Algorithmica (2010) 56: 364–382
DOI 10.1007/s00453-009-9289-0

Quantum Separation of Local Search and Fixed Point Computation

Xi Chen · Xiaoming Sun · Shang-Hua Teng

Received: 11 August 2008 / Accepted: 29 January 2009 / Published online: 25 February 2009

Abstract We give a lower bound of $\Omega(n^{(d-1)/2})$ on the quantum query complexity for finding a fixed point of a discrete Brouwer function over grid $[n]^d$. Our lower bound is nearly tight, as Grover Search can be used to find a fixed point with $O(n^{d/2})$ quantum queries. Our result establishes a nearly tight bound for the computation of d-dimensional approximate Brouwer fixed points defined by Scarf and by Hirsch, Papadimitriou, and Vavasis. It can be extended to the quantum model for Sperner's Lemma in any dimensions: The quantum query complexity of finding a panchromatic cell in a Sperner coloring of a triangulation of a d-dimensional simplex with n^d cells is $\Omega(n^{(d-1)/2})$. For $d = 2$, this result improves the bound of $\Omega(n^{1/4})$ of Friedl, Ivanyos, Santha, and Verhoeven.

More significantly, our result provides a quantum separation of local search and fixed point computation over $[n]^d$, for $d \geq 4$. Aaronson's local search algorithm for grid $[n]^d$, using Aldous Sampling and Grover Search, makes $O(n^{d/3})$ quantum queries. Thus, the quantum query model over $[n]^d$ for $d \geq 4$ strictly separates these two fundamental search problems.

X. Chen is supported by NSF Grant DMS-0635607.
X. Sun is supported by the National Natural Science Foundation of China Grant (60553001, 60603005 and 60621062), and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.
S.-H. Teng is supported by NSF grants CCR-0635102 and ITR CCR-0325630.

X. Chen (✉)
Institute for Advanced Study, Princeton, USA
e-mail: csxichen@gmail.com

X. Sun
Tsinghua University, Beijing, China
e-mail: xiaomings@tsinghua.edu.cn

S.-H. Teng
Boston University, Boston, USA
e-mail: steng@cs.bu.edu

Keywords Quantum query complexity · Fixed-point computation · Local search · Sperner's lemma · Quantum adversary method

1 Introduction

In this paper, we give a nearly tight bound on the quantum query complexity of fixed point computation over the grid $[n]^d = \{1, 2, \dots, n\}^d$. Our result demonstrates a strict separation of fixed point computation and local search in the quantum query model, resolving an open question posed in [1]. We also solve the problem left open in [1] about both the randomized and quantum query complexity of discrete fixed point computation over the hypercube $\{0, 1\}^n$.

1.1 Motivation

In various applications, we often need not only to decide whether solutions satisfying certain properties exist, but also to find a desirable solution. This family of computational problems is usually referred to as the *search problem*.

Three fundamental types of search problems are global optimization, local search, and fixed point computation (FPC). In a global optimization problem, we are given an objective function g over a domain D and are asked to find a solution $\mathbf{x} \in D$ such that $g(\mathbf{x}) \le g(\mathbf{y})$, for all $\mathbf{y} \in D$. In local search, we are given a function h over a domain D and a neighborhood function $N : D \to 2^D$. We are asked to find a solution $\mathbf{x} \in D$ such that $h(\mathbf{x}) \le h(\mathbf{y})$, for all $\mathbf{y} \in N(\mathbf{x})$. In practice, we also consider the approximation version of these problems.

FPC arises in geometry, topology, game theory, and mathematical economics. Brouwer proved that every continuous map f from a 3D simplex S to itself has a fixed point, i.e., $\mathbf{x} \in S$ such that $f(\mathbf{x}) = \mathbf{x}$. Applying Brouwer's theorem, Nash established that every finite, n-player game has an equilibrium point [2]. Arrow and Debreu [3] then extended the equilibrium theory to exchange markets that satisfy some very general conditions.

Mathematically, FPC and optimization are somewhat related. For example, one can reduce FPC to root finding: $\mathbf{x} \in S$ is a fixed point of f if $f(\mathbf{x}) - \mathbf{x} = 0$, or $\|f(\mathbf{x}) - \mathbf{x}\| = 0$; Every global optimum of $g(\mathbf{x}) = \|f(\mathbf{x}) - \mathbf{x}\|$ is a fixed point of f. One can also view a local optimum of h as a fixed point: For every $\mathbf{x} \in D$, let $f_h(\mathbf{x})$ be a point in $N(\mathbf{x})$ that minimizes $h(\mathbf{x})$; Then every fixed point $\mathbf{x}$ of f_h is a local optimum of h. Of course, this reduction from local search to FPC is less formal than the reduction from FPC to global optimization because the function f_h may not satisfy the "continuity" conditions required by the Fixed Point Theorems. The following are two fundamental complexity questions about these search problems:

- Is global optimization strictly harder than fixed point computation?
- Is a fixed point harder to find than a local optimum?

To address these questions in the framework traditionally considered in Theoretical Computer Science, one may want to compare global optimization, local search, and FPC over discrete domains. For optimization problems, it is somewhat easier to define the discrete or combinatorial analog of continuous optimization, by considering discrete input domains, such as the hypercube $\{0, 1\}^n$ or grid $[n]^d$: Given a function h over $D = \{0, 1\}^n$ or $[n]^d$, find a global or local optimum of h. In local search one may consider $N(\mathbf{x})$ to be the direct neighbors of $\mathbf{x}$ in $\{0, 1\}^n$ or $[n]^d$.

The discrete FPC is less straightforward, and some inaccuracy must be introduced to ensure the existence of a solution with finite description [4–8]. One idea is to consider approximate fixed points as suggested by Scarf [4] over a finite discretization of the convex domain, where a vertex $\mathbf{x}$ in the discretization is an approximate fixed point of a continuous map f if $\|f(\mathbf{x}) - \mathbf{x}\| \leq \epsilon$ for a given $\epsilon > 0$. Another idea is to use the direction-preserving functions (see Sect. 2) as introduced by Iimura, Murota, and Tamura [9] over $[n]^d$. One can also use Sperner's definition of discrete fixed points. Sperner's famous lemma states: Suppose that Ω is a d-dimensional simplex with vertices $v_1, v_2, \ldots, v_{d+1}$, and that $\mathcal{S}$ is a simplicial decomposition of Ω. Suppose Π assigns to each vertex of $\mathcal{S}$ a color from $\{1, 2, \ldots, d+1\}$ such that, for every vertex v of $\mathcal{S}$, $\Pi(v) \neq i$ if the i^{th} component of the barycentric coordinates of v (that is, the convex combination of $v_1, \ldots, v_{d+1}$ to express v) is 0. Sperner's Lemma asserts that there must exist a cell in $\mathcal{S}$ that contains all the $d+1$ colors. This fully-colored simplex cell is often referred to as a *Sperner simplex* of $(\mathcal{S}, \Pi)$. Now consider a Brouwer map f with Lipschitz constant L over the simplex Ω. Suppose further that the diameter of each simplex cell in $\mathcal{S}$ is at most ϵ/L. Then, one can define a color assignment Π_f such that each fully-colored simplex in $(\mathcal{S}, \Pi_f)$ must have a vertex $\mathbf{v}$ satisfying $\|f(\mathbf{v}) - \mathbf{v}\| \leq \Theta(\epsilon)$. Thus, a fully-colored cell of $(\mathcal{S}, \Pi_f)$ can be viewed as an approximate, discrete fixed point of f. The Hirsch, Papadimitriou, and Vavasis model [7] extends Sperner's Lemma from the simplex to the hypergrid $[n]^d$.

Note that if the function h for optimization or the map f for FPC is given succinctly by a boolean circuit, then these three problems are search problems in complexity classes FNP, PLS, and PPAD, respectively. Other than PPAD $\subseteq$ FNP and PLS $\subseteq$ FNP, the relations between these classes remain unclear.

In a recent paper, Chen and Teng demonstrated that the randomized query model over $[n]^d$ strictly separates these three search problems [1]:

Global optimization is harder than fixed-point computation,
and fixed-point computation is harder than local search.

In particular, they proved that, given a black-box, discrete Brouwer function f from $[n]^d$ to $[n]^d$, the randomized query complexity of finding a fixed point $\mathbf{x}$ is $\Theta(n^{d-1})$. The separation statement above then follows from two earlier results: A folklore theorem states that the randomized query complexity for finding a global optimum of a black-box function h from $[n]^d$ to $\mathbb{R}$ is $\Theta(n^d)$; Aldous [10] showed that the randomized query complexity of finding a local optimum of a black-box function h from $[n]^d$ to $\mathbb{R}$ is $O(n^{d/2})$.

They further conjectured that FPC is also strictly harder than local search in the quantum query model over $[n]^d$. In particular, they conjectured that the quantum query complexity of FPC over $[n]^d$ is $\Theta(n^{d/2})$. If this conjecture is true, then just like in its randomization counterpart, FPC is harder than local search under the quantum query model in two or higher dimensions.

1.2 Our Contributions

We prove a nearly tight bound of $\Omega(n^{(d-1)/2})$ on the quantum query complexity of FPC over $[n]^d$—Grover Search solves FPC with $O(n^{d/2})$ quantum queries. Our result also gives a nearly tight bound for the computation of d-dimensional approximate Brouwer fixed points as defined by Scarf and by Hirsch, Papadimitriou, and Vavasis [7]. It can be extended to the quantum model for Sperner's Lemma in any dimensions: the quantum query complexity of finding a panchromatic cell in a Sperner coloring of a uniform triangulation of a d-dimensional simplex with n^d cells is $\Omega(n^{(d-1)/2})$. For $d = 2$, this result improves the bound of $\Omega(n^{1/4})$ obtained by Friedl, Ivanyos, Santha, and Verhoeven [11].

Our result provides a quantum separation between local search and FPC over $[n]^d$, for $d \geq 4$. Aaronson's local search algorithm over $[n]^d$ makes $O(n^{d/3})$ quantum queries [12]. Thus the quantum query model over $[n]^d$ strictly separates these two fundamental search problems when $d \geq 4$.

We use the quantum adversary argument of Ambainis [13, 14] in the lower bound proof. We hide a distribution of random, directed paths in the host grid graph (over $[n]^d$) with a known starting vertex, and ask the algorithm to find the ending vertex of the path. This "path-hiding" approach was used in [12, 15, 16] for deriving quantum lower bounds of local search. It was also used in [11] for deriving the $\Omega(n^{1/4})$ lower bound of the two-dimensional Sperner's problem. The main difference between our work and previous works is that the paths used in previous works have some monotonicity properties: there is an increasing (or decreasing) value along the path. Given any two vertices on the path, without querying other vertices one can decide which vertex appears earlier on the path. Such a monotonicity property makes it easier to derive good bound on the collision probability needed for a lower bound on local search, but limits the length of the path, making it impossible to derive tight lower bounds for FPC.

Instead of using "monotone" paths, we improve the path construction technique of Chen and Teng [1] in their randomized query lower bound for FPC, and make it work for the quantum adversary argument. We also find an interesting connection between the two discrete domains—hypergrid $[n]^d$ and hypercube $\{0, 1\}^n$, which allows us to resolve a question left open in [1] on both the randomized and quantum query complexity of FPC over $\{0, 1\}^n$. We show that they are $\Omega(2^{n(1-\epsilon)})$ and $\Omega(2^{n(1-\epsilon)/2})$ respectively, for all $\epsilon > 0$.

It remains open whether the quantum query complexity of FPC over $[n]^d$ is indeed $\Theta(n^{d/2})$ or a better algorithm with query complexity $\Theta(n^{(d-1)/2})$ exists.

1.3 Related Work

In [7], Hirsch *et al.* introduced the first query model for discrete FPC over $[n]^d$. They proved a tight $\Theta(n)$ deterministic bound for $[n]^2$, and an $\Omega(n^{d-2})$ deterministic lower bound in general. Chen and Deng [17] improved their bound to $\Theta(n^{d-1})$. Friedl, Ivanyos, Santha, and Verhoeven considered the 2-dimensional Sperner's problem [11]. They proved an $\Omega(n^{1/2})$ bound for its randomized query complexity and an $\Omega(n^{1/4})$ bound for its quantum query complexity.

Aaronson [12] was the first to introduce the quantum query complexity of local search over $[n]^d$ (and also $\{0, 1\}^n$). He gave an upper bound $O(n^{d/3})$ and a lower bound $\Omega(n^{d/4-1/2}/\sqrt{\log n})$. Santha and Szegedy [18] proved a lower bound $\Omega(n^{1/4})$ for $d = 2$. Zhang [15] then proved a lower bound of $\Omega(n^{d/3})$ which is tight up to a log factor, for $d \geq 5$. In the same paper, he obtained a nearly tight quantum bound for $\{0,1\}^n$. For $d = 2$ and $d = 3$, Sun and Yao [16] eventually gave an almost optimal lower bound.

Following the work of [12, 15, 16], we use the quantum adversary method of Ambainis to establish our lower bound for FPC. There have been several extensions of Ambainis's method, including the weighted adversary method of Ambainis [13] and Zhang [14], the spectral method of Barnum, Saks and Szegedy [19], and the Kolmogorov complexity method of Laplante and Magniez [20]. It was shown by Spalek and Szegedy that the power of all these methods is equivalent [21]. Recently a new adversary method with negative weights was proposed by Hoyer, Lee, and Spalek [22].

We use the weighted adversary method. It might be possible that some new adversary method can be used to obtain the tight $\Omega(n^{d/2})$ lower bound.

2 Definition of Problems

We start with some notation. We let $\mathbb{Z}_n^d$ denote set $\{1,2,\ldots,n\}^d$, and G_n^d denote the natural *directed* graph over $\mathbb{Z}_n^d$: edge $(\mathbf{u},\mathbf{v}) \in G_n^d$ if there exists $i \in [d]$ such that $|u_i - v_i| = 1$ and $u_j = v_j$ for all other $j \in [d]$. We let H^n denote the following *directed* graph over hypercube $\{0,1\}^n$: edge $(\mathbf{u},\mathbf{v}) \in H^n$ if there exists $i \in [n]$ such that $|u_i - v_i| = 1$ and $u_j = v_j$ for all other $j \in [n]$.

We use K_n to denote the complete *directed* graph of size n: the vertex set of K_n is $\{1,2,\ldots,n\}$, and (i,j) is an edge in K_n for all $1 \leq i \neq j \leq n$, . We use K_n^d to denote the *Cartesian product* of d complete graphs: $K_n^d = K_n \Box K_n \Box \cdots \Box K_n$. More exactly, the vertex set of K_n^d is $\{1,2,\ldots,n\}^d$; $(\mathbf{u},\mathbf{v})$ is a directed edge of K_n^d if there exists $i \in [d]$ such that $u_i \neq v_i$ and $u_j = v_j$ for all other $j \in [d]$.

Let G be a directed graph, and P be a *simple* directed path in G. We say $P = \mathbf{v}^1\mathbf{v}^2\cdots\mathbf{v}^k$, where $k \geq 1$, is simple if for all $1 \leq i \neq j \leq k$, $\mathbf{v}^i \neq \mathbf{v}^j$. Then P naturally induces a map $\mathcal{F}_P$ from the edge set of G to $\{0,1\}$: for all $(\mathbf{u},\mathbf{v}) \in G$, $\mathcal{F}_P(\mathbf{u},\mathbf{v}) = 1$ if $(\mathbf{u},\mathbf{v}) \in P$; and $\mathcal{F}_P(\mathbf{u},\mathbf{v}) = 0$, otherwise. We let $\textsc{End}(P)$ denote the ending vertex of P. Finally, we let $\mathbb{E}^d = \{\pm\mathbf{e}_1, \pm\mathbf{e}_2, \ldots, \pm\mathbf{e}_d\}$ denote the set of *principle unit-vectors* in d-dimensions. Let $\|\cdot\|$ denote $\|\cdot\|_\infty$.

2.1 Discrete Brouwer Fixed-Points

A function $f: \mathbb{Z}_n^d \to \{\mathbf{0}\} \cup \mathbb{E}^d$ is *bounded* if $f(\mathbf{x}) + \mathbf{x} \in \mathbb{Z}_n^d$ for all $\mathbf{x} \in \mathbb{Z}_n^d$; $\mathbf{v} \in \mathbb{Z}_n^d$ is a *zero point* of f if $f(\mathbf{v}) = \mathbf{0}$. Clearly, if $F(\mathbf{x}) = \mathbf{x} + f(\mathbf{x})$, then $\mathbf{v}$ is a fixed point of F if and only if $\mathbf{v}$ is a zero point of f.

Definition 1 A function f from set $S \subset \mathbb{Z}^d$ to $\mathbf{0}\} \cup \mathbb{E}^d$ is *direction-preserving* if $\|f(\mathbf{u}) - f(\mathbf{v})\| \leq 1$ for all pairs $\mathbf{u},\mathbf{v} \in S$ such that $\|\mathbf{u} - \mathbf{v}\| \leq 1$.

Following the discrete fixed-point theorem of [9], we have: for every function $f: \mathbb{Z}_n^d \to \{\mathbf{0}\} \cup \mathbb{E}^d$, if f is both bounded and direction-preserving, then it has at least one zero point. We refer to a bounded and direction-preserving function f over $\mathbb{Z}_n^d$

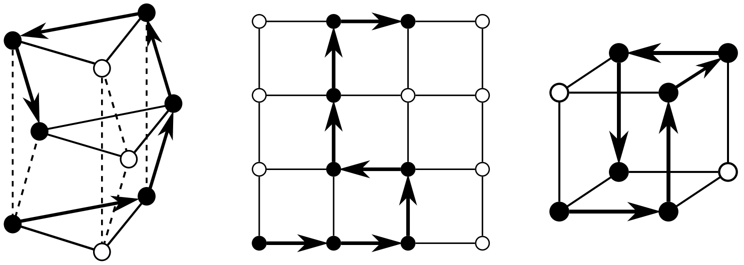

Fig. 1 END-OF-PATH problems over K_3^2, G_4^2, and H^3, respectively

as a *Brouwer function* over $\mathbb{Z}_n^d$. In the query model, one can only access f by asking queries of the form: "What is $f(\mathbf{v})$?" for a point $\mathbf{v} \in \mathbb{Z}_n^d$.

The problem ZP^d that we will study is: *Given a* Brouwer *function* $f : \mathbb{Z}_n^d \to \{\mathbf{0}\} \cup \mathbb{E}^d$ *in the query model, find a zero point of* f. We use $\mathsf{QQ}_{\mathsf{ZP}}^d(n)$ to denote the *quantum query complexity* of problem ZP^d. A description of the quantum query model can be found in [23] and [24]. The main result of the paper is

Theorem 1 (Main) *For all $d \geq 2$ and large enough n,* $\mathsf{QQ}_{\mathsf{ZP}}^d(n) = \Omega(n^{\frac{d-1}{2}})$.

2.2 The End-of-Path Problems over Graphs K_n^d, G_n^d and H^n

To prove Theorem 1, we need to introduce the following d-dimensional problem KP^d (the END-OF-PATH problem over K_n^d): Its input is a binary string of length $|K_n^d|$ (that is, the number of edges in K_n^d), which encodes the map $\mathcal{F}_P$ of a *simple directed* path P in K_n^d; P is known to start at $\mathbf{1} = (1, \ldots, 1) \in K_n^d$; and we need to find its ending vertex $\text{END}(P)$. We use $\mathsf{QQ}_{\mathsf{KP}}^d(n)$ to denote the quantum query complexity of problem KP^d.

Similarly, for $d \geq 2$, we define the END-OF-PATH problem GP^d over G_n^d, and use $\mathsf{QQ}_{\mathsf{GP}}^d(n)$ to denote its quantum query complexity. The following reduction from GP^d to ZP^d was given in [1]: From any input string $\mathcal{F}_P$ of GP^d, where P is a simple path in G_n^d (starting at $\mathbf{1}$), one can construct a Brouwer function f over $\mathbb{Z}_{24n+7}^d$ such that:

1. Function f has exactly one zero point $\mathbf{v}^*$. Once it is found, the ending vertex of P can be located immediately;
2. For any $\mathbf{v} \in \mathbb{Z}_{24n+7}^d$, $f(\mathbf{v})$ only depends on (at most) $4d$ bits of $\mathcal{F}_P$.

Using Lemma 1 of [18], we have

Lemma 1 *For all $d \geq 2$,* $\mathsf{QQ}_{\mathsf{GP}}^d(n) \leq O(d) \cdot \mathsf{QQ}_{\mathsf{ZP}}^d(24n+7)$.

To give a lower bound for $\mathsf{QQ}_{\mathsf{GP}}^d(n)$, we reduce KP^d to GP^{d+1}, and prove the following lemma. The proof can be found in Appendix B.

Lemma 2 *For all $d \geq 1$,* $\mathsf{QQ}_{\mathsf{KP}}^d(n) \leq O(d\sqrt{dn}) \cdot \mathsf{QQ}_{\mathsf{GP}}^{d+1}(4dn+1)$.

Finally, in Sect. 3, we prove an almost-tight lower bound for KP^d.

Theorem 2 *For all $d \geq 1$ and large enough n, $\mathsf{QQ}^d_{\mathsf{KP}}(2n+3) = \Omega((n/2^{11})^{\frac{d+1}{2}})$.*

As a result, Theorem 1 follows directly from Lemma 1, 2, and Theorem 2.

Besides, as a by-product, our work also implies an almost-tight lower bound for the END-OF-PATH problem HP over H^n: Its input is a binary string of length $|H^n|$ which encodes the map $\mathcal{F}_P$ of a *simple directed* path P in H^n; P is known to start at $\mathbf{0} = (0, 0, \ldots, 0) \in \{0, 1\}^n$ and we need to find $\textsc{End}(P)$. Let $\mathsf{QQ}_{\mathsf{HP}}(n)$ denote its quantum query complexity, then in Appendix A, we show that

Lemma 3 *For all $d \geq 2$ and $n \geq 1$, $\mathsf{QQ}^d_{\mathsf{GP}}(2^n) \leq O(1) \cdot \mathsf{QQ}_{\mathsf{HP}}(dn)$.*

As a corollary of Lemma 2, 3, and Theorem 2, we have

Corollary 1 *For all $\epsilon > 0$ and large enough n, $\mathsf{QQ}_{\mathsf{HP}}(n) = \Omega(2^{n(1-\epsilon)/2})$.*

3 An Almost-Tight Lower Bound for KP^d

Using Grover's search [25], we get the following upper bound for $\mathsf{QQ}^d_{\mathsf{KP}}$:

Lemma 4 *For all $d \geq 1$, $\mathsf{QQ}^d_{\mathsf{KP}}(n) = O(\sqrt{d \cdot n^{d+1}})$.*

To prove a matching lower bound, we need the following theorem from [13, 14]:

Theorem 3 *Let $f : S \to \{0, 1\}^{n_1}$ be a partial function, where $S \subset \{0, 1\}^{n_2}$. Let $w : S \times S \to \{0, 1\}$ be a map satisfying the following condition: $w(\mathbf{x}, \mathbf{y}) = w(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in S$ and $w(\mathbf{x}, \mathbf{y}) = 0$ whenever $f(\mathbf{x}) = f(\mathbf{y})$.*

Then the quantum query complexity $\mathsf{QQ}(f)$ of f satisfies

$$\mathsf{QQ}(f) = \Omega\left(\min_{\substack{\mathbf{x},\mathbf{y},i: x_i \neq y_i \\ w(\mathbf{x},\mathbf{y})=1}} \sqrt{\frac{1}{\theta(\mathbf{x}, i)\theta(\mathbf{y}, i)}}\right),$$

where

$$\theta(\mathbf{x}, i) = \frac{\sum_{\mathbf{y}' \in S, y'_i \neq x_i} w(\mathbf{x}, \mathbf{y}')}{\sum_{\mathbf{y}' \in S} w(\mathbf{x}, \mathbf{y}')}$$

for all $\mathbf{x} \in S$ and $i \in [n_2]$.

The sketch of the proof is as follows. First, we build a set of *hard paths* $\mathcal{S}^d_m$ in graph K^d_{2m+3} for $d \geq 1$ and $m \geq 2$. These paths induce a collection of binary strings $\{\mathcal{F}_P, P \in \mathcal{S}^d_m\}$ of length $|K^d_{2m+3}|$, which plays the role of S in Theorem 3. Naturally, the f in Theorem 3 maps each string $\mathcal{F}_P$ to $\textsc{End}(P)$. Then, given any small enough $\beta > 0$, we define a relation $R^d_{m,\beta}$ over set $\mathcal{S}^d_m \times \mathcal{S}^d_m$. It induces a relation over $\{\mathcal{F}_P, P \in \mathcal{S}^d_m\} \times \{\mathcal{F}_P, P \in \mathcal{S}^d_m\}$, which satisfies all the conditions for w in Theorem 3. Finally, we analyze θ and use Theorem 3 to obtain a lower bound for $\mathsf{QQ}^d_{\mathsf{KP}}(2m+3)$.

We let $\mathbf{v} = (v_1, \dots, v_d)$ denote a vertex in K_m^d, where $v_i \in [m]$ for all $i \in [d]$. For $d \geq 2$, we let D_d denote the map from $\mathbb{Z}^d$ to $\mathbb{Z}^{d-1}$: $D_d(\mathbf{v}) = (v_1, \dots, v_{d-1})$. For $\mathbf{v} \in \mathbb{Z}^{d-1}$ and $t \in \mathbb{Z}$, we let $(\mathbf{v}, t)$ denote the vertex $\mathbf{u} \in \mathbb{Z}^d$ with $u_d = t$ and $u_i = v_i$ for all $i \in [d-1]$.

3.1 Construction of the Hard Paths

For all $d \geq 1$ and $m \geq 2$, we now construct, inductively, a set of paths $\mathcal{S}_m^d$ over K_{2m+3}^d. All these paths start with $\mathbf{1} = (1, \dots, 1) \in \mathbb{Z}^d$.

Definition 2 (m-connector) Every permutation $\pi : [m+1] \to [m+1]$ with $\pi(1) = 1$ defines a sequence of $2m+3$ integers: $C = 1 \circ 2\pi(1) \circ (2\pi(1)+1) \circ 2\pi(2) \circ (2\pi(2)+1) \circ \cdots \circ 2\pi(m+1) \circ (2\pi(m+1)+1)$. Such a sequence C is called an *m-connector*. For each $i \in [m+1]$, we also use $C(i)$ to denote $2\pi(i)$, so $C = 1 \circ C(1) \circ (C(1)+1) \circ \cdots \circ C(m+1) \circ (C(m+1)+1)$.

We use $\mathcal{C}_m$ to denote the set of all m-connectors.

The construction of $\mathcal{S}_m^d$ when $d = 1$ is straightforward: $P \in \mathcal{S}_m^1$ if there is a $C \in \mathcal{C}_m$ such that P has the following edges: $(1, C(1)), (C(1), C(1)+1), (C(1)+1, C(2)) \cdots (C(m+1), C(m+1)+1)$. We also say P is generated by C.

For the case when $d > 1$, we assume $\mathcal{S}_m^{d-1}$ has already been constructed. A path P is in $\mathcal{S}_m^d$ if it can be generated by a $(2m+4)$-tuple $(C, P_1, \dots, P_{2m+3})$, where $C \in \mathcal{C}_m$ and $P_i \in \mathcal{S}_m^{d-1}$. The $2m+3$ paths $P_1, P_2, \dots, P_{2m+3}$ in the tuple must satisfy the following condition: $\textsc{End}(P_1) = \textsc{End}(P_{C(1)})$ and $\textsc{End}(P_{C(i)+1}) = \textsc{End}(P_{C(i+1)})$ for all $i \in [m]$.

Path P is a simple path in graph K_{2m+3}^d containing the following edges:

1. For all $i \in \{1, 3, \dots, 2m+1, 2m+3\}$ and $\mathbf{u}, \mathbf{v} \in K_m^d$ with $u_d = v_d = i$, edge $(\mathbf{u}, \mathbf{v}) \in P$ if and only if $(D_d(\mathbf{u}), D_d(\mathbf{v})) \in P_i$;
2. For all $i \in \{2, 4, \dots, 2m, 2m+2\}$ and vertices $\mathbf{u}, \mathbf{v} \in K_m^d$ with $u_d = v_d = i$, edge $(\mathbf{u}, \mathbf{v}) \in P$ if and only if $(D_d(\mathbf{v}), D_d(\mathbf{u})) \in P_i$;
3. For all $i \in [m+1]$, edge $((1, 1, \dots, 1, C(i)), (1, 1, \dots, 1, C(i)+1)) \in P$;
4. Let $\mathbf{v} = \textsc{End}(P_1)$, then edge $((\mathbf{v}, 1), (\mathbf{v}, C(1))) \in P$;
5. For all $i \in [m]$, let $\mathbf{v} = \textsc{End}(P_{C(i)+1})$, then $((\mathbf{v}, C(i)+1), (\mathbf{v}, C(i+1))) \in P$.

It is easy to see that the set $\mathcal{S}_m^d$ of hard paths constructed here are not "monotone": Let $\mathbf{u}$ and $\mathbf{v}$ be two vertices in K_{2m+3}^d in general positions; Then even if we are told that both $\mathbf{u}$ and $\mathbf{v}$ are on some path $P \in \mathcal{S}_m^d$, we have no idea which one appears earlier on P.

3.2 The Relation $R_{m,\beta}^d$ over $\mathcal{S}_m^d \times \mathcal{S}_m^d$

Let $r \in \mathbb{Z}^+$ be an integer such that $2r+1 \leq m$.

Let C_1 and C_2 be two m-connectors. For integers $k_1 \in [r]$ and $r+1 \leq k_2 \leq m-r$, we say C_1 can be *r-transformed* to C_2 with parameters (k_1, k_2) if: for all $i \in [k_1]$, $C_2(k_2 - k_1 + i) = C_1(m - k_1 + 1 + i)$ and $C_2(m - k_1 + 1 + i) = C_1(k_2 - k_1 + i)$; for all other indices $j \in [m+1]$, $C_2(j) = C_1(j)$.

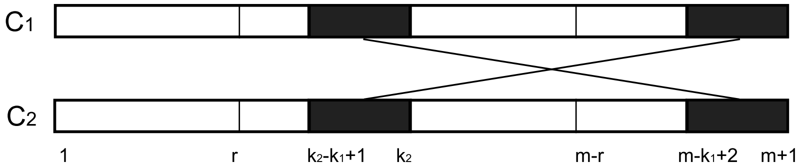

Fig. 2 Connectors C_1 and C_2, where C_1 can be r-transformed to C_2 with (k_1, k_2)

See Fig. 2 for an example. Clearly, if C_1 can be r-transformed to C_2, then C_2 can also be r-transformed to C_1 with the same parameters.

Now given a triple $\tau = (m, d, \beta)$ such that $\beta \in (0, 32^{-d}]$ and $m\beta \in \mathbb{Z}^+$, we inductively construct a symmetric relation $R^d_{m,\beta}$ from $\mathcal{S}^d_m \times \mathcal{S}^d_m$ to $\{0, 1\}$. For convenience, we also denote it by R_τ for short. We will use it as the map w in the adversary argument (see Theorem 3). Before presenting details of the construction, we introduce the following useful notation: Given a path $P \in \mathcal{S}^d_m$ and a vertex $\mathbf{v} \in K^d_{2m+3}$, we let

- $\mathcal{S}_\tau[P] = \{P' \in \mathcal{S}^d_m, R_\tau(P, P') = 1\}$, and $N_\tau[P] = |\mathcal{S}_\tau[P]|$;
- $\mathcal{S}_\tau[P, \mathbf{v}] = \{P' \in \mathcal{S}_\tau[P],\ \textsc{End}(P') = \mathbf{v}\}$, and $N_\tau[P, \mathbf{v}] = |\mathcal{S}_\tau[P, \mathbf{v}]|$;
- $V_\tau[P] = \{\mathbf{v} \in K^d_{2m+3},\ N_\tau[P, \mathbf{v}] > 0\}$.

For the case when $d = 1$, assume P and P' are two paths in $\mathcal{S}^1_m$, which are generated by m-connectors C and C' in $\mathcal{C}_m$, respectively. Then $R_\tau(P, P') = 1$ if and only if there exist integers k_1 and k_2 such that C can be (βm)-transformed to C' with parameters (k_1, k_2). Clearly, the definition of R_τ implies that

$$V_\tau[P] = \{C(r+1)+1, C(r+2)+1, \dots, C(m-r)+1\} \subset \{5, 7, \dots, 2m+3\},$$

where $r = \beta m$, and thus, $|V_\tau[P]| = (1 - 2\beta)m$.

For the case when $d > 1$, we use $\bar\tau$ to denote $(m, d-1, \beta)$. By induction on d, we may assume that $R_{\bar\tau}$ (from $\mathcal{S}^{d-1}_m \times \mathcal{S}^{d-1}_m$) has already been constructed since

$$\beta \in (0, 32^{-d}] \subset (0, 32^{-(d-1)}].$$

Now let P and P' be two paths in $\mathcal{S}^d_m$, which are generated by tuples

$$(C, P_1, \dots, P_{2m+3}) \quad \text{and} \quad (C', P'_1, \dots, P'_{2m+3}),$$

respectively. We set $R_\tau(P, P') = 1$ if the following conditions are satisfied:

- Let $r = \beta m$. There exist integers $k_1 \in [r]$ and $r + 1 \le k_2 \le m - r$ such that C can be r-transformed to C' with parameters (k_1, k_2);
- Let r_1, r_2, r_3, r_4 denote $C(k_2 - k_1) + 1$, $C(m+1) + 1$, $C(m - k_1 + 1) + 1$, and $C(k_2) + 1$, respectively. Let l_1, l_2, l_3 denote $C(m - k_1 + 2)$, $C(k_2 + 1)$, and $C(k_2 - k_1 + 1)$, respectively;
- For each $i = 1, 2$ and 3, there exists $\mathbf{v} \in V_{\bar\tau}[P_{r_i}] \cap V_{\bar\tau}[P_{l_i}]$ such that

$$P'_{r_i} \in \mathcal{S}_{\bar\tau}[P_{r_i}, \mathbf{v}] \quad \text{and} \quad P'_{l_i} \in \mathcal{S}_{\bar\tau}[P_{l_i}, \mathbf{v}];$$

- $P'_{r_4} \in \mathcal{S}_{\bar\tau}[P_{r_4}]$; and for all other $j \in [2m+3]$, $P'_j = P_j$.

This finishes the construction of R_τ.

First, it is easy to check that R_τ is a symmetric relation:

$$R_\tau(P, P') = 1 \iff R_\tau(P', P) = 1.$$

Moreover, we prove the following lemma concerning the set $V_\tau[P]$:

Lemma 5 *For every path $P \in \mathcal{S}_m^d$, we have*

$$|V_\tau[P]| = ((1-2\beta)m)^d \quad \textit{and} \quad V_\tau[P] \subset \{5, 7, \dots, 2m+3\}^d. \tag{1}$$

Proof We use induction on d. The case when $d = 1$ is trivial.

For the case when $d > 1$, we let $\bar{\tau}$ denote $(m, d-1, \beta)$, and prove that

$$V_\tau[P] = \bigcup_{t=C(k)+1, r+1 \le k \le m-r} V_{\bar{\tau}}[P_t] \times \{t\}. \tag{2}$$

Equation (1) then follows since by the inductive hypothesis, we have

$$|V_{\bar{\tau}}[P_t]| = ((1-2\beta)m)^{d-1} \quad \text{and} \quad V_{\bar{\tau}}[P_t] \subset \{5, 7, \dots, 2m+3\}^{d-1}$$

for every P_t in (2).

By the definition of $V_\tau[P]$, to prove (2), it suffices to show that, for any vertex $\mathbf{v} \in K_{2m+3}^d$ such that $v_d = C(k) + 1$ for some $k : r+1 \le k \le m-r$ and $(v_1, \dots, v_{d-1}) \in V_{\bar{\tau}}[P_{v_d}]$, we have $N_\tau[P, \mathbf{v}] > 0$.

To this end, we let $M_{i,j}$, for all $i, j : 1 \le i \ne j \le m+1$, denote

$$M_{i,j} = \sum_{\mathbf{v} \in V_{\bar{\tau}}[P_{C(i)+1}] \cap V_{\bar{\tau}}[P_{C(j)}]} N_{\bar{\tau}}[P_{C(i)+1}, \mathbf{v}] \cdot N_{\bar{\tau}}[P_{C(j)}, \mathbf{v}]. \tag{3}$$

Then by the inductive hypothesis, we have

$$|V_{\bar{\tau}}[P_{C(i)+1}] \cap V_{\bar{\tau}}[P_{C(j)}]| \ge 2((1-2\beta)m)^{d-1} - m^{d-1} > 0,$$

since $\beta < 32^{-d}$. Therefore, $M_{i,j} > 0$ for all i, j. The reason why we introduce these integers is because $N_\tau[P, \mathbf{v}]$ can be expressed as

$$\sum_{k_1=1}^{r} M_{k-k_1, m-k_1+2} M_{m+1, k+1} M_{m-k_1+1, k-k_1+1} N_{\bar{\tau}}[P_{v_d}, (v_1, \dots, v_{d-1})]. \tag{4}$$

As a result, $N_\tau[P, \mathbf{v}] > 0$ since we assumed that $(v_1, \dots, v_{d-1}) \in V_{\bar{\tau}}[P_{v_d}]$. □

Next, we use Lemma 5 to prove the following statement about $R_{m,\beta}^d \equiv R_\tau$:

Lemma 6 *For $d \ge 1$ and $\beta \in (0, 32^{-d}]$ such that $r = \beta m \in \mathbb{Z}^+$, we have*

$$\frac{1}{\mu_d(\beta)} \le \frac{N_\tau[P, \mathbf{v}]}{N_\tau[P', \mathbf{v}']} \le \mu_d(\beta),$$

for all $P, P' \in \mathcal{S}_m^d$, $\mathbf{v} \in V_\tau[P]$ *and* $\mathbf{v}' \in V_\tau[P']$, *where* $\mu_d(\beta)$ *is defined inductively on* d *as follows*: $\mu_1(\beta) = 1$; *for* $d \geq 2$,

$$\mu_d(\beta) = \frac{(\mu_{d-1}(\beta))^7}{(2(1-2\beta)^{d-1}-1)^3}.$$

Proof The case when $d = 1$ is trivial.

For $d > 1$, suppose P is generated by $(C, P_1, \dots, P_{2m+3})$ and P' is generated by $(C', P'_1, \dots, P'_{2m+3})$. We define integers $M_{i,j}$ and $M'_{i,j}$, as in (3), for P and P', respectively. Then, by using the inductive hypothesis and (1), we have

$$M_{i,j}/M_{i',j'} \leq (\mu_{d-1}(\beta))^2/(2(1-2\beta)^{d-1}-1).$$

The lemma then follows by applying this inequality to every item in (4). □

The following lemma concerning μ_d is easy to verify (by induction on d):

Lemma 7 *For all* $d \geq 1$ *and* $\beta \in (0, 32^{-d}]$, $\mu_d(\beta) \leq e^{32^{d-1}\beta}$.

Let P be a path in $\mathcal{S}_m^d$. For all $i, j : 1 \leq i \neq j \leq m+1$, $M_{i,j}$ is defined as in (3), then we have the following two corollaries of Lemma 7.

Corollary 2 *For all* $1 \leq i \neq j,\ i' \neq j' \leq m+1$, $M_{i,j}\big/M_{i',j'} < 2$.

Corollary 3 *For all paths* P *and* P' *in* $\mathcal{S}_m^d$, $N_\tau[P]\big/N_\tau[P'] \leq \mu_d(\beta) < 2$.

3.3 Proof of the Lower Bound

For $d \geq 1$ and $\beta \in (0, 32^{-d}]$, we show that, when m is large enough and satisfies $\beta m \in \mathbb{Z}^+$, relation $R_\tau \equiv R_{m,\beta}^d$ can serve as the function w in Theorem 3, and gives us an almost-tight lower bound for $\mathsf{QQ}_{\mathsf{KP}}^d(2m+3)$.

Let $(\mathbf{v}^1, \mathbf{v}^2)$ be a directed edge in K_{2m+3}^d, $\mathbf{v} \in K_{2m+3}^d$, and path $P \in \mathcal{S}_m^d$. We introduce the following notation:

- $\mathcal{S}_\tau[P, (\mathbf{v}^1, \mathbf{v}^2)] = \{P' \in \mathcal{S}_\tau[P],\ \mathcal{F}_P(\mathbf{v}^1, \mathbf{v}^2) \neq \mathcal{F}_{P'}(\mathbf{v}^1, \mathbf{v}^2)\}$;
- $\mathcal{S}_\tau[P, \mathbf{v}, (\mathbf{v}^1, \mathbf{v}^2)] = \mathcal{S}_\tau[P, \mathbf{v}] \cap \mathcal{S}_\tau[P, (\mathbf{v}^1, \mathbf{v}^2)]$;
- $N_\tau[P, (\mathbf{v}^1, \mathbf{v}^2)] = |\mathcal{S}_\tau[P, (\mathbf{v}^1, \mathbf{v}^2)]|$, $N_\tau[P, \mathbf{v}, (\mathbf{v}^1, \mathbf{v}^2)] = |\mathcal{S}_\tau[P, \mathbf{v}, (\mathbf{v}^1, \mathbf{v}^2)]|$.

We also let

$$\theta_\tau\big(P, (\mathbf{v}^1, \mathbf{v}^2)\big) = \frac{N_\tau[P, (\mathbf{v}^1, \mathbf{v}^2)]}{N_\tau[P]} = \frac{\sum_{\mathbf{v} \in V_\tau[P]} N_\tau[P, \mathbf{v}, (\mathbf{v}^1, \mathbf{v}^2)]}{N_\tau[P]}.$$

Theorem 2 follows as a corollary of Theorem 3 and Lemma 8 below.

Lemma 8 *Let* $d \geq 1$ *and* $\beta \in (0, 32^{-d}]$. *There exists a constant* $L_{d,\beta}$ *such that for all* $m \geq L_{d,\beta}$ *with* $\beta m \in \mathbb{Z}^+$, *if* $P, P' \in \mathcal{S}_m^d$ *satisfy*

$$R_{m,\beta}^d(P, P') = R_\tau(P, P') = 1 \quad \textit{and} \quad \mathcal{F}_P(\mathbf{v}^1, \mathbf{v}^2) \neq \mathcal{F}_{P'}(\mathbf{v}^1, \mathbf{v}^2)$$

for some edge $(\mathbf{v}^1, \mathbf{v}^2) \in K^d_{2m+3}$, *then*

$$\theta_\tau(P, (\mathbf{v}^1, \mathbf{v}^2)) \cdot \theta_\tau(P', (\mathbf{v}^1, \mathbf{v}^2)) \le \left(\frac{2^{11}}{m}\right)^{d+1}. \tag{5}$$

Proof Without loss of generality, we may assume $\mathcal{F}_P(\mathbf{v}^1, \mathbf{v}^2) = 0$ and $\mathcal{F}_{P'}(\mathbf{v}^1, \mathbf{v}^2) = 1$. We use mathematical induction on d.

When $d = 1$, we assume P and P' are generated by C and C', respectively. Since $R_\tau(P, P') = 1$, there exist integers $k_1 \in [r]$ and $r + 1 \le k_2 \le m - r$ such that C can be $(r = \beta m)$-transformed to C' with parameters (k_1, k_2). It is also easy to check that $N_\tau[P] = N_\tau[P'] = \beta(1 - 2\beta)m^2$. Because $\mathcal{F}_P(v^1, v^2) = 0$ and $\mathcal{F}_{P'}(v^1, v^2) = 1$, (v^1, v^2) must fall into one of the following three cases. For each case, we will prove upper bounds for $N_\tau[P, (v^1, v^2)]$ and $N_\tau[P', (v^1, v^2)]$, which in turn give us upper bounds for $\theta_\tau(P, (v^1, v^2))$ and $\theta_\tau(P', (v^1, v^2))$.

1. $(v^1, v^2) = (C(k_2 - k_1) + 1, C(m - k_1 + 2))$: In this case, it is easy to show that $N_\tau[P, (v^1, v^2)] = 1$. Actually P' is the only path in $\mathcal{S}_\tau[P, (v^1, v^2)]$. Next, we bound $N_\tau[P', (v^1, v^2)]$. For this purpose, we use P'' to denote a path in $\mathcal{S}_\tau[P', (v^1, v^2)]$, which is generated by C''. Moreover, we use k'_1 and k'_2 to denote the integers such that C' can be r-transformed to C'' with (k'_1, k'_2). Since $\mathcal{F}_{P'}(v^1, v^2) = 1$ but $\mathcal{F}_{P''}(v^1, v^2) = 0$, we must have

$$k_2 - k_1 \in \{k'_2, k'_2 - k'_1\}.$$

   Thus, the number of such paths P'' is at most $2r = 2\beta m$. As a result,

$$\theta_\tau(P, (v^1, v^2)) = \frac{1}{\beta(1 - 2\beta)m^2} \quad \text{and} \quad \theta_\tau(P', (v^1, v^2)) \le \frac{2}{(1 - 2\beta)m};$$

2. $(v^1, v^2) = (C(m + 1) + 1, C(k_2 + 1))$: By similar arguments, one can show that $N_\tau[P, (v^1, v^2)] = \beta m$ and $N_\tau[P', (v^1, v^2)] \le 2\beta m$. As a result, we have

$$\theta_\tau(P, (v^1, v^2)) = \frac{1}{(1 - 2\beta)m} \quad \text{and} \quad \theta_\tau(P', (v^1, v^2)) \le \frac{2}{(1 - 2\beta)m};$$

3. $(v^1, v^2) = (C(m - k_1 + 1) + 1, C(k_2 - k_1 + 1))$: By similar arguments, one can show that $N_\tau[P, (v^1, v^2)] = 1$ and $N_\tau[P', (v^1, v^2)] \le (1 - 2\beta)m$. As a result,

$$\theta_\tau(P, (v^1, v^2)) = \frac{1}{\beta(1 - 2\beta)m^2} \quad \text{and} \quad \theta_\tau(P', (v^1, v^2)) = \frac{1}{\beta m}.$$

When m is large enough (e.g., set $L_{1,\beta}$ to be $(1 - 2\beta)/(2\beta^2))$, it is clear that $\theta_\tau(P, (v^1, v^2)) \cdot \theta_\tau(P', (v^1, v^2))$ in the second case is greater than the other two cases, and we have

$$\theta_\tau(P, (v^1, v^2)) \cdot \theta_\tau(P', (v^1, v^2)) \le \frac{2}{((1 - 2\beta)m)^2} < \left(\frac{2^{11}}{m}\right)^2.$$

This finishes the proof for the case when $d = 1$.

When $d > 1$, suppose P and P' are generated by $(C, P_1, \dots, P_{2m+3})$ and $(C', P'_1, \dots, P'_{2m+3})$, respectively. Moreover, C can be (βm)-transformed to C' with (k_1, k_2). Integers $M_{i,j}$ and $M'_{i,j}$ are defined as previously. Let $\bar\tau = (m, d-1, \beta)$. For $i \in [m+1]$, we let

$$M_i = N_{\bar\tau}[P_{C(i)+1}] \quad \text{and} \quad M'_i = N_{\bar\tau}[P'_{C(i)+1}].$$

First, we consider the case when $v^1_d \neq v^2_d$, and $v^1_i = v^2_i$ for all $1 \le i \le d-1$. We use $\mathbf{v}^*$ to denote $(v^1_1, v^1_2, \dots, v^1_{d-1}) = (v^2_1, v^2_2, \dots, v^2_{d-1})$. Then there are again, three cases to consider.

1. $(v^1_d, v^2_d) = (C(k_2 - k_1) + 1, C(m - k_1 + 2))$: By Lemma 6 and Corollary 2, we can write $\theta_\tau(P, (\mathbf{v}^1, \mathbf{v}^2))$ as

$$\frac{N_{\bar\tau}[P_{C(k_2-k_1)+1}, \mathbf{v}^*]N_{\bar\tau}[P_{C(m-k_1+2)}, \mathbf{v}^*]M_{m+1,k_2+1}\,M_{m-k_1+1,k_2-k_1+1}M_{k_2}}{\sum_{t_1=1}^{r}\sum_{t_2=r+1}^{m-r} M_{t_2-t_1,m-t_1+2}M_{m+1,t_2+1}\,M_{m-t_1+1,t_2-t_1+1}M_{t_2}}$$
$$\le \frac{8(\mu_{d-1}(\beta))^2}{\beta m \cdot (1-2\beta)m \cdot (2(1-2\beta)^{d-1} - 1)m^{d-1}} = O\left(\frac{1}{m^{d+1}}\right),$$

and $\theta_\tau(P', (\mathbf{v}^1, \mathbf{v}^2)) = O(1/m)$. Equation (5) then follows when m is large enough.

2. $(v^1_d, v^2_d) = (C(m+1) + 1, C(k_2 + 1))$: By Lemma 6 and Corollary 2, we can write $\theta_\tau(P, (\mathbf{v}^1, \mathbf{v}^2))$ as

$$\frac{\sum_{t_1=1}^{r} M_{k_2-t_1,m-t_1+2}N_{\bar\tau}[P_{C(m+1)+1}, \mathbf{v}^*]N_{\bar\tau}[P_{C(k_2+1)+1}, \mathbf{v}^*]M_{m-t_1+1,k_2-t_1+1}M_{k_2}}{\sum_{t_1=1}^{r}\sum_{t_2=r+1}^{m-r} M_{t_2-t_1,m-t_1+2}M_{m+1,t_2+1}M_{m-t_1+1,t_2-t_1+1}M_{t_2}}$$
$$\le \frac{8(\mu_{d-1}(\beta))^2}{(1-2\beta)m \cdot (2(1-2\beta)^{d-1} - 1)m^{d-1}} < \frac{32}{m^d}.$$

Similarly, one can show that,

$$\theta_\tau(P', (\mathbf{v}^1, \mathbf{v}^2)) < \frac{32}{(1-2\beta)m},$$

and (5) follows.

Case 3, $(v^1_d, v^2_d) = (C(m - k_1 + 1) + 1, C(k_2 - k_1 + 1))$, can be proved similarly.

Second, we consider the case when $v^1_d = v^2_d$. By the inductive hypothesis, we know there exists a constant $L_{d-1,\beta}$ such that for all $m > L_{d-1,\beta}$ and $P, P' \in \mathcal{S}^{d-1}_m$, if (1) $R_{\bar\tau=(m,d-1,\beta)}(P, P') = 1$ and (2) $\mathcal{F}_P(\mathbf{u}^1, \mathbf{u}^2) \neq \mathcal{F}_{P'}(\mathbf{u}^1, \mathbf{u}^2)$ for some directed edge $(\mathbf{u}^1, \mathbf{u}^2) \in K^{d-1}_{2m+3}$, then

$$\theta_{\bar\tau}(P, (\mathbf{u}^1, \mathbf{u}^2)) \cdot \theta_{\bar\tau}(P', (\mathbf{u}^1, \mathbf{u}^2)\big) \le (2^{11}/m)^d.$$

Here we set $L_{d,\beta} \ge L_{d-1,\beta}$, so the inequality above holds for all $m > L_{d,\beta}$.

It is easy to check that

$$v_d^1 \in \{C(k_2-k_1)+1, C(k_2-k_1+1), C(k_2)+1, C(k_2+1),\\ C(m-k_1+1)+1, C(m-k_1+2), C(m+1)\},$$

since otherwise, $\mathcal{F}_P(\mathbf{v}^1,\mathbf{v}^2) = \mathcal{F}_{P'}(\mathbf{v}^1,\mathbf{v}^2)$. In the proof, we only consider the case when $v_d^1 = C(k_2)+1$. All the other cases can be proved similarly. We let $\mathbf{u}^1$ and $\mathbf{u}^2$ denote $D_d(\mathbf{v}^1)$ and $D_d(\mathbf{v}^2)$, respectively.

First, $N_\tau[P,(\mathbf{v}^1,\mathbf{v}^2)]$ can be divided into two parts. The first part is

$$\sum_{t_1=1}^{r} M_{k_2-t_1,m-t_1+2} M_{m+1,k_2+1} M_{m-t_1+1,k_2-t_1+1} N_{\bar{\tau}}[P_{C(k_2)+1},(\mathbf{u}^1,\mathbf{u}^2)].$$

For every path P_i, using Corollary 3, we have

$$\frac{N_{\bar{\tau}}[P_{C(k_2)+1},(\mathbf{u}^1,\mathbf{u}^2)]}{N_{\bar{\tau}}[P_i]} = \frac{N_{\bar{\tau}}[P_{C(k_2)+1},(\mathbf{u}^1,\mathbf{u}^2)]}{N_{\bar{\tau}}[P_{C(k_2)+1}]} \cdot \frac{N_{\bar{\tau}}[P_{C(k_2)+1}]}{N_{\bar{\tau}}[P_i]}\\ < 2\cdot\theta_{\bar{\tau}}(P_{C(k_2)+1},(\mathbf{u}^1,\mathbf{u}^2)).$$

The second part is

$$\sum_{t_2=k_2+1}^{\min(m-r,k_2+r)} M_{m+1,t_2+1} M_{m-(t_2-k_2)+1,k_2+1} M_{t_2} A_{t_2},$$

where

$$A_{t_2} = \sum_{\mathbf{v}\in V_{\bar{\tau}}[P_{C(k_2)+1}]\cap V_{\bar{\tau}}[P_{C(m-(t_2-k_2)+1)}]} N_{\bar{\tau}}[P_{C(k_2)+1},\mathbf{v},(\mathbf{u}^1,\mathbf{u}^2)]\\ \times N_{\bar{\tau}}[P_{C(m-(t_2-k_2)+1)},\mathbf{v}].$$

However, for all t_2 and $1\le i\ne j\le m+1$, we have

$$\frac{A_{t_2}}{M_{i,j}} \le \mu_{d-1}(\beta)\cdot\frac{\sum_{\mathbf{v}\in V_{\bar{\tau}}[P_{C(k_2)+1}]\cap V_{\bar{\tau}}[P_{C(m-(t_2-k_2)+1)}]} N_{\bar{\tau}}[P_{C(k_2)+1},\mathbf{v},(\mathbf{u}^1,\mathbf{u}^2)]}{\sum_{\mathbf{v}\in V_{\bar{\tau}}[P_{C(i)+1}]\cap V_{\bar{\tau}}[P_{C(j)}]} N_{\bar{\tau}}[P_{C(i)+1},\mathbf{v}]}\\ \le \mu_{d-1}(\beta)\cdot\frac{N_{\bar{\tau}}[P_{C(k_2)+1},(\mathbf{u}^1,\mathbf{u}^2)]}{N_{\bar{\tau}}[P_{C(k_2)+1}]}\cdot\frac{N_{\bar{\tau}}[P_{C(k_2)+1}]}{\sum_{\mathbf{v}\in V_{\bar{\tau}}[P_{C(i)+1}]\cap V_{\bar{\tau}}[P_{C(j)}]} N_{\bar{\tau}}[P_{C(i)+1},\mathbf{v}]}\\ \le \frac{(\mu_{d-1}(\beta))^2}{(2(1-2\beta)^{d-1}-1)}\cdot\theta_{\bar{\tau}}(P_{C(k)+1},(\mathbf{u}^1,\mathbf{u}^2)).$$

Therefore, we have

$$\theta_\tau(P,(\mathbf{v}^1,\mathbf{v}^2)) \le \frac{8\cdot\theta_{\bar{\tau}}(P_{C(k)+1},(\mathbf{u}^1,\mathbf{u}^2))}{(1-2\beta)m}\left(2+\frac{(\mu_{d-1}(\beta))^2}{(2(1-2\beta)^{d-1}-1)}\right)$$

$$\leq \frac{2^6}{m} \cdot \theta_{\bar{\tau}}(P_{C(k)+1}, (\mathbf{u}^1, \mathbf{u}^2)).$$

For $\theta_\tau(P', (\mathbf{v}^1, \mathbf{v}^2))$, one can similarly show that

$$\begin{aligned}\theta_\tau(P', (\mathbf{v}^1, \mathbf{v}^2)) &\leq 8 \cdot \mu_{d-1}(\beta) \cdot 2 \cdot \theta_{\bar{\tau}}(P'_{C(k)+1}, (\mathbf{u}^1, \mathbf{u}^2)) \\ &\leq 2^5 \cdot \theta_{\bar{\tau}}(P'_{C(k)+1}, (\mathbf{u}^1, \mathbf{u}^2)).\end{aligned}$$

On the other hand, since $R_{\bar{\tau}}(P_{C(k)+1}, P'_{C(k)+1}) = 1$, and $\mathcal{F}_{P_{C(k)+1}}(\mathbf{u}^1, \mathbf{u}^2) \neq \mathcal{F}_{P'_{C(k)+1}}(\mathbf{u}^1, \mathbf{u}^2)$, from the inductive hypothesis, we have

$$\theta_{\bar{\tau}}(P'_{C(k)+1}, (\mathbf{u}^1, \mathbf{u}^2)) \cdot \theta_{\bar{\tau}}(P_{C(k)+1}, (\mathbf{u}^1, \mathbf{u}^2)) \leq (2^{11}/m)^d.$$

As a result,

$$\theta_\tau(P, (\mathbf{v}^1, \mathbf{v}^2)) \cdot \theta_\tau(P', (\mathbf{v}^1, \mathbf{v}^2)) \leq (2^{11}/m)^{d+1}. \qquad \square$$

Appendix A: A Reduction from GP^d to HP^d

For $d \geq 2$ and $n \geq 1$, we let $N = 2^n$ and $m = dn$. We first define a one-to-one correspondence Υ from $\{0,1\}^m$ to $\mathbb{Z}_N^d$. In the presentation below, we use $\mathbf{p}, \mathbf{q}$ to denote vertices in $\mathbb{Z}_N^d$, and $\mathbf{u}, \mathbf{v}, \mathbf{w}$ to denote vertices in $\{0,1\}^m$.

First, we arbitrarily pick a hamiltonian path of graph H^n: $\mathbf{v}^1\mathbf{v}^2 \cdots \mathbf{v}^N$ with $\mathbf{v}^1 = \mathbf{0}$. This path gives us a correspondence Ψ from the vertices of H^n to $[N] = \{1, \ldots, N\}$: $\Psi(\mathbf{v}^i) = i$ for all $i \in [N]$. Then for each vertex $\mathbf{v} \in \{0,1\}^m$, we can write it as $(\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^d)$ in which every $\mathbf{v}^i$ is a vertex in H^n, and define Υ as

$$\Upsilon(\mathbf{v}) = \Upsilon(\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^d) = \big(\Psi(\mathbf{v}^1), \Psi(\mathbf{v}^2), \ldots, \Psi(\mathbf{v}^d)\big) \in \mathbb{Z}_N^d.$$

Given any simple path P in G_N^d starting at $\mathbf{1}$, one can build a simple path P' in H^m as follows:

$$\mathcal{F}_{P'}(\mathbf{u}, \mathbf{w}) = 1 \quad \text{iff} \quad \mathcal{F}_P(\mathbf{p}, \mathbf{q}) = 1,$$

where $\mathbf{p} = \Upsilon^{-1}(\mathbf{u})$ and $\mathbf{q} = \Upsilon^{-1}(\mathbf{w})$. It is easy to verify that the starting vertex of P' is $\mathbf{0}$; and $\mathbf{v}^*$ is the ending vertex of P' iff $\Upsilon^{-1}(\mathbf{v}^*)$ is the ending vertex of P. Lemma 3 follows directly from this reduction.

Appendix B: A Reduction from KP^d to GP^{d+1}

In this section, we prove Lemma 2. First, we define a search problem GG^d over graph G_n^d, which was first introduced in [1].

Let G be a subgraph of G_n^d. For each $\mathbf{v} \in \mathbb{Z}_n^d$, we use $\Delta_I(\mathbf{v})$ and $\Delta_O(\mathbf{v})$ to denote its in-degree and out-degree in G, respectively. G is called a *generalized path graph* (see Fig. 3 for an example), if

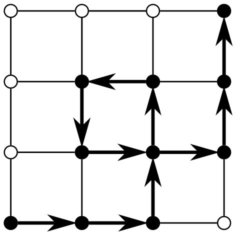

Fig. 3 A generalized path graph G in G_4^2

1. There exists exactly one vertex $\mathbf{v}_S \in \mathbb{Z}_n^d$ with $\Delta_O(\mathbf{v}_S) = \Delta_I(\mathbf{v}_S) + 1$, and exactly one vertex $\mathbf{v}_T$ with $\Delta_I(\mathbf{v}_T) = \Delta_O(\mathbf{v}_T) + 1$;
2. All vertices in $\mathbb{Z}_n^d - \{\mathbf{v}_S, \mathbf{v}_T\}$ satisfy Euler's condition: $\Delta_I(\mathbf{v}) = \Delta_O(\mathbf{v})$;
3. If $(\mathbf{u}, \mathbf{v})$ is a directed edge in G, then $(\mathbf{v}, \mathbf{u}) \notin G$.

We refer to $\mathbf{v}_S$ and $\mathbf{v}_T$ as the *starting* and *ending* vertices of G, respectively. Every such subgraph G induces a map $\mathcal{F}_G$ from the edge set of G_n^d to $\{0, 1\}$: for each $(\mathbf{u}, \mathbf{v})$ in G_n^d, $\mathcal{F}_G(\mathbf{u}, \mathbf{v}) = 1$ if $(\mathbf{u}, \mathbf{v})$ is a directed edge in G; and $\mathcal{F}_G(\mathbf{u}, \mathbf{v}) = 0$ otherwise.

We now define the search problem GG^d: the input is a binary string of length $|G_n^d|$, which encodes the map $\mathcal{F}_G$ of a *generalized path graph* G. The starting vertex of G is known to be $\mathbf{1} = (1, \ldots, 1) \in \mathbb{Z}_n^d$, and we need to find its ending vertex. For $d \geq 2$, the following reduction from problem GG^d to GP^d was given in [1]: from any input string $\mathcal{F}_G$ of GG^d, where G is a generalized path graph in G_n^d, one can construct a simple path P (and thus, $\mathcal{F}_P$) in G_{4n+1}^d, such that

1. The starting vertex of P is $\mathbf{1} = (1, \ldots, 1) \in \mathbb{Z}_n^d$;
2. Once the ending vertex of P is found, the ending vertex of G can be located immediately;
3. For every edge $(\mathbf{u}, \mathbf{v}) \in G_{4n+1}^d$, the value of $\mathcal{F}_P$ at $(\mathbf{u}, \mathbf{v})$ only depends on at most $4d$ bits of $\mathcal{F}_G$.

By using Lemma 1 of [18], we have the following relationship between $\mathsf{QQ}_{\mathsf{GG}}^d$ and $\mathsf{QQ}_{\mathsf{GP}}^d$, the quantum query complexity of GG^d and GP^d, respectively:

Lemma 9 *For all* $d \geq 2$, $\mathsf{QQ}_{\mathsf{GG}}^d(n) \leq O(d) \cdot \mathsf{QQ}_{\mathsf{GP}}^d(4n + 1)$.

Therefore, to prove Lemma 2, we only need to find a reduction from KP^d to GG^{d+1}. To this end, we first describe a construction that, given any input string $\mathcal{F}_P$ of KP^d (where P is a simple path in K_n^d), builds a generalized path graph G in G_{dn}^{d+1}.

In the presentation, we use $\mathbf{p}, \mathbf{q}, \mathbf{r}$ to denote vertices in $\mathbb{Z}_n^d$ (vertex set of K_n^d) and $\mathbf{u}, \mathbf{v}, \mathbf{w}$ to denote vertices in $\mathbb{Z}_{dn}^{d+1}$ (vertex set of G_{dn}^{d+1}). We start with some notation.

Suppose $\mathbf{u}, \mathbf{v} \in G_{dn}^{d+1}$ are two vertices that differ in only one coordinate, say the ith coordinate, and $\mathbf{e} = (\mathbf{v} - \mathbf{u})/|v_i - u_i|$. Let

$$E(\mathbf{u}, \mathbf{v}) = \{(\mathbf{u}, \mathbf{u} + \mathbf{e}), (\mathbf{u} + \mathbf{e}, \mathbf{u} + 2\mathbf{e}), \ldots, (\mathbf{v} - \mathbf{e}, \mathbf{v})\}$$

denote a set of directed edges. Let Γ be the following map from $\mathbb{Z}_n^d$ to $\mathbb{Z}_{dn}^{d+1}$:

$$\Gamma(\mathbf{p}) = \Gamma(p_1, p_2, \dots, p_d) = \left(p_1, p_2, \dots, p_d, \sum_{i=1}^{d} p_i - (d-1)\right).$$

Clearly, Γ maps $(1, 1, \dots, 1) \in \mathbb{Z}_n^d$ to $(1, 1, \dots, 1) \in \mathbb{Z}_{dn}^{d+1}$.

Let $P = \mathbf{p}^1\mathbf{p}^2 \cdots \mathbf{p}^k$ be a simple path in K_n^d with $\mathbf{p}^1 = \mathbf{1}$. We first apply Γ on P to get a sequence of k vertices $\mathbf{v}^1\mathbf{v}^2 \cdots \mathbf{v}^k$ in G_{dn}^{d+1}, where $\mathbf{v}^i = \Gamma(\mathbf{p}^i)$ for all $i \in [k]$. Now consider two consecutive vertices $\mathbf{u} = \mathbf{v}^i$ and $\mathbf{w} = \mathbf{v}^{i+1}$ in the sequence. There must exist an index $t \in [d]$ such that $u_t \neq w_t$ and $u_i = w_i$ for all other $i \in [d]$. We let $\mathbf{v} = (u_1, u_2, \dots, u_{t-1}, w_t, u_{t+1}, \dots, u_{d-1}, u_d, u_{d+1})$ and use $\Lambda(\mathbf{u}, \mathbf{w})$ to denote the following path from $\mathbf{u}$ to $\mathbf{w}$ by going through $\mathbf{v}$:

$$\Lambda(\mathbf{u}, \mathbf{w}) = E(\mathbf{u}, \mathbf{v}) \cup E(\mathbf{v}, \mathbf{w}).$$

Finally, we finish the construction of G by setting $G = \bigcup_{i=1}^{k-1} \Lambda(\mathbf{v}^i, \mathbf{v}^{i+1})$.

Now we prove that this construction indeed gives us a reduction from KP^d to GG^{d+1}. First, we show that G is a generalized path graph. This follows directly from the lemma below:

Lemma 10 *For each edge* $(\mathbf{u}, \mathbf{w}) \in G_{dn}^{d+1}$, *if* $(\mathbf{u}, \mathbf{w}) \in \Lambda(\mathbf{v}^m, \mathbf{v}^{m+1})$ *for some* m, *then* $(\mathbf{u}, \mathbf{w}),\ (\mathbf{w}, \mathbf{u}) \notin \Lambda(\mathbf{v}^r, \mathbf{v}^{r+1})$ *for all* $r : 1 \le r \neq m \le k-1$.

Proof Since P is a simple path in K_n^d, we have $\mathbf{p}^i \neq \mathbf{p}^j$, and thus, $\mathbf{v}^i \neq \mathbf{v}^j$ for all $i, j : 1 \le i \neq j \le k$. On the other hand, there exists exactly one $t \in [d+1]$ such that $u_t \neq w_t$.

Now suppose there exists an integer $r : 1 \le r \neq m \le k-1$ such that $(\mathbf{u}, \mathbf{w})$ or $(\mathbf{w}, \mathbf{u}) \in \Lambda(\mathbf{v}^r, \mathbf{v}^{r+1})$. We have two cases:

1. $t = d+1$: then $\mathbf{v}^{m+1} = \mathbf{v}^{r+1} = (w_1, w_2, \dots, w_d, \sum_{i=1}^{d} w_i - (d-1))$;
2. $1 \le t \le d$: then $\mathbf{v}^m = \mathbf{v}^r = (u_1, \dots, u_{t-1}, u'_t, u_{t+1}, \dots, u_d, u_{d+1})$, where $u'_t = u_{d+1} + (d-1) - \sum_{1 \le i \neq t \le d} u_i$.

For both cases, we get a contradiction. □

It is easy to show that if $\mathbf{v}^*$ is the ending vertex of graph G, then $\Gamma^{-1}(\mathbf{v}^*)$ must be the ending vertex of P. To finish the reduction, we prove the following two lemmas.

Lemma 11 *Let* $(\mathbf{u}, \mathbf{v})$ *be an edge in* G_{dn}^{d+1} *with* $u_{d+1} \neq v_{d+1}$. *Vertex* $\mathbf{u}$ *satisfies* $1 \le u_i \le n$ *for all* $i \in [d]$. *Let* $\mathbf{p} \in \mathbb{Z}_n^d$ *be the vertex in* K_n^d *such that* $p_i = u_i$ *for all* $i \in [d]$. *Then* $\mathcal{F}_G(\mathbf{u}, \mathbf{v})$ *only depends on the answers to the following questions concerning* $\mathcal{F}_P$:

Is there a vertex $\mathbf{q} \in \mathbb{Z}_n^d$ *such that* $\mathcal{F}_P(\mathbf{q}, \mathbf{p}) = 1$? *If there is, which one?*

Proof For integers $r, m_1, m_2 \in \mathbb{Z}$ and $s \in \{\pm 1\}$, we say (r, s) is *consistent* with (m_1, m_2) if (1) $m_1 \le r < m_2$ and $s = +1$; or (2) $m_2 < r \le m_1$ and $s = -1$.

Let $s = v_{d+1} - u_{d+1} \in \{\pm 1\}$. The lemma follows directly from the following statement: $\mathcal{F}_G(\mathbf{u}, \mathbf{v}) = 1$ if and only if

1. There exists a $\mathbf{q} \in \mathbb{Z}_n^d$ such that $\mathcal{F}_P(\mathbf{q}, \mathbf{p}) = 1$; and
2. (u_{d+1}, s) is consistent with $(\sum_{i=1}^d q_i - (d-1), \sum_{i=1}^d p_i - (d-1))$.

Clearly, whether these two conditions hold only depends on the answers to the two questions above. □

Lemma 12 *Let* $(\mathbf{u}, \mathbf{v})$ *be an edge in* G_{dn}^{d+1} *with* $u_t \neq v_t$ *for some index* $t \in [d]$. $\mathbf{u}$ *and* $\mathbf{v}$ *satisfy* $1 \le u_{d+1} + (d-1) - \sum_{1 \le i \neq t \le d} u_i \le n$, *and* $1 \le u_i, v_i \le n$ *for all* $i \in [d]$. *Let* $\mathbf{p}$ *be the vertex in* K_n^d *such that* $p_i = u_i$ *for all* $i : 1 \le i \neq t \le d$, *and* $p_t = u_{d+1} + (d-1) - \sum_{1 \le i \neq t \le d} u_i$. *Then* $\mathcal{F}_G(\mathbf{u}, \mathbf{v})$ *only depends on the answers to the following two questions concerning* $\mathcal{F}_P$:

Is there a vertex $\mathbf{q} \in \mathbb{Z}_n^d$ *such that* $\mathcal{F}_P(\mathbf{p}, \mathbf{q}) = 1$? *If there is*, *which one?*

Proof Let $s = v_t - u_t \in \{\pm 1\}$. The lemma follows directly from the following statement: $\mathcal{F}_G(\mathbf{u}, \mathbf{v}) = 1$ if and only if

1. There exists a $\mathbf{q} \in \mathbb{Z}_n^d$ such that $\mathcal{F}_P(\mathbf{p}, \mathbf{q}) = 1$; and
2. (u_t, s) is consistent with (p_t, q_t).

Whether these two conditions hold only depends on the answers to the two questions above. □

We know in K_n^d, every vertex has exactly $d(n-1)$ neighbors. So Lemmas 11 and 12 together imply that, to evaluate $\mathcal{F}_G(\mathbf{u}, \mathbf{v})$ for any edge $(\mathbf{u}, \mathbf{v}) \in G_{dn}^{d+1}$, one only need to make $O(\sqrt{d(n-1)})$ queries to the binary string $\mathcal{F}_P$ using Grover's search [25]. Following the idea of Theorem 1.14 in [26], we have

Lemma 13 *For all* $d \ge 1$, $\mathsf{QQ}_{\mathsf{KP}}^d(n) \le O(\sqrt{dn}) \cdot \mathsf{QQ}_{\mathsf{GG}}^{d+1}(dn)$.

Lemma 2 then follows from Lemmas 9 and 13.

References

1. Chen, X., Teng, S.H.: Paths beyond local search: a tight bound for randomized fixed-point computation. In: Proceedings of the 48th FOCS, pp. 124–134 (2007)
2. Nash, J.: Equilibrium point in n-person games. Proc. Natl. Acad. USA **36**(1), 48–49 (1950)
3. Arrow, K., Debreu, G.: Existence of an equilibrium for a competitive economy. Econometrica **22**(3), 265–290 (1954)
4. Scarf, H.: The approximation of fixed points of a continuous mapping. SIAM J. Appl. Math. **15**, 997–1007 (1967)
5. Scarf, H.: On the computation of equilibrium prices. In: Fellner, W. (ed.) Ten Economic Studies in the Tradition of Irving Fisher. Wiley, New York (1967)
6. Papadimitriou, C.: On inefficient proofs of existence and complexity classes. In: Proceedings of the 4th Czechoslovakian Symposium on Combinatorics (1991)
7. Hirsch, M., Papadimitriou, C., Vavasis, S.: Exponential lower bounds for finding Brouwer fixed points. J. Complex. **5**, 379–416 (1989)

8. Deng, X., Papadimitriou, C., Safra, S.: On the complexity of price equilibria. J. Comput. Syst. Sci. **67**(2), 311–324 (2003)
9. Iimura, T., Murota, K., Tamura, A.: Discrete fixed point theorem reconsidered. J. Math. Econ. **41**, 1030–1036 (2005)
10. Aldous, D.: Minimization algorithms and random walk on the d-cube. Ann. Probab. **11**(2), 403–413 (1983)
11. Friedl, K., Ivanyos, G., Santha, M., Verhoeven, F.: On the black-box complexity of Sperner's lemma. In: Proceedings of the 15th FCT, pp. 245–257 (2005)
12. Aaronson, S.: Lower bounds for local search by quantum arguments. In: Proceedings of the 36th STOC, pp. 465–474 (2004)
13. Ambainis, A.: Polynomial degree vs. quantum query complexity. In: Proceedings of the 44th FOCS, pp. 230–239 (2003)
14. Zhang, S.: On the power of Ambainis's lower bounds. Theor. Comput. Sci. **339**(2–3), 241–256 (2005)
15. Zhang, S.: New upper and lower bounds for randomized and quantum local search. In: Proceedings of the 38th STOC, pp. 634–643 (2006)
16. Sun, X., Yao, A.C.: On the quantum query complexity of local search in two and three dimensions. In: Proceedings of the 47th FOCS, pp. 429–438 (2006)
17. Chen, X., Deng, X.: On algorithms for discrete and approximate Brouwer fixed points. In: Proceedings of the 37th STOC, pp. 323–330 (2005)
18. Santha, M., Szegedy, M.: Quantum and classical query complexities of local search are polynomially related. In: Proceedings of the 36th STOC, pp. 494–501 (2004)
19. Barnum, H., Saks, M., Szegedy, M.: Quantum query complexity and semi-definite programming. In: Proceedings of the 18th CCC, pp. 179–193 (2003)
20. Laplante, S., Magniez, F.: Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. In: Proceedings of the 19th CCC, pp. 294–304 (2004)
21. Spalek, R., Szegedy, M.: All quantum adversary methods are equivalent. In: Proceedings of the 32nd ICALP, pp. 1299–1311 (2005)
22. Høyer, P., Lee, T., Spalek, R.: Negative weights make adversaries stronger. In: Proceedings of the 39th STOC, pp. 526–535 (2007)
23. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM **48**(4), 778–797 (2001)
24. Ambainis, A.: Quantum lower bounds by quantum arguments. In: Proceedings of the 32nd FOCS, pp. 636–643 (2000)
25. Grover, L.: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th STOC, pp. 212–219 (1996)
26. Buhrman, H., Cleve, R., Wigderson, A.: Quantum vs. classical communication and computation. In: Proceedings of the 30th STOC, pp. 63–68 (1998)