

# On the Quantum Query Complexity of Local Search in Two and Three Dimensions

Xiaoming Sun

Center for Advanced Study  
Tsinghua University, Beijing, China  
xiaomings@tsinghua.edu.cn

Andrew C. Yao\*

Center for Advanced Study  
Tsinghua University, Beijing, China  
andrewcyao@tsinghua.edu.cn

## Abstract

*The quantum query complexity of searching for local optima has been a subject of much interest in the recent literature. For the  $d$ -dimensional grid graphs, the complexity has been determined asymptotically for all fixed  $d \geq 5$ , but the lower dimensional cases present special difficulties, and considerable gaps exist in our knowledge. In the present paper we present near-optimal lower bounds, showing that the quantum query complexity for the 2-dimensional grid  $[n]^2$  is  $\Omega(n^{1/2-\delta})$ , and that for the 3-dimensional grid  $[n]^3$  is  $\Omega(n^{1-\delta})$ , for any fixed  $\delta > 0$ .*

*A general lower bound approach for this problem, initiated by Aaronson [1] (based on Ambainis' adversary method [3] for quantum lower bounds), uses random walks with low collision probabilities. This approach encounters obstacles in deriving tight lower bounds in low dimensions due to the lack of degrees of freedom in such spaces. We solve this problem by the novel construction and analysis of random walks with non-uniform step lengths. The proof employs in a nontrivial way sophisticated results of Sárközy and Szemerédi [14], Bose and Chowla [5], and Halász [9] from combinatorial number theory, as well as less familiar probability tools like Esseen's Inequality.*

## 1. Introduction

For any function  $f(x_1, x_2, \dots, x_n)$ , the decision tree complexity is the minimum number of queries " $x_i = ?$ " needed for any algorithm to determine the value of  $f$ . There are various flavors of this complexity, such as deterministic, non-deterministic, randomized, and randomized with error. The decision tree complexity, as well as related subjects such as property testing, has been a rich and active area of research for many years in theoretical computer science.

\*This work was supported in part by the National Natural Science Foundation of China Grant 60553001

In the last decade, an extension of decision tree complexities to quantum computation, called *quantum query complexity*, has been extensively studied, starting with Bennett et al [4] (which showed Grover's search was optimal). In particular, the complexity of *local search* has received much attention. In Turing complexity, the complexity class *PLS* (polynomial local search) was introduced by Johnson, Papadimitriou and Yannakakis [11] and was the subject of much study. In the context of query complexity, the problem of local search can be stated as follows: an integer valued function  $f$  is defined on the vertex set  $V$  of a known undirected graph  $G = (V, E)$ . A *local minimum*  $v \in V$ , defined as one vertex satisfying  $f(v) \leq f(w)$  for all  $\{w, v\} \in E$ , is to be determined with a series of queries of the form  $f(u) = ?$ . The complexity for a graph is the minimum number of queries required. Depending on the class of algorithms allowed, we denote the complexities respectively as  $DLS(G)$  (deterministic),  $RLS(G)$  (randomized with two-sided error  $\epsilon$ ), and  $QLS(G)$  (quantum with two-sided error  $\epsilon$ ).

In 1983, Aldous [2] showed that, for any  $N$ -vertex graph  $G$  of maximum degree  $\Delta$ ,  $RLS(G) = O(\sqrt{N\Delta})$ . For the Boolean hypercube this result implies  $RLS(B_n) = O(n^{1/2}2^{n/2})$ , and Aldous also showed a lower bound  $RLS(B_n) = \Omega(2^{n/2-o(n)})$  using a sophisticated random walk analysis. In 1989, Llewellyn, Tovey and Trick [12] showed for the boolean hypercube,  $D(B_n) = \Omega(2^n/\sqrt{n})$ .

In 2003, Aaronson [1] showed  $QLS(G) = O(N^{1/3}\Delta^{1/6})$  for general  $N$ -vertex graphs. He also developed a strategy for obtaining quantum lower bounds through random walk construction, using the quantum adversary method of Ambainis [3]. Interestingly, his approach also led to a new lower bound method for the randomized complexity, giving in particular a simplified and improved bound (over Aldous')  $RLS(B_n) = \Omega(2^{n/2}/n^2)$ . Santha and Szegedy [13] showed that  $DLS(G)$  and  $QLS(G)$  are polynomially related for all general graphs  $G$ .

In this paper we are mainly interested in the quantum complexity for  $d$ -dimensional grid graphs  $[n]^d$  (fixed  $d$ ).

We summarize the state of knowledge first: *up to log factors*, the randomized complexity is tight for  $d > 2$ , i.e.,  $RLS([n]^d) = \Theta(n^{d/2})$ , and the quantum complexity is tight for  $d > 4$ , i.e.,  $QLS([n]^d) = \Theta(n^{d/3})$ . For low dimensions, again up to log factors,

$$\begin{aligned}\Omega(n^{2/3}) &\leq RLS([n]^2) \leq O(n), \\ \Omega(n^{2/5}) &\leq QLS([n]^2) \leq O(n^{1/2}), \\ \Omega(n^{3/4}) &\leq QLS([n]^3) \leq O(n), \\ \Omega(n^{6/5}) &\leq QLS([n]^4) \leq O(n^{4/3}).\end{aligned}$$

In this paper, we give nearly optimal lower bounds for the  $d = 2, 3$  cases, proving the following main theorems. The gap in quantum complexity between the upper and lower bounds in the  $d = 4$  case remains an open question.

**Theorem 1**  $RLS([n]^2) = \Omega(n^{1-\delta})$ ,  $QLS([n]^2) = \Omega(n^{1/2-\delta})$ , for any constant  $\delta > 0$ .

**Theorem 2**  $QLS([n]^3) = \Omega(n^{1-\delta})$ , for any constant  $\delta > 0$ .

More detailed history for low dimensions: Aldous' result implies  $RLS([n]^d) = O(n^{d/2})$ . Aaronson [1] showed  $RLS([n]^d) = \Omega(n^{d/2-1}/\log n)$ ,  $QLS([n]^d) = O(n^{d/3})$ , and  $QLS([n]^d) = \Omega(n^{d/4-1/2}/\sqrt{\log n})$ . Recently, Zhang [17] improved the lower bounds, so that *up to log factors*, the randomized complexity is tight for  $d > 2$ , i.e.,  $RLS([n]^d) = \Theta(n^{d/2})$ , and the quantum complexity is tight for  $d > 4$ , i.e.,  $QLS([n]^d) = \Theta(n^{d/3})$ .

For 2-dimensional grid  $[n]^2$ , Santha and Szegedy [13] show that  $QLS([n]^2) = \Omega(n^{1/4})$ . Zhang [17] showed  $RLS([n]^2) = O(n^{2/3})$ ,  $\Omega(n^{2/5}) \leq QLS([n]^2) \leq O(n^{1/2}(\log \log n)^{3/2})$ . Verhoeven [15] showed  $QLS([n]^2) = O(\sqrt{n} \log \log n)$ . For 3 and 4 dimensional grids, Zhang [17] showed  $RLS([n]^3) = \Omega(\frac{n^{3/2}}{\sqrt{\log n}})$ ,  $QLS([n]^3) = \Omega(n^{3/4})$ , and  $RLS([n]^4) = \Omega(n^2)$ ,  $QLS([n]^4) = \Omega(n^{6/5})$ .

Other related works: Using the path technique Chen and Deng [6] show a  $\Omega(n^{d-1})$  deterministic lower bound for find a *fixed point* in grid  $[n]^d$ . Friedl et al [8] proved  $\Omega(\sqrt{n})$  and  $\Omega(\sqrt[4]{n})$  lower bound for random and quantum query complexity of *2D-Sperner* Problem by using a 2-d monotone path.

In Section 2, quantum lower bound tools from the literature are summarized, together with needed results from number theory and probability theory. In Section 3 top-level view of the approach to the proofs is given. A fairly complete proof for Theorem 1 (the  $d = 2$  case) is given in Sections 4 and 5, with some details left out for the Appendix. The proof of Theorem 2 (the  $d = 3$  case) requires additional twists; an outline of the proof is given in Sections 6 and 7.

## 2 Preliminaries

Lemma 1 gives a general lower bound based on the weighted adversary approach first developed by Ambainis [3]. This form is from Zhang [16]:

**Lemma 1** [3, 16] *Let  $F : S \rightarrow \{0, 1\}^m$  be a partial function. Let  $w : S^2 \rightarrow [0, \infty)$  and  $w' : S^2 \times [N] \rightarrow [0, \infty)$  be weight assignments satisfying the following conditions:*

1.  $w(x, y) = w(y, x)$  for every  $x, y$ , and  $w(x, y) = 0$  whenever  $F(x) = F(y)$ ;
2.  $w'(x, y, i) = 0$  whenever  $x_i = y_i$  or  $F(x) = F(y)$ , and  $w'(x, y, i)w'(y, x, i) \geq w(x, y)^2$  for all  $x, y, i$  with  $x_i \neq y_i$ .

Then

$$Q(F) = \Omega \left( \min_{\substack{x, y, i: x_i \neq y_i \\ w(x, y) > 0}} \sqrt{\frac{wt(x)wt(y)}{v(x, i)v(y, i)}} \right)$$

where  $wt(x) = \sum_y w(x, y)$  and  $v(x, i) = \sum_y w'(x, y, i)$  for all  $x \in S$  and  $i \in [N]$ .

For the lower bound of randomized query complexity, we use the method invented by Aaronson [1]:

**Lemma 2** [1] *Let  $F : S \rightarrow \{0, 1\}^m$  be a partial function. Let  $w : S \times S \rightarrow [0, \infty)$  be a function satisfying (1)  $w(x, y) = w(y, x)$ , and (2)  $w(x, y) = 0$  whenever  $F(x) = F(y)$ . Let  $wt(x) = \sum_y w(x, y)$  and  $v(x, i) = \sum_{y: y_i \neq x_i} w(x, y)$ , then*

$$R(F) = \Omega \left( \min_{\substack{x, y, i: \\ x_i \neq y_i, w(x, y) > 0}} \max \left\{ \frac{wt(x)}{v(x, i)}, \frac{wt(y)}{v(y, i)} \right\} \right)$$

To prove Theorem 1 we need use the following two inequalities proved by Sárközy and Szemerédi [14] and Esseen [7]:

**Lemma 3** [14] *Let  $0 < a_1 < a_2 < \dots < a_n$  be a sequence of real numbers. Denote by  $f_n(t)$  the number of solutions of  $\sum_{i=1}^n \epsilon_i a_i = t$ ,  $\epsilon_i = 0$  or  $1$ . For any  $\delta > 0$ , there exists a constant  $n_0(\delta)$  such that, for all  $n > n_0(\delta)$ ,*

$$\max_{0 \leq t < \infty} f_n(t) < (1 + \delta) \frac{8}{\pi^{1/2}} \frac{2^n}{n^{3/2}}$$

**Remark 1** *We will use Lemma 3 with the following form: Let  $0 < a_1 < a_2 < \dots < a_n$  be a sequence of real numbers, then*

$$\max_{y \in \mathbb{Z}} \Pr_{\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}} (\epsilon_1 a_1 + \dots + \epsilon_n a_n = y) \leq cn^{-3/2},$$

where  $c$  is a positive absolute constant.

**Lemma 4** [7] Let  $X_1, \dots, X_n$  be independent random variables such that  $E(X_k) = 0$ ,  $E[X_k^2] = \sigma_k^2$ , and  $E[|X_k|^3] < +\infty$ ,  $k = 1, \dots, n$ . Let  $B_n = \sum_{k=1}^n \sigma_k^2$ ,  $L_n = B_n^{-3/2} \sum_{k=1}^n E[|X_k|^3]$ , then

$$\sup_x \left| \Pr \left\{ \frac{\sum_{k=1}^n X_k}{\sqrt{B_n}} < x \right\} - \Phi(x) \right| \leq cL_n$$

where  $c$  is a positive absolute constant, and  $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt$ .

To prove Theorem 2 we need the following two results of Halász (Theorem 2 and Theorem 3 of [9]):

**Lemma 5** Let  $\mathbf{v}_k (k = 1, \dots, n)$  be  $n$  vectors in  $\mathbb{R}^2$ . Suppose that  $\|\mathbf{v}_k - \mathbf{v}_{k'}\| \geq 1 (\forall k \neq k')$ , and there exists a constant  $\delta > 0$  such that for any  $\|\mathbf{e}\| = 1$  one can select at least  $\delta n$  vectors  $\mathbf{v}_k$  with  $|\langle \mathbf{v}_k, \mathbf{e} \rangle| \geq 1$ , then

$$\max_{\mathbf{y} \in \mathbb{Z}^2} \Pr_{\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}} (\epsilon_1 \mathbf{v}_1 + \dots + \epsilon_n \mathbf{v}_n = \mathbf{y}) \leq c(\delta) n^{-2},$$

where  $c(\delta)$  depends only on  $\delta$ .

**Remark 2** Halász gave an upper bound  $n^{-1-d/2}$  for general space  $\mathbb{R}^d$ , we just set  $d = 2$  here.

**Lemma 6** Let  $\mathbf{v}_k (k = 1, \dots, n)$  be  $n$  vectors in  $\mathbb{R}^2$ . Suppose from among the  $2^{h-1} n^h$  vectors  $\mathbf{b} = \mathbf{v}_{k_1} \pm \dots \pm \mathbf{v}_{k_h}$  ( $1 \leq k_i \leq n$ ) one can select at least  $\delta n^h$  vectors, each two having a distance  $\|\mathbf{b} - \mathbf{b}'\| \geq 1$ . And also for any  $\|\mathbf{e}\| = 1$  one can select at least  $\delta n$  vectors  $\mathbf{v}_k$  with  $|\langle \mathbf{v}_k, \mathbf{e} \rangle| \geq 1$ , then

$$\max_{\mathbf{y} \in \mathbb{Z}^2} \Pr_{\epsilon_1, \dots, \epsilon_n \in \{\pm 1\}} (\epsilon_1 \mathbf{v}_1 + \dots + \epsilon_n \mathbf{v}_n = \mathbf{y}) \leq c(\delta, h) n^{-h},$$

where  $c(\delta)$  depends only on  $\delta$  and  $h$ .

**Remark 3** Lemma 6 used here is a weak version of Halász's original result (Theorem 3 in [9]). In his paper the space is  $\mathbb{R}^d$ , and in his statement of Theorem 3,  $h$  equals  $d$ . But through the proof this is not necessary, at least not necessary for our weak version here.

We also need some tools from number theory for both Theorem 1 and Theorem 2.

**Definition 1** [10] A positive integer sequence  $B = b_1 b_2 \dots b_n$  is called a  $B_h$ -sequence if all the sums

$$b_{i_1} + b_{i_2} + \dots + b_{i_h}$$

are distinct, where  $1 \leq i_1 \leq \dots \leq i_h \leq n$ .

For example  $1, 2, \dots, n$  is a  $B_1$ -sequence. It is clear that a  $B_h$ -sequence ( $h > 1$ ) is also a  $B_1$ -sequence, so  $b_i \neq b_j$  ( $i \neq j$ ). The following result is due to Bose and Chowla [5]:

**Lemma 7**  $\{1, 2, \dots, m\}$  contains a  $B_h$ -sequence  $B$  of size  $|B| = m^{1/h} (1 + o(1))$ .

### 3 Top Level View of the Proof

In proving lower bounds, it is a standard technique to relate the local search problem to some related search problem about finding paths. We relate the local search on grid graphs to a certain path problem on pyramid graphs.

Let  $G = (V, E)$  be a directed acyclic graph. Given a source  $v_0$  and an unknown path  $P$  starting at  $v_0$  and ending in a sink, we would like to locate the endpoint of  $P$  by making queries of the form "Is  $x_i \in P$ ". Let  $D(G), R(G), Q(G)$  be respectively the deterministic decision tree complexity, the randomized decision tree complexity (with error  $\leq \epsilon = 1/3$ ), and the quantum query complexity (with error  $\leq \epsilon = 1/3$ ).

Let  $\mathcal{P}_{d,n} = (V_{d,n}, E_{d,n})$  denote the  $d$ -dimensional pyramid graph, where  $V_{d,n}$  is the set of lattice points  $\{x \in \mathbb{N}_0^d : \sum_{j=1}^d x_j \leq n\}$ , and  $E_{d,n}$  is the set of all  $(x, x')$ , where  $x, x' \in V_{d,n}$  and  $x' = x + e_k$  for some  $k \in \{1, 2, \dots, d\}$ . Here  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ,  $e_k = (0, \dots, 0, 1, 0, \dots, 0)$  is the  $k$ -th unit vector in  $\mathbb{Z}^d$ . A pyramid path is a path in  $\mathcal{P}_{d,n}$  starting at the source node  $(0, \dots, 0)$  and ending in a sink node at the bottom (the hyperplane  $\{x : \sum_{i=1}^d x_i = n\}$ ).

The following Proposition allows us to reduce the proof of Theorems 1 and 2 to the proof of lower bounds to the complexity of the corresponding path problems in pyramid graphs. The proof is standard.

**Proposition 1**  $RLS([n]^d) \geq R(\mathcal{P}_{d,n})$ ,  $QLS([n]^d) \geq Q(\mathcal{P}_{d,n})$ .

**Proof.** Suppose we have an instance for the Pyramid Path problem: a path  $\mathbf{P} = p_0 \dots p_n \in \mathcal{P}_{d,n}$ , we construct a Local Search problem in  $[n]^d$ : We define function  $f_{\mathbf{P}}$  in the same way as [1]:

$$f_{\mathbf{P}}(p) = \begin{cases} n - \|p\|_1, & \text{if } p \in \mathbf{P} \\ n + \|p\|_1, & \text{if } p \notin \mathbf{P} \end{cases}$$

It is clear that  $p_n$  is the unique local minimum of  $f_{\mathbf{P}}$ .

If a local search algorithm  $\mathcal{A}$  queries a point  $p$ , we just ask the Pyramid oracle the same query and return  $n - \|p\|_1$  or  $n + \|p\|_1$  to  $\mathcal{A}$  according to the oracle's answers.  $\square$

We will prove Theorem 1 in two steps. First, for any sequence of integers  $A = a_1, a_2, \dots, a_n$ , we define a certain random walk which in turn gives rise to an assignment of weights in the quantum adversary method. Proposition 2 below gives lower bounds to  $R(\mathcal{P}_{2,N})$  and  $Q(\mathcal{P}_{2,N})$  in terms of a parameter  $\rho$  (which is determined by the sequence  $A$ ). Proposition 3 shows that, using results from combinatorial number theory, we can construct a sequence  $A$  such that  $\rho$  is small which then implies strong lower bounds via Proposition 2.

Similarly, the proof of Theorem 2 is in two steps. Proposition 4 show that any sequence of two-dimensional vectors gives rise to a lower bound to  $R(\mathcal{P}_{3,N})$  and  $Q(\mathcal{P}_{3,N})$ .

Proposition 5 then shows that, with the help of certain results in number theory, there exist sequences giving rise to strong lower bounds that almost match known upper bounds.

**Proposition 2** Let  $a_1, \dots, a_n$  be a positive integer sequence (no need to be distinct). Let  $N = \sum_{i=1}^n a_i$ . Define

$$\mu_{i,j} = \max_{y \in \mathbb{Z}} \Pr_{\epsilon_i, \dots, \epsilon_j \in \{\pm 1\}} (\epsilon_i a_i + \epsilon_{i+1} a_{i+1} + \dots + \epsilon_j a_j = y)$$

( $1 \leq i \leq j \leq n$ ),  $\rho_j = \sum_{i=1}^j \mu_{i,j}$  ( $j = 1, \dots, n$ ), and  $\rho = \max_{1 \leq j \leq n} \rho_j$ . Then

$$R(\mathcal{P}_{2,N}) = \Omega\left(\frac{n}{\rho}\right), Q(\mathcal{P}_{2,N}) = \Omega\left(\sqrt{\frac{n}{\rho}}\right).$$

For example  $a_1 = \dots = a_n = 1$ :  $\rho_j = \Theta(\sqrt{j})$ ,  $\rho = \Theta(\sqrt{n})$ .  $R(\mathcal{P}_{2,n}) = \Omega(\sqrt{n})$ ,  $Q(\mathcal{P}_{2,n}) = \Omega(\sqrt[4]{n})$ .

**Proposition 3** Given any constant  $\delta > 0$ , for any sufficient large  $n \in \mathbb{N}$ , there exists a positive integer sequence  $A = a_1, a_2, \dots, a_n$ , such that  $\sum_j a_j = O(n^{1+\delta})$  and  $\rho = O(1)$ , where the constants in  $O(*)$  depend only on  $\delta$ , and  $\rho$  is defined in the same way as in Proposition 2.

Combining Proposition 1, Proposition 2 and Proposition 3, we obtain Theorem 1.

**Proposition 4** Let  $\mathbf{v}_1, \dots, \mathbf{v}_n$  be a sequence of vectors in  $\mathbb{N}^2$  (no need to be distinct). Let  $N = \sum_{i=1}^n \|\mathbf{v}_i\|_1$ . Define

$$\mu_{i,j} = \sup_{y \in \mathbb{Z}^2} \Pr_{\epsilon_i, \dots, \epsilon_j \in \{\pm 1\}} (\epsilon_i \mathbf{v}_i + \epsilon_{i+1} \mathbf{v}_{i+1} + \dots + \epsilon_j \mathbf{v}_j = y)$$

( $1 \leq i \leq j \leq n$ ),  $\lambda_j = \sum_{i=1}^j \sqrt{\mu_{i,j}}$  ( $j = 1, \dots, n$ ), and  $\lambda = \max_{1 \leq j \leq n} \lambda_j$ . Then  $Q(\mathcal{P}_{3,N}) = \Omega\left(\frac{n}{\lambda}\right)$ .

**Proposition 5** Given any constant  $\delta > 0$ , for any sufficient large  $n \in \mathbb{N}$ , there exists a vector sequence  $V = \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in \mathbb{N}^2$ , such that

$$\sum_j \|\mathbf{v}_j\|_1 = O(n^{1+\delta}) \text{ and } \lambda = O(\log n),$$

where the constants in  $O(*)$  depend only on  $\delta$ , and  $\lambda$  is defined in the same way as in Proposition 4.

Combining Proposition 1, Proposition 4 and Proposition 5, we obtain Theorem 2.

## 4 Proof of Proposition 2

Consider the following  $n$ -step random walk in  $\mathbb{Z}^2$ :  $Y_0 = (0, 0)$ ,  $Y_k = Y_{k-1} + (a_k, 0)$  with probability  $\frac{1}{2}$ , and  $Y_k = Y_{k-1} + (0, a_k)$  with probability  $\frac{1}{2}$ ,  $k = 1, \dots, n$ . It is clear that  $\|Y_k\|_1 = \sum_{j=1}^k a_j$ ,  $k = 1, \dots, n$ , especially  $Y_n$  is on the bottom plane of the pyramid  $\mathcal{P}_{2,N}$ . Using the definition of  $\mu_{i,j}$  we can prove

**Lemma 8** For any  $\mathbf{y} \in \mathbb{Z}^2$ ,  $0 \leq i < j \leq n$ ,

$$\Pr(Y_j - Y_i = \mathbf{y}) \leq \mu_{i+1,j}.$$

Due to page limitation we do not give the proof here.

Consider all the  $2^n$  paths  $\mathbf{P} = p_0 p_1 \dots p_n \in \mathcal{P}_{2,N}$  which are generated by the random walk:  $p_k = p_{k-1} + (a_k, 0)$  or  $p_k = p_{k-1} + (0, a_k)$ . We use the adversary methods to prove that in order to separate these  $2^n$  paths,  $\Omega\left(\frac{n}{\rho}\right)$  randomized queries or  $\Omega\left(\sqrt{\frac{n}{\rho}}\right)$  quantum queries are needed.

For any two paths  $\mathbf{P} = p_0 \dots p_n$  and  $\mathbf{P}' = p'_0 \dots p'_n$ , define  $|\mathbf{P} \wedge \mathbf{P}'| = k$  if  $p_0 = p'_0, \dots, p_k = p'_k$  and  $p_{k+1} \neq p'_{k+1}$ . For any point  $x \in V_{2,N} \setminus (0, 0)$ , define  $|x|_* = \{k \in \mathbb{N} : \sum_{i=1}^{k-1} a_i < \|x\|_1 \leq \sum_{i=1}^k a_i\}$ , i.e.  $p_{k-1} p_k$  is the only possible line segment of the path that point  $x$  belongs to.

Now we let

$$w(\mathbf{P}, \mathbf{P}') = \begin{cases} 0 & \text{if } p_n = p'_n, \\ \frac{1}{2^{n-|\mathbf{P} \wedge \mathbf{P}'|}} & \text{otherwise.} \end{cases}$$

for both the random and the quantum case. For the quantum case, let  $w'(\mathbf{P}, \mathbf{P}', x) = w'(\mathbf{P}', \mathbf{P}, x) = w(\mathbf{P}, \mathbf{P}')$  if  $\mathbf{P}(x) \neq \mathbf{P}'(x)$ , otherwise  $w'(\mathbf{P}, \mathbf{P}', x) = w'(\mathbf{P}', \mathbf{P}, x) = 0$ . From the definition it is clear that  $w'(\mathbf{P}, \mathbf{P}', x) w'(\mathbf{P}', \mathbf{P}, x) \geq w(\mathbf{P}, \mathbf{P}')^2$ .

We first give lower bound for  $wt(\mathbf{P})$ :

$$\begin{aligned} wt(\mathbf{P}) &= \sum_{\mathbf{P}'} w(\mathbf{P}, \mathbf{P}') = \sum_{k=0}^{n-1} \sum_{\substack{\mathbf{P}': p_n \neq p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} \frac{1}{2^{n-k}} \\ &= \sum_{k=0}^{n-1} \frac{1}{2^{n-k}} \left( 2^{(n-k-1)} - \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1 \right) \\ &= \frac{n}{2} - \sum_{k=0}^{n-1} \frac{1}{2^{(n-k)}} \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1. \end{aligned} \quad (1)$$

We know

$$\frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1 \leq \Pr(Y_n - Y_k = p_n - p_k),$$

and from Lemma 8  $\Pr(Y_n - Y_k = p_n - p_k) \leq \mu_{k+1,n}$ , thus

$$\sum_{k=0}^{n-1} \frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1 \leq \sum_{k=0}^{n-1} \mu_{k+1,n} = \rho_n \leq \rho. \quad (2)$$

Combine inequality (1) with (2),

$$wt(\mathbf{P}) \geq \frac{n}{2} - \rho. \quad (3)$$

Next we derive upper bounds to  $v(\mathbf{P}, x)$  and  $v(\mathbf{P}', x)$ , when  $\mathbf{P}(x) \neq \mathbf{P}'(x)$  and  $w(\mathbf{P}, \mathbf{P}') > 0$ . Without loss of generality, we can assume  $\mathbf{P}(x) = 1$ ,  $\mathbf{P}'(x) = 0$ . We trivially bound  $v(\mathbf{P}, x)$  by  $wt(\mathbf{P})$ :

$$v(\mathbf{P}, x) = \sum_{\mathbf{P}''} w'(\mathbf{P}, \mathbf{P}'', x) \leq \sum_{\mathbf{P}''} w(\mathbf{P}, \mathbf{P}'') = wt(\mathbf{P}). \quad (4)$$

Now we need to bound  $v(\mathbf{P}', x)$ :

$$\begin{aligned} v(\mathbf{P}', x) &= \sum_{\mathbf{P}''} w'(\mathbf{P}', \mathbf{P}'', x) = \sum_{\substack{\mathbf{P}'': \mathbf{P}''(x)=1, \\ p''_n \neq p'_n}} \frac{1}{2^{n-|\mathbf{P}' \wedge \mathbf{P}''|}} \\ &= \sum_{k=0}^{|x|_*-1} \frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}'': |\mathbf{P}'' \wedge \mathbf{P}'| = k, \\ \mathbf{P}''(x)=1, p''_n \neq p'_n}} 1 \\ &\leq \sum_{k=0}^{|x|_*-1} \frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}'': |\mathbf{P}'' \wedge \mathbf{P}'| = k, \\ \mathbf{P}''(x)=1}} 1. \end{aligned} \quad (5)$$

Suppose  $\mathbf{P}'' = p''_0 \dots p''_m$ . Since  $\mathbf{P}''(x) = 1$ , i.e. path  $\mathbf{P}''$  contains point  $x$ . We know  $p''_{|x|_*} = p''_{|x|_*-1} + (a_{|x|_*}, 0)$  or  $p''_{|x|_*} = p''_{|x|_*-1} + (0, a_{|x|_*})$ , according to the construction of the path,  $p''_{|x|_*}$  has at most two different possible choices. Therefore,

$$\frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}'': |\mathbf{P}'' \wedge \mathbf{P}'| = k, \\ \mathbf{P}''(x)=1}} 1 \leq 2 \max_{\mathbf{y} \in V_{2,N}} \Pr(Y_{|x|_*} - Y_k = \mathbf{y} - p''_k). \quad (6)$$

From Lemma 8,

$$\max_{\mathbf{y} \in V_{2,N}} \Pr(Y_{|x|_*} - Y_k = \mathbf{y} - p''_k) \leq \mu_{k+1, |x|_*}, \quad (7)$$

Combine inequalities (5),(6),(7),

$$v(\mathbf{P}', x) \leq \sum_{k=0}^{|x|_*-1} 2\mu_{k+1, |x|_*} = 2\rho_{|x|_*} \leq 2\rho. \quad (8)$$

Finally combine inequalities (3),(4) and (8),

$$\begin{aligned} R(\mathcal{P}_{2,N}) &= \Omega \left( \max \left\{ \frac{wt(\mathbf{P})}{v(\mathbf{P}, x)}, \frac{wt(\mathbf{P}')}{v(\mathbf{P}', x)} \right\} \right) \\ &= \Omega \left( \max \left\{ \frac{wt(\mathbf{P})}{wt(\mathbf{P})}, \frac{\frac{n}{2} - \rho}{2\rho} \right\} \right) = \Omega \left( \frac{n}{\rho} \right), \\ Q(\mathcal{P}_{2,N}) &= \Omega \left( \sqrt{\frac{wt(\mathbf{P})wt(\mathbf{P}')}{v(\mathbf{P}, x)v(\mathbf{P}', x)}} \right) \\ &= \Omega \left( \sqrt{\frac{wt(\mathbf{P}) \cdot (\frac{n}{2} - \rho)}{wt(\mathbf{P}) \cdot 2\rho}} \right) = \Omega \left( \sqrt{\frac{n}{\rho}} \right). \end{aligned}$$

□

## 5 Proof of Proposition 3

To simplify our representation, for a vector sequence  $W = \mathbf{w}_1, \dots, \mathbf{w}_t \in \mathbb{Z}^d$ , we define

$$\mu(W) = \max_{\mathbf{y} \in \mathbb{Z}^d} \Pr_{\epsilon_1, \dots, \epsilon_t \in \{\pm 1\}} (\epsilon_1 \mathbf{w}_1 + \dots + \epsilon_t \mathbf{w}_t = \mathbf{y}),$$

so in Proposition 3 our  $\mu_{i,j} = \mu(a_i, a_{i+1}, \dots, a_j)$ , and in Proposition 5  $\mu_{i,j} = \mu(\mathbf{v}_i, \mathbf{v}_{i+1}, \dots, \mathbf{v}_j)$  ( $1 \leq i \leq j \leq n$ ).

**Fact 1** If  $W'$  is a subsequence of  $W$  (no need to be consecutive), then  $\mu(W) \leq \mu(W')$ .

**Proof of Proposition 3:** Pick a large integer  $h_0$  such that  $\frac{1}{2^{h_0+1}} < \delta$ . We recursively construct sequence  $A$ .

For any finite sequence  $A$  of integers, let  $N(A)$  denote the sum of all the integers in the sequence. Let  $A^{(1)} = 1, 2, \dots, m$ , then  $N(A^{(1)}) = O(m^2)$ , and  $\mu_{i,j} = \mu(i, i+1, \dots, j)$ , from Lemma 3  $\mu(i, \dots, j) \leq O(\frac{1}{(j-i+1)^{3/2}})$ , thus  $\rho_j(A^{(1)}) \leq \sum_{i=1}^j O(\frac{1}{(j-i+1)^{3/2}}) = O(1)$  ( $j = 1, \dots, m$ ).

Suppose we have already constructed  $A^{(k)} = a_1, \dots, a_{m_k}$ , such that  $N(A^{(k)}) = O(m_k^{d_k})$ , and  $\forall 1 \leq j \leq m_k$ ,  $\rho_j(A^{(k)}) = O(1)$ . We have  $d_1 = 2$ . We will construct a new sequence  $A^{(k+1)}$  with length  $m_{(k+1)}$  ( $m_{(k+1)} > m_k$ ), s.t.  $N(A^{(k+1)}) = O(m_{(k+1)}^{d_{k+1}})$ , where  $1 + \frac{1}{2^{h_0+1}} < d_{k+1} < d_k$ ,  $\{d_j\} \downarrow 1 + \frac{1}{2^{h_0+1}}$ , and also  $\rho_j(A^{(k+1)}) = O(1)$  for  $j = 1, \dots, m_{(k+1)}$ .

We construct  $A^{(k+1)}$  from  $A^{(k)}$ . Let

$$s = m_k^{\frac{d_k}{h_0+1}}, \quad t = m_k^{\frac{(h_0+\frac{1}{2})d_k}{h_0+1} - 1}.$$

Since  $d_k > 1 + \frac{1}{2^{h_0+1}}$ ,  $t$  is well defined.

From Lemma 7 we know that there exists a  $B_{h_0}$ -sequence in  $\{1, \dots, cs^{h_0}\}$  with size  $s$ ,  $c$  is some constant. Let  $b'_1, \dots, b'_s$  be the  $B_{h_0}$  sequence, let  $b_j = b'_j + cs^{h_0}$ ,  $j = 1, \dots, s$ , then  $b_1, \dots, b_s$  is also a  $B_{h_0}$  sequence, and for  $1 \leq j \leq s$ ,  $cs^{h_0} < b_j \leq 2cs^{h_0}$ . Construct

$$A^{(k+1)} = \left. \begin{array}{l} A^{(k)}, \quad b_1, \quad \dots \quad b_s; \\ \vdots \\ A^{(k)}, \quad b_1, \quad \dots \quad b_s. \end{array} \right\} t \text{ times}$$

here  $(A^{(k)}, b_1, \dots, b_s)$  repeats  $t$  times. Write the sequence  $b_1, \dots, b_s$  by  $B$ . The following is true:

**Lemma 9**  $\mu(B) = \mu(b_1, \dots, b_s) \leq O(s^{-h_0 - \frac{1}{2}})$ .

We leave the proof of Lemma 9 to the Appendix.

Now we show that sequence  $A^{(k+1)}$  is better than  $A^{(k)}$ :

$$m_{(k+1)} = |A^{(k+1)}| = t(m_k + s) = \Theta(m_k^{\frac{(h_0+\frac{1}{2})d_k}{h_0+1}}),$$

(since  $s = o(m_k)$ ), and

$$\begin{aligned} N(A^{(k+1)}) &= t(N(A^{(k)}) + \sum_{j=1}^s b_j) \\ &\leq t(O(m_k^{d_k}) + s \cdot 2cs^{h_0}) \\ &= O(m_k^{\frac{(2h_0 + \frac{3}{2})d_k}{h_0 + 1} - 1}). \end{aligned}$$

Thus

$$d_{k+1} = \frac{\frac{(2h_0 + \frac{3}{2})d_k}{h_0 + 1} - 1}{\frac{(h_0 + \frac{1}{2})d_k}{h_0 + 1}} = \frac{(4h_0 + 3)d_k - 2(h_0 + 1)}{(2h_0 + 1)d_k}.$$

Therefore,

$$\frac{d_{(k+1)} - (1 + \frac{1}{2h_0 + 1})}{d_k - (1 + \frac{1}{2h_0 + 1})} = \frac{1}{d_k}. \quad (9)$$

Since  $d_1 = 2 > 1 + \frac{1}{2h_0 + 1}$ , so  $\{d_j\} \downarrow 1 + \frac{1}{2h_0 + 1} < 1 + \delta$ .

We need to show  $A^{(k+1)}$  satisfy  $\rho_j(A^{(k+1)}) = O(1)$  ( $j = 1, \dots, m_{(k+1)}$ ). Write  $j = q(m_k + s) + r$ , where  $q \in \mathbb{N} \cup \{0\}$  and  $0 < r \leq m_k + s$ . There are two cases, either  $j$  is in  $A^{(k)}$  part or  $j$  is in  $B$  part:

Case 1:  $1 \leq r \leq m_k$ , i.e.  $j$  is in  $A^{(k)}$  part, from the construction of  $A^{(k+1)}$ ,

$$\begin{aligned} \rho_j(A^{(k+1)}) &= \sum_{i \leq j-r-s} \mu_{i,j}(A^{(k+1)}) \\ &+ \sum_{i=j-r-s+1}^{j-r} \mu_{i,j}(A^{(k+1)}) + \sum_{i=j-r+1}^j \mu_{i,j}(A^{(k+1)}) \\ &= \sum_{i \leq j-r-s} \mu_{i,j}(A^{(k+1)}) + \sum_{i=1}^s \mu_{i,s+r}(B, A^{(k)}) \\ &+ \sum_{i=1}^r \mu_{i,r}(A^{(k)}). \end{aligned}$$

The last additive term is nothing but  $\rho_r(A^{(k)})$ , we already know  $\rho_r(A^{(k)}) = O(1)$ . By Fact 1

$$\mu_{i,s+r}(B, A^{(k)}) \leq \mu_{i,s}(B, A^{(k)}) = \mu(b_i, \dots, b_s),$$

and from Lemma 3  $\mu(b_i, \dots, b_s) \leq O(\frac{1}{(s-i+1)^{3/2}})$ , therefore the second additive term satisfies

$$\sum_{i=1}^s \mu_{i,s+r}(B, A^{(k)}) \leq \sum_{i=1}^s O(\frac{1}{(s-i+1)^{3/2}}) = O(1).$$

It remains to upper bound the first term  $\sum_{i \leq j-r-s} \mu_{i,j}(A^{(k+1)})$ . Since  $i \leq j-r-s$ , by Fact 1 we have

$$\mu_{i,j}(A^{(k+1)}) \leq \mu_{j-r-s+1,j}(A^{(k+1)}) = \mu(B, A^{(k)}) \leq \mu(B).$$

From lemma 9  $\mu(B) = \mu(b_1, \dots, b_s) \leq O(s^{-h_0 - \frac{1}{2}})$ . Thus

$$\begin{aligned} \sum_{i \leq j-r-s} \mu_{i,j}(A^{(k+1)}) &\leq (j-r-s)O(s^{-h_0 - \frac{1}{2}}) \\ &\leq m_{(k+1)}O(s^{-h_0 - \frac{1}{2}}) = O(1). \end{aligned}$$

Therefore in case 1  $\rho_j(A^{(k+1)}) = O(1)$  for each  $j = 1, \dots, m_{(k+1)}$ .

Case 2:  $m_k + 1 \leq r \leq m_k + s$ , i.e.  $j$  is in  $B$  part. Let  $r_1 = r - m_k$ , then

$$\begin{aligned} \rho_j(A^{(k+1)}) &= \sum_{i \leq j-m_k-s} \mu_{i,j}(A^{(k+1)}) + \sum_{i=j-m_k-s+1}^{j-r} \mu_{i,j}(A^{(k+1)}) \\ &+ \sum_{i=j-r+1}^{j-r_1} \mu_{i,j}(A^{(k+1)}) + \sum_{i=j-r_1+1}^j \mu_{i,j}(A^{(k+1)}) \\ &= \sum_{i \leq j-m-s} \mu_{i,j}(A^{(k+1)}) \\ &+ \sum_{i=r_1+1}^s \mu(b_i, \dots, b_s, A^{(k)}, b_1, \dots, b_{r_1}) \\ &+ \sum_{i=1}^{m_k} \mu_{i,m_k+r_1}(A^{(k)}, b_1, \dots, b_{r_1}) + \sum_{i=1}^{r_1} \mu(b_i, \dots, b_{r_1}). \end{aligned}$$

First we use Fact 1 on the third term,

$$\begin{aligned} \sum_{i=1}^{m_k} \mu_{i,m_k+r_1}(A^{(k)}, b_1, \dots, b_{r_1}) &\leq \sum_{i=1}^{m_k} \mu_{i,m_k}(A^{(k)}) \\ &= \rho_{m_k}(A^{(k)}) = O(1). \end{aligned}$$

Next we use Lemma 3 and Fact 1 to upper bound the second and fourth term,

$$\begin{aligned} \sum_{i=r_1+1}^s \mu(b_i, \dots, b_s, A^{(k)}, b_1, \dots, b_{r_1}) \\ &\leq \sum_{i=r_1+1}^s \mu(b_i, \dots, b_s, b_1, \dots, b_{r_1}) \\ &\leq \sum_{i=r_1+1}^s O(\frac{1}{(r_1 + s - i + 1)^{3/2}}) = O(1), \end{aligned}$$

$$\sum_{i=1}^{r_1} \mu(b_i, \dots, b_{r_1}) \leq \sum_{i=1}^{r_1} O(\frac{1}{(r_1 - i + 1)^{3/2}}) = O(1).$$

For the first term, since  $i < j - m_k - s$ ,  $\mu_{i,j}(A^{(k+1)}) \leq \mu(B) = O(s^{-h_0 - \frac{1}{2}})$ , so

$$\begin{aligned} \sum_{i \leq j-m-u} \mu_{i,j}(A^{(k+1)}) &\leq jO(s^{-h_0 - \frac{1}{2}}) \\ &\leq m_{(k+1)}O(s^{-h_0 - \frac{1}{2}}) = O(1). \end{aligned}$$

This finishes the proof of case 2.

Since  $d_1 = 2$ ,  $d_{k+1} = \frac{(4h_0 + \frac{3}{2})d_k - 2(h_0 + 1)}{(2h_0 + 1)d_k}$ , from Eq. (9)  $d_{k+1} \rightarrow 1 + \frac{1}{2h_0 + 1} < 1 + \delta$ , and after constant steps (more precisely  $\log_{(1+\delta)/(2h_0+1)}\left(\frac{1 - \frac{1}{2h_0+1}}{\delta - \frac{1}{2h_0+1}}\right)$  steps), we can get a sequence  $A$  satisfy both conditions.  $\square$

## 6. Proof of Proposition 4(Sketch)

Most part of the proof is the same as Proposition 2, except we have a 3-d random path, and also we need to define unequal  $w'(\mathbf{P}, \mathbf{P}', x)$  and  $w'(\mathbf{P}', \mathbf{P}, x)$ , in order to derive better quantum lower bound.

Consider the following  $n$ -step random walk in  $\mathbb{Z}^3$ :  $Y_0 = (0, 0, 0)$ ,  $Y_k = Y_{k-1} + (\mathbf{v}_k, 0)$  with probability  $\frac{1}{2}$ , and  $Y_k = Y_{k-1} + (0, 0, \|\mathbf{v}_k\|_1)$  with probability  $\frac{1}{2}$ ,  $k = 1, \dots, n$ . It is clear that  $\|Y_k\|_1 = \sum_{j=1}^k \|\mathbf{v}_j\|_1$ , ( $k = 1, \dots, n$ ), especially  $Y_n$  is on the bottom plane of the pyramid  $\mathcal{P}_{3,N}$ .

**Lemma 10** For any  $\mathbf{y} \in \mathbb{Z}^3$ ,  $0 \leq i < j \leq n$ ,

$$\Pr(Y_j - Y_i = \mathbf{y}) \leq \mu_{i+1,j}.$$

Consider all the  $2^n$  paths  $\mathbf{P} = p_0 p_1 \dots p_n \in \mathcal{P}_{3,N}$  which are generated by the random walk:  $p_k = p_{k-1} + (\mathbf{v}_k, 0)$  or  $p_k = p_{k-1} + (0, 0, \|\mathbf{v}_k\|_1)$ . To make the path more precisely, if  $p_k = p_{k-1} + (x_1, x_2, x_3)$ , the path first goes  $x_1$  steps along  $x$ -axis, then  $x_2$  steps along  $y$ -axis, then  $x_3$  steps along  $z$ -axis. We use the quantum adversary method to prove that in order to separate these  $2^n$  paths,  $\Omega(\frac{n}{\lambda})$  quantum queries are needed.

For any two paths  $\mathbf{P} = p_0 \dots p_n$  and  $\mathbf{P}' = p'_0 \dots p'_n$ , define  $|\mathbf{P} \wedge \mathbf{P}'| = k$  if  $p_0 = p'_0, \dots, p_k = p'_k$  and  $p_{k+1} \neq p'_{k+1}$ . For any point  $x \in V_{3,N} \setminus (0, 0, 0)$ , define  $|x|_* = \{k \in \mathbb{N} : \sum_{i=1}^{k-1} \|\mathbf{v}_i\|_1 < \|x\|_1 \leq \sum_{i=1}^k \|\mathbf{v}_i\|_1\}$ , i.e.  $p_{k-1} p_k$  is the only possible segment of the path that point  $x$  belongs to. Now we let

$$w(\mathbf{P}, \mathbf{P}') = \begin{cases} 0 & \text{if } p_n = p'_n, \\ \frac{1}{2^{n-|\mathbf{P} \wedge \mathbf{P}'|}} & \text{otherwise.} \end{cases}$$

and let

$$w'(\mathbf{P}, \mathbf{P}', x) = \frac{\sqrt{\mu_{|\mathbf{P} \wedge \mathbf{P}'|+1, |x|_*}}}{2^{n-|\mathbf{P} \wedge \mathbf{P}'|}},$$

if  $\mathbf{P}(x) = 1, \mathbf{P}'(x) = 0, p_n \neq p'_n$ ;

$$w'(\mathbf{P}, \mathbf{P}', x) = \frac{1}{2^{n-|\mathbf{P} \wedge \mathbf{P}'|} \sqrt{\mu_{|\mathbf{P} \wedge \mathbf{P}'|+1, |x|_*}}},$$

if  $\mathbf{P}(x) = 0, \mathbf{P}'(x) = 1, p_n \neq p'_n$ ;  $w'(\mathbf{P}, \mathbf{P}', x) = 0$  otherwise. Notice that if  $\mathbf{P}(x) \neq \mathbf{P}'(x)$ , then it must be  $|\mathbf{P} \wedge \mathbf{P}'| < |x|_*$ , so the notation  $\mu_{|\mathbf{P} \wedge \mathbf{P}'|+1, |x|_*}$  is well defined. From the definition it is clear that  $w'(\mathbf{P}, \mathbf{P}', x)w'(\mathbf{P}', \mathbf{P}, x) \geq w(\mathbf{P}, \mathbf{P}')^2$ .

We first give lower bound for  $w(\mathbf{P}, x)$ :

$$\begin{aligned} w(\mathbf{P}) &= \sum_{\mathbf{P}'} w(\mathbf{P}, \mathbf{P}') = \sum_{k=0}^{n-1} \sum_{\substack{\mathbf{P}': p_n \neq p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} \frac{1}{2^{n-k}} \\ &= \sum_{k=0}^{n-1} \frac{1}{2^{n-k}} \left( 2^{(n-k-1)} - \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1 \right) \\ &= \frac{n}{2} - \sum_{k=0}^{n-1} \frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1. \end{aligned} \quad (10)$$

We know

$$\frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1 \leq \Pr(Y_n - Y_k = p_n - p_k),$$

and from Lemma 10  $\Pr(Y_n - Y_k = p_n - p_k) \leq \mu_{k+1,n} \leq \sqrt{\mu_{k+1,n}}$  (the last " $\leq$ " is due to  $\mu_{k+1,n} \leq 1$ ). Thus

$$\sum_{k=0}^{n-1} \frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}': p_n = p'_n \\ |\mathbf{P}' \wedge \mathbf{P}|=k}} 1 \leq \sum_{k=0}^{n-1} \sqrt{\mu_{k+1,n}} = \lambda_n \leq \lambda. \quad (11)$$

Combine inequality (10) with (11),

$$w(\mathbf{P}) \geq \frac{n}{2} - \lambda. \quad (12)$$

Next we derive an upper bound to  $v(\mathbf{P}, x)v(\mathbf{P}', x)$  when  $\mathbf{P}(x) \neq \mathbf{P}'(x)$  and  $w(\mathbf{P}, \mathbf{P}') > 0$ . Without loss of generality, we assume  $\mathbf{P}(x) = 1$  and  $\mathbf{P}'(x) = 0$ . Then

$$\begin{aligned} v(\mathbf{P}, x) &= \sum_{\mathbf{P}''} w'(\mathbf{P}, \mathbf{P}'', x) = \sum_{\substack{\mathbf{P}'': \mathbf{P}''(x)=0, \\ p''_n \neq p_n}} \frac{\sqrt{\mu_{|\mathbf{P} \wedge \mathbf{P}''|+1, |x|_*}}}{2^{n-|\mathbf{P} \wedge \mathbf{P}''|}} \\ &= \sum_{k=0}^{|x|_*-1} \sum_{\substack{\mathbf{P}'': |\mathbf{P} \wedge \mathbf{P}''|=k, \\ \mathbf{P}''(x)=0, p''_n \neq p_n}} \frac{\sqrt{\mu_{k+1, |x|_*}}}{2^{n-k}} \\ &= \sum_{k=0}^{|x|_*-1} \frac{\sqrt{\mu_{k+1, |x|_*}}}{2^{n-k}} \sum_{\substack{\mathbf{P}'': |\mathbf{P} \wedge \mathbf{P}''|=k, \\ \mathbf{P}''(x)=0, p''_n \neq p_n}} 1. \end{aligned}$$

We trivially bound the number of path  $\mathbf{P}''$  such that  $|\mathbf{P} \wedge \mathbf{P}''| = k, \mathbf{P}''(x) = 0$  and  $p''_n \neq p_n$  by  $2^{n-k}$ , so

$$\begin{aligned} v(\mathbf{P}, x) &\leq \sum_{k=0}^{|x|_*-1} \frac{\sqrt{\mu_{k+1, |x|_*}}}{2^{n-k}} \cdot 2^{n-k} \\ &\leq \sum_{k=0}^{|x|_*-1} \sqrt{\mu_{k+1, |x|_*}} = \lambda_{|x|_*} \leq \lambda. \end{aligned} \quad (13)$$

Now it turns to bound  $v(\mathbf{P}', x)$ :

$$\begin{aligned}
v(\mathbf{P}', x) &= \sum_{\mathbf{P}''} w'(\mathbf{P}', \mathbf{P}'', x) \\
&= \sum_{\substack{\mathbf{P}'': \mathbf{P}''(x)=1, \\ p''_n \neq p'_n}} \frac{1}{2^{n-|\mathbf{P}' \wedge \mathbf{P}''|} \sqrt{\mu_{|\mathbf{P}' \wedge \mathbf{P}''|+1, |x|_*}}} \\
&= \sum_{k=0}^{|x|_*-1} \frac{1}{2^{n-k} \sqrt{\mu_{k+1, |x|_*}}} \sum_{\substack{\mathbf{P}'': |\mathbf{P}' \wedge \mathbf{P}''|=k, \\ \mathbf{P}''(x)=1, p''_n \neq p'_n}} 1 \\
&\leq \sum_{k=0}^{|x|_*-1} \frac{1}{2^{n-k} \sqrt{\mu_{k+1, |x|_*}}} \sum_{\substack{\mathbf{P}'': |\mathbf{P}' \wedge \mathbf{P}''|=k, \\ \mathbf{P}''(x)=1}} 1. \quad (14)
\end{aligned}$$

Suppose  $\mathbf{P}'' = p''_0 \dots p''_n$ . Since  $\mathbf{P}''(x) = 1$ , i.e. path  $\mathbf{P}''$  contains point  $x$ , we know  $p''_{|x|_*} = p''_{|x|_*-1} + (\mathbf{v}_{|x|_*}, 0)$  or  $p''_{|x|_*} = p''_{|x|_*-1} + (0, \|\mathbf{v}_{|x|_*}\|_1)$ , according to the construction of the path,  $p''_{|x|_*}$  has at most two different choices. Therefore,

$$\frac{1}{2^{n-k}} \sum_{\substack{\mathbf{P}'': |\mathbf{P}' \wedge \mathbf{P}''|=k, \\ \mathbf{P}''(x)=1}} 1 \leq 2 \max_{\mathbf{y} \in V_{3,N}} \Pr(Y_{|x|_*} - Y_k = \mathbf{y} - p''_k). \quad (15)$$

From Lemma 10,

$$\max_{\mathbf{y} \in V_{3,N}} \Pr(Y_{|x|_*} - Y_k = \mathbf{y} - p''_k) \leq \mu_{k+1, |x|_*}, \quad (16)$$

Combine inequality (14),(15),(16),

$$v(\mathbf{P}', x) \leq \sum_{k=0}^{|x|_*-1} \frac{2\mu_{k+1, |x|_*}}{\sqrt{\mu_{k+1, |x|_*}}} = 2\lambda_{|x|_*} \leq 2\lambda. \quad (17)$$

Combine inequality (12),(13) and (17),

$$\begin{aligned}
Q(\mathcal{P}_{3,N}) &= \Omega \left( \sqrt{\frac{wt(\mathbf{P})wt(\mathbf{P}')}{v(\mathbf{P}, x)v(\mathbf{P}', x)}} \right) \\
&= \Omega \left( \sqrt{\frac{(\frac{n}{2} - \lambda) \cdot (\frac{n}{2} - \lambda)}{\lambda \cdot 2\lambda}} \right) = \Omega\left(\frac{n}{\lambda}\right).
\end{aligned}$$

□

## 7. Proof of Proposition 5(Sketch)

Pick a fixed integer  $h_0 > 3$  such that  $\frac{2}{h_0} < \delta$ . We recursively construct our vector sequence  $V$ .

Similarly as the proof of Proposition 3, for any vector sequence  $W$  we will use  $N(W)$  to denote the sum of 1-norm of the vectors in the sequence.

(1) Let  $V^{(1)} = \{(1, m), (2, m-1), \dots, (m, 1)\}$ . Then the length of sequence  $V^{(1)}$  is  $m$ , and  $N(V^{(1)}) = m(m+1) = O(m^2)$ .

It is clear that vectors  $\{(i, m+1-i), (i+1, m-i), \dots, (j, m+1-j)\}$  satisfy the conditions  $\|\mathbf{v}_k - \mathbf{v}_{k'}\| \geq 1 (k \neq k')$ , and also it is easy to check if  $j-i \geq 6$ , then for any  $\|\mathbf{e}\| = 1$  we can select at least  $(j-i+1)/2$  vectors  $\mathbf{v}_k$  from  $\{(i, m+1-i), (i+1, m-i), \dots, (j, m+1-j)\}$  with  $|\langle \mathbf{v}_k, \mathbf{e} \rangle| \geq 1$ , so from Lemma 5

$$\mu\{(i, m+1-i), \dots, (j, m+1-j)\} \leq c_1(j-i+1)^{-2}.$$

We can pick another constant  $c_2 > c_1$  to handle the case when  $j-i < 6$ , thus

$$\mu_{i,j}(V^{(1)}) = \mu\{(i, m+1-i), \dots, (j, m+1-j)\} \leq c_2(j-i+1)^{-2},$$

thus  $\lambda_j(V^{(1)}) = \sum_{i=1}^j \sqrt{\mu_{i,j}(V^{(1)})} \leq \sum_{i=1}^j \frac{\sqrt{c_2}}{(j-i+1)} = O(\log j) \leq O(\log m)$ .

(2) Suppose we have already constructed sequence  $V^{(k)} = \mathbf{v}_1 \mathbf{v}_2 \dots \mathbf{v}_{m_k}$  such that  $N(V^{(k)}) = O(m_k^{d_k})$  ( $d_k > 1 + \frac{2}{h_0}$ ), and  $\forall 1 \leq j \leq m_k, \lambda_j(V^{(k)}) = O(\log m_k)$ . We have  $d_1 = 2$ . We try to construct a sequence  $V^{(k+1)}$  with length  $m_{(k+1)}$  ( $m_{(k+1)} > m_k$ ), s.t.  $N(V^{(k+1)}) = O(m_{(k+1)}^{d_{k+1}})$ , where  $1 + \frac{2}{h_0} < d_{k+1} < d_k$ ,  $\{d_j\} \downarrow 1 + \frac{2}{h_0}$ , and also  $\lambda_j(V^{(k+1)}) = O(\log m_{(k+1)})$  ( $j = 1, \dots, m_{(k+1)}$ ).

Let

$$s = m_k^{\frac{d_k}{h_0+2}}, \quad t = m_k^{\frac{h_0}{h_0+2}d_k-1},$$

since  $d_k > 1 + \frac{2}{h_0}$ ,  $t$  is well defined.

From Lemma 7 we know there is a  $B_{h_0}$ -sequence in  $\{1, \dots, c_3 s^{h_0}\}$  with size  $s$ , here  $c_3$  is a constant. Suppose  $b_1, b_2, \dots, b_s$  be the  $B_{h_0}$ -sequence. Now we append  $V^{(k)}$  by all the vectors  $(3b_{i_1}, 3b_{i_2})$  ( $i_1 \neq i_2$ ) with certain order, and then repeat the sequence  $t$  times, more precisely

$$\left. \begin{array}{cccc}
V^{(k+1)} = V^{(k)}, & (3b_1, 3b_2), & (3b_2, 3b_1), & \dots & (3b_s, 3b_{s-1}); \\
& \vdots & \vdots & & \vdots \\
V^{(k)}, & (3b_1, 3b_2), & (3b_2, 3b_1), & \dots & (3b_s, 3b_{s-1}).
\end{array} \right\} t$$

here vector  $(3b_{i_1}, 3b_{i_2})$  ( $i_1 < i_2$ ) is followed by the vector  $(3b_{i_2}, 3b_{i_1})$ . Let  $W = (3b_1, 3b_2), \dots, (3b_s, 3b_{s-1})$ . We claim that

**Lemma 11** Suppose  $\mathbf{w}_1, \dots, \mathbf{w}_l$  be a consecutive subsequence of  $W$ , then  $\mu(\mathbf{w}_1, \dots, \mathbf{w}_l) \leq O(l^{-2})$ .

**Lemma 12**  $\mu(W) \leq O(|W|^{-h_0}) = O(s^{-2h_0})$ .

Lemma 11 can be proved using Lemma 5 and Lemma 12 can be proved using Lemma 6. Due to page limitation we will give more details in a full version paper.

Lemma 11 and Lemma 12 can be considered as the 3-d version of Lemma 3 and Lemma 9. It will be used to upper bound  $\lambda_j(V^{(k+1)})$ .

The total length of the sequence  $V^{(k+1)}$  is  $m_{(k+1)} = t(m_k + |W|) = t(m_k + s(s-1)) = \Theta(tm_k) =$



$\Theta(m_k^{\frac{h_0}{h_0+2}d_k})$ . The third "=" is due to  $s(s-1) < s^2 = m_k^{\frac{2d_k}{h_0+2}} \leq m_k^{\frac{4}{h_0+2}} = o(m_k)$ , since  $h_0 > 3$ . And

$$\begin{aligned} N(V^{(k+1)}) &= t(N(V^{(k)}) + N(W)) \\ &= t(O(m_k^{d_k}) + \sum_{i \neq j}^s (3b_i + 3b_j)) \\ &\leq t(O(m_k^{d_k}) + s^2 \cdot 6c_3s^{h_0}) \\ &= t(O(m_k^{d_k}) + 6c_3m_k^{d_k}) \\ &= O(tm_k^{d_k}) = O(m_k^{\frac{2h_0+2}{h_0+2}d_k-1}). \end{aligned}$$

Therefore

$$d_{(k+1)} = \frac{\frac{2h_0+2}{h_0+2}d_k - 1}{\frac{h_0}{h_0+2}d_k} = \frac{(2h_0+2)d_k - (h_0+2)}{h_0d_k},$$

which implies

$$\frac{d_{(k+1)} - (1 + \frac{2}{h_0})}{d_k - (1 + \frac{2}{h_0})} = \frac{1}{d_k}. \quad (18)$$

We know  $d_1 = 2 > 1 + \frac{2}{h_0}$ , so  $\{d_j\} \downarrow (1 + \frac{2}{h_0})$ .

The rest thing is to show sequence  $V^{(k+1)}$  satisfies  $\lambda_j(V^{(k+1)}) = O(\log m_{(k+1)})$  for  $j = 1, \dots, m_{(k+1)}$ . The idea is similar to the proof in Proposition 3. Instead of Lemma 3 and Lemma 9, we use Lemma 11 and Lemma 12 here. Because of space limitation we omit the proof of this part.

From Eq. (18) we know  $d_k \rightarrow 1 + \frac{2}{h_0} < 1 + \delta$ , so after constant steps (more precisely  $\log_{(1+2/h_0)}(\frac{1-2/h_0}{\delta-2/h_0})$  steps) we will obtain a vector sequence  $V$  which satisfies the conditions in Proposition 5.  $\square$

## References

- [1] S. Aaronson. Lower bounds for local search by quantum arguments, *Proc. of 36th STOC*, pp. 465-474, 2004.
- [2] D. Aldous. Minimization algorithms and random walk on the d-Cube, *Annals of Probability* 11(2), pp. 403-413, 1983.
- [3] A. Ambainis. Polynomial degree vs. quantum query complexity, *Proc. of 44th FOCS*, pp. 230-239, 2003.
- [4] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computation, *SIAM journal on Computing* 26, pp. 1510-1523, 1997.

- [5] R. C. Bose and S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helv.* 37 (1962-63), 141-147.
- [6] Xi Chen and Xiaotie Deng. On algorithms for discrete and approximate brouwer fixed points, *Proc. of 37th STOC*, pp. 323-330, 2005.
- [7] C. G. Esseen. Fourier analysis of distribution functions, *Acta Mathematica* 77, pp. 1-125, 1945.
- [8] K. Friedl, G. Ivanyos, M. Santha and Y. Verhoeven. On the black-box Complexity of Sperner's Lemma, *15th FCT*, pp. 245-257, 2005.
- [9] G. Halász. Estimates for the concentration function of combinatorial number theory and probability, *Periodica Mathematica Hungarica* Vol. 8 (3-4), (1977) 197-211.
- [10] H. Halberstam and K. F. Roth. *Sequences*, Oxford, 1966.
- [11] D. Johnson, C. Papadimitriou, M. Yannakakis. How Easy is Local Search? *Journal of Computer System Sciences* 37(1) 79-100, 1988.
- [12] D. Llewellyn, C. Tovey, and M. Trick. Local optimization on graphs, *Discrete Applied Mathematics* 23:157-178, 1989. Erratum: 46: 93-94, 1993.
- [13] M. Santha and M. Szegedy. Quantum and classical query complexities of local search are polynomially related, *Proc. of 36th STOC*, pp. 494-501, 2004.
- [14] A. Sárközy and E. Szemerédi. Über ein Problem von Erdős und Moser, *Acta Arithmetica* 11, 1965, 205-208.
- [15] Y. Verhoeven. Enhanced algorithms for local search, *Information Processing Letters* 97, 171-176, 2006.
- [16] Shengyu Zhang. On the power of Ambainis's lower bounds, In *Proc. of 31st ICALP*, LNCS 3142, pp. 1238-1250, 2004.
- [17] Shengyu Zhang. New upper and lower bounds for randomized and quantum Local Search, *Proc. of 38th STOC* 2006.

## Appendix: Proof of Lemma 9

**Proof of Lemma 9:** Define  $s$  independent random variable  $X_j$ :  $\Pr(X_j = b_j) = \Pr(X_j = -b_j) = \frac{1}{2}$ . Let  $M = cs^{h_0}$ , then  $M < b_j \leq 2M$  ( $j = 1, \dots, s$ ). The inequality we need to prove is

$$\Pr(X_1 + \dots + X_s = y) \leq O\left(\frac{1}{s^{h_0}\sqrt{s}}\right) \quad (19)$$

We prove it by the following two steps:

$$\Pr(y - 4h_0M \leq X_1 + \dots + X_s \leq y + 4h_0M) \leq O\left(\frac{1}{\sqrt{s}}\right),$$

and

$$\Pr(X_1 + \dots + X_s = y) \leq O\left(\frac{1}{s^{h_0}}\right) \cdot \Pr(y - 4h_0M \leq X_1 + \dots + X_s \leq y + 4h_0M) \quad (21)$$

**Proof of Inequality (20):** Since  $M < b_j \leq 2M$ ,  $\Sigma_2 = \sum_{j=1}^s E[X_j^2] = \sum_{j=1}^s b_j^2 = \Theta(sM^2)$ , and  $\Sigma_3 = \sum_{j=1}^s E[|X_j|^3] = \sum_{j=1}^s b_j^3 = \Theta(sM^3)$ . From Esseen's inequality we have

$$\left| \Pr\left(\frac{X_1 + \dots + X_s}{\sqrt{\Sigma_2}} < y\right) - \Phi(y) \right| \leq c \frac{\Sigma_3}{\Sigma_2^{3/2}} = O\left(\frac{1}{\sqrt{s}}\right).$$

By picking two different  $y$ :  $y_1 = \frac{y}{\sqrt{\Sigma_2}} - \frac{c_1}{\sqrt{s}}$  and  $y_2 = \frac{y}{\sqrt{\Sigma_2}} + \frac{c_1}{\sqrt{s}}$  in the Inequality and adding up the two inequalities, we get

$$\begin{aligned} & \left| \Pr\left(\frac{X_1 + \dots + X_s}{\sqrt{\Sigma_2}} < \frac{y}{\sqrt{\Sigma_2}} + \frac{c_1}{\sqrt{s}}\right) \right. \\ & \left. - \Pr\left(\frac{X_1 + \dots + X_s}{\sqrt{\Sigma_2}} < \frac{y}{\sqrt{\Sigma_2}} - \frac{c_1}{\sqrt{s}}\right) \right| \\ & \leq O\left(\frac{1}{\sqrt{s}}\right) + \left| \Phi\left(\frac{z}{\sqrt{\Sigma_2}} + \frac{c_1}{\sqrt{s}}\right) - \Phi\left(\frac{z}{\sqrt{\Sigma_2}} - \frac{c_1}{\sqrt{s}}\right) \right| \\ & = O\left(\frac{1}{\sqrt{s}}\right), \end{aligned}$$

here  $c_1$  is a constant to be fixed later. Thus

$$\Pr(y - c_1 \frac{\sqrt{\Sigma_2}}{\sqrt{s}} \leq X_1 + \dots + X_s < y + c_1 \frac{\sqrt{\Sigma_2}}{\sqrt{s}}) \leq O\left(\frac{1}{\sqrt{s}}\right).$$

Since  $\Sigma_2 = \Theta(sM^2)$ , we can choose a suitable  $c_1$  such that  $c_1 \frac{\sqrt{\Sigma_2}}{\sqrt{s}} > 4h_0M$  (notice  $h_0$  is a constant). Hence

$$\Pr(y - 4h_0M \leq X_1 + \dots + X_s \leq y + 4h_0M) \leq O\left(\frac{1}{\sqrt{s}}\right).$$

**Proof of Inequality (21):** For any  $h_0$ -element subset  $\{i_1, \dots, i_{h_0}\} \subset \{1, \dots, s\}$ , we have

$$\begin{aligned} & \Pr\left(\sum_{j=1}^s X_j = y\right) \\ & = \sum_{\substack{\epsilon_1, \dots, \epsilon_{h_0} \\ \in \{\pm 1\}}} \Pr\left(\sum_{j=1}^s X_j = y, x_{i_1} = \epsilon_1 b_{i_1}, \dots, x_{i_{h_0}} = \epsilon_{h_0} b_{i_{h_0}}\right) \\ & = \sum_{\substack{\epsilon_1, \dots, \epsilon_{h_0} \\ \in \{\pm 1\}}} \Pr\left(\sum_{\substack{1 \leq j \leq s, \\ j \neq i_1, \dots, i_{h_0}}} X_j = y - \sum_{j=1}^{h_0} \epsilon_j b_{i_j}\right) \cdot \frac{1}{2^{h_0}}. \end{aligned}$$

The last "=" is due to  $\Pr(X_j = b_j) = \Pr(X_j = -b_j) = 1/2$ . Now change  $\epsilon_j b_{i_j}$  to  $-\epsilon_j b_{i_j}$ ,

$$\begin{aligned} \Pr\left(\sum_{j=1}^s X_j = y\right) & = \sum_{\substack{\epsilon_1, \dots, \epsilon_{h_0} \\ \in \{\pm 1\}}} \Pr\left(\sum_{\substack{1 \leq j \leq s, \\ j \neq i_1, \dots, i_{h_0}}} X_j = y - \sum_{j=1}^{h_0} \epsilon_j b_{i_j}\right) \\ & \quad \cdot \Pr(x_{i_1} = -\epsilon_1 b_{i_1}, \dots, x_{i_{h_0}} = -\epsilon_{h_0} b_{i_{h_0}}) \\ & \leq \sum_{\substack{\epsilon_1, \dots, \epsilon_{h_0} \\ \in \{\pm 1\}}} \Pr\left(\sum_{j=1}^s X_j = y - 2 \sum_{j=1}^{h_0} \epsilon_j b_{i_j}\right). \end{aligned}$$

Therefore

$$\begin{aligned} & \Pr\left(\sum_{j=1}^s X_j = y\right) \\ & \leq \frac{1}{\binom{s}{h_0}} \sum_{i_1 < \dots < i_{h_0}} \left[ \sum_{\epsilon_1, \dots, \epsilon_{h_0} \in \{\pm 1\}} \Pr\left(\sum_{j=1}^s X_j = y - 2 \sum_{j=1}^{h_0} \epsilon_j b_{i_j}\right) \right] \\ & \leq O\left(\frac{1}{s^{h_0}}\right) \sum_{\substack{\epsilon_1, \dots, \epsilon_{h_0} \\ \in \{\pm 1\}}} \left[ \sum_{i_1 < \dots < i_{h_0}} \Pr\left(\sum_{j=1}^s X_j = y - 2 \sum_{j=1}^{h_0} \epsilon_j b_{i_j}\right) \right] \quad (22) \end{aligned}$$

For a fixed  $(\epsilon_1, \dots, \epsilon_{h_0}) \in \{\pm 1\}^{h_0}$ , all the  $\binom{s}{h_0}$  value

$$\left\{ \sum_{j=1}^{h_0} \epsilon_j b_{i_j} : 1 \leq i_1 < \dots < i_{h_0} \leq s \right\}$$

are distinct, otherwise we will have two  $h_0$ -subset with same sum, contradiction to  $B_{h_0}$ -sequence. Therefore  $z - 2 \sum_{j=1}^{h_0} \epsilon_j b_{i_j}$  are all distinct. But we know  $M < b_j \leq 2M$ , so

$$y - 4h_0M \leq y - 2 \sum_{j=1}^{h_0} \epsilon_j b_{i_j} \leq y + 4h_0M.$$

Thus

$$\begin{aligned} & \sum_{i_1 < \dots < i_{h_0}} \Pr\left(\sum_{j=1}^s X_j = y - 2 \sum_{j=1}^{h_0} \epsilon_j b_{i_j}\right) \\ & \leq \Pr\left(y - 4h_0M \leq \sum_{j=1}^s X_j \leq y + 4h_0M\right) \quad (23) \end{aligned}$$

Combine Eq. (22), Eq. (23)

$$\begin{aligned} & \Pr\left(\sum_{j=1}^s X_j = y\right) \\ & \leq O\left(\frac{1}{s^{h_0}}\right) \sum_{\substack{\epsilon_1, \dots, \epsilon_{h_0} \\ \in \{\pm 1\}}} \Pr(y - 4h_0M \leq \sum_{j=1}^s X_j \leq y + 4h_0M) \\ & = O\left(\frac{2^{h_0}}{s^{h_0}}\right) \Pr(y - 4h_0M \leq \sum_{j=1}^s X_j \leq y + 4h_0M). \end{aligned}$$

□