Algorithmica
DOI 10.1007/s00453-008-9170-6

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

Xiaoming Sun · Andrew Chi-Chih Yao

Received: 23 April 2007 / Accepted: 10 January 2008

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 (based on Ambainis' adversary method 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, Bose and Chowla, and Halász from combinatorial number theory, as well as less familiar probability tools like Esseen's Inequality.

Keywords Local search · Quantum query complexity

This work was supported in part by the National Natural Science Foundation of China Grant 60553001, 60603005, and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.

X. Sun (✉) · A.C.-C. Yao
Institute for Theoretical Computer Science, Tsinghua University, Beijing 100084,
People's Republic of China
e-mail: xiaomings@tsinghua.edu.cn

A.C.-C. Yao
e-mail: andrewcyao@tsinghua.edu.cn

1 Introduction

For any function $f(x_1, x_2, \ldots, x_n)$, 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.

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. [5] (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 [12] 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 a vertex satisfying $f(v) \le f(w)$ 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 ϵ), and $QLS(G)$ (quantum with two-sided error ϵ).

In 1983, Aldous [2] showed that, for any N-vertex graph G of maximum degree Δ, $RLS(G) = O(\sqrt{N\Delta})$. 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 [13] 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 [14] 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., $QLS([n]^d) = \Theta(n^{d/3})$. The following table summarizes the low dimension case (again up to log factors), considerable gaps remain:

d	2	3	4
$RLS([n]^d)$	$\Omega(n^{2/3})$, $O(n)$	–	–
$QLS([n]^d)$	$\Omega(n^{2/5})$, $O(\sqrt{n})$	$\Omega(n^{3/4})$, $O(n)$	$\Omega(n^{6/5})$, $O(n^{4/3})$

The technique used in previous works is first related Local Search problem with some finding paths problem in the graph (finding the endpoint of a path which starts from a given vertex), and then constructs a "hard" path using some standard random walk technique on the graph. In this paper we follow this hiding-path approach. The main difference between our paper and previous works is that we use a novel construction of random walk with various step lengths: We first construct an integer sequence which has some nice properties, and then use them as the steps length of the random walk. By analyzing this novel random walk, we give nearly optimal lower bounds of local search 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 [18] 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 [14] showed that $QLS([n]^2) = \Omega(n^{1/4})$. Zhang [18] showed $RLS([n]^2) = \Omega(n^{2/3})$, $QLS([n]^2) = \Omega(n^{2/5})$ and $QLS([n]^2) = O(\sqrt{n}(\log\log n)^{3/2})$. Verhoeven [16] showed $QLS([n]^2) = O(\sqrt{n} \times \log\log n)$. For 3 and 4 dimensional grids, Zhang [18] 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 [7] show a $\Omega(n^{d-1})$ deterministic lower bound for finding a *fixed point* in grid $[n]^d$. Friedl et al [9] proved $\Omega(\sqrt{n})$ and $\Omega(n^{1/4})$ lower bound for random and quantum query complexity of *2D-Sperner* Problem by using a 2-d monotone path.

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

2 Preliminaries

Lemma 1 gives a general quantum lower bound based on the weighted adversary approach first developed by Ambainis [4]. This form is from Zhang [17]:

Lemma 1 ([4, 17]) *Let* $F : S \to \{0, 1\}^m$ *be a partial function. Let* $w : S \times S \to [0, \infty)$ *and* $w' : S \times S \times [N] \to [0, \infty)$ *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 $F:S\to\{0,1\}^m$ be a partial function. Let $w:S\times S\to[0,\infty)$ 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 to construct a random walk in two dimension space. In order to construct and analyze the sequence used in the random walk we need to use the following two inequalities proved by Sárközy and Szemerédi [15] and Esseen [8]:

Lemma 3 ([15]) *Let $0<a_1<a_2<\cdots<a_n$ 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 $0<a_1<a_2<\cdots<a_n$ be a sequence of real numbers, then

$$\max_{y\in\mathbb{Z}}\Pr_{\epsilon_1,\ldots,\epsilon_n\in\{\pm1\}}(\epsilon_1a_1+\cdots+\epsilon_na_n=y)\leq cn^{-3/2},$$

where c is a positive absolute constant.

Lemma 4 ([8]) *Let $X_1,\ldots,X_n$ be independent random variables such that $E(X_k)=0$, $E[X_k^2]=\sigma_k^2$, and $E[|X_k|^3]<+\infty$, $k=1,\ldots,n$. Let $B_n=\sum_{k=1}^n\sigma_k^2$, $L_n=B_n^{-3/2}\sum_{k=1}^nE[|X_k|^3]$, then*

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

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 to construct a 3-dimensional random walk. The construction and analysis of this random walk involves the following two results of Halász (Theorem 2 and Theorem 3 of [10]):

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* δn *vectors* $\mathbf{v}_k$ *with* $|\langle\mathbf{v}_k,\mathbf{e}\rangle|\geq 1$, *then*

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

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

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* $\mathbf{b}=\mathbf{v}_{k_1}\pm\cdots\pm\mathbf{v}_{k_h}$ $(1\leq k_i\leq n)$ *one can select at least* δn^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* δn *vectors* $\mathbf{v}_k$ *with* $|\langle\mathbf{v}_k,\mathbf{e}\rangle|\geq 1$, *then*

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

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

Remark 3 Lemma 6 used here is a weak version of Halász's original result (Theorem 3 in [10]). 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.

In order to build the 2-dimensional and 3-dimensional random walk we also need the following tools from number theory.

Definition 1 ([11]) A positive integer sequence $B=b_1b_2\cdots b_n$ is called a B_h-sequence if all the sums

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

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

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 [6]:

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

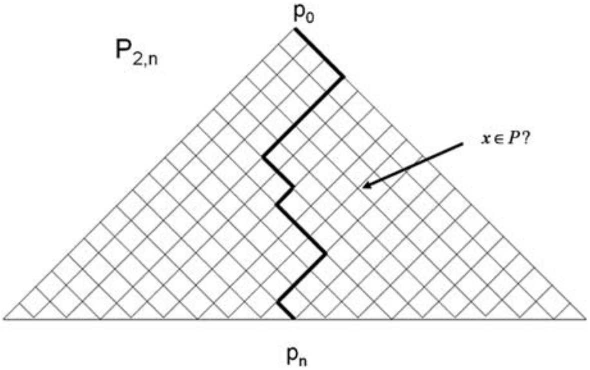

Fig. 1 2-dimensional pyramid path

3 Top Level View of the Proof

When proving lower bounds, it is a standard technique to relate the local search problem to some 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 $k \in \{1,2,\ldots,d\}$. Here $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $e_k = (0,\ldots,0,1,0,\ldots,0)$ 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 $(0,\ldots,0)$ and ending in a sink node at the bottom (the hyperplane $\{x : \sum_{i=1}^d x_i = n\}$). Figure 1 shows a 2-dimensional pyramid path.

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 $\mathbf{P} = p_0 \ldots p_n \in \mathcal{P}_{d,n}$, 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. □

We will prove Theorem 1 in two steps. First, for any sequence of integers $A = a_1, a_2, \ldots, a_n$, 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 ρ (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 ρ is small which then implies strong lower bounds via Proposition 2.

Similarly, the proof of Theorem 2 has two steps. Proposition 4 show that any sequence of two-dimensional vectors gives rise to a lower bound to $Q(\mathcal{P}_{3,N})$. Proposition 5 then shows that, with the help of certain results in combinatorial number theory, there exist sequences giving rise to strong lower bounds that almost match known upper bounds.

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

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

$$\rho_j = \sum_{i=1}^{j} \mu_{i,j} \quad (j = 1, \ldots, n),$$

and $\rho = \max_{1 \le j \le n} \rho_j$. Then $R(\mathcal{P}_{2,N}) = \Omega(\frac{n}{\rho})$, $Q(\mathcal{P}_{2,N}) = \Omega(\sqrt{\frac{n}{\rho}})$.

For example, consider sequence $a_1 = \cdots = a_n = 1$, $\rho_j = \Theta(\sqrt{j})$, $\rho = \Theta(\sqrt{n})$. So it gives lower bound $R(\mathcal{P}_{2,n}) = \Omega(\sqrt{n})$, $Q(\mathcal{P}_{2,n}) = \Omega(\sqrt[4]{n})$.

Proposition 3 *Given any constant $\delta > 0$, for any sufficient large $n \in \mathbb{N}$, there exists a positive integer sequence $A = a_1, a_2, \ldots, a_n$, such that*

$$\sum_j a_j = O(n^{1+\delta}) \quad \text{and} \quad \rho = O(1),$$

where the constants in both $O(*)$ depend only on δ, and ρ 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 $\mathbf{v}_1, \ldots, \mathbf{v}_n$ 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*

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

$$\lambda_j = \sum_{i=1}^{j} \sqrt{\mu_{i,j}} \quad (j = 1, \ldots, n),$$

and $\lambda = \max_{1 \le j \le n} \lambda_j$. Then $Q(\mathcal{P}_{3,N}) = \Omega(\frac{n}{\lambda})$.

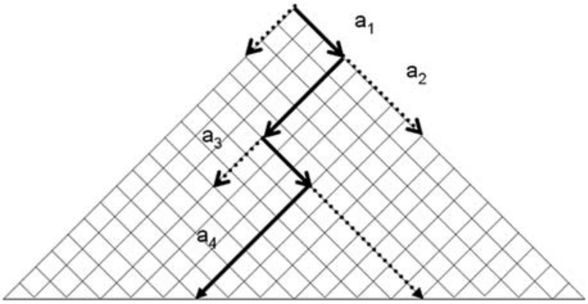

Fig. 2 A 4-step random walk constructed from sequence a_1, a_2, a_3, a_4

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

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

where the constants in both $O(*)$ *depend only on* δ, *and* λ *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 $\frac{1}{2}$, $k = 1, \ldots, n$ (Fig. 2 gives an example for $n = 4$). It is clear that $\|Y_k\|_1 = \sum_{j=1}^{k} a_j$, $k = 1, \ldots, n$, especially Y_n is on the bottom line of the pyramid $\mathcal{P}_{2,N}$.

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

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

Proof of Lemma 8 Define s independent random variables $\epsilon_{i+1}, \ldots, \epsilon_j$: $\Pr(\epsilon_k = 1) = \Pr(\epsilon_k = -1) = \frac{1}{2}$ $(k = i + 1, \ldots, j)$. Then we can write

$$Y_k = Y_{k-1} + \frac{\epsilon_k + 1}{2}(a_k, 0) + \frac{1 - \epsilon_k}{2}(0, a_k).$$

Suppose $\mathbf{y} = (y_1, y_2)$, then

$$\Pr(Y_j - Y_i = \mathbf{y}) = \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\left(\frac{\epsilon_k + 1}{2}(a_k, 0) + \frac{1 - \epsilon_k}{2}(0, a_k)\right) = (y_1, y_2)\right)$$
$$= \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\frac{\epsilon_k + 1}{2}a_k = y_1, \sum_{k=i+1}^{j}\frac{1 - \epsilon_k}{2}a_k = y_2\right)$$

$$
\begin{aligned}
&\le \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\frac{\epsilon_k+1}{2}a_k = y_1\right)\\
&= \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\epsilon_k a_k = 2y_1 - \sum_{k=i+1}^{j} a_k\right)\\
&\le \max_{y'\in\mathbb{Z}}\Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\epsilon_k a_k = y'\right)\\
&= \mu_{i+1,j}.
\end{aligned}
$$

□

Consider all the 2^n paths $\mathbf{P} = p_0 p_1 \cdots p_n \in \mathcal{P}_{2,N}$ 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, $\Omega(\frac{n}{\rho})$ randomized queries or $\Omega(\sqrt{\frac{n}{\rho}})$ quantum queries are needed.

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

We first give lower bound for $wt(\mathbf{P})$ of Lemma 1:

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

We know

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

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

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

Combine inequality (1) with (2),

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

Next we derive upper bounds to $v(\mathbf{P}, x)$ and $v(\mathbf{P}', x)$, when $\mathbf{P}(x) \ne \mathbf{P}'(x)$ 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 $wt(\mathbf{P})$:

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

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

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

Suppose $\mathbf{P}'' = p''_0 \dots p''_n$. Since $\mathbf{P}''(x) = 1$, i.e. path $\mathbf{P}''$ contains point x. We know $p''_{|x|_*} = p''_{|x|_*-1} + (a_{|x|_*}, 0)$ 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,

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

From Lemma 8,

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

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

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

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

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

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

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

Proof of Proposition 3 Pick a large integer h_0 such that $\frac{1}{2h_0+1} < \delta$. 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 by Lemma 3 $\mu_{i,j} = \mu(i, \dots, j) = O(\frac{1}{(j-i+1)^{3/2}})$, thus $\rho_j(A^{(1)}) \le \sum_{i=1}^{j} O(\frac{1}{(j-i+1)^{3/2}}) = O(1)$ $(\forall j = 1, \dots, m)$.

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

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

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

Since $d_k > 1 + \frac{1}{2h_0+1}$, 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 $1 \le j \le s$, $cs^{h_0} < b_j \le 2cs^{h_0}$. Construct

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

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

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

We leave the proof of Lemma 9 to Appendix.

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

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

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

$$N(A^{(k+1)}) = t\left(N(A^{(k)}) + \sum_{j=1}^{s} b_j\right) \le t(O(m_k^{d_k}) + s \cdot 2cs^{h_0}) = O\big(m_k^{\frac{(2h_0+\frac{3}{2})d_k}{h_0+1}-1}\big).$$

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,

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

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 that $A^{(k+1)}$ 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 $0 < r \le m_k + s$. There are two cases, either j is in $A^{(k)}$ part or j is in the B part.

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

$$\rho_j(A^{(k+1)}) = \sum_{i \le j-r-s} \mu_{i,j}(A^{(k+1)}) + \sum_{i=j-r-s+1}^{j-r} \mu_{i,j}(A^{(k+1)})$$

$$+\sum_{i=j-r+1}^{j}\mu_{i,j}(A^{(k+1)})$$

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

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

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

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

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

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

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

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

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

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

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

$$\rho_j(A^{(k+1)})=\sum_{i\le j-m_k-s}\mu_{i,j}(A^{(k+1)})+\sum_{i=j-m_k-s+1}^{j-r}\mu_{i,j}(A^{(k+1)})$$

$$+\sum_{i=j-r+1}^{j-r_1}\mu_{i,j}(A^{(k+1)})+\sum_{i=j-r_1+1}^{j}\mu_{i,j}(A^{(k+1)})$$

$$=\sum_{i\le j-m_k-s}\mu_{i,j}(A^{(k+1)})+\sum_{i=r_1+1}^{s}\mu(b_i,\dots,b_s,A^{(k)},b_1,\dots,b_{r_1})$$

$$+\sum_{i=1}^{m_k}\mu_{i,m_k+r_1}(A^{(k)},b_1,\dots,b_{r_1})+\sum_{i=1}^{r_1}\mu(b_i,\dots,b_{r_1}).$$

First we use Fact 1 on the third term,

$$\sum_{i=1}^{m_k} \mu_{i,m_k+r_1}(A^{(k)}, b_1, \ldots, b_{r_1}) \le \sum_{i=1}^{m_k} \mu_{i,m_k}(A^{(k)}) = \rho_{m_k}(A^{(k)}) = O(1).$$

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

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

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

$$\sum_{i \le j-m_k-s} \mu_{i,j}(A^{(k+1)}) \le j O(s^{-h_0-\frac{1}{2}}) \le m_{(k+1)} O(s^{-h_0-\frac{1}{2}}) = O(1).$$

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 (9) $d_{k+1} \to 1 + \frac{1}{2h_0+1} < 1 + \delta$, and after constant steps, we can get a sequence A satisfies both conditions. □

6 Proof of Proposition 4

Most part of the proof is the same as of Proposition 2, except we have a 3-d random path, and also we need use $w'(\mathbf{P}, \mathbf{P}', x)$ and $w'(\mathbf{P}', \mathbf{P}, x)$, in order to derive a 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 $\frac{1}{2}$, $k = 1, \ldots, n$. It is clear that

$$\|Y_k\|_1 = \sum_{j=1}^{k} \|\mathbf{v}_j\|_1 \quad (k = 1, \ldots, n),$$

especially Y_n is on the bottom plane of the pyramid $\mathcal{P}_{3,N}$.

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

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

We put the proof of Lemma 10 in Appendix.

Consider all the 2^n paths $\mathbf{P} = p_0 p_1 \cdots p_n \in \mathcal{P}_{3,N}$ 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 precise, if $p_k = p_{k-1} + (x_1, x_2, x_3)$, after p_{k-1} the path first takes 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 $\mathbf{P} = p_0 \ldots p_n$ and $\mathbf{P}' = p'_0 \ldots p'_n$, define $|\mathbf{P} \wedge \mathbf{P}'| = k$ if $p_0 = p'_0, \ldots, p_k = p'_k$ 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

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

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 $wt(x)$:

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

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

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

Combine inequality (10) with (11),

$$wt(\mathbf{P}) \ge \frac{n}{2} - \lambda. \tag{12}$$

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 $\mathbf{P}(x) = 1$, $\mathbf{P}'(x) = 0$. 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 P'' such that $|\mathbf{P} \wedge \mathbf{P}''| = k$, $\mathbf{P}''(x) = 0$ and $p''_n \neq p_n$ by 2^{n-k},

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

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

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

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,

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

From Lemma 10,

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

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

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

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

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

7 Proof of Proposition 5

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 $\|\mathbf{v}_k - \mathbf{v}_{k'}\| \ge 1$ $(k \ne k')$, and also it is easy to check if $j - i \ge 6$, 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 $|\langle \mathbf{v}_k, \mathbf{e}\rangle| \ge 1$, so from Lemma 5

$$\mu\{(i, m+1-i), \dots, (j, m+1-j)\} \le c_1(j-i+1)^{-2} \ (j-i \ge 6).$$

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

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

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

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

Let

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

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 $\{1, \ldots, c_3 s^{h_0}\}$ with size s, here c_3 is a constant. Suppose that $b_1, b_2, \ldots, b_s$ is the B_{h_0}-sequence. Now we append to $V^{(k)}$ 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

$$V^{(k+1)} = \left.\begin{array}{llllll} V^{(k)}, & (3b_1, 3b_2), & (3b_2, 3b_1), & (3b_1, 3b_3), & (3b_3, 3b_1), \ldots, & (3b_s, 3b_{s-1}); \\ \vdots & \vdots & \vdots & & & \vdots \\ V^{(k)}, & (3b_1, 3b_2), & (3b_2, 3b_1), & (3b_1, 3b_3), & (3b_3, 3b_1), \ldots, & (3b_s, 3b_{s-1}). \end{array}\right\} t \text{ times}$$

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

Lemma 11 *Suppose that* $\mathbf{w}_1, \ldots, \mathbf{w}_l$ *is a consecutive subsequence of* W, *then*

$$\mu(\mathbf{w}_1, \ldots, \mathbf{w}_l) \le O(l^{-2}). \tag{18}$$

Lemma 12

$$\mu(W) \le O(|W|^{-h_0}) = O(s^{-2h_0}). \tag{19}$$

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 $\lambda_j(V^{(k+1)})$. Lemma 11 can be proved directly from Lemma 5. The proof of Lemma 12 will use Lemma 6. We leave it in the Appendix.

The total length of the sequence $V^{(k+1)}$ is

$$m_{(k+1)} = t(m_k + |W|) = t(m_k + s(s-1)) = \Theta(tm_k) = \Theta\left(m_k^{\frac{h_0}{h_0+2}d_k}\right).$$

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

$$N(V^{(k+1)}) = t(N(V^{(k)}) + N(W)) = t\left(O(m_k^{d_k}) + \sum_{i \neq j}^{s}(3b_i + 3b_j)\right)$$

$$\begin{aligned}&\le t(O(m_k^{d_k}) + s^2 \cdot 6c_3 s^{h_0}) = t(O(m_k^{d_k}) + 6c_3 m^{d_k})\\&= O(tm_k^{d_k}) = O\big(m_k^{\frac{2h_0+2}{h_0+2}d_k-1}\big).\end{aligned}$$

Therefore

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

which implies

$$\frac{d_{(k+1)} - (1+\frac{2}{h_0})}{d_k - (1+\frac{2}{h_0})} = \frac{1}{d_k}. \tag{20}$$

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

What remained to show is that the sequence $V^{(k+1)}$ satisfies $\lambda_j(V^{(k+1)}) = O(\log m_{k+1})$ for $j = 1, \dots, m_{k+1}$. According to the construction of $V^{(k+1)}$, we can write $j = q(m_k + |W|) + r$ where $1 \le r \le (m_k + |W|)$, $q \in \mathbb{N} \cup \{0\}$. We separate two different cases, $\mathbf{v}_j$ is in the $V^{(k)}$ part or $\mathbf{v}_j$ is in the W part:

Case 1: $1 \le r \le m_k$, i.e. $\mathbf{v}_j$ is in the $V^{(k)}$ part, from the construction of $V^{(k+1)}$, we have

$$\begin{aligned}\lambda_j(V^{(k+1)}) &= \sum_{i \le j-r-|W|} \sqrt{\mu_{i,j}(V^{(k+1)})} + \sum_{i=j-r-|W|+1}^{j-r} \sqrt{\mu_{i,j}(V^{(k+1)})}\\&\quad + \sum_{i=j-r+1}^{j} \sqrt{\mu_{i,j}(V^{(k+1)})}\\&= \sum_{i \le j-r-|W|} \sqrt{\mu_{i,j}(V^{(k+1)})} + \sum_{i=1}^{|W|} \sqrt{\mu_{i,|W|+r}(W, V^{(k)})}\\&\quad + \sum_{i=1}^{r} \sqrt{\mu_{i,r}(V^{(k)})}.\end{aligned}$$

The last additive term is nothing but $\lambda_r(V^{(k)})$ and we already know $\lambda_r(V^{(k)}) = O(\log m_k)$.

By Fact 1

$$\mu_{i,|W|+r}(W, V^{(k)}) \le \mu_{i,|W|}(W) \quad (i = 1, \dots, |W|)$$

and from Lemma 11,

$$\mu_{i,|W|}(W) \le O((|W| - i + 1)^{-2}) \quad (i = 1, \dots, |W|),$$

thus the second additive term

$$\sum_{i=1}^{|W|} \sqrt{\mu_{i,|W|+r}(W, V^{(k)})} \le \sum_{i=1}^{|W|} O((|W| - i + 1)^{-1}) = O(\log|W|) = O(\log m_k).$$

The rest thing is to upper bound the first term $\sum_{i\le j-r-|W|}\sqrt{\mu_{i,j}(V^{(k+1)})}$. For $i=1,\dots,(j-r-|W|)$, by Fact 1

$$\begin{aligned}\mu_{i,j}(V^{(k+1)}) &\le \mu_{j-r-|W|+1,j}(V^{(k+1)}) = \mu_{1,|W|+r}(W,V^{(k)})\\ &\le \mu_{1,|W|}(W,V^{(k)}) = \mu(W),\end{aligned}$$

and from Lemma 12, $\mu(W)\le O(s^{-2h_0})$, so

$$\sum_{i\le j-r-|W|}\sqrt{\mu_{i,j}(V^{(k+1)})} \le (j-r-|W|)O(s^{-h_0}) \le m_{k+1}O(s^{-h_0}) = O(1).$$

Therefore in this case $\lambda_j(V^{(k+1)}) = O(\log m_{k+1})$ $(j=1,\dots,m_{k+1})$.

Case 2: $m_k+1\le r\le m_k+|W|$, i.e. $\mathbf{v}_j$ is in W part. Let $r_1 = r-m_k$,

$$\begin{aligned}\lambda_j(V^{(k+1)}) = &\sum_{i\le j-m_k-|W|}\sqrt{\mu_{i,j}(V^{(k+1)})} + \sum_{i=j-m_k-|W|+1}^{j-r}\sqrt{\mu_{i,j}(V^{(k+1)})}\\ &+\sum_{i=j-r+1}^{j-r_1}\sqrt{\mu_{i,j}(V^{(k+1)})} + \sum_{i=j-r_1+1}^{j}\sqrt{\mu_{i,j}(V^{(k+1)})}\\ = &\sum_{i\le j-m_k-|W|}\sqrt{\mu_{i,j}(V^{(k+1)})} + \sum_{i=r_1+1}^{|W|}\sqrt{\mu_{i,|W|+m_k+r_1}(W,V^{(k)},W)}\\ &+\sum_{i=1}^{m_k}\sqrt{\mu_{i,m_k+r_1}(V^{(k)},W)} + \sum_{i=1}^{r_1}\sqrt{\mu_{i,r_1}(W)}.\end{aligned}$$

First we use Fact 1 on the third term,

$$\sum_{i=1}^{m_k}\sqrt{\mu_{i,m_k+r_1}(V^{(k)},W)} \le \sum_{i=1}^{m_k}\sqrt{\mu_{i,m_k}(V^{(k)})} = \lambda_{m_k}(V^{(k)}) = O(\log m_k).$$

Using Fact 1 and Lemma 11 on the second and fourth terms, we have

$$\begin{aligned}\sum_{i=r_1+1}^{|W|}\sqrt{\mu_{i,|W|+m_k+r_1}(W,V^{(k)},W)} &\le \sum_{i=r_1+1}^{|W|}\sqrt{\mu_{i,|W|}(W)}\\ &\le \sum_{i=r_1+1}^{|W|}O((|W|-i+1)^{-1})\\ &= O(\log|W|) = O(\log m_k),\end{aligned}$$

$$\sum_{i=1}^{r_1}\sqrt{\mu_{i,r_1}(W)} \le \sum_{i=1}^{r_1}O((r_1-i+1)^{-1}) = O(\log|W|) = O(\log m_k).$$

For the first term, since $i \leq j - |V^{(k)}| - |W|$, $\mu_{i,j}(V^{(k+1)}) \leq \mu(W) = O(s^{-2h_0})$. Therefore

$$\sum_{i \leq j - |V^{(k)}| - |W|} \sqrt{\mu_{i,j}(V^{(k+1)})} \leq m_{k+1} O(s^{-h_0}) = O(1).$$

Combining the two cases we conclude that $\lambda_j(V^{(k+1)}) = O(\log m_{k+1})$ $(j = 1, \ldots, m_{k+1})$.

From (20) we know $d_k \to 1 + \frac{2}{h_0} < 1 + \delta$ and after constant steps, we will obtain a vector sequence V which satisfies the conditions in Proposition 5.

Appendix

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 $M < b_j \leq 2M$ $(j = 1, \ldots, s)$. The inequality we need to prove is

$$\Pr(X_1 + \cdots + X_s = y) \leq O\left(\frac{1}{s^{h_0}\sqrt{s}}\right). \tag{21}$$

We prove it by the following two steps:

$$\Pr(y - 4h_0 M \leq X_1 + \cdots + X_s \leq y + 4h_0 M) \leq O\left(\frac{1}{\sqrt{s}}\right), \tag{22}$$

and

$$\Pr(X_1 + \ldots + X_s = y) \leq O\left(\frac{1}{s^{h_0}}\right) \Pr(y - 4h_0 M \leq X_1 + \cdots + X_s \leq y + 4h_0 M). \tag{23}$$

Proof of inequality (22) 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 [8] we have

$$\left|\Pr\left(\frac{X_1 + \cdots + X_s}{\sqrt{\Sigma_2}} < y\right) - \Phi(y)\right| \leq c\frac{\Sigma_3}{\Sigma_2^{3/2}} = O\left(\frac{1}{\sqrt{s}}\right). \tag{24}$$

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 inequality (24) and adding up the two inequalities, we get

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

here c_1 is a constant to be fixed later. Thus

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

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

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

Proof of inequality (23) For any h_0-element subset $\{i_1, \ldots, i_{h_0}\} \subset \{1, \ldots, s\}$, we have

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

Therefore

$$\begin{aligned}
&\Pr\left(\sum_{j=1}^{s} X_j = y\right) \\
&\quad \le \frac{1}{\binom{s}{h_0}} \sum_{i_1<\cdots<i_{h_0}} \left[\sum_{\epsilon_1,\ldots,\epsilon_{h_0}\in\{\pm 1\}} \Pr\left(\sum_{j=1}^{s} X_j = y - 2\sum_{j=1}^{h_0}\epsilon_j b_{i_j}\right)\right] \\
&\quad \le O\left(\frac{1}{s^{h_0}}\right) \sum_{\epsilon_1,\ldots,\epsilon_{h_0}\in\{\pm 1\}} \left[\sum_{i_1<\cdots<i_{h_0}} \Pr\left(\sum_{j=1}^{s} X_j = y - 2\sum_{j=1}^{h_0}\epsilon_j b_{i_j}\right)\right]. \quad (25)
\end{aligned}$$

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

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

are distinct, otherwise there must be two h_0-subset with the same sum, which contradicts the property of B_{h_0}-sequence. Therefore $y - 2\sum_{j=1}^{h_0} \epsilon_j b_{i_j}$ are all distinct. But we know $M < b_j \le 2M$, so

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

Thus

$$\sum_{i_1<\cdots<i_{h_0}} \Pr\left(\sum_{j=1}^{s} X_j = y - 2\sum_{j=1}^{h_0}\epsilon_j b_{i_j}\right) \le \Pr\left(y - 4h_0 M \le \sum_{j=1}^{s} X_j \le y + 4h_0 M\right). \quad (26)$$

Combine (25), (26)

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

□

Proof of Lemma 10 Define $\epsilon_{i+1}, \ldots, \epsilon_j$ in the same way of Lemma 8. Then we have

$$Y_k = Y_{k-1} + \frac{\epsilon_k + 1}{2}(\mathbf{v}_k, 0) + \frac{1 - \epsilon_k}{2}(0, 0, \|\mathbf{v}_k\|_1).$$

Suppose $\mathbf{y} = (y_1, y_2, y_3)$, then

$$\begin{aligned}
&\Pr(Y_j - Y_i = \mathbf{y})\\
&\quad = \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\left(\frac{\epsilon_k+1}{2}(\mathbf{v}_k, 0) + \frac{1-\epsilon_k}{2}(0, 0, \|\mathbf{v}_k\|_1)\right) = (y_1, y_2, y_3)\right)\\
&\quad = \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\frac{\epsilon_k+1}{2}\mathbf{v}_k = (y_1, y_2), \sum_{k=i+1}^{j}\frac{1-\epsilon_k}{2}\|\mathbf{v}_k\|_1 = y_3\right)\\
&\quad \le \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\frac{\epsilon_k+1}{2}\mathbf{v}_k = (y_1, y_2)\right)\\
&\quad = \Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\epsilon_k\mathbf{v}_k = (2y_1, 2y_2) - \sum_{k=i+1}^{j}\mathbf{v}_k\right)\\
&\quad \le \max_{\mathbf{y}'\in\mathbb{Z}^2}\Pr_{\epsilon_{i+1},\ldots,\epsilon_j}\left(\sum_{k=i+1}^{j}\epsilon_k\mathbf{v}_k = \mathbf{y}'\right) = \mu_{i+1,j}.
\end{aligned}$$

□

Proof of Lemma 12 We use Lemma 6. In addition to the proof of Lemma 11, we only need to prove that the set $\{\mathbf{b} = \mathbf{w}_{i_1} + \cdots + \mathbf{w}_{i_{h_0}} : \mathbf{w}_{i_k} \in W\}$ contains enough different vectors.

Since $b_1, \ldots, b_s$ is a B_{h_0}-sequence, so does $3b_1, \ldots, 3b_s$. Thus set $\{3b_{i_1} + \cdots + 3b_{i_{h_0}} : i_1 < \cdots < i_{h_0}\}$ contains at least $\binom{s}{h_0}$ different elements. Since $W = \{(3b_i, 3b_j) : i \neq j\}$, all the vectors of the form $(3b_{i_1} + \cdots + 3b_{i_{h_0}}, 3b_{j_1} + \cdots + 3b_{j_{h_0}})$,$(i_1 < \cdots < i_{h_0}$,$j_1 < \cdots < j_{h_0})$ are contained in the set $\{\mathbf{w}_{i_1} + \cdots + \mathbf{w}_{i_{h_0}} : \mathbf{w}_{i_k} \in W\}$, there are at least $\binom{s}{h_0}^2 \ge (\frac{s}{h_0})^{2h_0} \ge \delta(h_0)|W|^{h_0}$ vectors of this type, so we can use Lemma 6, $\mu(W) \le c(h_0)|W|^{-h_0} = \tilde{c}(h_0)s^{-2h_0}$. □

References

1. Aaronson, S.: Lower bounds for local search by quantum arguments. SIAM J. Comput. **35**(4), 804–824 (2006)
2. Aldous, D.: Minimization algorithms and random walk on the d-Cube. Ann. Probab. **11**(2), 403–413 (1983)
3. Ambainis, A.: Quantum lower bounds by quantum arguments. J. Comput. Syst. Sci. **64**(4), 750–767 (2002)
4. Ambainis, A.: Polynomial degree vs. quantum query complexity. J. Comput. Syst. Sci. **72**(2), 220–238 (2006)
5. Bennett, C., Bernstein, E., Brassard, G., Vazirani, U.: Strengths and weaknesses of quantum computation. SIAM J. Comput. **26**(5), 1510–1523 (1997)
6. Bose, R.C., Chowla, S.: Theorems in the additive theory of numbers. Comment. Math. Helv. **37**(1), 141–147 (1962)
7. Chen, X., Deng, X.: On algorithms for discrete and approximate brouwer fixed points. In: Proc. of the 37th Annual ACM Symposium on Theory of Computing, pp. 323–330. Assoc. Comput. Mach., New York (2005)

8. Esseen, C.G.: Fourier analysis of distribution functions. Acta Math. **77**, 1–125 (1945)
9. Friedl, K., Ivanyos, G., Santha, M., Verhoeven, Y.: On the black-box complexity of Sperner's Lemma. In: Proc. of the 15th International Symposium on Fundamentals of Computation Theory, pp. 245–257. Springer, Berlin (2005)
10. Halász, G.: Estimates for the concentration function of combinatorial number theory and probability. Period. Math. Hung. **8**(3–4), 197–211 (1977)
11. Halberstam, H., Roth, K.F.: Sequences. Oxford University Press, Oxford (1966)
12. Johnson, D., Papadimitriou, C., Yannakakis, M.: How easy is local search? J. Comput. Syst. Sci. **37**(1), 79–100 (1988)
13. Llewellyn, D., Tovey, C., Trick, M.: Local optimization on graphs. Discrete Appl. Math. **23**, 157–178 (1989). Erratum: **46**, 93–94 (1993)
14. Santha, M., Szegedy, M.: Quantum and classical query complexities of local search are polynomially related. In: Proc. of the 36th Annual ACM Symposium on Theory of Computing, pp. 494–501. Assoc. Comput. Mach., New York (2004)
15. Sárközy, A., Szemerédi, E.: Über ein Problem von Erdös und Moser. Acta Arith. **11**, 205–208 (1965)
16. Verhoeven, Y.: Enhanced algorithms for local search. Inf. Process. Lett. **97**, 171–176 (2006)
17. Zhang, S.: On the power of Ambainis's lower bounds. Theor. Comput. Sci. **339**, 241–256 (2005)
18. Zhang, S.: New upper and lower bounds for randomized and quantum Local Search. In: Proc. of the 38th ACM Symposium on Theory of Computing, pp. 634–643. Assoc. Comput. Mach., New York (2006)