulating H

Hermitian operator T

$$
\begin{aligned}
T|a,b,0\rangle &= |b,a,0\rangle \quad (9)\\
T|a,b,1\rangle &= 0\,. \quad (10)
\end{aligned}
$$

It is obvious that $V_c^\dagger = V_c$ and

$$H = \sum_c V_c^\dagger T V_c \quad (11)$$

So it remains to simulate T efficiently.

Simulating T

The operator T may be written as

$$T = \left(\bigotimes_{l=1}^{2n} S^{(l,2n+l)} \right) \otimes |0\rangle\langle 0| \tag{12}$$

$S|z_1 z_2\rangle = |z_2 z_1\rangle$, the superscript indicates which two qubits S acts on.

Observe that the eigenvalues of S are ± 1, so the eigenvalues of T are $0, \pm 1$. And an operator can be uniquely determined by its behavior on its eigenbasis. So T is implemented with the circuit in Fig.3.

Simulating T II

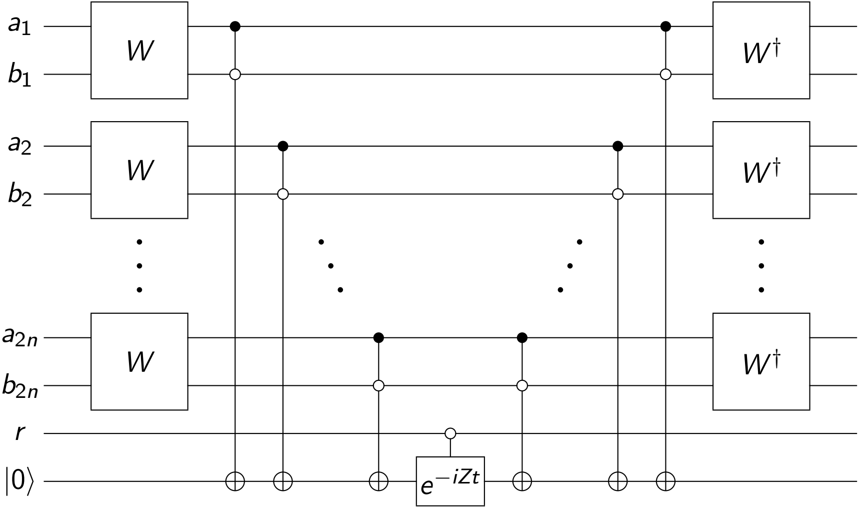


Figure: A circuit for simulating e^{-iTt}.

Simulating T III

let W be the two-qubit unitary operator that diagonalizes S.

$$\begin{aligned} W|00\rangle &= |00\rangle & (13)\\ W\tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) &= |01\rangle & (14)\\ W\tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &= |10\rangle & (15)\\ W|11\rangle &= |11\rangle\,. & (16)\end{aligned}$$

$W^{\otimes 2n}$ diagonalizes T, and the Toffoli gates compute the argument of the eigenvalue in an ancilla register initially prepared in the state $|0\rangle$, and then apply the appropriate phase shift.

Propagation on a line - Physics Intuition

In the section, we use physics techniques to provide intuition that the quantum walk propagates from the ENTRANCE to the EXIT in linear time.

By introducing the *column space*, we show the walk on G_n' can be viewed as a walk on a finite line with a defect at the center.

For this presentation, we will go through the simplest case with infinite spaces and no defect and explain briefly why the defect and the boundaries do not significantly affect the walk.

Propagation on a line - Column Space I

Column Space

the $(2n+2)$-dimensional subspace spanned by the states

$$|\,\mathrm{col}\,j\rangle = \frac{1}{\sqrt{N_j}} \sum_{a\in\mathrm{column}\ j} |a\rangle\,, \tag{17}$$

where

$$N_j = \begin{cases} 2^j & 0 \leq j \leq n \\ 2^{2n+1-j} & n+1 \leq j \leq 2n+1\,. \end{cases} \tag{18}$$

The column subspace is invariant under H (every vertex in column j is connected to the same number of vertices in column j + 1 and vice versa).

Propagation on a line - Column Space II

H in column space

$$\langle \mathrm{col}\, j | H | \mathrm{col}(j+1) \rangle = \begin{cases} \sqrt{2}\gamma & 0 \le j \le n-1\,, \quad n+1 \le j \le 2n \\ 2\gamma & j = n \end{cases} \tag{19}$$

For simplicity, we set $\gamma = 1/\sqrt{2}$.

Propagation on a line - Column Space III

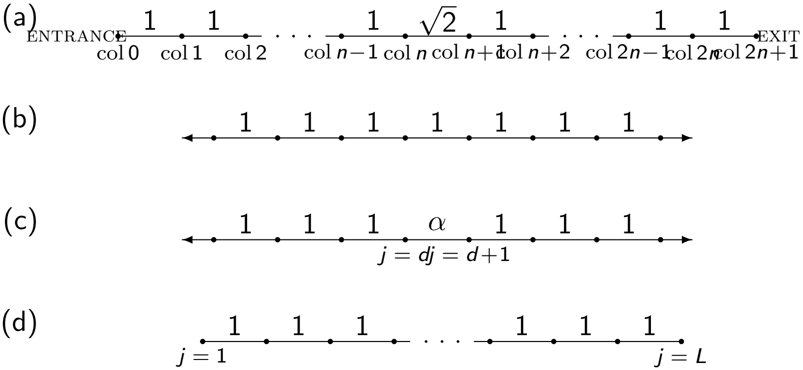


Figure: Quantum walks on lines. (a) Reduction of the quantum walk on G_n' to a quantum walk on a line. (b) Quantum walk on an infinite, translationally invariant line. (c) Quantum walk on an infinite line with a defect. (d) Quantum walk on a finite line without a defect.

Propagation on a line - Infinite Line w/o Defects I

Hamiltonian H for an infinite line w/o defect

$$\langle j|H|j \pm 1\rangle = 1\,, \quad -\infty < j < \infty\,. \tag{20}$$

The eigenstates of this Hamiltonian are the momentum eigenstates $|p\rangle$ with components

$$\langle j|p\rangle = \frac{1}{\sqrt{2\pi}} e^{ipj}\,, \quad -\pi \le p \le \pi \tag{21}$$

having energies

$$E_p = 2\cos p\,. \tag{22}$$

Propagation on a line - Infinite Line w/o Defects II

Propagator $G(j, k, t)$ from j to k in time t

$$
\begin{aligned}
G(j,k,t) &= \langle k|e^{-iHt}|j\rangle && (23)\\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \mathrm{d}p\, e^{ip(k-j)-2it\cos p} && (24)\\
&= (-i)^{k-j} J_{k-j}(2t)\,, \quad -\infty < j,k < \infty && (25)
\end{aligned}
$$

where $J_\nu(\cdot)$ is a Bessel function of order ν.

Note: here use $|j\rangle = \int_p |p\rangle\langle p|j\rangle$

Propagation on a line - Infinite Line w/o Defects III

the Bessel function has the following asymptotic expansions for $\nu \gg 1$:

$$\begin{aligned} J_\nu(\nu \operatorname{sech} \xi) &\sim \frac{e^{-\nu(\xi - \tanh \xi)}}{\sqrt{2\pi\nu \tanh \xi}} && (26) \\ J_\nu(\nu + \xi \nu^{1/3}) &= (2/\nu)^{1/3} \, \mathrm{Ai}(-2^{1/3}\xi) + O(\nu^{-1}) && (27) \\ J_\nu(\nu \sec \xi) &= \sqrt{\frac{2}{\pi\nu \tan \xi}} \left\{ \cos[\tfrac{\pi}{4} - \nu(\xi - \tan \xi)] + O(\nu^{-1}) \right\} , \quad 0 < \xi < \frac{\pi}{2} && (28) \end{aligned}$$

which means for $|k - j| \gg 1$

$$G(j,k,t) \text{ is } \begin{cases} \text{exponentially small in } |k-j| & \text{for } t < 0.99 \cdot |k-j|/2 \\ \text{of order } |k-j|^{-1/3} & \text{for } t \text{ near } |k-j|/2 \\ \text{of order } |k-j|^{-1/2} & \text{for } t > 1.01 \cdot |k-j|/2 \end{cases}$$

Upper bound on the hitting time — Reflector and Commutablility I

Recap — the Hamiltonian for G'_{n-1}

$$\langle \mathrm{col}\, j | H | \mathrm{col}(j+1) \rangle = \begin{cases} 1 & 1 \le j \le n-1\,, \quad n+1 \le j \le 2n-1 \\ \sqrt{2} & j = n\,, \end{cases} \tag{29}$$

Definition — the Reflection Operator

$$R | \mathrm{col}\, j \rangle = | \mathrm{col}(2n+1-j) \rangle\,. \tag{30}$$

Note that $R^2 = 1$, so R has eigenvalues ± 1. R commutes with H on the column subspace, so we can find simultaneous eigenstates of R and H.

Upper bound on the hitting time — Reflector and Commutablility II

simultaneous eigenstates of R and H.

$$\langle \mathrm{col}\, j | E \rangle = \begin{cases} \sin pj & 1 \le j \le n \\ \pm \sin(p(2n+1-j)) & n+1 \le j \le 2n\,, \end{cases} \tag{31}$$

The eigenvalue corresponding to the eigenstate $|E\rangle$ is $E = 2\cos p$, and the quantization condition (to be discussed later) comes from matching at vertices n and $n+1$. The ENTRANCE vertex corresponds to $|\,\mathrm{col}\, 1\rangle$ and the EXIT vertex to $|\,\mathrm{col}\, 2n\rangle$.

Remark

The proof of the lemma make use of the fact that $\langle E|\,\mathrm{col}\, 1\rangle = \pm\langle E|\,\mathrm{col}\, 2n\rangle$ so that one can bound the probability term easily.

Upper bound on the hitting time — Linking Success Probability to Spectral Gap I

Lemma

Consider the quantum walk in G'_{n-1} starting at the ENTRANCE*. Let the walk run for a time t chosen uniformly in $[0, \tau]$ and then measure in the computational basis. If $\tau \geq \frac{4n}{\epsilon \Delta E}$ for any constant $\epsilon > 0$, where ΔE is the magnitude of the smallest gap between any pair of eigenvalues of the Hamiltonian, then the probability of finding the* EXIT *is greater than $\frac{1}{2n}(1-\epsilon)$.*

Upper bound on the hitting time — Proof for Lemma 1 I

The probability of finding the EXIT after the randomly chosen time $t \in [0, \tau]$ is

$$\begin{aligned}
&\frac{1}{\tau}\int_0^\tau \mathrm{d}t\, |\langle \mathrm{col}\, 2n | e^{-iHt} | \mathrm{col}\, 1\rangle|^2 \\
&\quad = \frac{1}{\tau}\sum_{E,E'} \int_0^\tau \mathrm{d}t\, e^{-i(E-E')t} \langle \mathrm{col}\, 2n | E\rangle \langle E | \mathrm{col}\, 1\rangle \langle \mathrm{col}\, 1 | E'\rangle \langle E' | \mathrm{col}\, 2n\rangle \qquad (32) \\
&\quad = \sum_{E} |\langle E | \mathrm{col}\, 1\rangle|^2 |\langle E | \mathrm{col}\, 2n\rangle|^2 \\
&\qquad + \sum_{E \neq E'} \frac{1 - e^{-i(E-E')\tau}}{i(E-E')\tau} \langle \mathrm{col}\, 2n | E\rangle \langle E | \mathrm{col}\, 1\rangle \langle \mathrm{col}\, 1 | E'\rangle \langle E' | \mathrm{col}\, 2n\rangle \qquad (33)
\end{aligned}$$

Because of (31), we have $\langle E | \mathrm{col}\, 1\rangle = \pm \langle E | \mathrm{col}\, 2n\rangle$. Thus the first term is

$$\sum_{E} |\langle E | \mathrm{col}\, 1\rangle|^4 \geq \frac{1}{2n} \tag{34}$$

Upper bound on the hitting time — Proof for Lemma 1 II

as is easily established using the Cauchy-Schwartz inequality. The second term can be bounded as follows:

$$\left| \sum_{E \neq E'} \frac{1 - e^{-i(E-E')\tau}}{i(E-E')\tau} \langle \mathrm{col}\, 2n | E \rangle \langle E | \, \mathrm{col}\, 1 \rangle \langle \mathrm{col}\, 1 | E' \rangle \langle E' | \, \mathrm{col}\, 2n \rangle \right|$$
$$\leq \frac{2}{\tau \Delta E} \sum_{E,E'} |\langle E | \, \mathrm{col}\, 1 \rangle|^2 |\langle E' | \, \mathrm{col}\, 2n \rangle|^2 = \frac{2}{\tau \Delta E} \,. \qquad (35)$$

Thus we have

$$\frac{1}{\tau} \int_0^\tau \mathrm{d}t \, |\langle \mathrm{col}\, 2n | e^{-iHt} | \, \mathrm{col}\, 1 \rangle|^2 \geq \frac{1}{2n} - \frac{2}{\tau \Delta E} \geq \frac{1}{2n}(1 - \epsilon) \qquad (36)$$

where the last inequality follows since $\tau \geq \frac{4n}{\epsilon \, \Delta E}$ by assumption.

Upper bound on the hitting time — Bounding the spectral gaps I

Lemma

The smallest gap between any pair of eigenvalues of the Hamiltonian satisfies

$$\Delta E > \frac{2\pi^2}{(1+\sqrt{2})n^3} + O(1/n^4)\,. \tag{37}$$

Upper bound on the hitting time — Proof of Lemma 2 I

To evaluate the spacings between eigenvalues, we need to use the quantization condition. We have

$$\langle \mathrm{col}\, n | H | E \rangle = 2\cos p\, \langle \mathrm{col}\, n | E \rangle \tag{38}$$

so that

$$\sqrt{2}\langle \mathrm{col}(n+1) | E \rangle + \langle \mathrm{col}(n-1) | E \rangle = 2\cos p\, \langle \mathrm{col}\, n | E \rangle \tag{39}$$

and using (31), we have

$$\pm\sqrt{2}\sin np + \sin((n-1)p) = 2\cos p\, \sin np \tag{40}$$

which simplifies to

$$\frac{\sin((n+1)p)}{\sin np} = \pm\sqrt{2}\,. \tag{41}$$

Upper bound on the hitting time — Proof of Lemma 2 II

In Figure 5 we plot the left hand side of (41) for $n = 5$. The intersections with $-\sqrt{2}$ occur to the left of the zeros of $\sin np$, which occur at $\pi l/n$ for $l = 1, 2, \ldots, n-1$. For the values of p that intersect $-\sqrt{2}$, we can write $p = (\pi l/n) - \delta$. Equation (41) with $-\sqrt{2}$ on the right hand side is now

$$-\sqrt{2}\sin n\delta = \sin\left(n\delta - \frac{l\pi}{n} + \delta\right). \tag{42}$$

Write $\delta = (c/n) + (d/n^2) + O(1/n^3)$. Taking $n \to \infty$ in (42) gives $-\sqrt{2}\sin c = \sin c$, which implies that $c = 0$. We then get

$$-\sqrt{2}\sin\left(\frac{d}{n} + O(1/n^2)\right) = \sin\left(\frac{d}{n} - \frac{l\pi}{n} + O(1/n^2)\right) \tag{43}$$

which gives, as $n \to \infty$,

$$d = \frac{l\pi}{1+\sqrt{2}}. \tag{44}$$

Upper bound on the hitting time — Proof of Lemma 2 III

Thus we have that the roots of (41) with $-\sqrt{2}$ on the right hand side are of the form

$$p = \frac{l\pi}{n} - \frac{l\pi}{(1+\sqrt{2})n^2} + O(1/n^3)\,. \tag{45}$$

Upper bound on the hitting time — Proof of Lemma 2 IV

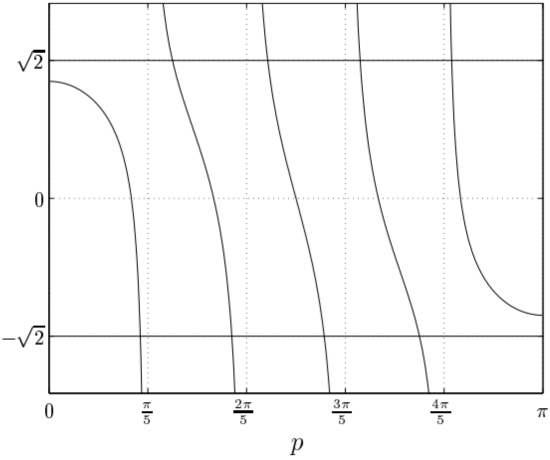


Figure: Left hand side of (41) for $n = 5$.

Upper bound on the hitting time — Proof of Lemma 2 V

Let p' and p'' be the two roots of (41) closest to the root p just found, with $p' < p < p''$. From the figure we see that p' and p'' both are roots of (41) with $+\sqrt{2}$. (Note that the smallest p, corresponding to $l = 1$, does not have a p'.) We see that p'' lies to the right of the zero of $\sin np$ at $p = l\pi/n$. We also see that p' lies to the left of the zero of $\sin((n+1)p)$ at $l\pi/(n+1)$. Therefore we have

$$\begin{aligned} p' &< \frac{l\pi}{n} - \frac{l\pi}{n^2} + O(1/n^3) \qquad (46) \\ p'' &> \frac{l\pi}{n}\,, \qquad (47) \end{aligned}$$

from which we conclude that

$$\begin{aligned} p - p' &> \frac{l\pi\sqrt{2}}{(1+\sqrt{2})n^2} + O(1/n^3)\,, \quad l = 2, 3, \ldots, n-1 \qquad (48) \\ p'' - p &> \frac{l\pi}{(1+\sqrt{2})n^2} + O(1/n^3)\,, \quad l = 1, 2, \ldots, n-1\,. \qquad (49) \end{aligned}$$

Upper bound on the hitting time — Proof of Lemma 2 VI

Thus the smallest spacing is at least $\pi/[(1+\sqrt{2})n^2] + O(1/n^3)$.
Now for a given p, the corresponding eigenvalue is $2\cos p$. For small Δp, the spacing ΔE is related to the spacing Δp by

$$\Delta E = 2|\Delta p \sin p| + O\left((\Delta p)^2\right) \ . \tag{50}$$

The factor $\sin p = \sin(l\pi/n + O(1/n^2))$ is smallest when $l = 1$, so we have

$$\Delta E > \frac{2\pi^2}{(1+\sqrt{2})n^3} + O(1/n^4) > \frac{8}{n^3} \ \text{for } n \text{ sufficiently large.} \tag{51}$$

Upper bound on the hitting time — Proof of Lemma 2 VII

Notice that there are actually 10 eigenvalues. we can find two other eigenvalues at $\pm(\sqrt{2}+\frac{1}{\sqrt{2}})$ with corrections that vanish exponentially as $n \to \infty$. Since the other $n-2$ eigenvalues are all in the range $[-2, 2]$, our conclusion about the minimum spacing is unchanged.

Remark

The proof is sketched as follow. First, find the plotting to gain intuition of the solutions. Then, use distance to $\frac{l\pi}{n}$ to bound Δp. Finally, use Δp to bind ΔE

Upper bound on the hitting time — Conclusion

Using Lemma 2 and Lemma 3, we find

Theorem

For n sufficiently large, running the quantum walk for a time chosen uniformly in $[0, \frac{n^4}{2\epsilon}]$ and then measuring in the computational basis yields a probability of finding the EXIT *that is greater than $\frac{1}{2n}(1-\epsilon)$.*

An Efficient Quantum Algorithm for Traversing G_n's

The computer is prepared in the state corresponding to the ENTRANCE, and the quantum walk is simulated using the construction described in Section 2. After running the walk for an appropriate $t = \mathrm{poly}(n)$, the state of the computer is measured. The probability of finding the name of the EXIT can be $O(1/n)$. By repeating this process $\mathrm{poly}(n)$ times, the success probability can be made arbitrarily close to 1.

1 Introduction

2 The problem

3 Quantum algorithm

4 Classical lower bound

- Overview
- Coloring
- Reduction to a Simpler Game
- Linking to a Tree Embedding Problem

5 Discussion

Classical lower bound — Overview

Claim

No classical algorithm can find the EXIT with high probability in subexponential time.

We proof this by considering a series of games and proving relations between them. The first game is equivalent to our problem, and each new game will be as easy to win. Finally, we will show that the easiest game cannot be won in subexponential time.

Classical lower bound — Coloring

To prove the classical lower bound, we need to specify a coloring that does not supply information about the graph.

Algorithm for a consistent coloring

In an even numbered column, randomly color the incident edges A, B, C. In an odd numbered column, randomly append the colors of the incident edges $1, 2, 3$.

It is obvious that any such coloring is consistent. And we will show it does not provide any useful information to a classical algorithm.

Classical lower bound — Reduction

Restrict to Known Vertices

Since we have 2-n bit string name, which means the probability of guessing a unknown name yield a valid vertex name is exponentially small.

Removal of Coloring

The coloring of graph can be made by the classical algorithm itself. For by restricting the explored subgraph to be connected, we know the parity of the column a vertex is in. So it does not gain additional information about the graph with the coloring.

Adding Win Condition — Finding a Cycle

Note the only information we have is the parity of the column of vertices, extra information cannot be gained unless we find a cycle. Thus we define a easier to win game that the player A wins if it finds the EXIT or it finds a cycle.

Classical lower bound — Linking to Random Tree Embedding I

We show the subgraph an algorithm sees must be a random embedding of a rooted binary tree.

Tree Embedding into G

$\pi : T \to G$ such that $\pi(\text{ROOT}) = \text{ENTRANCE}$ and for all vertices u and v that are neighbors in T, $\pi(u)$ and $\pi(v)$ are neighbors in G. We say that an embedding of T is *proper* if $\pi(u) \neq \pi(v)$ for $u \neq v$.

Random Embedding for a Tree into G

A random embedding of a tree is obtained by setting $\pi(\text{ROOT}) = \text{ENTRANCE}$ and then mapping the rest of T into G at random. (with prob $\frac{1}{2}$ take (u, v) or (v, u))

Classical lower bound — Linking to Random Tree Embedding II

Embedding Game

The algorithm outputs a rooted binary tree T with t vertices in which each internal vertex has two children. A random π is chosen. The algorithm wins if π is an improper embedding of T in G_n' or if T exits G_n' under π.

Classical lower bound — Linking to Random Tree Embedding III

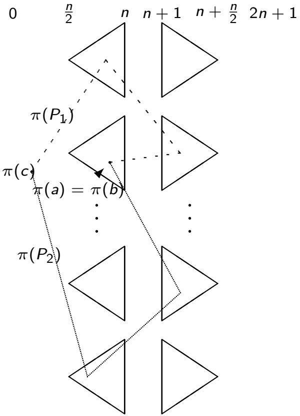
$\frac{n}{2}$ subtrees

Let T be a tree with t vertices, $t \leq 2^{n/6}$, with image $\pi(T)$ in G'_n under the random embedding π. The vertices of columns $n+1, n+2, \ldots n+\frac{n}{2}$ in G'_n divide naturally into $2^{n/2}$ complete binary subtrees of height $n/2$.

It is very unlikely that $\pi(T)$ contains the root of any of these subtrees. Consider a path in T from the root to a leaf. The path has length at most t, and there are at most t such paths. To reach column $n+\frac{n}{2}$ from column $n+1$, π must choose to move right $\frac{n}{2}-1$ times in a row, which has probability $2^{1-n/2}$. The probability is bounded by $t^2 \cdot 2^{1-n/2}$.

Classical lower bound — Linking to Random Tree Embedding IV

If $\pi(T)$ contains a cycle, $\exists a, b \in T \ni \pi(a) = \pi(b)$. Consider $c = \mathrm{LCA}(a, b)$, $\pi(c \to a), \pi(c \to b)$ forms a cycle. The probability of a, b exceed the two $\frac{n}{2}$ lines is low. For forming a cycle, P(path to a, b ends in the same subtree) $\leq \frac{2^{\frac{n}{2}}}{2^{n-t}}$ (by the construction of G, it is equally possible to pass any of the vertices in the nth column). We have to consider $\binom{t}{2}$ a, b pairs.



Classical lower bound — Linking to Random Tree Embedding V

Overall we have shown that

$$\begin{aligned} \mathop{\mathrm{E}}_{G}\left[\mathbb{P}^{G}(T)\right] &\leq t^2 \cdot 2^{-n/2} + t^2 \cdot 2^{1-n/2} && (52) \\ &\leq 3 \cdot 2^{-n/6} && (53) \end{aligned}$$

if $t \leq 2^{n/6}$.

1. Introduction
2. The problem
3. Quantum algorithm
4. Classical lower bound
5. Discussion

Discussion

- Exponential quantum-classical separation with quantum walks
- A new oracle relative to $\mathrm{BQP} \overset{?}{=} \mathrm{BPP}$
- The path is not found along with EXIT
- Open Problems
  - General graph oracles w/o coloring?
  - Applications?

References I

- D. Deutsch, *Quantum theory, the Church-Turing principle, and the universal quantum computer*, Proc. Roy. Soc. London A **400**, 97 (1985).

- D. Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proc. Roy. Soc. London A **439**, 553 (1992).

- E. Bernstein and U. Vazirani, *Quantum complexity theory*, Proc. 25th ACM Symposium on the Theory of Computing, 11 (1993).

- D. Simon, *On the power of quantum computation*, Proc. 35th IEEE Symposium on the Foundations of Computer Science, 116 (1994).

- P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proc. 35th IEEE Symposium on Foundations of Computer Science, 124 (1994).

References II

- A. Kitaev, *Quantum measurements and the abelian stabilizer problem*, quant-ph/9511026.

- M. Mosca and A. Ekert, *The hidden subgroup problem and eigenvalue estimation on a quantum computer*, Proc. 1st NASA International Conference on Quantum Computing and Quantum Communication, Vol. 1509 of *Lecture Notes in Computer Science* (1999).

- J. N. de Beaudrap, R. Cleve, and J. Watrous, *Sharp quantum vs. classical query complexity separations*, quant-ph/0011065.

- W. van Dam and S. Hallgren, *Efficient quantum algorithms for shifted quadratic character problems*, quant-ph/0011067.

References III

- S. Hallgren, A. Russell, and A. Ta-Shma, *Normal subgroup reconstruction and quantum computation using group representations*, Proc. 32nd ACM Symposium on the Theory of Computing, 627 (2000).
- W. van Dam, S. Hallgren, and L. Ip, *Quantum algorithms for hidden coset problems*, unpublished.
- M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani, *Quantum mechanical algorithms for the nonabelian hidden subgroup problem*, Proc. 33rd ACM Symposium on the Theory of Computing, 68 (2001).
- G. Ivanos, F. Magniez, and M. Santha, *Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem*, quant-ph/0102014.

References IV

- J. Watrous, *Quantum algorithms for solvable groups*, Proc. 33rd ACM Symposium on the Theory of Computing, 60 (2001).

- S. Hallgren, *Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*, Proc. 34th ACM Symposium on the Theory of Computing, 653 (2002).

- E. Farhi and S. Gutmann, *Quantum computation and decision trees*, Phys. Rev. A **58**, 915 (1998).

- A. M. Childs, E. Farhi, and S. Gutmann, *An example of the difference between quantum and classical random walks*, Quantum Information Processing **1**, 35 (2002).

- Y. Aharonov, L. Davidovich, and N. Zagury, *Quantum random walks*, Phys. Rev. A **48**, 1687 (1993).

References V

- D. A. Meyer, *From quantum cellular automata to quantum lattice gasses*, J. Stat. Phys. **85**, 551 (1996).
- J. Watrous, *Quantum simulations of classical random walks and undirected graph connectivity*, J. Computer and System Sciences **62**, 376 (2001).
- D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani, *Quantum walks on graphs*, in Proceedings of the 33rd ACM Symposium on the Theory of Computing, 50 (ACM Press, New York, 2001).
- A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous, *One-dimensional quantum walks*, Proc. 33rd ACM Symposium on the Theory of Computing, 37 (ACM Press, New York, 2001).
- C. Moore and A. Russell, *Quantum walks on the hypercube*, quant-ph/0104137.

References VI

- J. Kempe, *Quantum random walks hit exponentially faster*, quant-ph/0205083.
- V. G. Vizing, *On an estimate of the chromatic class of a p-graph*, Diskret. Analiz **3**, 23 (1964).
- S. Lloyd, *Universal quantum simulators*, Science **273**, 1073 (1996).
- M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions* (Dover, New York, 1972).
- J. Goldstone, personal communication, September 2002.