

On the black-box complexity of Sperner’s Lemma

Katalin Friedl¹, Gábor Ivanyos², Miklos Santha³, and Yves F. Verhoeven^{3,4}

¹ BUTE, H-1521 Budapest, P.O.Box 91, Hungary. friedl@cs.bme.hu

² MTA SZTAKI, H-1518 Budapest, P.O. Box 63, Hungary.

Gabor.Ivanyos@sztaki.hu

³ CNRS–LRI, UMR 8623, Université Paris XI, 91405 Orsay, France.

{santha,verhoeve}@lri.fr

⁴ ENST, 46 rue Barrault, 75013 Paris, France. verhoeve@enst.fr

Abstract. We present several results on the complexity of various forms of Sperner’s Lemma in the black-box model of computing. We give a deterministic algorithm for Sperner problems over pseudo-manifolds of arbitrary dimension. The query complexity of our algorithm is linear in the separation number of the skeleton graph of the manifold and the size of its boundary. As a corollary we get an $O(\sqrt{n})$ deterministic query algorithm for the black-box version of the problem **2D-SPERNER**, a well studied member of Papadimitriou’s complexity class PPAD. This upper bound matches the $\Omega(\sqrt{n})$ deterministic lower bound of Crescenzi and Silvestri. The tightness of this bound was not known before. In another result we prove for the same problem an $\Omega(\sqrt[4]{n})$ lower bound for its probabilistic, and an $\Omega(\sqrt[8]{n})$ lower bound for its quantum query complexity, showing that all these measures are polynomially related.

Classification: computational and structural complexity, quantum computation and information.

1 Introduction

Papadimitriou defined in [17, 18] the complexity classes PPA, PPAD, and PSK in order to classify total search problems which have always a solution. The class PSK was renamed PPADS in [5]. These classes can be characterized by some underlying combinatorial principles. The class Polynomial Parity Argument (PPA) is the class of NP search problems, where the existence of the solution is guaranteed by the fact that in every finite graph the number of vertices with odd degree is even. The class PPAD is the directed version of PPA, and its basic search problem is the following: in a directed graph, where the in-degree and the out-degree of every vertex is at most one, given a source, find another source or a sink. In the class PPADS the basic search problem is more restricted than in PPAD: given a source, find a sink.

These classes are in fact subfamilies of TFNP, the family of all total NP-search problems, introduced by Megiddo and Papadimitriou [16]. Other important subclasses of TFNP are Polynomial Pigeonhole Principle (PPP) and Polynomial Local Search (PLS). The elements of PPP are problems which by their

combinatorial nature obey the pigeonhole principle and therefore have a solution. In a PLS problem, one is looking for a local optimum for a particular objective function, in some neighborhood structure. All these classes are interesting because they contain search problems not known to be solvable in polynomial time, but which are also somewhat easy in the sense that they can not be NP-hard unless $\text{NP} = \text{co-NP}$.

Another point that makes the parity argument classes interesting is that there are several natural problems from different branches of mathematics that belong to them. For example, in a graph with odd degrees, when a Hamiltonian path is given, a theorem of Smith [25] ensures that there is another Hamiltonian path. It turns out that finding this second path belongs to the class PPA [18]. A search problem coming from a modulo 2 version of Chevalley’s theorem [18] from number theory is also in PPA. Complete problems in PPAD are the search versions of Brouwer’s fixed point theorem, Kakutani’s fixed point theorem, Borsuk-Ulam theorem, and Nash equilibrium (see [18]).

The classical Sperner’s Lemma [22] states that in a triangle with a regular triangulation whose vertices are labelled with three colors, there is always a trichromatic triangle. This lemma is of special interest since some customary proofs for the above topological fixed point theorems rely on its combinatorial content. However, it is unknown whether the corresponding search problem, that Papadimitriou [18] calls **2D-SPERNER**, is complete in PPAD. Variants of Sperner’s Lemma also give rise to other problems in the parity argument classes. Papadimitriou [18] has proven that a 3-dimensional analogue of **2D-SPERNER** is in fact complete in PPAD.

The study of query complexities of the black-box versions of several problems in TFNP is an active field of research. Several recent results point into the direction that quantum algorithms can give only a limited speedup over deterministic ones in this framework. The collision lower bound of Aaronson [1] and Shi [20] about PPP, and the recent result of Santha and Szegedy [19] on PLS imply that the respective deterministic and quantum complexities are polynomially related. As a consequence, if an efficient quantum algorithm exists for a problem in these classes, it must exploit its specific structure. In a related issue, Buhrman-Oppenheimer and Morioka [8] have obtained relative separation results among PLS and the polynomial parity argument classes.

2 Results

A *black-box problem* is a relation $R \subseteq S \times T$ where T is a finite set and $S \subseteq \Sigma^n$ for some finite set Σ . The oracle input is a function $x \in S$, hidden by a black-box, such that x_i , for $i \in \{1, \dots, n\}$ can be accessed via a query parameterized by i . The output of the problem is some $y \in T$ such that $(x, y) \in R$. A special case is the *functional oracle problem* when the relation is given by a function $A : S \rightarrow T$, the (unique) output is then $A(x)$. We say that A is *total* if $S = \Sigma^n$.

In the query model of computation each query adds one to the complexity of the algorithm, but all other computations are free. The state of the computation

is represented by three registers, the query register $i \in \{1, \dots, n\}$, the answer register $a \in \Sigma$, and the work register z . The computation takes place in the vector space spanned by all basis states $|i\rangle|a\rangle|z\rangle$. In the *quantum query model* introduced by Beals et al. [4] the state of the computation is a complex combination of all basis states which has unit length in the norm l_2 . In the randomized model it is a non-negative real combination of unit length in the norm l_1 , and in the deterministic model it is always one of the basis states.

The query operation O_x maps the basis state $|i\rangle|a\rangle|z\rangle$ into the state $|i\rangle|(a + x_i) \bmod |\Sigma||z\rangle$ (here we identify Σ with the residue classes $\bmod |\Sigma|$). Non-query operations are independent of x . A *k-query algorithm* is a sequence of $(k + 1)$ operations (U_0, U_1, \dots, U_k) where U_i is unitary in the quantum and stochastic in the randomized model, and it is a permutation in the deterministic case. Initially the state of the computation is set to some fixed value $|0\rangle|0\rangle|0\rangle$, and then the sequence of operations $U_0, O_x, U_1, O_x, \dots, U_{k-1}, O_x, U_k$ is applied. A quantum or randomized algorithm computes (with two-sided error) R if the observation of the appropriate last bits of the work register yield some $y \in T$ such that $(x, y) \in R$ with probability at least $2/3$. Then $\text{QQC}(R)$ (resp. $\text{RQC}(R)$) is the smallest k for which there exists a k -query quantum (resp. randomized) algorithm which computes R . In the case of deterministic algorithms of course exact computation is required, and the deterministic query complexity $\text{DQC}(R)$ is defined then analogously. We have $\text{DQC}(R) \geq \text{RQC}(R) \geq \text{QQC}(R)$.

Beals et al. [4] have shown that in the case of total functional oracle problems the deterministic and quantum complexities are polynomially related. For several partial functional problems exponential quantum speedups are known [10, 21].

In this paper we will give several results about Sperner problems in the black-box framework. In Section 5, we will prove that the deterministic query complexity of **REGULAR 2-SPM**, the black-box version of **2D-SPERNER** is $O(\sqrt{n})$. This matches the deterministic $\Omega(\sqrt{n})$ lower bound of Crescenzi and Silvestri [9]. The tightness of this bound was not known before. In fact, this result is the corollary of a general algorithm that solves the Sperner problems over pseudo-manifolds of arbitrary dimension. The complexity analysis of the algorithm will be expressed in **Theorem 4** in two combinatorial parameters of the pseudo-manifold: the size of its boundary and the separation number of its skeleton graph. In Section 6, we show that quantum, probabilistic, and deterministic query complexities of **REGULAR 2-SPM** are polynomially related. More precisely, in **Theorem 8** we will prove that its randomized complexity is $\Omega(\sqrt[4]{n})$ and that its quantum complexity is $\Omega(\sqrt[3]{n})$. This result is analogous to the polynomial relations obtained for the respective query complexities of PPP and PLS. Because of lack of space, most proofs are absent from this extended abstract, but can be found in the full paper.

3 Mathematical background on simplicial complexes

For an undirected graph $G = (V, E)$, and for a subset $V' \subseteq V$ of the vertices, we denote by $G[V']$ the induced subgraph of G by V' . A graph $G'' = (V'', E'')$

is a subgraph of G , in notation $G'' \subseteq G$, if $V'' \subseteq V$ and $E'' \subseteq E$. The ring $\mathbb{Z}/(2)$ denotes the ring with 2 elements.

Definition 1 (Simplicial complex) A simplicial complex K is a non-empty collection of subsets of a finite set U , such that whenever $S \in K$ then $S' \in K$ for every $S' \subseteq S$. An element S of K of cardinality $d + 1$ is called a d -simplex. A d' -simplex $S' \subseteq S$ is called a d' -face of S . We denote by K_d the set of d -simplices of K . An elementary d -complex is a simplicial complex that contains exactly one d -simplex and its subsets. The dimension of K , denoted by $\dim(K)$, is the largest d such that K contains a d -simplex. The elements of K_0 are called the vertices of K , and the elements of K_1 are called the edges of K . The skeleton graph $G_K = (V_K, E_K)$ is the graph whose vertices are the vertices of K , and the edges are the edges of K .

Without loss of generality, we suppose that U consists of integers, and we identify $\{u\}$ with u , for $u \in U$.

Fact 1 Let d be a positive integer. If S is an elementary d -complex, then G_S is the complete graph.

Definition 2 (Oriented Simplex) For every positive integer n , we define an equivalence relation \equiv_n over \mathbb{Z}^n , by $a \equiv_n b$ if there exists an even permutation σ such that $\sigma \cdot a = b$. For every $a \in \mathbb{Z}^n$ we denote by $[a]_{\equiv_n}$ the equivalence class of a for \equiv_n . The two equivalence classes of the orderings of the 0-faces of a simplex are called its orientations. An oriented simplex is a pair formed of a simplex and one of its orientations.

For an oriented d -simplex $(S, [\tau]_{\equiv_{d+1}})$, where τ is an ordering of the 0-faces of S , and a permutation σ over $\{1, \dots, d + 1\}$, we denote by $\sigma \cdot (S, [\tau]_{\equiv_{d+1}})$ the oriented d -simplex $(S, [\sigma \cdot \tau]_{\equiv_{d+1}})$. For every integer d , and every simplicial complex K whose simplices have been oriented, we denote by K_d the set of oriented d -simplices of K . From now on, S may denote an oriented or a non-oriented simplex. When S is an oriented simplex, \bar{S} will denote the same simplex with the opposite orientation. We also define $S^{(i)}$ to be S if i is even, and to be \bar{S} if i is odd. We will often specify an oriented simplex by an ordering of its 0-faces.

Definition 3 Let $S = (v_0, \dots, v_d)$ be an oriented d -simplex. For every $0 \leq i \leq d$, for every $(d - 1)$ -face $\{v_0, \dots, v_{i-1}, v_{i+1}, \dots, v_d\}$ of S , the induced orientation is the oriented $(d - 1)$ -simplex $(v_0, \dots, v_{i-1}, v_{i+1}, \dots, v_d)^{(i)}$.

Definition 4 Let K be a simplicial complex whose simplices have been oriented, and let R be a ring. We define $C_d(K; R)$ as the submodule of the free R -module over the d -simplices of K with both possible orientations, whose elements are of the form $\sum_{S \in K_d} (c_S \cdot S + c_{\bar{S}} \cdot \bar{S})$, with $c_S \in R$, satisfying the relation $c_S = -c_{\bar{S}}$. The elements of $C_d(K; R)$ are called d -chains. For every oriented simplex S of K , we denote by $\langle S \rangle$ the element $S - \bar{S}$ of $C_d(K; R)$.

Let S be an oriented d -simplex (v_0, v_1, \dots, v_d) of K . The algebraic boundary of $\langle S \rangle$, denoted by $\partial_d \langle S \rangle$, is the $(d-1)$ -chain of $C_{d-1}(K; R)$ defined as $\partial_d \langle S \rangle = \sum_{i=0}^d (-1)^i \langle (v_0, \dots, v_{i-1}, v_{i+1}, \dots, v_d) \rangle$.

Since $\partial_d \langle S \rangle = -\partial_d \langle \bar{S} \rangle$, the operator ∂_d has been correctly defined on a basis of $C_d(K; R)$ and can therefore be uniquely extended into a homomorphism $\partial_d : C_d(K; R) \rightarrow C_{d-1}(K; R)$. The proof of the next Lemma is straightforward.

Lemma 1 *Let S be an oriented d -simplex of a simplicial complex K . Denote by F_S the set of $(d-1)$ -faces of S , and for every $S' \in F_S$ by $\tau_{S'}^S$ the induced orientation on S' . Then $\partial_d \langle S \rangle = \sum_{S' \in F_S} \langle (S', \tau_{S'}^S) \rangle$.*

Following an early version of a paper of Bloch [7], in the next definition we generalize the notion of pseudo-manifold, without the usual requirements of connectivity and pure dimensionality.

Definition 5 *A simplicial complex \mathcal{M} is a pseudo d -manifold, for a positive integer d , if (i) \mathcal{M} is a union of elementary d -complexes, and (ii) every $(d-1)$ -simplex in \mathcal{M} is a $(d-1)$ -face of at most two d -simplices of \mathcal{M} . The boundary of \mathcal{M} is the set of elementary $(d-1)$ -complexes in \mathcal{M} that belong exactly to one d -simplex of \mathcal{M} . We denote it by $\partial \mathcal{M}$. A pseudo d -manifold \mathcal{M} is said to be orientable if it is possible to assign an orientation to each d -simplex of \mathcal{M} , such that for all $(d-1)$ -simplex of \mathcal{M} that is not on its boundary the orientations induced by the two d -simplices to which it belongs are opposite. Such a choice of orientations for all the d -simplices of \mathcal{M} makes \mathcal{M} oriented.*

If the d -simplices of \mathcal{M} are oriented, then there is a natural orientation of the $(d-1)$ -simplices of $\partial \mathcal{M}$, where each $(d-1)$ -simplex has the orientation induced by the oriented d -simplex of which it is a $(d-1)$ -face. Notice that if \mathcal{M} is a pseudo d -manifold, then $\partial \mathcal{M}$ need not be a pseudo $(d-1)$ -manifold. From now, all the simplicial complexes will be pseudo-manifolds. Observe that if $R = \mathbb{Z}/(2)$, then for any oriented d -simplex S , we have $\langle S \rangle = \langle \bar{S} \rangle$.

Definition 6 *Given a simplicial complex K of dimension d , the standard d -chain \widehat{K} of K will be defined depending on whether K is oriented as follows:*
– if K is non-oriented, then $\widehat{K} = \sum_{S \in K_d} \langle (S, \tau_S) \rangle \in C_d(K, \mathbb{Z}/(2))$, for an arbitrary choice of orientations τ_S of the d -simplices S in K ,
– if K is oriented, then $\widehat{K} = \sum_{S \in K_d} \langle (S, \tau_S) \rangle \in C_d(K, \mathbb{Z})$ where τ_S is the orientation of S in K .

Fact 2 *Let d be an integer, and let \mathcal{M} be a pseudo d -manifold. Then, if \mathcal{M} is not oriented the equality $\widehat{\partial \mathcal{M}} = \partial_d \widehat{\mathcal{M}}$ holds in $C_{d-1}(\partial \mathcal{M}, \mathbb{Z}/(2))$, and if \mathcal{M} is oriented the equality $\widehat{\partial \mathcal{M}} = \partial_d \widehat{\mathcal{M}}$ holds in $C_{d-1}(\partial \mathcal{M}, \mathbb{Z})$.*

4 Sperner Problems

We state now a very general form of Sperner's Lemma due to Fan [11]. The exact formulation of the statement we reproduce here was given by Taylor in [24].

Definition 7 Let K be a simplicial complex. A labelling of K is a mapping ℓ of the vertices of K into the set $\{0, \dots, \dim(K)\}$. If a simplex S of K is labelled with all possible labels, then we say that S is fully labelled.

A labelling ℓ naturally maps every oriented d -simplex $S = (v_0, \dots, v_d)$ to the equivalence class $\ell(S) = [\ell(v_0), \dots, \ell(v_d)]_{\equiv_{d+1}}$.

Definition 8 Given a labelling ℓ of a simplicial complex K , and an integer $0 \leq d \leq \dim(K)$, we define the d -dimensional flow $N_d[\langle S \rangle]$ by $N_d[\langle S \rangle] = 1$ if $\ell(S) = [(0, 1, 2, \dots, d)]_{\equiv_{d+1}}$, $N_d[\langle S \rangle] = -1$ if $\ell(S) = [(1, 0, 2, \dots, d)]_{\equiv_{d+1}}$, and $N_d[\langle S \rangle] = 0$ otherwise, and then extend it by linearity into a homomorphism $N_d : C_d(K; R) \rightarrow R$.

Theorem 1 (Sperner's Lemma [22, 11, 24]) Let K be a simplicial complex of dimension d , let ℓ be a labelling of K , and let R be a ring. For an element C of $C_d(K; R)$, we have $N_d[C] = (-1)^d N_{d-1}[\partial_d C]$.

Using Fact 2, we translate Theorem 1 into terms of pseudo-manifolds.

Theorem 2 (Sperner's Lemma on pseudo-manifolds) Let d be an integer, let \mathcal{M} be a pseudo d -manifold, and let ℓ be a labelling of \mathcal{M} . Then $N_d[\widehat{\mathcal{M}}] = (-1)^d N_{d-1}[\partial \widehat{\mathcal{M}}]$ where $\widehat{\mathcal{M}} \in C_d(\mathcal{M}, \mathbb{Z}/(2))$, $\partial \widehat{\mathcal{M}} \in C_{d-1}(\partial \mathcal{M}, \mathbb{Z}/(2))$ if \mathcal{M} is not oriented, and $\widehat{\mathcal{M}} \in C_d(\mathcal{M}, \mathbb{Z})$, $\partial \widehat{\mathcal{M}} \in C_{d-1}(\partial \mathcal{M}, \mathbb{Z})$ if \mathcal{M} is oriented.

This version of Sperner's lemma can be viewed, from a physicist's point of view, as a result equivalent to a global conservation law of a flow. If there is a source for the flow and the space is bounded then there must be a sink for that flow. More concretely, the lines of flow can be drawn over d -simplices, that goes from one d -simplex to another if they share a $(d-1)$ -face that has all possible labels in $\{0, \dots, d-1\}$. The sources and sinks of the flow are the fully labelled d -simplices. The lemma basically says that if the amount of flow entering the manifold at the boundary is larger than the exiting flow, then there must exist sinks inside. The local conservation is stated by the fact that if there is an ingoing edge, there will not be two outgoing edges, and conversely. Formally, we have the following.

Fact 3 Let (S, τ_S) be an oriented d -simplex. Then at most two of its oriented $(d-1)$ -faces have a non-zero image by N_{d-1} . Moreover, if there are exactly two $(d-1)$ -faces $(S', \tau_{S'})$ and $(S'', \tau_{S''})$ that have non-zero image by N_{d-1} , then $N_d[\langle (S, \tau_S) \rangle] = 0$ and $N_{d-1}[\langle (S', \tau_{S'}) \rangle] = -N_{d-1}[\langle (S'', \tau_{S''}) \rangle]$.

This gives a relation between the problem of finding fully labelled d -simplices and the natural complete problems for the parity argument classes. We can consider an oriented d -simplex (S, τ_S) with $N_d[\langle (S, \tau_S) \rangle] = 1$ as a source for the flow, and $(S', \tau_{S'})$ with $N_d[\langle (S', \tau_{S'}) \rangle] = -1$ as a sink.

We now state the non-oriented black-box Sperner problems we will consider. The statement of d -OSPM, the general oriented problem can be found in the full paper.

Sperner on Pseudo d -Manifolds (d -SPM)

Input: a pseudo d -manifold \mathcal{M} , and $S \in \mathcal{M}_d$.

Oracle input: a labelling $\ell : \mathcal{M}_0 \rightarrow \{0, 1, \dots, d\}$.

Promise: one of the two conditions holds, with $R = \mathbb{Z}/(2)$:

a) $N_{d-1}[\partial \widehat{\mathcal{M}}] = 1$,

b) $N_{d-1}[\partial \widehat{\mathcal{M}}] = 0$ and $N_d[\langle S \rangle] = 1$.

Output: $S' \in \mathcal{M}_d$ such that $N_d[\langle S' \rangle] = 1$, with $S \neq S'$ for case b.

We will deal in particular with the following important special case of **2-SPM**.

Let $V_m = \{(i, j) \in \mathbb{N}^2 \mid 0 \leq i + j \leq m\}$. Observe that $|V_m| = \binom{m+2}{2}$.

Regular Sperner (REGULAR 2-SPM)

Input: $n = \binom{m+2}{2}$ for some integer m .

Oracle input: a labelling $\ell : V_m \rightarrow \{0, 1, 2\}$.

Promise: for $0 \leq k \leq m$, $\ell(0, k) \neq 1$, $\ell(k, 0) \neq 0$, and $\ell(k, m - k) \neq 2$.

Output: p, p' and $p'' \in V$, such that $p' = p + (\varepsilon, 0)$, $p'' = p + (0, \varepsilon)$ for some $\varepsilon \in \{-1, 1\}$, and $\{\ell(p), \ell(p'), \ell(p'')\} = \{0, 1, 2\}$.

In fact, **REGULAR 2-SPM** on input $n = \binom{m+2}{2}$ is the instance of **d -SPM** on the regular m -subdivision of an elementary 2-simplex. Theorem 2 states that both **d -SPM** and **d -OSPM** have always a solution. The solution is not necessarily unique as it can be easily checked on simple instances. Thus the problems are not functional oracle problems.

5 Black-box algorithms for pseudo d -manifolds

The purpose of this section is to give a black-box algorithm for **d -SPM**. The corresponding algorithm for **d -OSPM** can be found in the full paper. To solve these problems, we adopt a divide and conquer approach. This kind of approach was successfully used in [15, 14] and [19], to study the query complexity of the oracle version of the Local Search problem. However, the success of the divide and conquer paradigm for Sperner problems relies heavily on the use of the very strong statement of Sperner's Lemma that is given in Theorem 2. The usual, simpler version of Sperner's Lemma, like the one given in [18] does not appear to be strong enough for this purpose. Observe that though the standard proof of Sperner's Lemma is constructive, it yields only an algorithm of complexity $O(n)$. In our algorithms the division of the pseudo d -manifold \mathcal{M} will be done according to the combinatorial properties of its skeleton graph. The particular parameter we will need is its *iterated separation number* that we introduce now for general graphs.

Definition 9 Let $G = (V, E)$ be a graph. If A and C are subsets of V such that $V = A \cup C$, and that there is no edge between $A \setminus C$ and $C \setminus A$, then (A, C) is said to be a *separation* of the graph G , in notation $(A, C) \prec G$. The set $A \cap C$ is called a *separator* of the graph G .

The iterated separation number is defined by induction on the size of the graph G by $s(G) = \min_{(A, C) \prec G} \{|A \cap C| + \max(s(G[A \setminus C]), s(G[C \setminus A]))\}$. A

pair $(A, C) \prec G$ such that $s(G) = |A \cap C| + \max(s(G[A \setminus C]), s(G[C \setminus A]))$ is called a best separation of G .

The iterated separation number of a graph is equal to the *value of the separation game* on the graph G , which was introduced in [15]. In that article, that value was defined as the gain of a player in a certain game. Notice, also, that the iterated separation number is at most $\log |V|$ times the *separation number* as defined in [19]. Before giving the algorithms, and their analyses, we still need a few observations.

Lemma 2 *Let \mathcal{A} and \mathcal{B} be two pseudo d -manifolds, such that $\mathcal{A} \cup \mathcal{B}$ is also a pseudo d -manifold. Let ℓ be a labelling of $\mathcal{A} \cup \mathcal{B}$. If \mathcal{A} and \mathcal{B} have no d -simplex in their intersection, then $N_d[\widehat{\mathcal{A} \cup \mathcal{B}}] = N_d[\widehat{\mathcal{A}}] + N_d[\widehat{\mathcal{B}}]$.*

Lemma 3 *Let \mathcal{M} be a pseudo d -manifold, and \mathcal{M}' be a union of elementary d -complexes such that $\mathcal{M}' \subseteq \mathcal{M}$. Then \mathcal{M}' is a pseudo d -manifold.*

Theorem 3 *Let \mathcal{M} be a pseudo d -manifold, H a subset of \mathcal{M}_0 , and ℓ be a labelling of the vertices of \mathcal{M} . Let $(A, C) \prec G_{\mathcal{M}}[\mathcal{M}_0 \setminus H]$, $B = H \cup (A \cap C)$, and $M' = A \setminus C$ and $M'' = C \setminus A$. Denote by \mathcal{B} the set of elementary d -complexes of \mathcal{M} whose vertices are all in B , and by \mathcal{M}' (resp. \mathcal{M}'') the set of elementary d -complexes of which at least one of the vertices belongs to M' (resp. M''). Denote also by \mathcal{B}' the set of elementary $(d-1)$ -complexes of \mathcal{M} whose vertices are all in B . Then,*

- (i) \mathcal{B} , \mathcal{M}' , \mathcal{M}'' and $\mathcal{M}' \cup \mathcal{M}''$ are pseudo d -manifolds,
- (ii) if $H \neq \mathcal{M}_0$ then \mathcal{B} , \mathcal{M}' and \mathcal{M}'' are proper subsets of \mathcal{M} ,
- (iii) $N_d[\widehat{\mathcal{M}}] = N_d[\widehat{\mathcal{B}}] + N_d[\widehat{\mathcal{M}'}] + N_d[\widehat{\mathcal{M}''}]$,
- (iv) the inclusions $\partial \mathcal{M}' \subseteq (\partial \mathcal{M}) \cup \mathcal{B}'$ and $\partial \mathcal{M}'' \subseteq (\partial \mathcal{M}) \cup \mathcal{B}'$ hold,

We are now ready to state Algorithm 1 which solves d -SPM when the labels of the 0-faces of $\partial \mathcal{M}$ are also known. The analogous Algorithm 2 for d -OSPM can be again found in the full paper. We next give the result which states the correctness of our algorithms and specifies their complexities.

Lemma 4 *If \mathcal{M} and S satisfy the promises of the respective Sperner problems, then Algorithms 1 and 2 return a solution and use at most $s(G_{\mathcal{M}}[\mathcal{M}_0 \setminus H])$ queries.*

Theorem 4 $\text{DQC}(d\text{-SPM}) = O(s(G_{\mathcal{M}}[\mathcal{M}_0 \setminus (\partial \mathcal{M})_0])) + |(\partial \mathcal{M})_0|$ and $\text{DQC}(d\text{-OSPM}) = O(s(G_{\mathcal{M}}[\mathcal{M}_0 \setminus (\partial \mathcal{M})_0])) + |(\partial \mathcal{M})_0|$.

Proof. The algorithms consist in querying the labels of the vertices of $\partial \mathcal{M}$ and then running respectively Algorithm 1 or Algorithm 2 with the initial choice $H = (\partial \mathcal{M})_0$.

To bound the complexity of our algorithms we need an upper-bound on the iterated separator number of the skeleton graph. The following theorem gives, for any graph, an upper bound on the size of a balancing separator, whose deletion leaves the graph with two roughly equal size components. The bound depends on the genus and the number of vertices of the graph.

Algorithm 1 Main routine for solving d -SPM.

Input: A pseudo d -manifold \mathcal{M} , $S \in \mathcal{M}_d$, a set $H \supseteq (\partial\mathcal{M})_0$ together with the labels of its elements.

Let $(A, C) \prec G_{\mathcal{M}}[\mathcal{M}_0 \setminus H]$ be a best separation, and $B = H \cup (A \cap C)$.

Let the complexes \mathcal{B} , \mathcal{M}' and \mathcal{M}'' be defined as in Theorem 3.

Query the labels of the vertices in $A \cap C$.

if \mathcal{B} contains a fully labelled elementary d -complex **then**

 Return the corresponding oriented d -simplex.

end if

Evaluate $N_{d-1}[\widehat{\partial\mathcal{B}}]$, $N_{d-1}[\widehat{\partial\mathcal{M}'}]$ and $N_{d-1}[\widehat{\partial\mathcal{M}''}]$.

if $N_{d-1}[\widehat{\partial K}] = 1$ for $K \in \{\mathcal{B}, \mathcal{M}', \mathcal{M}''\}$ **then**

 Iterate on K , any d -simplex $S \in K$, and B with the labels of its elements.

else

 Iterate on $K \in \{\mathcal{B}, \mathcal{M}', \mathcal{M}''\}$ containing S , S and B with the labels of its elements.

end if

Theorem 5 (Gilbert, Hutchinson, Tarjan [12]) *A graph of genus g with n vertices has a set of at most $6\sqrt{g \cdot n} + 2\sqrt{2n} + 1$ vertices whose removal leaves no component with more than $2n/3$ vertices.*

For our purposes we can immediately derive an upper bound on the iterated separation number.

Corollary 1 *For graphs $G = (V, E)$ of size n and genus g we have $s(G) \leq \lambda(6\sqrt{g \cdot n} + 2\sqrt{2n}) + \log_{3/2} n$, where λ is solution of $\lambda = 1 + \lambda\sqrt{2/3}$.*

In general, there is no immediate relationship between the genus of a pseudo d -manifold and the genus of its skeleton graph. However, if the pseudo d -manifold \mathcal{M} is a triangulated oriented surface, then the genus of the graph is equal to the genus of \mathcal{M} . Used in conjunction with Corollary 1, Theorem 4 gives an effective upper bound for pseudo d -manifolds.

Corollary 2 *Let \mathcal{M} be a pseudo d -manifold such that $G_{\mathcal{M}}$ is of size n and of genus g . Then, $\text{DQC}(d\text{-SPM}) = O(\sqrt{g}) \cdot \sqrt{n} + |(\partial\mathcal{M})_0|$ and $\text{DQC}(d\text{-OSPM}) = O(\sqrt{g}) \cdot \sqrt{n} + |(\partial\mathcal{M})_0|$.*

Since the skeleton graph of the underlying pseudo 2-manifold of **REGULAR 2-SPM** is planar, it has genus 0. Thus we get:

Theorem 6 $\text{DQC}(\text{REGULAR 2-SPM}) = O(\sqrt{n})$.

In the next section, we show nontrivial lower bounds on the randomized and the quantum query complexity of the **REGULAR 2-SPM** problem. Observe that for some general instances of the **2-SPM** over the same pseudo 2-manifold we can easily derive exact lower bounds from the known complexity of Grover's search problem [6]. For example, if a labelling is 2 everywhere, except on two consecutive vertices on the boundary where it takes respectively the values 0 and 1, then finding a fully labelled 2-simplex is of the same complexity as finding a distinguished element on the boundary.

6 Lower bounds for REGULAR 2-SPM

We denote by **UNIQUE-SPERNER** all those instances of **REGULAR 2-SPM** for which there exists a unique fully labelled triangle. There exist several equivalent adversary methods for proving quantum lower bounds in the query model [23]. Here, we will use the weighted adversary method [2, 3, 13].

Theorem 7 *Let Σ be a finite set, let $n \geq 1$ be an integer, and let $S \subseteq \Sigma^n$ and S' be sets. Let $f : S \rightarrow S'$. Let Γ be an arbitrary $S \times S$ nonnegative symmetric matrix that satisfies $\Gamma[x, y] = 0$ whenever $f(x) \neq f(y)$. For $1 \leq k \leq n$, let Γ_k be the matrix such that $\Gamma_k[x, y] = 0$ if $x_k = y_k$, and $\Gamma_k[x, y] = \Gamma[x, y]$ otherwise. For all $S \times S$ matrix M and $x \in S$, let $\sigma(M, x) = \sum_{y \in S} M[x, y]$. Then*

$$\text{QQC}(f) = \Omega \left(\min_{\Gamma[x, y] \neq 0, x_k \neq y_k} \sqrt{\frac{\sigma(\Gamma, x)\sigma(\Gamma, y)}{\sigma(\Gamma_k, x)\sigma(\Gamma_k, y)}} \right),$$

$$\text{RQC}(f) = \Omega \left(\min_{\Gamma[x, y] \neq 0, x_k \neq y_k} \max \left(\frac{\sigma(\Gamma, x)}{\sigma(\Gamma_k, x)}, \frac{\sigma(\Gamma, y)}{\sigma(\Gamma_k, y)} \right) \right).$$

For the lower bound we will consider specific instances of **REGULAR 2-SPM**. For that, we need a few definitions. For any binary sequence b , let $|b|$ denote the length of the sequence b , and for $i = 0, 1$ let $w_i(b)$ be the number of bits i in b . For $0 \leq t \leq |b|$, let $b^t = b_1 \dots b_t$ denote the prefix of length t of b .

The instances of **REGULAR 2-SPM** we will consider are those whose oracle inputs C_b are induced by binary sequences $b = b_1 \dots b_{m-2}$ of length $m - 2$ as follows:

$$C_b(i, j) = \begin{cases} 1 & \text{if } j = 0 \text{ and } i \neq 0, \\ 2 & \text{if } i = 0 \text{ and } j \neq m, \\ 0 & \text{if } i + j = m \text{ and } j \neq 0, \\ 1 & \text{if there exists } 0 \leq t \leq m - 2 \text{ with } (i, j) = (w_0(b^t) + 1, w_1(b^t)), \\ 2 & \text{if there exists } 0 \leq t \leq m - 2 \text{ with } (i, j) = (w_0(b^t), w_1(b^t) + 1), \\ 0 & \text{otherwise.} \end{cases}$$

Notice that the first and fourth (*resp.* second and fifth) conditions can be simultaneously satisfied, but the labelling definition is consistent. Also observe that, for any b , there is a unique fully labelled triangle, whose coordinates are $\{(w_0(b) + 1, w_1(b)), (w_0(b), w_1(b) + 1), (w_0(b) + 1, w_1(b) + 1)\}$. Therefore C_b is an instance of **UNIQUE-SPERNER**. We illustrate an instance of C_b in Figure 1.

It turns out that technically it will be easier to prove the lower bound for a problem which is closely related to the above instances of **REGULAR 2-SPM**, that we call **SNAKE**. Recall that $V_m = \{(i, j) \in \mathbb{N}^2 \mid 0 \leq i + j \leq m\}$. For every binary sequence $b = b_1 \dots b_{m-2}$, we denote by O_b the function $V_m \rightarrow \{0, 1\}$ defined for $p \in V_m$ by

$$O_b(p) = \begin{cases} 1 & \text{if there exists } 0 \leq t \leq m - 2 \text{ with } (i, j) = (w_0(b^t) + 1, w_1(b^t)), \\ 0 & \text{otherwise.} \end{cases}$$

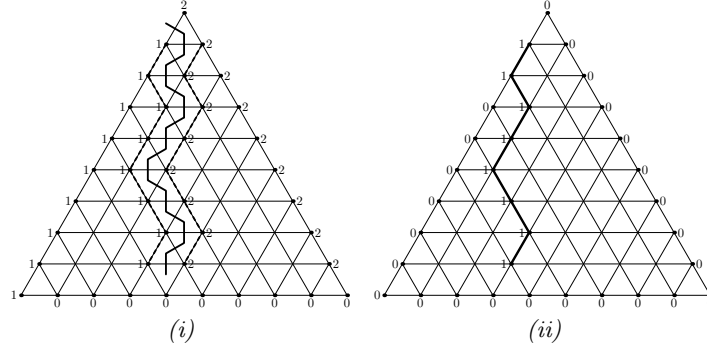


Fig. 1: In the coordinates system of the Figure, the point $(0,0)$ is the highest corner of the triangles, the x coordinates increase by going down and left, and the y coordinates increase by going down and right. On sub-figure (i), the labelling C_b corresponds to the binary sequence $b = 0100110$. On sub-figure (ii), the labelling O_b corresponds to the same sequence b . The unmarked vertices are all labelled 0.

See again Figure 1 for an example.

SNAKE

Input: $n = \binom{m}{2}$ for some integer m .

Oracle input: a function $f : V_m \rightarrow \{0, 1\}$.

Promise: there exists a binary sequence $b = b_1 \dots b_{m-2}$ such that $f = O_b$.

Output: $(w_0(b), w_1(b))$.

We recall here the definition of [19] of c -query reducibility between black-box problems, which we will use to prove our lower bound.

Definition 10 For an integer $c > 0$, a functional oracle problem $A : S_1 \rightarrow T_1$ with $S_1 \subseteq \Sigma_1^n$ is c -query reducible to a functional oracle problem $B : S_2 \rightarrow T_2$ with $S_2 \subseteq \Sigma_2^{n'}$ if the following two conditions hold:

- (i) $\exists \alpha : S_1 \rightarrow S_2, \exists \beta : T_2 \rightarrow T_1$, such that $\forall x \in S_1, A(x) = \beta(B(\alpha(x)))$,
- (ii) $\exists \gamma_1, \dots, \gamma_c : \{1, \dots, n'\} \rightarrow \{1, \dots, n\}$ and $\gamma : \{1, \dots, n'\} \times \Sigma_1^c \rightarrow \Sigma_2$ such that $\forall x \in S_1, k \in \{1, \dots, n'\}, \alpha(x)(k) = \gamma(k, x_{\gamma_1(k)}, \dots, x_{\gamma_c(k)})$.

Lemma 5 ([19]) If A is c -query reducible to B then $\text{QQC}(B) \geq \text{QQC}(A)/2c$, and $\text{RQC}(B) \geq \text{RQC}(A)/c$.

Lemma 6 **SNAKE** is 3-query reducible to **UNIQUE-SPERNER**.

Lemma 7 $\text{RQC}(\text{SNAKE}) = \Omega(\sqrt[4]{n})$ and $\text{QQC}(\text{SNAKE}) = \Omega(\sqrt[3]{n})$.

Theorem 8 The query complexity of **REGULAR 2-SPM** satisfies $\text{RQC}(\text{REGULAR 2-SPM}) = \Omega(\sqrt[4]{n})$ and $\text{QQC}(\text{REGULAR 2-SPM}) = \Omega(\sqrt[3]{n})$.

Proof. By Lemma 5 and 6, the lower bounds of Lemma 7 for **SNAKE** also apply to **REGULAR 2-SPM**.

References

1. S. Aaronson. Quantum lower bound for the collision problem. In *34th STOC*, pp. 635–642, 2002.
2. S. Aaronson. Lower bounds for local search by quantum arguments. In *36th STOC*, pp. 465–474, 2004.
3. A. Ambainis. Polynomial degree vs. quantum query complexity. In *44th FOCS*, pp. 230–239, 2003.
4. R. Beals, H. Buhrman, R. Cleve, M. Mosca and R. de Wolf. Quantum lower bounds by polynomials. *J. of the ACM* (48):4, pp. 778–797, 2001.
5. P. Beame, S. Cook, J. Edmonds, R. Impagliazzo and T. Pitassi. The relative complexity of NP search problems. *J. Comput. System Sci.*, 57(1):3–19, 1998.
6. C. Bennett, E. Bernstein, G. Brassard and U. Vazirani. Strength and weaknesses of quantum computing. *SIAM J. on Computing*, 26(5):1510–1523, 1997.
7. E. Bloch. Mod 2 degree and a generalized no retraction Theorem. To appear in *Mathematische Nachrichten*.
8. J. Buresh-Oppenheim and T. Morioka. Relativized NP search problems and propositional proof systems. In *19th Conference on Computational Complexity*, pp. 54–67, 2004.
9. P. Crescenzi and R. Silvestri. Sperner’s lemma and robust machines. *Comput. Complexity*, 7(2):163–173, 1998.
10. D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. of the Royal Society A*, volume 439, 1985.
11. K. Fan. Simplicial maps from an orientable n -pseudomanifold into S^m with the octahedral triangulation. *J. Combinatorial Theory*, 2:588–602, 1967.
12. J. Gilbert, J. Hutchinson and R. Tarjan. A separator theorem for graphs of bounded genus. *J. Algorithms*, 5(3):391–407, 1984.
13. S. Laplante and F. Magniez. Lower bounds for randomized and quantum query complexity using kolmogorov arguments. In *19th Conference on Computational Complexity*, pp. 294–304, 2004.
14. D. Llewellyn and C. Tovey. Dividing and conquering the square. *Discrete Appl. Math.*, 43(2):131–153, 1993.
15. D. Llewellyn, C. Tovey and M. Trick. Local optimization on graphs. *Discrete Appl. Math.*, 23(2):157–178, 1989.
16. N. Megiddo and C. Papadimitriou. On total functions, existence theorems and computational complexity. *Theoret. Comput. Sci.*, 81:317–324, 1991.
17. C. Papadimitriou. On graph-theoretic lemmata and complexity classes. In *31st FOCS*, pp. 794–801, 1990.
18. C. Papadimitriou. On the complexity of the parity argument and other inefficient proofs of existence. *J. Comput. System Sci.*, 48(3):498–532, 1994.
19. M. Santha and M. Szegedy. Quantum and classical query complexities of local search are polynomially related. In *36th STOC*, pp. 494–501, 2004.
20. Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. In *43rd FOCS*, pp. 513–519, 2002.
21. D. Simon. On the power of quantum computation. *SIAM J. on Computing* (26):5, pp. 1474–1783, 1997.
22. E. Sperner. Neuer Beweis für die Invarianz der Dimensionzahl und des Gebietes. *Abh. Math. Sem. Hamburg Univ.* 6:265–272, 1928.
23. R. Špalek and M. Szegedy. All quantum adversary methods are equivalent. <http://xxx.lanl.gov/abs/quant-ph/0409116>.
24. L. Taylor. Sperner’s Lemma, Brouwer’s Fixed Point Theorem, The Fundamental Theorem of Algebra. <http://www.cs.csubak.edu/~larry/math/sperner.pdf>.
25. A. Thomason. Hamilton cycles and uniquely edge colourable graphs. *Ann. Discrete Math.* 3: 259–268, 1978.