All Classical Adversary Methods are Equivalent for Total Functions

Andris Ambainis
Centre for Quantum Computer Science, Faculty of Computing, University of Latvia, Raiņa 19, Riga, Latvia, LV-1586
andris.ambainis@lu.lv

Martins Kokainis
Centre for Quantum Computer Science, Faculty of Computing, University of Latvia, Raiņa 19, Riga, Latvia, LV-1586
martins.kokainis,krisjanis.prusis@lu.lv

Krišjānis Prūsis
Centre for Quantum Computer Science, Faculty of Computing, University of Latvia, Raiņa 19, Riga, Latvia, LV-1586
krisjanis.prusis@lu.lv

Jevgēnijs Vihrovs
Centre for Quantum Computer Science, Faculty of Computing, University of Latvia, Raiņa 19, Riga, Latvia, LV-1586

Abstract

We show that all known classical adversary lower bounds on randomized query complexity are equivalent for total functions, and are equal to the fractional block sensitivity $\mathrm{fbs}(f)$. That includes the Kolmogorov complexity bound of Laplante and Magniez and the earlier relational adversary bound of Aaronson. For partial functions, we show unbounded separations between $\mathrm{fbs}(f)$ and other adversary bounds, as well as between the relational and Kolmogorov complexity bounds.

We also show that, for partial functions, fractional block sensitivity cannot give lower bounds larger than $\sqrt{n \cdot \mathrm{bs}(f)}$, where n is the number of variables and $\mathrm{bs}(f)$ is the block sensitivity. Then we exhibit a partial function f that matches this upper bound, $\mathrm{fbs}(f) = \Omega(\sqrt{n \cdot \mathrm{bs}(f)})$.

2012 ACM Subject Classification Theory of computation → Probabilistic computation

Keywords and phrases Randomized Query Complexity, Lower Bounds, Adversary Bounds, Fractional Block Sensitivity

Digital Object Identifier 10.4230/LIPIcs.STACS.2018.8

Funding This work is supported by the ERC Advanced Grant MQC and Latvian State Research Programme NexIT Project No. 1.

Acknowledgements We are grateful to Rahul Jain for igniting our interest in the classical adversary bounds and Srijita Kundu and Swagato Sanyal for helpful discussions. We also thank Jānis Iraids for helpful discussions on block sensitivity versus fractional block sensitivity problem.

1 Introduction

Query complexity of functions is one of the simplest and most useful models of computation. It is used to show lower bounds on the amount of time required to solve a computational task, and to compare the capabilities of the quantum, randomized and deterministic models of

35th Symposium on Theoretical Aspects of Computer Science (STACS 2018).
Editors: Rolf Niedermeier and Brigitte Vallée; Article No. 8; pp. 8:1–8:14

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

computation. Thus, providing lower bounds in the query model is essential in understanding the complexity of computational problems.

In the query model, an algorithm has to compute a function $f : S \to H$, given a string x from $S \subseteq G^n$, where G and H are finite alphabets. With a single query, it can provide the oracle with an index $i \in [n]$ and receive back the value x_i. After a number of queries (possibly, adaptive), the algorithm must compute $f(x)$. The cost of the computation is the number of queries made by the algorithm.

The query complexity of a function f in the deterministic setting is denoted by $\mathrm{D}(f)$ and is also called the decision tree complexity. The two-sided bounded-error randomized and quantum query complexities are denoted by $\mathrm{R}(f)$ and $\mathrm{Q}(f)$, respectively (which means that given any input, the algorithm must produce a correct answer with probability at least 2/3). For a comprehensive survey on the power of these models, see [9], and for the state-of-the-art relationships between them, see [3].

In this work, we investigate the relations among a certain set of lower bound techniques on $\mathrm{R}(f)$, called the classical adversary methods, and how they connect to other well-known lower bounds on the randomized query complexity.

1.1 Known Lower Bounds

One of the first general lower bound methods on randomized query complexity is Yao's minimax principle, which states that it is sufficient to exhibit a hard distribution on the inputs and lower bound the complexity of any deterministic algorithm under such distribution [21]. Yao's minimax principle is known to be optimal for any function but involves a hard-to-describe and hard-to-compute quantity (the complexity of the best deterministic algorithm under some distribution).

More concrete randomized lower bounds are block sensitivity $\mathrm{bs}(f)$ [16] and the approximate degree of the polynomial representing the function $\widetilde{\deg}(f)$ [17] introduced by Nisan and Szegedy. Afterwards, Aaronson extended the notion of the certificate complexity $\mathrm{C}(f)$ (a deterministic lower bound) to the randomized setting by introducing randomized certificate complexity $\mathrm{RC}(f)$ [2]. Following this result, both Tal and Gilmer, Saks and Srinivasan independently discovered the fractional block sensitivity $\mathrm{fbs}(f)$ lower bound [20, 10], which is equal to the fractional certificate complexity $\mathrm{FC}(f)$ measure, as respective dual linear programs. Since these measures are relaxations of block sensitivity and certificate complexity if written as integer programs, they satisfy the following hierarchy:

$$\mathrm{bs}(f) \leq \mathrm{fbs}(f) = \mathrm{FC}(f) \leq \mathrm{C}(f).$$

Perhaps surprisingly, fractional block sensitivity turned out to be equivalent to randomized certificate complexity, $\mathrm{fbs}(f) = \Theta(\mathrm{RC}(f))$. Approximate degree and fractional block sensitivity are incomparable in general, but it has been shown that $\mathrm{fbs}(f) \leq \widetilde{\deg}(f)^2$ [13] and $\widetilde{\deg}(f) \leq \mathrm{bs}(f)^3 \leq \mathrm{fbs}(f)^3$ [16, 7].

Currently one of the strongest lower bounds is the partition bound $\mathrm{prt}(f)$ of Jain and Klauck [12], which is larger than all of the above mentioned randomized lower bounds (even the approximate degree), and the classical adversary methods listed below. Its power is illustrated by the $\textsc{Tribes}_n$ function (an $\textsc{And}$ of $\sqrt{n}$ $\textsc{Or}$s on $\sqrt{n}$ variables), where it gives a tight $\Omega(n)$ lower bound, while all of the other lower bounds give only $O(\sqrt{n})$. Recently, Ben-David and Kothari introduced the randomized sabotage complexity measure $\mathrm{RS}(f)$ [8], which is an even stronger classical lower bound than the partition bound.

In a separate line of research, Ambainis gave a versatile quantum adversary lower bound method with a wide range of applications [4]. Since then, many generalizations of the

quantum adversary method have been introduced (see [19] for a list of known quantum adversary bounds). Several of these formulations have been lifted back to the randomized setting. Aaronson proved a classical analogue of Ambainis' relational adversary bound and used it to provide a lower bound for the local search problem [1]. Laplante and Magniez introduced the Kolmogorov complexity adversary bound for both quantum and classical settings and showed that it subsumes many other adversary techniques. [14]. They also gave a classical variation of Ambainis' adversary bound in a different way than Aaronson. Some of the other adversary methods like spectral adversary have not been generalized back to the randomized setting.

While some relations between the adversary bounds had been known before, Špalek and Szegedy proved that practically all known quantum adversary methods are in fact equivalent [19] (this excludes the general quantum adversary bound, which gives an exact estimate on quantum query complexity for all Boolean functions [11, 18]). This result cannot be immediately generalized to the classical setting, as the equivalence follows through the spectral adversary which has no classical analogue. They also showed that the quantum adversary cannot give lower bounds better than a certain "certificate complexity barrier". Recently, Kulkarni and Tal strengthened the barrier using fractional certificate complexity. Specifically, for any Boolean function f the quantum adversary is at most $\sqrt{\mathrm{FC}^0(f)\,\mathrm{FC}^1(f)}$, if f is total, and at most $2\sqrt{n \cdot \min\{\mathrm{FC}^0(f), \mathrm{FC}^1(f)\}}$, if f is partial [13].[1]

With the advances on the quantum adversary front, one could hope for a similar equivalence result to also hold for the classical adversary bounds. Some relations are known: Laplante and Magniez have shown that the Kolmogorov complexity lower bound is at least as strong as Aaronson's relational and Ambainis' weighted adversary bounds [14]. Jain and Klauck have noted that the minimax over probability distributions adversary bound is at most $\mathrm{C}(f)$ for total functions [12]. In general, the relationships among the classical adversary bounds until this point remained unclear.

1.2 Our Results

Our main result shows that the known classical adversary bounds are all equivalent for total functions. That includes Aaronson's relational adversary bound $\mathrm{CRA}(f)$, Ambainis' weighted adversary bound $\mathrm{CWA}(f)$, the Kolmogorov complexity adversary bound $\mathrm{CKA}(f)$ and the minimax over probability distributions adversary bound $\mathrm{CMM}(f)$. Surprisingly, they are equivalent to the fractional block sensitivity $\mathrm{fbs}(f)$.

We also add to this list a certain restricted version of the relational adversary bound. More specifically, we require that the relation matrix between the inputs has rank 1, and denote this (seemingly weaker) lower bound by $\mathrm{CRA}_1(f)$. Thus for total functions $\mathrm{CRA}(f) = \Theta\left(\mathrm{CRA}_1(f)\right)$, where the latter is much easier to calculate for Boolean functions.

All this shows that $\mathrm{fbs}(f)$ is a fundamental lower bound measure for total functions with many different formulations, including the previously known $\mathrm{FC}(f)$ and $\mathrm{RC}(f)$. Another interesting corollary is that since the quantum certificate complexity $\mathrm{QC}(f) = \Theta(\sqrt{\mathrm{RC}(f)})$ is a lower bound on the quantum query complexity [2], we have that by taking the square root of any of the adversary bounds above, we obtain a quantum lower bound for total functions.

Along the way, for partial functions we show the equivalence between $\mathrm{CRA}(f)$ and $\mathrm{CWA}(f)$, and also between $\mathrm{CKA}(f)$ and $\mathrm{CMM}(f)$. In the case of partial functions, $\mathrm{fbs}(f)$

[1] Here, $\mathrm{FC}^0(f)$ and $\mathrm{FC}^1(f)$ stand for the maximum fractional certificate complexity over negative and positive inputs, respectively.

becomes weaker than all these adversary methods. In particular, we show an example of a function where each of these adversary methods gives an $\Omega(n)$ lower bound, while fractional block sensitivity is $O(1)$. We also show that $\mathrm{CRA}(f)$ and $\mathrm{CMM}(f)$ are not equivalent for partial functions, as there exists an example where $\mathrm{CRA}(f)$ is constant, but $\mathrm{CMM}(f) = \Theta(\log n)$.

We also show a "block sensitivity" barrier for fractional block sensitivity. Namely, for any partial function f, the fractional block sensitivity is at most $\sqrt{n \cdot \mathrm{bs}(f)}$. Note that the adversary bounds do not bear this limitation, as witnessed by the aforementioned example. This result is tight, as we exhibit a partial function that matches this upper bound.

Even though our results are similar to the quantum case in [19] in spirit, the proof methods are different.

2 Preliminaries

In this section we define the complexity measures we are going to work with in the paper. In the following definitions and the rest of the paper consider f to be a partial function $f : S \to H$ with domain $S \subseteq G^n$, where G, H are some finite alphabets and n is the length of the input string. Throughout the paper we assume that f is not constant.

2.1 Block Sensitivity

For $x \in S$, a subset of indices $B \subseteq [n]$ is a *sensitive block* of x if there exists a y such that $f(x) \neq f(y)$ and $B = \{i \mid x_i \neq y_i\}$. The *block sensitivity* $\mathrm{bs}(f, x)$ of f on x is the maximum number k of disjoint subsets $B_1, \ldots, B_k \subseteq [n]$ such that B_i is a sensitive block of x for each $i \in [k]$. The block sensitivity of f is defined as $\mathrm{bs}(f) = \max_{x \in S} \mathrm{bs}(f, x)$.

Let $\mathcal{B} = \{B \mid \exists y : f(x) \neq f(y) \text{ and } B = \{i \mid x_i \neq y_i\}\}$ be the set of sensitive blocks of x. The *fractional block sensitivity* $\mathrm{fbs}(f, x)$ of f on x is defined as the optimal value of the following linear program:

$$\text{maximize} \sum_{B \in \mathcal{B}} w_x(B) \qquad \text{subject to} \quad \forall i \in [n] : \sum_{\substack{B \in \mathcal{B} \\ i \in B}} w_x(B) \leq 1.$$

Here, $w_x : \mathcal{B} \to [0; 1]$. The fractional block sensitivity of f is defined as $\mathrm{fbs}(f) = \max_{x \in S} \mathrm{fbs}(f, x)$.

When the weights are taken as either 0 or 1, the optimal solution to the corresponding integer program is equal to $\mathrm{bs}(f, x)$. Hence $\mathrm{fbs}(f, x)$ is a relaxation of $\mathrm{bs}(f, x)$, and we have $\mathrm{bs}(f, x) \leq \mathrm{fbs}(f, x)$.

2.2 Certificate Complexity

An *assignment* is a map $A : \{1, \ldots, n\} \to G \cup \{*\}$. Informally, the elements of G are the values fixed by the assignment and * is a wildcard symbol that can be any letter of G. A string $x \in S$ is said to be consistent with A if for all $i \in [n]$ such that $A(i) \neq *$, we have $x_i = A(i)$. The length of A is the number of positions that A fixes to a letter of G.

For an $h \in H$, an h-certificate for f is an assignment A such that for all strings $x \in A$ we have $f(x) = h$. The *certificate complexity* $\mathrm{C}(f, x)$ of f on x is the size of the shortest $f(x)$-certificate that x is consistent with. The certificate complexity of f is defined as $\mathrm{C}(f) = \max_{x \in S} \mathrm{C}(f, x)$.

The *fractional certificate complexity* $\mathrm{FC}(f,x)$ of f on $x \in S$ is defined as the optimal value of the following linear program:

$$\text{minimize} \sum_{i\in[n]} v_x(i) \qquad \text{subject to} \quad \forall y \in S \text{ s.t. } f(x)\neq f(y): \sum_{i:x_i\neq y_i} v_x(i) \geq 1.$$

Here, $v_x : [n] \to [0;1]$ for each $x \in S$. The fractional certificate complexity of f is defined as $\mathrm{FC}(f) = \max_{x\in S} \mathrm{FC}(f,x)$.

When the weights are taken as either 0 or 1, the optimal solution to the corresponding integer program is equal to $\mathrm{C}(f,x)$. Hence $\mathrm{FC}(f,x)$ is a relaxation of $\mathrm{C}(f,x)$, and we have $\mathrm{FC}(f,x) \leq \mathrm{C}(f,x)$.

It has been shown that $\mathrm{fbs}(f,x)$ and $\mathrm{FC}(f,x)$ are dual linear programs, hence their optimal values are equal, $\mathrm{fbs}(f,x) = \mathrm{FC}(f,x)$. As an immediate corollary, $\mathrm{fbs}(f) = \mathrm{FC}(f)$.

2.3 One-Sided Measures

For Boolean functions with $H = \{0,1\}$, for each measure M from $\mathrm{bs}(f), \mathrm{fbs}(f), \mathrm{FC}(f), \mathrm{C}(f)$ and a Boolean value $b \in \{0,1\}$, define the corresponding one-sided measure as

$$M^b(f) = \max_{x\in f^{-1}(b)} M(f,x).$$

According to the earlier definitions, we then have $M(f) = \max\{M^0(f), M^1(f)\}$. These one-sided measures are useful when, for example, working with compositions of Or with some Boolean function.

2.4 Kolmogorov Complexity

A set of strings $\mathcal{S} \subset \{0,1\}^*$ is called *prefix-free* if there are no two strings in $\mathcal{S}$ such that one is a proper prefix of the other. Let M be a universal Turing machine and fix a prefix-free set $\mathcal{S}$. The prefix-free *Kolmogorov complexity* of x given y, is defined as the length of the shortest program from $\mathcal{S}$ that prints x when given y:

$$K(x|y) = \min\{|P| \mid P \in \mathcal{S}, M(P,y) = x\}.$$

For a detailed introduction on Kolmogorov complexity, we refer the reader to [15].

3 Classical Adversary Bounds

Let $f : S \to H$ be a function, where $S \subseteq G^n$. The following are all known to be lower bounds on bounded-error randomized query complexity.

3.1 Relational Adversary Bound

Let $R : S \times S \to \mathbb{R}_{\geq 0}$ be a real-valued function such that $R(x,y) = R(y,x)$ for all $x,y \in S$ and $R(x,y) = 0$ whenever $f(x) = f(y)$. Then for $x \in S$ and an index i, let[2]

$$\theta(x,i) = \frac{\sum_{y\in S} R(x,y)}{\sum_{y\in S: x_i\neq y_i} R(x,y)},$$

[2] We take the reciprocals of the expressions, compared to Aaronson's definition.

where $\theta(x,i)$ is undefined if the denominator is 0. Denote[3]

$$\mathrm{CRA}(f) = \max_{R} \min_{\substack{x,y\in S, i\in[n]:\\ R(x,y)>0, x_i\neq y_i}} \max\{\theta(x,i),\theta(y,i)\}.$$

See [1] for details.

3.2 Rank-1 Relational Adversary Bound

We introduce the following restriction of the relational adversary bound. Let R' be any $|S|\times|S|$ matrix of rank 1, such that:

- There exist $u,v : S\to\mathbb{R}_{\geq 0}$ such that $R'(x,y)=u(x)v(y)$ for all $x,y\in S$.
- $R'(x,y)=0$ whenever $f(x)=f(y)$.

Then set $R(x,y)=\max\{R'(x,y),R'(y,x)\}$.

Let $X=\{x \mid u(x)>0\}$ and $Y=\{y \mid v(y)>0\}$. Note that for every $x\in S$, either $u(x)$ or $v(x)$ must be 0, as $R(x,x)$ must be 0, therefore $X\cap Y=\varnothing$. Then denote

$$\mathrm{CRA}_1(f) = \max_{u,v} \min_{\substack{x\in X, y\in Y, i\in[n]:\\ u(x)v(y)>0, x_i\neq y_i}} \max\{\theta(x,i),\theta(y,i)\}.$$

where $\theta(x,i)$ can be simplified to

$$\theta(x,i)=\frac{\sum_{y\in Y} v(y)}{\sum_{y\in Y: x_i\neq y_i} v(y)} \qquad \text{and} \qquad \theta(y,i)=\frac{\sum_{x\in X} u(x)}{\sum_{x\in X: x_i\neq y_i} u(x)}.$$

Naturally, $\mathrm{CRA}_1(f)\leq\mathrm{CRA}(f)$.

As $R(x,y)=0$ whenever $f(x)=f(y)$, we have that for every output $h\in H$ either $f^{-1}(h)\cap X=\varnothing$ or $f^{-1}(h)\cap Y=\varnothing$. Therefore, $\mathrm{CRA}_1(f)$ effectively bounds the complexity of differentiating between two non-overlapping sets of outputs. This leads to the following equivalent definition for $\mathrm{CRA}_1(f)$:

▶ **Proposition 1.** *Let $A\cup B=H$ be a partition of the output alphabet, i.e., $A\cap B=\varnothing$. Let p and q be probability distributions over $X:=f^{-1}(A)$ and $Y:=f^{-1}(B)$, respectively. Then*

$$\mathrm{CRA}_1(f) = \max_{\substack{A,B\\ p,q}} \min_{\substack{i\in[n],\\ g_1,g_2\in G: g_1\neq g_2\\ \exists x\in X, y\in Y: p(x)q(y)>0}} \frac{1}{\min\{\Pr_{x\sim p}[x_i\neq g_1],\Pr_{y\sim q}[y_i\neq g_2]\}}.$$

For the proof of this proposition, see [6].

3.3 Weighted Adversary Bound

Let w,w' be weight schemes as follows.

- Every pair $(x,y)\in S^2$ is assigned a non-negative weight $w(x,y)=w(y,x)$ such that $w(x,y)=0$ whenever $f(x)=f(y)$.
- Every triple (x,y,i) is assigned a non-negative weight $w'(x,y,i)$ such that $w'(x,y,i)=0$ whenever $x_i=y_i$ or $f(x)=f(y)$, and $w'(x,y,i), w'(y,x,i)\geq w(x,y)$ for all x,y,i such that $x_i\neq y_i$.

[3] One can show that there exist optimal solutions for R, thus we can maximize over R instead of taking the supremum.

For all x, i, let $wt(x) = \sum_{y \in S} w(x,y)$ and $v(x,i) = \sum_{y \in S} w'(x,y,i)$. Denote

$$\mathrm{CWA}(f) = \max_{w,w'} \min_{\substack{x,y \in S, i \in [n] \\ w(x,y) \neq 0, x_i \neq y_i}} \max \left\{ \frac{wt(x)}{v(x,i)}, \frac{wt(y)}{v(y,i)} \right\}.$$

This adversary method is formulated in [14] and is an adaptation of Ambainis' quantum adversary method [5].

3.4 Kolmogorov Complexity

Let $\sigma \in \{0,1\}^*$ be any finite string.[4] Denote

$$\mathrm{CKA}(f) = \min_{\sigma} \max_{\substack{x,y \in S \\ f(x) \neq f(y)}} \frac{1}{\sum_{i: x_i \neq y_i} \min\{2^{-K(i|x,\sigma)}, 2^{-K(i|y,\sigma)}\}}.$$

See [14] for details.

3.5 Minimax over probability distributions

Let $\{p_x\}_{x \in S}$ be a set of probability distributions over $[n]$. Denote

$$\mathrm{CMM}(f) = \min_{p} \max_{\substack{x,y \in S \\ f(x) \neq f(y)}} \frac{1}{\sum_{i: x_i \neq y_i} \min\{p_x(i), p_y(i)\}}.$$

See [14] for details.

4 Equivalence of the Adversary Bounds

In this section we prove the main theorem:

▶ **Theorem 2.** *Let $f : S \to H$ be a partial Boolean function, where $S \subseteq G^n$. Then*

- $\mathrm{fbs}(f) \leq \mathrm{CRA}_1(f) \leq \mathrm{CRA}(f) = \mathrm{CWA}(f)$,
- $\mathrm{CWA}(f) = O(\mathrm{CKA}(f))$,
- $\mathrm{CKA}(f) = \Theta(\mathrm{CMM}(f))$.

Moreover, for total functions $f : G^n \to H$, we have $\mathrm{fbs}(f) = \mathrm{CMM}(f)$.

The part $\mathrm{CWA}(f) = O(\mathrm{CKA}(f))$ has been already proven in [14].

4.1 Fractional Block Sensitivity and the Weighted Adversary Method

First, we prove that fractional block sensitivity lower bounds the relational adversary bound for any partial function.

▶ **Proposition 3.** *Let $f : S \to H$ be a partial Boolean function, where $S \subseteq G^n$. Then* $\mathrm{fbs}(f) \leq \mathrm{CRA}_1(f)$.

[4] By the argument of [19], we take the minimum over the strings instead of the algorithms computing f.

Proof. Let $x \in S$ be such that $\mathrm{fbs}(f,x) = \mathrm{fbs}(f)$ and denote $h = f(x)$. Let $H' = H \setminus \{h\}$ and $S' = f^{-1}(H')$.

Let $\mathcal{B}$ be the set of sensitive blocks of x. Let $w : \mathcal{B} \to [0,1]$ be an optimal solution to the $\mathrm{fbs}(f,x)$ linear program, that is, $\sum_{B\in\mathcal{B}} w(B) = \mathrm{fbs}(f,x)$. For each $B \in \mathcal{B}$, pick a single $y_B \in S'$ such that $B = \{i \mid x_i \neq y_i\}$. Then define $R(x, y_B) := w(B)$ for all $B \in \mathcal{B}$. It is clear that R has a corresponding rank 1 matrix R', as it has only one row (corresponding to x) that is not all zeros.

Let $y \in S'$ be any input such that $R(x,y) > 0$. Then for any $i \in [n]$ such that $x_i \neq y_i$,

$$\theta(x,i) = \frac{\sum_{B\in\mathcal{B}} w(B)}{\sum_{B\in\mathcal{B}:i\in B} w(B)} = \frac{\mathrm{fbs}(f,x)}{\sum_{B\in\mathcal{B}:i\in B} w(B)} \geq \mathrm{fbs}(f),$$

as $0 < \sum_{B\in\mathcal{B}:i\in B} w(B) \leq 1$. On the other hand, note that $\theta(y,i) = \frac{w(B)}{w(B)} = 1$, where $B = \{i \mid x_i \neq y_i\}$. Therefore, for this R,

$$\min_{\substack{x,y\in S, i\in[n]:\\ R(x,y)>0, x_i\neq y_i}} \max\{\theta(x,i), \theta(y,i)\} \geq \min_{\substack{y\in S', i\in[n]:\\ R(x,y)>0, x_i\neq y_i}} \max\{\mathrm{fbs}(f), 1\} = \mathrm{fbs}(f),$$

and the claim follows. ◀

As mentioned in [14], $\mathrm{CRA}(f)$ is a weaker version of $\mathrm{CWA}(f)$. We show that in fact they are exactly equal:

▶ **Proposition 4.** *Let $f : S \to H$ be a partial Boolean function, where $S \subseteq G^n$. Then* $\mathrm{CRA}(f) = \mathrm{CWA}(f)$.

Proof.

- First we show that $\mathrm{CRA}(f) \leq \mathrm{CWA}(f)$.
  Suppose that R is the function for which the relational bound achieves maximum value. Let $w(x,y) = w(y,x) = w(x,y,i) = w(y,x,i) = R(x,y)$ for any x, y, i such that $f(x) \neq f(y)$ and $x_i \neq y_i$. This pair of weight schemes satisfies the conditions of the weighted adversary bound. The value of the latter with w, w' is equal to $\mathrm{CRA}(f)$. As the weighted adversary bound is a maximization measure, $\mathrm{CRA}(f) \leq \mathrm{CWA}(f)$.
- Now we show that $\mathrm{CRA}(f) \geq \mathrm{CWA}(f)$.
  Let w, w' be optimal weight schemes for the weighted adversary bound. Let $R(x,y) = w(x,y)$ for any $x, y \in S$ such that $f(x) \neq f(y)$. Let $S' = f^{-1}(H \setminus f(x))$. Then

  $$\theta(x,i) = \frac{\sum_{y\in S'} R(x,y)}{\sum_{y\in S':x_i\neq y_i} R(x,y)} = \frac{\sum_{y\in S'} w(x,y)}{\sum_{y\in S':x_i\neq y_i} w(x,y)} \geq \frac{\sum_{y\in S'} w(x,y)}{\sum_{y\in S':x_i\neq y_i} w'(x,y,i)} = \frac{wt(x)}{v(x,i)},$$

  as $w'(x,y,i) \geq w(x,y)$ by the properties of w, w'. Similarly, $\theta(y,i) \geq \frac{wt(y)}{v(y,i)}$. Therefore, for any $x, y \in S$ and $i \in [n]$ such that $f(x) \neq f(y)$ and $x_i \neq y_i$, we have

  $$\max\{\theta(x,i), \theta(y,i)\} \geq \max\left\{\frac{wt(x)}{v(x,i)}, \frac{wt(y)}{v(y,i)}\right\}.$$

  As the relational adversary bound is a maximization measure, $\mathrm{CRA}(f) \geq \mathrm{CWA}(f)$. ◀

The proof of this proposition also shows why $\mathrm{CRA}(f)$ and $\mathrm{CWA}(f)$ are equivalent — the weight function w' is redundant in the classical case (in contrast to the quantum setting).

4.2 Kolmogorov Complexity and Minimax over Distributions

In this section we prove the equivalence between the minimax over probability distributions and Kolmogorov complexity adversary bound. It has been shown in the proof of the main theorem of [14] that $\mathrm{CMM}(f) = \Omega(\mathrm{CKA}(f))$. Here we show the other direction using a well-known result from coding theory.

▶ **Proposition 5** (Kraft's inequality). *Let S be any prefix-free set of finite strings. Then $\sum_{x\in S} 2^{-|x|} \leq 1$.*

▶ **Proposition 6.** *Let $f : S \to H$ be a partial Boolean function, where $S \subseteq G^n$. Then $\mathrm{CKA}(f) \geq \mathrm{CMM}(f)$.*

Proof. Let σ be the binary string for which $\mathrm{CKA}(f)$ achieves the smallest value. Define the set of probability distributions $\{p_x\}_{x\in S}$ on $[n]$ as follows. Let $s_x = \sum_{i\in[n]} 2^{-K(i|x,\sigma)}$ and $p_x(i) = 2^{-K(i|x,\sigma)}/s_x$. The set of programs that print out $i \in [n]$, given x and σ, is prefix-free (by the definition of $\mathcal{S}$), as the information given to all programs is the same. Thus, by Kraft's inequality, we have $s_x \leq 1$.

Examine the value of the minimax bound with this set of probability distributions. For any $x, y \in S$ and $i \in [n]$, we have

$$\min\{p_x(i), p_y(i)\} = \min\left\{\frac{2^{-K(i|x,\sigma)}}{s_x}, \frac{2^{-K(i|y,\sigma)}}{s_y}\right\} \geq \min\{2^{-K(i|x,\sigma)}, 2^{-K(i|y,\sigma)}\}.$$

Therefore, $\mathrm{CKA}(f) = \Theta(\mathrm{CMM}(f))$. ◀

4.3 Fractional Block Sensitivity and Minimax over Distributions

Now we proceed to prove that for total functions, fractional block sensitivity is equal to the minimax over probability distributions. The latter has the following equivalent form.

▶ **Lemma 7.** *For any partial Boolean function $f : S \to H$, where $S \subseteq G^n$,*

$$\mathrm{CMM}(f) = \min_{v} \max_{x\in S} \sum_{i\in[n]} v_x(i) \quad \text{s.t. } \forall y \in S \text{ s.t. } f(x) \neq f(y) : \sum_{i:x_i\neq y_i} \min\{v_x(i), v_y(i)\} \geq 1,$$

where $\{v_x\}_{x\in S}$ is any set of weight functions $v_x : [n] \to \mathbb{R}_{\geq 0}$.

For the proof of this lemma, see [6].

In this case we prove that for total functions the minimax over probability distributions is equal to the fractional certificate complexity $\mathrm{FC}(f)$. The result follows since $\mathrm{FC}(f) = \mathrm{fbs}(f)$. The proof of this claim is almost immediate in light of the following "fractional certificate intersection" lemma by Kulkarni and Tal:

▶ **Proposition 8** ([13], Lemma 6.2). *Let $f : G^n \to H$ be a total function[5] and $\{v_x\}_{x\in G^n}$ be a feasible solution for the $\mathrm{FC}(f)$ linear program. Then for any two inputs $x, y \in G^n$ such that $f(x) \neq f(y)$, we have $\sum_{i:x_i\neq y_i} \min\{v_x(i), v_y(i)\} \geq 1$.*

Let f be a total function. Suppose that $\{v_x\}_{x\in G^n}$ is a feasible solution for the $\mathrm{CMM}(f)$ program. Then for any $x, y \in G^n$ such that $f(x) \neq f(y)$, we have $\sum_{i:x_i\neq y_i} v_x(i) \geq$

[5] Kulkarni and Tal prove the lemma for Boolean functions, but it is straightforward to check that their proof also works for functions with arbitrary input and output alphabets.

$\sum_{i:x_i \neq y_i} \min\{v_x(i), v_y(i)\} \geq 1$. Hence this is also a feasible solution for the $\mathrm{FC}(f)$ linear program. On the other hand, if $\{v_x\}_{x \in G^n}$ is a feasible solution for $\mathrm{FC}(f)$ linear program, then it is also a feasible solution for the $\mathrm{CMM}(f)$ program by Proposition 8. Therefore, $\mathrm{CMM}(f) = \mathrm{FC}(f)$.

5 Separations for Partial Functions

5.1 Fractional Block Sensitivity vs. Adversary Bounds

Here we show an example of a partial function that provides an unbounded separation between the adversary measures and fractional block sensitivity.

▶ **Theorem 9.** *There exists a partial Boolean function $f : S \to \{0,1\}$, where $S \subseteq \{0,1\}^n$, such that $\mathrm{fbs}(f) = O(1)$ and $\mathrm{CRA}_1(f), \mathrm{CRA}(f), \mathrm{CWA}(f), \mathrm{CKA}(f), \mathrm{CMM}(f) = \Omega(n)$.*

Proof. Let n be an even number and $S = \{x \in \{0,1\}^n \mid |x| = 1\}$ be the set of bit strings of Hamming weight 1. Define the "greater than half" function $\textsc{Gth}_n : S \to \{0,1\}$ to be 1 iff $x_i = 1$ for $i > n/2$.

For the first part, the certificate complexity is constant $\mathrm{C}(\textsc{Gth}_n) = 1$. To certify the value of greater than half, it is enough to certify the position of the unique i such that $x_i = 1$. The claim follows, as $\mathrm{C}(f) \geq \mathrm{fbs}(f)$ for any f.

For the second part, by Theorem 2, it suffices to show that $\mathrm{CRA}_1(\textsc{Gth}_n) = \Omega(n)$. Let $X = f^{-1}(0)$ and $Y = f^{-1}(1)$. Let $R(x,y) = 1$ for all $x \in X, y \in Y$. Suppose that $x \in X, y \in Y, i \in [n]$ are such that $x_i = 1$ (and thus $y_i = 0$). Then

$$\theta(x,i) = \frac{\sum_{y^* \in Y} R(x,y^*)}{\sum_{\substack{y^* \in Y: \\ x_i \neq y^*_i}} R(x,y^*)} = \frac{n/2}{n/2} = 1, \qquad \theta(y,i) = \frac{\sum_{x^* \in X} R(x^*,y)}{\sum_{\substack{x^* \in X: \\ x^*_i \neq y_i}} R(x^*,y)} = \frac{n/2}{1} = n/2.$$

Therefore, $\max\{\theta(x,i), \theta(y,i)\} = n/2$. Similarly, if i is such an index that $y_i = 1$ and $x_i = 0$, we also have $\max\{\theta(x,i), \theta(y,i)\} = n/2$. Also note that R has a corresponding rank 1 matrix R', hence $\mathrm{CRA}_1(f) \geq n/2 = \Omega(n)$. ◀

We note that a similar function was used to prove lower bounds on the problem of inverting a permutation [4, 1]. More specifically, we are given a permutation $\sigma(1), \ldots, \sigma(n)$, and the function is 0 if $\sigma^{-1}(1) \leq n/2$ and 1 otherwise. With a single query, one can find the value of $\sigma(i)$ for any i. By construction, a lower bound on $\textsc{Gth}_n$ also gives a lower bound on computing this function.

5.2 Relational Adversary vs. Kolmogorov Complexity Bound

Here we show that, for a variant of the ordered search problem, the Kolmogorov complexity bound gives a tight logarithmic lower bound, while the relational adversary gives only a constant value lower bound.

Let $S = \{x \in \{0,1\}^n \mid \exists i \in [0;n] : x_1 = \ldots x_i = 0 \text{ and } x_{i+1} = \ldots = x_n = 1\}$. In other words, x is any string starting with some number of 0s followed by all 1s. Define the "ordered search parity" function $\textsc{Osp}_n : S \to \{0,1\}$ to be $\textsc{Ind}(x) \bmod 2$, where $\textsc{Ind}(x)$ is the last index i such that $x_i = 0$ (in the special case $x = 1^n$, assume that $i = 0$).

▶ **Theorem 10.** *For the ordered search parity, $\mathrm{CRA}_1(\textsc{Osp}_n), \mathrm{CRA}(\textsc{Osp}_n), \mathrm{CWA}(\textsc{Osp}_n) = O(1)$ and $\mathrm{CKA}(\textsc{Osp}_n), \mathrm{CMM}(\textsc{Osp}_n) = \Omega(\log n)$.*

For the proof of this theorem, see [6].

6 Limitation of Fractional Block Sensitivity

In this section we show that there is a certain barrier that the fractional block sensitivity cannot overcome for partial functions.

6.1 Upper Bound in Terms of Block Sensitivity

▶ **Theorem 11.** *For any partial function $f : S \to H$, where $S \subseteq G^n$, $\mathrm{fbs}(f) \le \sqrt{n \cdot \mathrm{bs}(f)}$.*

Proof. We will prove that $\mathrm{fbs}(f,x) \le \sqrt{n \cdot \mathrm{bs}(f,x)}$ for any $x \in S$. First we introduce a parametrized version of the fractional block sensitivity. Let $x \in S$ be any input, $\mathcal{B}$ the set of sensitive blocks of x and $N \le n$ a positive real number. Define

$$\mathrm{fbs}_N(f,x) = \max_w \sum_{B\in\mathcal{B}} w(B) \quad \text{s.t.} \quad \forall i \in [n] : \sum_{B\in\mathcal{B}: i\in B} w(B) \le 1, \quad \sum_{B\in\mathcal{B}} |B| \cdot w(B) \le N.$$

where $w : \mathcal{B} \to [0;1]$. If we let $N = n$, then the second condition becomes redundant and $\mathrm{fbs}_n(f,x) = \mathrm{fbs}(f,x)$.

For simplicity, let $k = \mathrm{bs}(f,x)$. We will prove by induction on k that $\mathrm{fbs}_N(f,x) \le \sqrt{Nk}$. If $k = 0$, the claim obviously holds, so assume $k > 0$. Let ℓ be the length of the shortest block in $\mathcal{B}$. Then

$$\sum_{B\in\mathcal{B}} \ell \cdot w(B) \le \sum_{B\in\mathcal{B}} |B| \cdot w(B) \le N$$

and $\mathrm{fbs}_N(f,x) = \sum_{B\in\mathcal{B}} w(B) \le N/\ell$.

On the other hand, let D be any shortest sensitive block. Let f' be the restriction of f where the variables with indices in D are fixed to the values of x_i for all $i \in D$. Note that $\mathrm{bs}(f',x) \le k-1$, as we have removed all sensitive blocks that overlap with D. Let $\mathcal{B}'$ be the set of sensitive blocks of x on f' and let $\mathcal{T} = \{B \in \mathcal{B} \mid B \cap D \ne \varnothing\}$, the set of sensitive blocks that overlap with D (including D itself). Then no $T \in \mathcal{T}$ is a member of $\mathcal{B}'$, therefore

$$\sum_{B'\in\mathcal{B}'} |B'| \cdot w(B') \le N - \sum_{T\in\mathcal{T}} |T| \cdot w(T) \le N - \ell \cdot \sum_{T\in\mathcal{T}} w(T).$$

Denote $t = \sum_{T\in\mathcal{T}} w(T)$. We have that $t \le |D| = \ell$, as any $T \in \mathcal{T}$ overlaps with D. By combining the two inequalities we get

$$\begin{aligned}\mathrm{fbs}_N(f,x) &\le \max_{\ell\in[0;n]} \min\left\{\frac{N}{\ell}, \max_{t\in[0;\ell]} \{t + \mathrm{fbs}_{N-\ell t}(f',x)\}\right\} \\ &\le \max_{\ell\in[0;n]} \min\left\{\frac{N}{\ell}, \max_{t\in[0;\ell]} \left\{t + \sqrt{(N-\ell t)(k-1)}\right\}\right\}.\end{aligned}$$

If $N/\ell \le \sqrt{Nk}$, we are done. Thus further assume that $\ell < \sqrt{N/k}$.

Denote $g(t) = t + \sqrt{(N-\ell t)(k-1)}$. We need to find the maximum of this function on the interval $[0;\ell]$ for a given ℓ. Its derivative, $g'(t) = 1 - \frac{\ell}{2}\sqrt{\frac{k-1}{N-\ell t}}$, is a monotone function in t. Thus, it has exactly one root, $t_0 = N/\ell - (k-1)\cdot\ell/4$. Therefore, $g(t)$ attains its maximum value on $[0;\ell]$ at one of the points $\{0, t_0, \ell\}$.

- If $t = 0$, then $g(0) = \sqrt{N(k-1)} \le \sqrt{Nk}$.
- If $t = t_0$, then, as $t \le \ell < \sqrt{N/k}$,

$$\begin{aligned}\sqrt{Nk} - \frac{k-1}{4}\cdot\sqrt{\frac{N}{k}} &< \frac{N}{\ell} - (k-1)\frac{\ell}{4} < \sqrt{\frac{N}{k}} \\ \sqrt{k} - \frac{k-1}{4\sqrt{k}} &< \sqrt{\frac{1}{k}}.\end{aligned}$$

Thus $3k < 0$, which has no solutions in natural numbers for k, so this case is not possible.

- If $t = \ell$, then $g(t) = \ell + \sqrt{(N-\ell^2)(k-1)}$.

Now it remains to find the maximum value of $h(k) = \ell + \sqrt{(N-\ell^2)(k-1)}$ on the interval $[0; \sqrt{N/k}]$. The derivative is equal to $h'(\ell) = 1 - \ell \cdot \sqrt{\frac{k-1}{N-\ell^2}}$. The only non-negative root of $h'(\ell)$ is equal to $\ell_0 = \sqrt{N/k}$. Then $h(\ell)$ is monotone on the interval $[0; \sqrt{N/k}]$. Thus $h(\ell)$ attains its maximal value at one of the points $\{0, \sqrt{N/k}\}$.

- If $\ell = 0$, then $h(\ell) = \sqrt{N(k-1)} < \sqrt{Nk}$.
- If $\ell = \ell_0 = \sqrt{N/k}$, then

$$h(\ell) = \sqrt{\frac{N}{k}} + \sqrt{\left(N - \frac{N}{k}\right)(k-1)} = \sqrt{N}\left(\sqrt{\frac{1}{k}} + (k-1)\sqrt{\frac{1}{k}}\right) = \sqrt{Nk}.$$

Thus, $h(\ell) \le \sqrt{Nk}$ and that concludes the induction.

Therefore, $\mathrm{fbs}(f,x) = \mathrm{fbs}_n(f,x) \le \sqrt{n \cdot \mathrm{bs}(f,x)}$, hence also $\mathrm{fbs}(f) \le \sqrt{n \cdot \mathrm{bs}(f)}$. ◀

6.2 A Matching Construction

▶ **Theorem 12.** *For any $k \in \mathbb{N}$, there exists a partial Boolean function $f : S \to \{0,1\}$, where $S \subseteq \{0,1\}^n$, such that $\mathrm{bs}(f) = k$ and $\mathrm{fbs}(f) = \Omega(\sqrt{n \cdot \mathrm{bs}(f)})$.*

Proof. Take any finite projective plane of order t, then it has $\ell = t^2 + t + 1$ many points. Let $n = k\ell$ and enumerate the points with integers from 1 to ℓ. Let $X = \{0^\ell\}$ and $Y = \{y \mid$ there exists a line L such that $y_i = 1$ iff $i \in L\}$. Define the (partial) finite projective plane function $\textsc{Fpp}_t : X \cup Y \to \{0,1\}$ as $\textsc{Fpp}_t(y) = 1 \iff y \in Y$.

We can calculate the 1-sided block sensitivity measures for this function:

- $\mathrm{fbs}^0(\textsc{Fpp}_t) \ge (t^2+t+1) \cdot \frac{1}{t+1} = \Omega(t)$, as each line gives a sensitive block for 0^n; since each point belongs to $t+1$ lines, we can assign weight $1/(t+1)$ for each sensitive block and that is a feasible solution for the fractional block sensitivity linear program.
- $\mathrm{bs}^0(\textsc{Fpp}_t) = 1$, as any two lines intersect, so any two sensitive blocks of 0^n overlap.
- $\mathrm{bs}^1(\textsc{Fpp}_t) = 1$, as there is only one negative input.

Next, define $f : S^{\times k} \to \{0,1\}$ as the composition of $\textsc{Or}$ with the finite projective plane function, $f = \textsc{Or}_k(\textsc{Fpp}_t(x^{(1)}), \ldots, \textsc{Fpp}_t(x^{(k)}))$. By the properties of composition with $\textsc{Or}$ (see Proposition 31 in [10] for details), we have

- $\mathrm{fbs}(f) = \max\{\mathrm{fbs}^0(f), \mathrm{fbs}^1(f)\} \ge \mathrm{fbs}^0(f) = \mathrm{fbs}^0(\textsc{Fpp}_t) \cdot k = \Theta(t) \cdot k = \Theta(t \cdot n/t^2) = \Theta(n/t)$,
- $\mathrm{bs}(f) = \max\{\mathrm{bs}^0(f), \mathrm{bs}^1(f)\} = \mathrm{bs}^0(\textsc{Fpp}_t) \cdot k = k = \Theta(n/t^2)$.

As $\sqrt{n \cdot n/t^2} = n/t$, we have $\mathrm{fbs}(f) = \Omega(\sqrt{n \cdot \mathrm{bs}(f)})$ and hence the result. ◀

Note that our example is also tight in regard to the multiplicative constant, since t can be unboundedly large (and the constant arbitrarily close to 1).

7 Open Ends

Rank 1 Weighted Adversary

Although we have shown that $\mathrm{CRA}(f)$ and $\mathrm{CKA}(f)$ are not equivalent for partial functions, there is still a possibility that $\mathrm{CRA}_1(f) = \Theta(\mathrm{CRA}(f))$ might be true. If they are indeed equivalent, then the weighted adversary would have a simpler formulation to use.

Limitation of the Adversary Bounds

In the quantum setting, the certificate barrier shows a limitation on the quantum adversary bounds. In the classical setting, by our results, fractional block sensitivity characterizes the classical adversary bounds for total functions and thus is of course an upper bound. Is there a general limitation on the classical adversary methods for partial functions?

Block Sensitivity vs. Fractional Block Sensitivity

We have exhibited an example with the largest separation between the two measures for partial functions, $\mathrm{bs}(f) = O(\sqrt{n \cdot \mathrm{bs}(f)})$. For total functions, one can show that $\mathrm{fbs}(f) \leq \mathrm{bs}(f)^2$, but the best known separation achieves $\mathrm{fbs}(f) = \Omega(\mathrm{bs}(f)^{3/2})$ [10]. Can our results be somehow extended for total functions to close the gap?

References

1 Scott Aaronson. Lower bounds for local search by quantum arguments. *SIAM Journal on Computing*, 35(4):804–824, 2006.

2 Scott Aaronson. Quantum certificate complexity. *Journal of Computer and System Sciences*, 74(3):313–322, 2008.

3 Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC'16, pages 863–876, New York, NY, USA, 2016. ACM.

4 Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC'00, pages 636–643, New York, NY, USA, 2000. ACM.

5 Andris Ambainis. Polynomial degree vs. quantum query complexity. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, FOCS'03, pages 230–239, Washington, DC, USA, 2003. IEEE Computer Society.

6 Andris Ambainis, Martins Kokainis, Krisjanis Prusis, and Jevgenijs Vihrovs. All classical adversary methods are equivalent for total functions. *CoRR*, abs/1709.08985, 2017. `arXiv:1709.08985`.

7 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001.

8 Shalev Ben-David and Robin Kothari. Randomized query complexity of sabotaged and composed functions. In *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, volume 55 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 60:1–60:14, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

9 Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002.

10 Justin Gilmer, Michael Saks, and Srikanth Srinivasan. Composition limits and separating examples for some Boolean function complexity measures. *Combinatorica*, 36(3):265–311, 2016.

11 Peter Hoyer, Troy Lee, and Robert Spalek. Negative weights make adversaries stronger. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC'07, pages 526–535, New York, NY, USA, 2007. ACM.

12 Rahul Jain and Hartmut Klauck. The partition bound for classical communication complexity and query complexity. In *Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity*, CCC'10, pages 247–258, Washington, DC, USA, 2010. IEEE Computer Society.

13 Raghav Kulkarni and Avishay Tal. On fractional block sensitivity. *Chicago Journal Of Theoretical Computer Science*, 8:1–16, 2016.

14 Sophie Laplante and Frédéric Magniez. Lower bounds for randomized and quantum query complexity using Kolmogorov arguments. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, CCC'04, pages 294–304, Washington, DC, USA, 2004. IEEE Computer Society.

15 Ming Li and Paul M.B. Vitnyi. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer Publishing Company, Incorporated, 3 edition, 2008.

16 Noam Nisan. CREW PRAMs and decision trees. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC'89, pages 327–335, New York, NY, USA, 1989. ACM.

17 Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, 1994.

18 Ben W. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean function. In *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, FOCS'09, pages 544–551, Washington, DC, USA, 2009. IEEE Computer Society.

19 Robert Špalek and Mario Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006.

20 Avishay Tal. Properties and applications of Boolean function composition. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ITCS'13, pages 441–454, New York, NY, USA, 2013. ACM.

21 Andrew Chi-Chin Yao. Probabilistic computations: Toward a unified measure of complexity. In *18th Annual Symposium on Foundations of Computer Science*, pages 222–227, 1977.