Electronic Colloquium on Computational Complexity, Report No. 123 (2017)

# Quadratically Tight Relations for Randomized Query Complexity

Dmitry Gavinsky [*] Rahul Jain [†‡] Hartmut Klauck [†§] Srijita Kundu [†]
Troy Lee [†§] Miklos Santha [†¶] Swagato Sanyal [†§] Jevgēnijs Vihrovs [‖]

**Abstract**

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. The certificate complexity $\mathsf{C}(f)$ is a complexity measure that is quadratically tight for the zero-error randomized query complexity $\mathsf{R}_0(f)$: $\mathsf{C}(f) \leq \mathsf{R}_0(f) \leq \mathsf{C}(f)^2$. In this paper we study a new complexity measure that we call expectational certificate complexity $\mathsf{EC}(f)$, which is also a quadratically tight bound on $\mathsf{R}_0(f)$: $\mathsf{EC}(f) \leq \mathsf{R}_0(f) = O(\mathsf{EC}(f)^2)$. We prove that $\mathsf{EC}(f) \leq \mathsf{C}(f) \leq \mathsf{EC}(f)^2$ and show that there is a quadratic separation between the two, thus $\mathsf{EC}(f)$ gives a tighter upper bound for $\mathsf{R}_0(f)$. The measure is also related to the fractional certificate complexity $\mathsf{FC}(f)$ as follows: $\mathsf{FC}(f) \leq \mathsf{EC}(f) = O(\mathsf{FC}(f)^{3/2})$. This also connects to an open question by Aaronson whether $\mathsf{FC}(f)$ is a quadratically tight bound for $\mathsf{R}_0(f)$, as $\mathsf{EC}(f)$ is in fact a relaxation of $\mathsf{FC}(f)$.

In the second part of the work, we upper bound the distributed query complexity $\mathsf{D}^{\mu}_{\epsilon}(f)$ for product distributions $\mu$ by the square of the query corruption bound ($\mathsf{corr}_{\epsilon}(f)$) which improves upon a result of Harsha, Jain and Radhakrishnan [2015]. A similar statement for communication complexity is open.

## 1 Introduction

The query model is arguably the simplest model for computation of Boolean functions. Its simplicity is convenient for showing lower bounds for the amount of time required to accomplish a computational task. In this model, an algorithm computing a function $f : \{0,1\}^n \to \{0,1\}$ on $n$ bits is given query access to the input $x \in \{0,1\}^n$. The algorithm can *query* different bits of $x$, possibly in an adaptive fashion, and finally produces an output. The complexity of the algorithm is the number of queries made; in particular, the algorithm does not incur additional cost for any computation other than the queries.

Unlike the more general models of computation (e.g. Boolean circuits, Turing machines), it is often possible to completely determine the query complexity of explicit functions using existing tools and techniques. The study of query algorithms can thus be a natural first step towards understanding the computational power and limitations of more general and complex models. Query complexity has seen a long line of research by computational complexity theorists. We refer the reader to the survey by Buhrman and de Wolf [BdW02] for a comprehensive introduction to this line of work.

To understand query algorithms, researchers have defined many complexity measures of Boolean functions and investigated their relationship to query complexity, and to one another. For a summary of the current state of knowledge about these measures, see [ABDK16]. In this work,

[*]Institute of Mathematics, Czech Academy of Sciences, 115 67 Žitna 25, Praha 1, Czech Republic.
[†]Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543. rahul@comp.nus.edu.sg, cqthk@nus.edu.sg, srijita.kundu@u.nus.edu.
[‡]MajuLab, UMI 3654, Singapore.
[§]SPMS, Nanyang Technological University, 21 Nanyang Link, Singapore 637371. troyjlee@gmail.com, ssanyal@ntu.edu.sg.
[¶]IRIF, Université Paris Diderot, CNRS, 75205 Paris, France. santha@irif.fr.
[‖]Centre for Quantum Computer Science, University of Latvia, Raiņa 19, Riga, Latvia, LV-1586. jevgenijs.vihrovs@lu.lv.



ISSN 1433-8092

we focus on characterizing the bounded-error query complexity $\mathsf{R}(f)$ and the zero-error query complexity $\mathsf{R}_0(f)$.

The following measures are known to lower bound $\mathsf{R}_0(f)$: block sensitivity $\mathsf{bs}(f)$, fractional certificate complexity $\mathsf{FC}(f)$ (also known as fractional block sensitivity $\mathsf{fbs}(f)$, [Tal13]), and certificate complexity $\mathsf{C}(f)$. They are related as follows:

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

It is known that $\mathsf{R}_0(f) \leq \mathsf{D}(f) \leq \mathsf{C}(f)^2$, and the Tribes function (an And of $\sqrt{n}$ Ors on $\sqrt{n}$ bits) demonstrates that this relation is tight [JK10]. It is also known that $\mathsf{R}_0(f) = O(\mathsf{bs}(f)^3) = O(\mathsf{FC}(f)^3)$ [Nis89, BBC+01]. A quadratic separation between $\mathsf{R}_0(f)$ and $\mathsf{FC}(f)$ is also achieved by Tribes. Aaronson posed a question whether $\mathsf{R}_0(f) = O(\mathsf{FC}^2(f))$ holds [Aar08] (stated in terms of the randomized certificate complexity $\mathsf{RC}(f)$, which later has been shown to be equivalent to $\mathsf{FC}(f)$ [GSS16]). A positive answer to this question would imply that $\mathsf{R}_0(f) = O(\widetilde{\deg}(f)^4) = O(\mathsf{Q}(f)^4)$ [ABDK16], where $\widetilde{\deg}(\cdot)$ and $\mathsf{Q}(\cdot)$ stand for approximate polynomial degree and quantum query complexity respectively.

One approach to showing $\mathsf{R}_0(f) \leq \mathsf{FC}(f)^2$ is to consider the natural generalization of the proof $\mathsf{D}(f) \leq \mathsf{C}(f)^2$ to the randomized case; the analysis of this algorithm, however, has met some unresolved obstacles [KT16]. We define a new complexity measure *expectational certificate complexity* $\mathsf{EC}(f)$ that is specifically designed to avert these problems and is of a similar form to $\mathsf{FC}(f)$. We show that $\mathsf{EC}$ gives a quadratically tight bound for $\mathsf{R}_0$:

**Theorem 1.** *For all total Boolean functions $f$,*

$$\mathsf{EC}(f) \leq \mathsf{R}_0(f) \leq O(\mathsf{EC}(f)^2).$$

In fact, $\mathsf{FC}(f)$ is a relaxation of $\mathsf{EC}(f)$, and we show that $\mathsf{FC}(f) \leq \mathsf{EC}(f) \leq \mathsf{C}(f)$. Moreover, we show that $\mathsf{EC}(f)$ lies closer to $\mathsf{FC}(f)$ than $\mathsf{C}(f)$ does: $\mathsf{FC}(f) \leq \mathsf{EC}(f) \leq \mathsf{FC}(f)^{3/2}$. While we don't know whether $\mathsf{EC}(f)$ is a lower bound on $\mathsf{R}(f)$, the last property gives $\mathsf{EC}(f)^{2/3} \leq \mathsf{R}(f)$.

As mentioned earlier, $\mathsf{C}(f)^2$ bounds $\mathsf{R}_0(f)$ from above. But for specific functions, $\mathsf{EC}(f)^2$ can be an asymptotically tighter upper bound than $\mathsf{C}(f)^2$. We demonstrate that by showing that the same example that provides a quadratic separation between $\mathsf{C}(f)$ and $\mathsf{FC}(f)$ [GSS16] also gives $\mathsf{C}(f) = \Omega(\mathsf{EC}(f)^2)$. This is the widest separation possible between $\mathsf{EC}(f)$ and $\mathsf{C}(f)$, because $\mathsf{C}(f) \leq \mathsf{R}_0(f) = O(\mathsf{EC}(f)^2)$.

In the second part of the paper, we upper bound the distributional query complexity for product distributions in terms of the minimum product query corruption bound and the block sensitivity (see Definition 9 and Section 2).

**Theorem 2.** *Let $\epsilon \in [0, 1/2)$ and $\mu$ a product distribution over the inputs. Then*

$$\mathsf{D}^{\mu}_{4\epsilon}(f) = O(\mathsf{corr}^{\times}_{\min,\epsilon}(f) \cdot \mathsf{bs}(f)).$$

We contrast Theorem 2 with the past work by Harsha, Jain and Radhakrishnan [HJR15], who showed that for product distributions, the distributional query complexity is bounded above by the square of the smooth corruption bound corresponding to inverse polynomial error. Theorem 2 improves upon their result, firstly by upper bounding the distributional complexity by minimum query corruption bound, which is an asymptotically smaller measure than the smooth corruption bound, and secondly by losing a constant factor in the error as opposed to a polynomial worsening in their work. Theorem 17, a consequence of Theorem 2, shows that for product distribution over the inputs, the distributional query complexity is asymptotically bounded above by the square of the query corruption bound. Thus Theorem 17 resolves a question that was open after the work of Harsha et. al. The analogous question in communication complexity is still open.

Theorem 2 also bounds distributional query complexity in terms of the *partition bound* $\mathsf{prt}(\cdot)$ of Jain and Klauck [JK10]. The following theorem follows from Theorems 2 and 16.

**Theorem 3.** *If $\epsilon \in \left[0, \frac{1}{8}\right]$ then $\mathsf{D}^{\mu}_{8\epsilon}(f) = O(\mathsf{prt}_{\epsilon}(f)^2 \cdot \log(1/\epsilon))$.*

Jain and Klauck showed that $\mathsf{prt}(f)$ is a powerful lower bound on $\mathsf{R}(f)$. In the same work, $\mathsf{prt}(f)$ was used to give a tight $\Omega(n)$ lower bound on $\mathsf{R}(f)$ for the Tribes function on $n$ bits. The authors

proved that $\mathsf{prt}(f)$ is asymptotically larger than $\mathsf{FC}(f)$. This implies that $\mathsf{R}(f) = O(\mathsf{prt}(f)^3)$, since $\mathsf{R}(f) = O(\mathsf{bs}(f)^3)$. While a quadratic separation between $\mathsf{R}(f)$ and $\mathsf{prt}(f)$ is known [AKK16], it is open whether $\mathsf{R}(f) = O(\mathsf{prt}(f)^2)$. Theorem 4 proves a distributional version of this quadratic relation, for the special case in which the input is sampled from a product distribution. We remark here that Jain, Harsha and Radhakrishnan proved in their work that $\mathsf{D}^{\mu}_{1/3}(f) = O(\mathsf{prt}_{1/3}(f)^2 \cdot (\log \mathsf{prt}_{1/3}(f))^2)$; Theorem 4 achieves polylogarithmic improvement over this bound. We note here that an analogous statement for an arbitrary distribution together with the Minimax Principle (see Fact 4) will imply that $\mathsf{R}(f) = O(\mathsf{prt}(f)^2)$.

The paper is organized as follows. In Section 2, we give the definitions for some of the complexity measures. In Section 3, we define the expectational certificate complexity and prove the results concerning this measure, starting with Theorem 1. In Section 4, we define the minimum query corruption bound and prove Theorems 2 and 3. In Section 5, we list some open problems concerning our measures.

## 2 Preliminaries

In this section we recall the definitions of some known complexity measures. For detailed introduction on the query model, see the survey [BdW02]. For the rest of this paper, $f$ is any total Boolean function on $n$ bits, $f : \{0,1\}^n \to \{0,1\}$.

**Definition 1** (Randomized Query Complexity)**.** Let $\mathcal{A}$ be a randomized algorithm that as an input takes $x \in \{0,1\}^n$ and returns a Boolean value $\mathcal{A}(x,r)$, where $r$ is any random string used by $\mathcal{A}$. With one query $\mathcal{A}$ can ask the value of any input variable $x_i$, for $i \in [n]$. The complexity $C(\mathcal{A},x,r)$ of $\mathcal{A}$ on $x$ is the number of queries the algorithm performs under randomness $r$, given $x$. The worst-case complexity of $\mathcal{A}$ is $C(\mathcal{A}) = \max_{r,x\in\{0,1\}^n} C(\mathcal{A},x,r)$.

The *zero-error randomized query complexity* $\mathsf{R}_0(f)$ is defined as $\min_{\mathcal{A}} \max_x \mathbb{E}_r[C(\mathcal{A},x,r)]$, where $\mathcal{A}$ is any randomized algorithm such that for all $x \in \{0,1\}^n$, we have $\Pr_r[\mathcal{A}(x,r) = f(x)] = 1$.

The *one-sided error randomized query complexity* $\mathsf{R}^0_\epsilon(f)$ is defined as $\min_{\mathcal{A}} C(\mathcal{A})$, where $\mathcal{A}$ is any randomized algorithm such that for every $x$ such that $f(x) = 0$, we have $\Pr_r[\mathcal{A}(x,r) = 1] \le \epsilon$, and for all $x$ such that $f(x) = 1$, we have $\Pr_r[\mathcal{A}(x,r) = 1] = 1$. Similarly we define $\mathsf{R}^1_\epsilon(f)$.

The *two-sided error randomized query complexity* $\mathsf{R}_\epsilon(f)$ is defined as $\min_{\mathcal{A}} C(\mathcal{A})$, where $\mathcal{A}$ is any randomized algorithm such that for every $x \in \{0,1\}^n$, we have $\Pr_r[\mathcal{A}(x,r) \neq f(x)] \le \epsilon$. We denote $\mathsf{R}_{1/3}(f)$ simply by $\mathsf{R}(f)$.

**Definition 2** (Distributional Query Complexity)**.** Let $\mu$ be a probability distribution over $\{0,1\}^n$, and $\epsilon \in [0,1/2)$. The *distributional query complexity* $\mathsf{D}^{\mu}_\epsilon(f)$ is the minimum number of queries made in the worst case (over inputs) by a deterministic query algorithm $\mathcal{A}$ for which $\Pr_{x\sim\mu}[\mathcal{A}(x) = f(x)] \ge 1 - \epsilon$.

The *Minimax Principle* relates the randomized query complexity and distributional query complexity measures of Boolean functions.

**Fact 4** (Minimax Principle)**.** *For any Boolean function* $f, \mathsf{R}_\epsilon(f) = \max_\mu \mathsf{D}^{\mu}_\epsilon(f)$.

**Definition 3** (Product Distribution)**.** A probability distribution $\mu$ over $\{0,1\}^n$ is a *product distribution* if there exist $n$ functions $\mu_1, \ldots, \mu_n : \{0,1\} \to [0,1]$ such that $\mu_i(0) + \mu_i(1) = 1$ for all $i$ and for all $x \in \{0,1\}^n$,

$$\mu(x) = \prod_{i\in[n]} \mu_i(x_i).$$

**Definition 4** (Certificate Complexity)**.** An *assignment* is a map $A : \{1,\ldots,n\} \to \{0,1,*\}$. All inputs consistent with $A$ form a subcube $\{x \in \{0,1\}^n \mid \forall i \in [n] : x_i = A(i) \text{ or } A(i) = *\}$. The length or size of an assignment, denoted by $|A|$, is defined to be the co-dimension of the subcube it corresponds to. Let $Q_A := \{j : A(j) \neq *\}$ be the set of variables fixed by $A$.

For $b \in \{0,1\}$, a $b$-certificate for $f$ is an assignment $A$ such that $x \in A \Rightarrow f(x) = b$. The *certificate complexity* $\mathsf{C}(f,x)$ of $f$ on $x$ is the size of the shortest $f(x)$-certificate that is consistent with $x$. The certificate complexity of $f$ is defined as $\mathsf{C}(f) = \max_{x\in\{0,1\}^n} \mathsf{C}(f,x)$. The $b$-certificate complexity of $f$ is defined as $\mathsf{C}^b(f) = \max_{x:f^{-1}(b)} \mathsf{C}(f,x)$.

**Definition 5** (Sensitivity and Block Sensitivity)**.** For $x \in \{0,1\}^n$ and $S \subseteq [n]$, let $x^S$ be $x$ flipped on locations in $S$. The *sensitivity* $\mathsf{s}(f,x)$ of $f$ on $x$ is the number of different $i \in [n]$ such that $f(x) \neq f(x^{\{i\}})$. The sensitivity of $f$ is defined as $\mathsf{s}(f) = \max_{x\in\{0,1\}^n} \mathsf{s}(f,x)$.

The *block sensitivity* $\mathsf{bs}(f,x)$ of $f$ on $x$ is the maximum number $k$ of disjoint subsets $B_1,\ldots,B_k \subseteq [n]$ such that $f(x) \neq f(x^{B_i})$ for each $i \in [k]$. The block sensitivity of $f$ is defined as $\mathsf{bs}(f) = \max_{x\in\{0,1\}^n} \mathsf{bs}(f,x)$.

**Definition 6** (Fractional Certificate Complexity)**.** The *fractional certificate complexity* $\mathsf{FC}(f,x)$ of $f$ on $x \in \{0,1\}^n$ is defined as the optimal value of the following linear program:

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

Here $v_x \in \mathbb{R}^n$ and $v_x(i) \geq 0$ for each $x \in \{0,1\}^n$ and $i \in [n]$. The fractional certificate complexity of $f$ is defined as $\mathsf{FC}(f) = \max_{x\in\{0,1\}^n} \mathsf{FC}(f,x)$.

**Definition 7** (Fractional Block Sensitivity)**.** Let $\mathcal{B} = \{B \mid f(x) \neq f(x^B)\}$ be the set of sensitive blocks of $x$. The *fractional block sensitivity* $\mathsf{fbs}(f,x)$ of $f$ on $x$ is defined as the optimal value of the following linear program:

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

Here $u_x \in \mathbb{R}^{|\mathcal{B}|}$ and $u_x(B) \leq 1$ for each $x \in \{0,1\}^n$ and $B \in \mathcal{B}$. The fractional block sensitivity of $f$ is defined as $\mathsf{fbs}(f) = \max_{x\in\{0,1\}^n} \mathsf{fbs}(f,x)$.

The linear programs $\mathsf{FC}(f,x)$ and $\mathsf{fbs}(f,x)$ are duals of each other, hence their optimal solutions are equal and $\mathsf{FC}(f) = \mathsf{fbs}(f)$ [GSS16].

# 3 Expectational Certificate Complexity

In this section, we give the results for the expectational certificate complexity. The measure is motivated by the well-known $\mathsf{D}(f) \leq \mathsf{C}^0(f)\mathsf{C}^1(f)$ deterministic query algorithm which was independently discovered several times [BI87, HH87, Tar90]. In each iteration, the algorithm queries the set of variables fixed by some consistent 1-certificate. Either the query answers agree with the fixed values of the 1-certificate, in which case the input must evaluate to 1, or the algorithm makes progress as the 0-certificate complexity of all 0-inputs still consistent with the query answers is decreased by at least 1. The latter property is due to the crucial fact that the set of fixed values of any 0-certificate and 1-certificate must intersect.

In hopes of proving $\mathsf{R}(f) \leq \mathsf{FC}^0(f)\mathsf{FC}^1(f)$, a straightforward generalization to a randomized algorithm would be to pick a consistent 1-input $x$ and query each variable independently with probability $v_x(i)$, where $v_x$ is a fractional certificate for $x$. To show that such an algorithm makes progress, one needs a property analogous to the fact that 0-certificates and 1-certificates overlap. Kulkarni and Tal give a similar intersection property for the fractional certificates:

**Lemma 5** ([KT16], Lemma 6.2)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a total Boolean function and $\{v_x\}_{x\in\{0,1\}^n}$ be an optimal solution for the $\mathsf{FC}(f)$ linear program. Then for any two inputs $x,y \in \{0,1\}^n$ such that $f(x) \neq f(y)$, we have*

$$\sum_{i:x_i\neq y_i} \min\{v_x(i), v_y(i)\} \geq 1.$$

However, it is not clear whether the algorithm makes progress in terms of reducing the fractional certificates of the 0-inputs. We get around this problem by replacing $\min\{v_x(i), v_y(i)\}$ with the product $v_x(i)v_y(i)$ and putting that the sum of these terms over $i$ where $x_i \neq y_i$ is at least 1 as a constraint:

**Definition 8** (Expectational Certificate Complexity)**.** The *expectational certificate complexity* $\mathsf{EC}(f)$ of $f$ is defined as the optimal value of the following program:

$$\text{minimize } \max_x \sum_{i=1}^{n} w_x(i) \quad \text{s.t.} \quad \sum_{i:x_i \neq y_i} w_x(i) w_y(i) \geq 1 \text{ for all } x, y \text{ s.t. } f(x) \neq f(y),$$
$$0 \leq w_x(i) \leq 1 \text{ for all } x \in \{0,1\}^n,\ i \in [n].$$

We use the term "expectational" because the described algorithm on expectation queries at least weight 1 in total from input $y$, when querying the variables with probabilities being the weights of $x$. While the informally described algorithm shows a quadratic upper bound on the worst-case expected complexity, in the next section we show a slight modification that directly makes a quadratic number of queries in the worst case.

## 3.1 Quadratic Upper Bound on Randomized Query Complexity

In this section we prove Theorem 1 (restated below).

**Theorem 1.**

$$\mathsf{EC}(f) \leq \mathsf{R}_0(f) \leq O(\mathsf{EC}(f)^2).$$

*Proof.* The first inequality follows from Lemma 10 and $\mathsf{C}(f) \leq \mathsf{R}_0(f)$.

To prove the second inequality, we give randomized query algorithms for $f$ with 1-sided error $\epsilon$.

**Claim 6.** For any $b \in \{0,1\}$, we have $\mathsf{R}^b_\epsilon(f) \leq \lceil \mathsf{EC}(f)^2/\epsilon \rceil$.

The second inequality of Theorem 1 follows from Claim 6 by standard arguments of $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.

*Proof of Claim 6.* We prove the claim for $b = 0$. The case $b = 1$ is similar.

Let $\{w_x\}_{x \in \{0,1\}^n}$ be an optimal solution to the $\mathsf{EC}(f)$ program. We say that an input $y$ is consistent with the queries made by $\mathcal{A}$ on $x$ if $y_i = x_i$ for all queries $i \in [n]$ that have been made. Also define a probability distribution $\mu_y(i) = w_y(i) / \sum_{i \in [n]} w_y(i)$ for each input $y \in \{0,1\}^n$.

**Algorithm 1:** The randomized query algorithm $\mathcal{A}$.

**Input:** $x \in \{0,1\}^n$

1. Repeat $\lceil \mathsf{EC}(f)^2/\epsilon \rceil$ many times:
   (a) Pick the lexicographically first consistent 1-input $y$. If there is no such $y$, return 0.
   (b) Sample a position $i$ from $\mu_y$ and query $x_i$.
   (c) If the queried values form a $c$-certificate, return $c$.
2. Return 1.

The complexity bound is clear as $\mathcal{A}$ always performs at most $\lceil \mathsf{EC}(f)^2/\epsilon \rceil$ queries.

For correctness, note that the algorithm outputs 1 on all 1-inputs. Thus assume $x$ is a 0-input from here on in the analysis. Then we have to prove that $\mathcal{A}$ outputs 0 with probability at least $1 - \epsilon$. This amounts to showing that the function reduces to a constant 0 function and the algorithm terminates within $\lceil \mathsf{EC}(f)^2/\epsilon \rceil$ iterations with probability at least $1 - \epsilon$. (For notational convenience, in what follows we will drop the ceilings and assume $\mathsf{EC}(f)^2/\epsilon$ is an integer.)

Define a random variable $T_k$ as

$$T_k = \begin{cases} \frac{1}{\mathsf{EC}(f)}, & \text{if } \mathcal{A} \text{ has terminated before the } k\text{-th iteration,} \\ w_x(i), & \text{if at the } k\text{-th iteration } \mathcal{A} \text{ has queried } x_i \text{ for the first time,} \\ 0, & \text{if } x_i \text{ has been queried before the } k\text{-th iteration.} \end{cases}$$

Let $T = \sum_{k=1}^{\mathsf{EC}(f)^2/\epsilon} T_k$. As $\sum_{i \in [n]} w_x(i) \leq \mathsf{EC}(f)$ by definition, $T > \mathsf{EC}(f)$ implies that $\mathcal{A}$ has terminated before point 2. Then it has returned 0, and the answer is correct. Let $p = \Pr[T > \mathsf{EC}(f)]$. We will prove that $p \geq 1 - \epsilon$, in which case we would be done.

We continue by showing an upper and a lower bound on $\mathbb{E}[T]$.

- The maximum possible value of $T$ is at most

$$T \leq \sum_{i \in [n]} w_x(i) + \frac{\mathsf{EC}(f)^2}{\epsilon} \cdot \frac{1}{\mathsf{EC}(f)} \leq \left(1 + \frac{1}{\epsilon}\right) \mathsf{EC}(f).$$

  Therefore,

$$\mathbb{E}[T] \leq p \cdot \left(1 + \frac{1}{\epsilon}\right) \mathsf{EC}(f) + (1-p) \cdot \mathsf{EC}(f) \leq \left(1 + \frac{p}{\epsilon}\right) \mathsf{EC}(f).$$

- Let $\mathcal{E}_k$ be the event that $\mathcal{A}$ has terminated before the $k$-th iteration. In case $\mathcal{A}$ performs the $k$-th iteration, let $y$ be consistent 1-input chosen and the random variable $i_k$ be the position that $\mathcal{A}$ queries.

$$\begin{aligned}
\mathbb{E}[T_k] &= \Pr[\mathcal{E}_k] \cdot \frac{1}{\mathsf{EC}(f)} + \Pr[\overline{\mathcal{E}_k}] \cdot \mathbb{E}[w_x(i_k) \mid \overline{\mathcal{E}_k}] \\
&\geq \Pr[\mathcal{E}_k] \cdot \frac{1}{\mathsf{EC}(f)} + \Pr[\overline{\mathcal{E}_k}] \cdot \sum_{i : x_i \neq y_i} w_x(i) \mu_y(i) \\
&= \Pr[\mathcal{E}_k] \cdot \frac{1}{\mathsf{EC}(f)} + \Pr[\overline{\mathcal{E}_k}] \cdot \sum_{i : x_i \neq y_i} w_x(i) w_y(i) / \sum_{i \in [n]} w_y(i) \\
&\geq \Pr[\mathcal{E}_k] \cdot \frac{1}{\mathsf{EC}(f)} + \Pr[\overline{\mathcal{E}_k}] \cdot \frac{1}{\mathsf{EC}(f)} \\
&= \frac{1}{\mathsf{EC}(f)},
\end{aligned}$$

  The first inequality here follows from the fact that any $i$ such that $x_i \neq y_i$ has not been queried yet, because $x$ and $y$ are both consistent with the queries made so far. Thus, the inequality holds regardless of the randomness chosen by $\mathcal{A}$. The second inequality follows from the expectational certificate properties $\sum_{i : x_i \neq y_i} w_x(i) w_y(i) \geq 1$ and $\sum_{i \in [n]} w_y(i) \leq \mathsf{EC}(f)$. By the linearity of expectation, we have that

$$\mathbb{E}[T] = \sum_{k=1}^{\mathsf{EC}(f)^2/\epsilon} \mathbb{E}[T_k] \geq \mathsf{EC}(f)/\epsilon.$$

Combining the two bounds together, we get $\frac{\mathsf{EC}(f)}{\epsilon} \leq \left(1 + \frac{p}{\epsilon}\right) \mathsf{EC}(f)$. Thus, $p \geq 1 - \epsilon$. □

□

### 3.2 Relation with the Fractional Certificate Complexity

**Lemma 7.** $\mathsf{FC}(f) \leq \mathsf{EC}(f)$.

*Proof.* We show that a feasible solution $\{w_x\}_x$ for $\mathsf{EC}(f)$ is also feasible for $\mathsf{FC}(f)$. Since $0 \leq w_x(i) \leq 1$ for any $x, i$,

$$\sum_{i : x_i \neq y_i} w_x(i) \geq \sum_{i : x_i \neq y_i} w_x(i) w_y(i) \geq 1,$$

and we are done. □

**Lemma 8.** $\mathsf{EC}(f) = O(\mathsf{FC}(f) \sqrt{\mathsf{s}(f)})$.

*Proof.* Let $\{v_x\}_x$ be an optimal solution to the fractional certificate linear program for $f$. We first modify each $v_x$ to a new feasible solution $v'_x$ by eliminating the entries $v_x(i)$ that are very small, and boosting the large entries by a constant factor. Namely, let

$$v'_x(i) = \begin{cases} \min\left\{\frac{3}{2} v_x(i), 1\right\}, & \text{if } v_x(i) \geq \frac{1}{3\mathsf{s}(f)}, \\ 0, & \text{otherwise.} \end{cases}$$

We first claim that $\{v'_x\}_x$ is still a feasible solution. Fix any $x \in \{0,1\}^n$, and let $B$ be a minimal sensitive block for $x$. As $v_x$ is part of a feasible solution, we have

$$1 \le \sum_{i \in B} v_x(i) = \sum_{\substack{i \in B, \\ v_x(i) < 1/3s(f)}} v_x(i) + \sum_{\substack{i \in B, \\ v_x(i) \ge 1/3s(f)}} v_x(i) \le \frac{1}{3} + \sum_{\substack{i \in B, \\ v_x(i) \ge 1/3s(f)}} v_x(i).$$

The second line follows because $|B| \le s(f)$, as $B$ is a minimal sensitive block and therefore every index in $B$ is sensitive. Rearranging the last inequality, we have $\sum_{\substack{i \in B \\ v_x(i) \ge 1/3s(f)}} v_x(i) \ge \frac{2}{3}$, and therefore, $\sum_{i \in B} v'_x(i) \ge 1$.

Next, $w_x(i) := \sqrt{v'_x(i)}$ is a feasible solution to the expectational certificate program, as

$$\sum_{i : x_i \neq y_i} w_x(i) w_y(i) = \sum_{i : x_i \neq y_i} \sqrt{v'_x(i) v'_y(i)} \ge \sum_{i : x_i \neq y_i} \min\{v'_x(i), v'_y(i)\} \ge 1.$$

The second inequality holds by Lemma 5.

Now that we have shown that $\{w_x\}_x$ forms a feasible solution to the expectation certificate program, it remains to bound its objective value:

$$\sum_{i \in [n]} w_x(i) = \sum_{i \in [n]} \sqrt{v'_x(i)} = \sum_{i : v'_x(i) \neq 0} \frac{v'_x(i)}{\sqrt{v'_x(i)}} \le \sqrt{3s(f)} \sum_{i \in [n]} v'_x(i) \le \sqrt{3s(f)} \frac{3}{2} \mathsf{FC}(f), \qquad \square$$

where the first inequality follows from $v'_x(i) \ge v_x(i) \ge 1/3s(f)$ for $v'_x(i) \neq 0$.

Since $\mathsf{s}(f) \le \mathsf{FC}(f)$ and $\mathsf{FC}(f) \le \mathsf{R}(f)$, we immediately get

**Corollary 9.** $\mathsf{EC}(f) = O(\mathsf{FC}(f)^{3/2}) = O(\mathsf{R}(f)^{3/2})$.

### 3.3 Relation with the Certificate Complexity

**Lemma 10.** $\mathsf{EC}(f) \le \mathsf{C}(f)$.

*Proof.* We construct a feasible solution $\{w_x\}_x$ for $\mathsf{EC}(f)$ from $\mathsf{C}(f)$. Let $A_x$ be the shortest certificate for $x$. Assign $w_x(i) = 1$ iff $i \in A_x$, otherwise let $w_x(i) = 0$. Let $x, y$ be any two inputs such that $f(x) \neq f(y)$. There is a position $i$ where $A_x(i) \neq A_y(i)$, otherwise there would be an input consistent with both $A_x$ and $A_y$, which would give a contradiction. Therefore, $w_x(i) w_y(i) \ge 1$. The value of this solution is $\max_x \sum_{i \in [n]} w_x(i) = \max_x \mathsf{C}(f, x) = \mathsf{C}(f)$. $\square$

As $\mathsf{FC}(f) \le \mathsf{EC}(f) \le \mathsf{C}(f) \le \mathsf{FC}(f)^2$, there can be at most quadratic separation between $\mathsf{EC}(f)$ and $\mathsf{C}(f)$. We show that this is achieved by the example of Gilmer et. al. that separates $\mathsf{FC}(f)$ and $\mathsf{C}(f)$ quadratically:

**Theorem 11** ([GSS16], Theorem 32)**.** *For every $n \in \mathbb{N}$ sufficiently large, there is a function $f : \{0,1\}^{n^2} \to \{0,1\}$ such that $\mathsf{FC}(f) = O(n)$ and $\mathsf{C}(f) = \Omega(n^2)$.*

Their construction for $f$ is as follows. First a function $g : \{0,1\}^n \to \{0,1\}$ is exhibited such that $\mathsf{FC}^0(g) = \Theta(1)$, $\mathsf{C}^0(g) = \Theta(n)$ and $\mathsf{FC}^1(g) = \mathsf{C}^1(f) = n$. The function $f : \{0,1\}^{n^2} \to \{0,1\}$ is defined as a composition $\textsc{Or}(g(x^{(1)}), \ldots, g(x^{(n)}))$. This gives $\mathsf{FC}(f) = \max\{n\mathsf{FC}^0(g), \mathsf{FC}^1(g)\} = \Theta(n)$ and $\mathsf{C}(f) \ge n\mathsf{C}^0(g) = \Theta(n^2)$ (both properties follow by Proposition 31 in their paper).

Let us construct a feasible solution $w$ for $\mathsf{EC}(f)$. For any $x = x^{(1)} \ldots x^{(n)}$ such that $f(x) = 1$, let $j$ be the first index such that $g(x^{(j)}) = 1$. Let $S \subseteq [n^2]$ be the set of positions that correspond to $x^j$. Let $w_x(i) = 1$ for each position $i$ in $S$, and $w_x(i) = 0$ for all other positions. Then $\sum_{i=1}^{n^2} w_x(i) = n$.

On the other hand, let $\{v_x\}_{x \in \{0,1\}^n}$ be an optimal solution to $\mathsf{FC}(f)$. For any $x \in \{0,1\}^{n^2}$ such that $f(x) = 0$, let $w_x(i) = v_x(i)$ for all $i \in [n^2]$. Then $\sum_{i=1}^{n^2} w_x(i) = \mathsf{FC}(f, x) = O(n)$.

Now, for any two inputs $x, y$ such that $f(x) = 1$ and $f(y) = 0$, let $j$ be the smallest index such that $g(x^{(j)}) = 1$, then we have $g(y^{(j)}) = 0$. By construction,

$$\sum_{i : x_i \neq y_i} w_x(i) w_y(i) = \sum_{i : x_i \neq y_i} w_y(i) \ge 1.$$

Hence $\{w_x\}_x$ is a feasible solution to the expectational certificate and $\mathsf{EC}(f) = n$.

# 4 Minimum Query Corruption Bound and Partition Bound

In this section we prove Theorem 2. We first consider the *query corruption bound* and *minimum query corruption bound*.

**Definition 9** (Query Corruption Bound and Minimum Query Corruption Bound for product distributions)**.** Let $\epsilon \in [0, 1/2)$ and $\mu : \{0,1\}^n \to [0,1]$ be a probability distribution over the inputs. For a $b \in \{0,1\}$, let an assignment $A$ be an $\epsilon$-error $b$-certificate under $\mu$, if

$$\Pr_{x\sim\mu}[f(x) \neq b \,|\, x \in A] \leq \epsilon.$$

Define the *query corruption bound* for $b$, distribution $\mu$ and error $\epsilon$ as

$$\mathsf{corr}_\epsilon^{b,\mu}(f) = \min\{|A| \mid A \text{ is an } \epsilon\text{-error } b\text{-certificate under } \mu\}.$$

The query corruption bound of $f$ is defined as $\mathsf{corr}_\epsilon(f) = \max_\mu \max_b \mathsf{corr}_\epsilon^{b,\mu}(f)$, where $\mu$ ranges over all distributions on $\{0,1\}^n$. The *minimum* query corruption bound of $f$ *for product distributions* is defined as $\mathsf{corr}^\times_{\min,\epsilon}(f) = \max_\mu \min_b \mathsf{corr}_\epsilon^{b,\mu}(f)$, where $\mu$ ranges over all product distributions on $\{0,1\}^n$.

We now proceed to the proof of Theorem 2 (restated below).

**Theorem 2.** Let $\epsilon \in [0, 1/2)$ and $\mu$ a product distribution over the inputs. Then

$$\mathsf{D}^\mu_{4\epsilon}(f) = O(\mathsf{corr}^\times_{\min,\epsilon}(f) \cdot \mathsf{bs}(f)).$$

In the proof we will have restrictions of probability distributions. Let $\eta$ be a probability distribution over $\{0,1\}^n$, $x \in \{0,1\}^n$ be a $n$-bit string, and $Q \subseteq \{1,\ldots,n\}$ be a set of indices. The restriction of $x$ to the indices of $Q$, $(x_j : j \in Q)$, will be denoted by $x_Q$. Then the distribution $\eta\,|_{x_Q}$ is the distribution obtained by conditioning $\eta$ on the event that the bits in the locations in $Q$ agree with $x$. Formally, for each $y \in \{0,1\}^n$

$$\eta_{x_Q}(y) = \begin{cases} \frac{\eta(y)}{\sum_{z:\forall i\in Q, z_i = x_i}\eta(z)} & \text{if } \forall i \in Q, y_i = x_i, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof of Theorem 2.* We present a deterministic query algorithm, and analyse its performance for inputs sampled according to $\mu$. Examine the following algorithm:

**Algorithm 2:** The deterministic query algorithm $\mathcal{B}$.

**Input:** $x \in \{0,1\}^n$

1. Set $t_0, t_1 \leftarrow 0, i \leftarrow 1, \eta^{(1)} \leftarrow \mu$.
2. Repeat:
   (a) Pick a shortest $\epsilon$-error certificate $A$ under $\eta$.
   (b) Query all the variables in $Q_A$ that are still unknown.
   (c) Let $A$ be an $\epsilon$-error $b$-certificate for some $b \in \{0,1\}$. Set $t_b \leftarrow t_b + 1$.
   (d) If the results of the queries are consistent with $A$, return $b$.
   (e) If $t_b = 2\mathsf{bs}(f)$, return $b$.
   (f) $\eta^{(i+1)} \leftarrow \eta^{(i)}\,|_{x_{Q_A}}$.
   (g) $i \leftarrow i + 1$.

For each $i = 2,\ldots,4\mathsf{bs}(f)$, define $T^{(i)}$ to be the event that $\mathcal{B}$ completes at least $i-1$ iterations and define $T^{(1)}$ to be the *true* event. Let $i$ be arbitrary, and assume that $T^{(i)}$ occurs. Then $A^{(i)}$ denotes the $\epsilon$-error certificate (under $\eta^{(i)}$) picked in the $i$-th iteration in step 2a. Let $b^{(i)} \in \{0,1\}$ be the value approximately certified by $A^{(i)}$ under $\eta^{(i)}$. Let $E^{(i)} \subseteq A^{(i)}$ denote the set of inputs $y \in A^{(i)}$ such that $f(y) \neq b^{(i)}$. Recall from Section 2 $Q_{A^{(i)}}$ is the set of variables set by $A^{(i)}$. For

each assignment $s \in \{0,1\}^{Q_{A^{(i)}}}$ to the variables fixed by $A^{(i)}$ and subset $U \subseteq A^{(i)}$, let $U \oplus s$ denote the shift of $U$ by the vector $s$. Formally ('$\oplus$' stands for bitwise exlusive or),

$$U \oplus s := \{y \in \{0,1\}^n : \forall j \in Q_{A^{(i)}}, y_j = A^{(i)}_j \oplus s_j \text{ and } \exists z \in U \text{ such that } \forall j \notin Q_{A^{(i)}}, y_j = z_j\}.$$

For $i \geq 2$, define $\mathcal{L}^{(i)}$ to be the set of variables queried in first $i-1$ iterations and define $\mathcal{L}^{(1)} := \varnothing$. Note that $\eta^{(i)} = \mu\,|_{x_{\mathcal{L}^{(i)}}}$, and $\eta^{(i)}$ is a product distribution.

Define all the above random variables to be $\perp$ if $T^{(i)}$ does not take place. Now define

$$X^{(i)} = \begin{cases} 1 & \text{if } T^{(i)} \text{ occurs and } x \in \bigcup_{s \in \{0,1\}^{Q^{(i)}}} E^{(i)} \oplus s, \\ 0 & \text{otherwise.} \end{cases}$$

First we bound the number of queries made by $\mathcal{B}$. Since $\mathcal{B}$ terminates when either $t_0 = 2\mathsf{bs}(f)$ or $t_1 = 2\mathsf{bs}(f)$, it performs at most $4\mathsf{bs}(f) - 1$ many iterations. On the other hand since $\eta^{(i)}$ is a product distribution for each $i$, therefore $|A^{(i)}| \leq \mathsf{corr}^{\times}_{\min,\epsilon}(f)$. Therefore, the algorithm makes $O(\mathsf{corr}^{\times}_{\min,\epsilon}(f) \cdot \mathsf{bs}(f))$ many queries.

Now we prove that it errs on at most $4\epsilon$ fraction of the inputs according to $\mu$.

**Claim 12.** For every $i$ and $s \in \{0,1\}^{Q_A}, \Pr[x \in E^{(i)} \oplus s \mid T^{(i)}, x \in A^{(i)} \oplus s] \leq \epsilon$.

*Proof.* Condition on the events $T^{(i)}, x \in A^{(i)} \oplus s$. Furthermore, condition on $x_{\mathcal{L}^{(i)}}$. Notice that under this conditioning, the distribution of the input $x$ is $\eta^{(i)} = \mu\,|_{x_{\mathcal{L}^{(i)}}}$.

If $T^{(i)}$ occurs, $A^{(i)}$ is an $\epsilon$-error $b^{(i)}$-certificate under $\eta^{(i)}$. So $\Pr_{x\sim\eta^{(i)}}[x \in E^{(i)} \mid T^{(i)}, x \in A^{(i)}] \leq \epsilon$. Since $\eta^{(i)}$ is a product distribution as observed before, we have that for each $s \in \{0,1\}^{Q_{A^{(i)}}}, \Pr_{x\sim\eta^{(i)}}[x \in E^{(i)} \oplus s \mid T^{(i)}, x \in A^{(i)} \oplus s] = \Pr_{x\sim\eta^{(i)}}[x \in E^{(i)} \mid T^{(i)}, x \in A^{(i)}] \leq \epsilon$. The claim follows. □

In particular, Claim 12 implies that for all $i = 1, \ldots, 4\mathsf{bs}(f)$,

$$\Pr[X^{(i)} = 1] \leq \epsilon. \tag{1}$$

Since $\mathcal{B}$ runs for at most $4\mathsf{bs}(f) - 1 < 4\mathsf{bs}(f)$ steps, by Equation (1), linearity of expectation and Markov's inequality we have that

$$\Pr[|\{i \mid X^{(i)} = 1\}| \geq \mathsf{bs}(f)] \leq 4\epsilon. \tag{2}$$

For $i$ such that $T^{(i)}$ occurs, define $S^{(i)} := \{j \in Q_{A^{(i)}} \mid x_j \neq A^{(i)}(j)\}$. The following claim will play a central role in our analysis.

**Claim 13.** Let $i_1 < i_2$. For each $i \in \{i_1, i_2\}$, let $T^{(i)}$ happen and $X^{(i)} = 0$. Then $f(x^{S^{(i)}}) = b^{(i)}, S^{(i_1)} \cap S^{(i_2)} = \varnothing$. In particular, if $b^{(i_1)} = b^{(i_2)}$ and $f(x) = 1 - b^{(i_1)}$ then $S^{(i_1)}$ and $S^{(i_2)}$ are disjoint sensitive blocks for $x$.

*Proof.* Clearly, $x^{S^{(i)}} \in A^{(i)}$. Also, since $X^{(i)} = 0, x \notin E^{(i)} + s$ for any $s$. Thus $x^{S^{(i)}} \notin E^{(i)}$. Hence $f(x^{S^{(i)}}) = b^{(i)}$. To see that $S^{(i_1)} \cap S^{(i_2)} = \varnothing$, let $j \in S^{(i_1)}$. It is easy to see that $i_2 > i_1$ implies that the distribution $\eta^{(i_2)}$ at step $i_2$ is supported only on inputs consistent with $x_{Q_{A^{(i_1)}}}$. Hence, if $j \in Q_{A^{(i_2)}}$, then $x_j = A^{(i_2)}(j)$ which implies that $j \notin S^{(i_2)}$. □

For the rest of the proof, condition on the event that $\mathcal{B}$ terminates at iteration $i$. We will bound the probability that $\mathcal{B}$ errs.

First, condition on the event that $\mathcal{B}$ terminates in step 2d. Then the probability that it errs is $\Pr[x \in E^{(i)} \mid T^{(i)}, x \in A^{(i)}] \leq \epsilon$ (by Claim 12 invoked with $s = 0^{Q_{A^{(i)}}}$).

Next, condition on the event that $\mathcal{B}$ terminates at step 2e, and $t_0 = 2\mathsf{bs}(f)$ (the case $t_1 = 2\mathsf{bs}(f)$ is symmetrical). By Equation (2), $|\{i \mid X^{(i)} = 1\}| \geq \mathsf{bs}(f)$ with probability at most $4\epsilon$. Condition on $|\{i \mid X^{(i)} = 1\}| < \mathsf{bs}(f)$. Then $\mathcal{B}$ outputs 0. We claim that $f(x) = 0$ with probability 1. Towards a contradiction, assume that $f(x) = 1$. As $t_0 = 2\mathsf{bs}(f)$ and $|\{i \mid X^{(i)} = 1\}| < \mathsf{bs}(f)$, then in at least $2\mathsf{bs}(f) - (\mathsf{bs}(f) - 1) = \mathsf{bs}(f) + 1$ iterations $j \leq i$, $b^{(j)} = 0$ and $X^{(j)} = 0$. By Claim 13, the blocks $S^{(j)}$ for those $j$ iterations are sensitive for $x$ and are disjoint. Since any input can have at most $\mathsf{bs}(f)$ sensitive blocks, we have the desired contradiction.

Thus the probability that $\mathcal{B}$ errs is at most $\max\{\epsilon, 4\epsilon\} = 4\epsilon$. □

Now we prove Theorem 3. Below we reproduce the definition of the partition bound by Jain and Klauck [JK10]. Here $\epsilon$ is an error parameter between 0 and 1, $A$ stands for subcubes, or equivalently, partial assignments, $z$ stands for a bit, i.e., a 0 or a 1, and $x$ stands for an input to $f$ from $\{0,1\}^n$.

**Definition 10** (Partition Bound)**.** The *$\epsilon$-partition bound* bound of $f$, denoted $\mathsf{prt}_\epsilon(f)$, is given by the logarithm of the optimal value of the following linear program[1]:

$$\text{minimize} \sum_{z,A} w_{z,A} \cdot 2^{|A|} \qquad \text{subject to} \quad \forall x : \sum_{A \ni x} w_{f(x),A} \geq 1 - \epsilon,$$
$$\forall x : \sum_{z, A \ni x} w_{z,A} = 1,$$
$$\forall z, A : w_{z,A} \geq 0.$$

Jain and Klauck showed that the partition bound bounds randomized query-complexity from below. They also showed that randomized query complexity is bounded above by the third power of the partition bound.

**Theorem 14** ([JK10], Theorem 3)**.**

1. $\mathsf{R}_\epsilon(f) \geq \frac{1}{2}\mathsf{prt}_\epsilon(f)$.
2. $\mathsf{R}_{1/3}(f) \leq \mathsf{D}(f) = O(\mathsf{prt}_{1/3}(f)^3)$.

The best known separation between $\mathsf{D}(f)$ and $\mathsf{prt}(f)$ is quadratic [AKK16]. Theorem 3 proves that this is tight for product distributions. As stated in Section 1, Theorem 3 improves upon the result of Jain et al. by a polylogarithmic factor.

Jain and Klauck showed that the partition bound is bounded below by the block sensitivity.

**Theorem 15** ([JK10], Theorem 3)**.** *For any error parameter $\epsilon \in [0, 1/2)$,*

$$\mathsf{prt}_{\epsilon/4}(f) \geq \epsilon \cdot \mathsf{bs}(f) + \log \epsilon - 2.$$

We show that the minimum query corruption bound lower bounds the partition bound (see Appendix A for the proof). Our proof closely follows the proof that the corruption bound is asymptotically bounded above by square of the partition bound shown in [JK10].

**Lemma 16.** *For any error parameter $\epsilon \in [0, 1/2)$,*

$$\mathsf{corr}^{\times}_{\min,2\epsilon}(f) \leq \mathsf{prt}_\epsilon(f) \cdot \log(1/\epsilon).$$

Theorem 3 now follows, combining Theorems 2, 15 and Lemma 16 together.

We conclude by showing that the query corruption bound is a quadratic upper bound on the distributional query complexity.

**Theorem 17.** *Let $\epsilon \in [0, 1/2)$ and $\mu$ a product distribution over the inputs. Then*

$$\mathsf{D}^{\mu}_{4\epsilon}(f) = O\left(\mathsf{corr}_\epsilon(f)^2\right).$$

The result follows by combining Theorem 2 with the following lemma (see Appendix B for the proof).

**Lemma 18.** *For any $\epsilon \in [0, 1)$, $\mathsf{fbs}(f) \leq \mathsf{corr}_\epsilon(f)$.*

# 5 Open Problems

**Expectational vs. Fractional Certificate.** What is the largest separation between the two measures? Is the upper bound $\mathsf{EC}(f) \leq \mathsf{FC}(f)^{3/2}$ tight? Any smaller upper bound would improve the $\mathsf{R}(f) \leq \mathsf{FC}(f)^3$ upper bound. Our attempts in finding a function where $\mathsf{EC}(f)$ is asymptotically larger than $\mathsf{FC}(f)$ so far have been unsuccessful. As evident by the proof of the quadratic separation between $\mathsf{EC}(f)$ and $\mathsf{C}(f)$, such an example would need to have $\mathsf{FC}^z(f) = o(\mathsf{C}^z(f))$ for both $z \in \{0,1\}$. Examples of separations between $\mathsf{FC}(f)$ and $\mathsf{C}(f)$ given in [Aar08] and [GSS16] do not satisfy these properties.

[1] Jain and Klauck in their paper defined $\mathsf{prt}_\epsilon(f)$ to be the value of the linear program, instead of the logarithm of the value of the program.

**Corruption and Partition Bounds.** Can the proof of Theorem 2 be extended to non-product distributions? The definition of the corruption bound is in some sense a relaxation of the certificate compexity. Can the argument of $\mathsf{D}(f) \leq \mathsf{C}(f)^2$ be extended to the randomized setting in terms of the corruption bound?

## Acknowledgements.

This work is supported in part by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13, the Ministry of Education, Singapore under the Research Centres of Excellence programme by the Tier-3 grant Grant "Random numbers from quantum processes" No. MOE2012-T3-1-009.

D.G. is partially funded by the grant P202/12/G061 of GA ČR and by RVO: 67985840. Part of this work was done while D.G. was visiting the Centre for Quantum Technologies at the National University of Singapore.

M.S. is partially funded by the ANR Blanc program under contract ANR-12-BS02-005 (RDAM project).

J.V. is supported by the ERC Advanced Grant MQC. Part of this work was done while J.V. was an intern at the Centre for Quantum Technologies at the National University of Singapore.

We thank Anurag Anshu for helpful discussions.

## References

[Aar08] Scott Aaronson. Quantum certificate complexity. *Journal of Computer and System Sciences*, 74(3):313–322, 2008.

[ABDK16] 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.

[AKK16] Andris Ambainis, Martins Kokainis, and Robin Kothari. Nearly optimal separations between communication (or query) complexity and partitions. In *Proceedings of the 31st Conference on Computational Complexity*, CCC '16, pages 4:1–4:14, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001.

[BdW02] Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002.

[BI87] Manuel Blum and Russell Impagliazzo. Generic oracles and oracle classes. In *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, SFCS '87, pages 118–126, Washington, DC, USA, 1987. IEEE Computer Society.

[GSS16] Justin Gilmer, Michael Saks, and Srikanth Srinivasan. Composition limits and separating examples for some Boolean function complexity measures. *Combinatorica*, 36(3):265–311, 2016.

[HH87] Juris Hartmanis and Lane A. Hemachandra. One-way functions, robustness, and non-isomorphism of **NP**-complete sets. In *Proceedings of 2nd Structure in Complexity Theory*, pages 160–173, 1987.

[HJR15] Prahladh Harsha, Rahul Jain, and Jaikumar Radhakrishnan. Relaxed partition bound is quadratically tight for product distributions. *CoRR*, abs/1512.01968, 2015.

[JK10] 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.

[KT16] Raghav Kulkarni and Avishay Tal. On fractional block sensitivity. *Chicago Journal Of Theoretical Computer Science*, 8:1–16, 2016.

[Nis89] N. 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.

[Tal13] 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.

[Tar90] G. Tardos. Query complexity or why is it difficult to separate $\mathbf{NP}^A \cap \mathbf{coNP}^A$ from $\mathbf{P}^A$ by a random oracle. *Combinatorica*, 9:385–392, 1990.

# A Proof of Lemma 16

*Proof.* Let $c = \mathsf{prt}_\epsilon(f)$. Abusing notation, let $\{w_{z,A}\}_{z,A}$ be a primal feasible point which minimizes the objective. Thus $\sum_{z,A} w_{z,A} \cdot 2^{|A|} = 2^c$. We immediately have that,

$$2^c \geq \sum_{z,A:|A|>c\log(1/\epsilon)} w_{z,A} \cdot 2^{|A|} \geq \frac{2^c}{\epsilon} \sum_{z,A:|A|>c\log(1/\epsilon)} w_{z,A}.$$

implying,

$$\sum_{z,A:|A|>c\log(1/\epsilon)} w_{z,A} \leq \epsilon. \tag{3}$$

Let $\mu$ be any product probability distribution on $\{0,1\}^n$ (in fact, the proof works for any distribution $\mu$). Without loss of generality, assume that, $\Pr_{x\sim\mu}[f(x)=1] \geq \Pr_{x\sim\mu}[f(x)=0]$. We shall show that $\mathsf{corr}^{1,\mu}_\epsilon(f) = O(c)$. That will prove the theorem.

If $\Pr_{x\sim\mu}[f(x)=0] = 0$ then $\{0,1\}^n$ is a 0-error 1-certificate of co-dimension 0, and we are done. From now on, we will assume that $\Pr_{x\sim\mu}[f(x)=0] > 0$.

Equation (3) and the two primal constraints imply that for each $x \in \{0,1\}^n$,

$$\sum_{A\ni x,|A|\leq c\log(1/\epsilon)} w_{f(x),A} \geq 1-2\epsilon; \tag{4}$$

$$\sum_{A\ni x,|A|\leq c\log(1/\epsilon)} w_{1-f(x),A} \leq 2\epsilon. \tag{5}$$

Multiplying Equations (4) and (5) by $\mu_x$, adding the former over $f^{-1}(1)$ and the later over $f^{-1}(0)$, and re-arranging the order of summations we have,

$$\sum_{A:|A|\leq c\log(1/\epsilon)} \sum_{x\in A,f(x)=1} \mu(x)\cdot w_{1,A} \geq (1-2\epsilon)\cdot \sum_{x\in f^{-1}(1)} \mu(x); \tag{6}$$

$$\sum_{A:|A|\leq c\log(1/\epsilon)} \sum_{x\in A,f(x)=0} \mu(x)\cdot w_{1,A} \leq 2\epsilon\cdot \sum_{x\in f^{-1}(0)} \mu(x). \tag{7}$$

Dividing Equation (6) by Equation (7) (note that $\sum_{x\in f^{-1}(0)}\mu_x \neq 0$ by our assumption about $\mu$), we have that,

$$\frac{\sum_{A:|A|\leq c\log(1/\epsilon)} w_{1,A}\cdot\left(\sum_{x\in A,f(x)=1}\mu(x)\right)}{\sum_{A:|A|\leq c\log(1/\epsilon)} w_{1,A}\cdot\left(\sum_{x\in A,f(x)=0}\mu(x)\right)} \geq \frac{1-2\epsilon}{2\epsilon}\cdot\frac{\sum_{x\in f^{-1}(1)}\mu(x)}{\sum_{x\in f^{-1}(0)}\mu(x)} \geq \frac{1-2\epsilon}{2\epsilon}.$$

The last inequality above holds because of our assumption about $\mu$. This implies that there exists a subcube $A$ with co-dimension $|A| \leq c\log(1/\epsilon)$ such that,

$$\frac{\sum_{x\in A,f(x)=1}\mu(x)}{\sum_{x\in A,f(x)=0}\mu(x)} \geq \frac{1-2\epsilon}{2\epsilon}.$$

Thus,

$$\Pr_{x\sim\mu}[f(x)=1 \mid x\in A] \geq 1-2\epsilon.$$

In other words, $A$ is a $2\epsilon$-error 1-certificate under $\mu$. We have,

$$\mathsf{corr}^{\mu}_{\min,2\epsilon}(f) \leq \mathsf{corr}^{1,\mu}_{2\epsilon}(f) \leq |A| \leq \mathsf{prt}_\epsilon(f)\cdot\log(1/\epsilon). \qquad \square$$

# B Proof of Lemma 18

*Proof.* Let $x$ be such that $\mathsf{fbs}(f,x) = \mathsf{fbs}(f)$, and let $b = f(x)$. We construct a distribution $\mu$ such that $\mathsf{corr}^{b,\mu}_\epsilon(f) \geq \mathsf{fbs}(f)$.

Suppose that $x$ has $k$ sensitive blocks $B_1, \ldots, B_k$. Let $u_1, \ldots, u_k$ be the corresponding solution to the $\mathsf{fbs}(f, x)$ linear program. Let $c \in (0, 1-\epsilon)$ be a constant and define $\mu(x) = c$ and $\mu(x^{B_i}) = (1-c)\frac{u_i}{\sum_{i=1}^k u_i} = (1-c)\frac{u_i}{\mathsf{fbs}(f)}$. Clearly, $\mu$ is a probability distribution on $\{0,1\}^n$.

Let $A$ be an $\epsilon$-error $b$-certificate according to $\mu$ and recall that $Q_A$ is the set of variables fixed by $A$. Any input $x^{B_i}$ is inconsistent with $A$ iff $B_i \cap Q_A \neq \varnothing$, thus

$$\sum_{i:B_i \cap Q_A \neq \varnothing} \mu(x^{B_i}) = \Pr_{y\sim\mu}\left[f(y) \neq b, y \notin A\right].$$

We also have

$$\frac{\Pr_{y\sim\mu}\left[f(y) = b, y \in A\right]}{\Pr_{y\sim\mu}\left[f(y) = b, y \in A\right] + \Pr_{y\sim\mu}\left[f(y) \neq b, y \in A\right]} \geq 1 - \epsilon$$

by definition of $A$. Since $\Pr_{y\sim\mu}\left[f(y) = b, y \in A\right] = c$, this implies

$$\Pr_{y\sim\mu}\left[f(y) \neq b, y \in A\right] \leq c \cdot \frac{\epsilon}{1-\epsilon}.$$

Then we get

$$\Pr_{y\sim\mu}\left[f(y) \neq b, y \notin A\right] = \Pr_{y\sim\mu}\left[f(y) \neq b\right] - \Pr_{y\sim\mu}\left[f(y) \neq b, y \in A\right] \geq (1-c) - c \cdot \frac{\epsilon}{1-\epsilon} = 1 - c \cdot \frac{1}{1-\epsilon}.$$

On the other hand, since $\sum_{i:j\in B_i} u_i \leq 1$ for each $j \in [n]$, we have

$$\sum_{i:B_i \cap Q_A \neq \varnothing} \mu(x^{B_i}) \leq \sum_{j\in Q_A} \sum_{i:j\in B_i} \mu(x^{B_i}) = \sum_{j\in Q_A} \sum_{i:j\in B_i} (1-c)\frac{u_i}{\mathsf{fbs}(f)} \leq (1-c)\frac{|A|}{\mathsf{fbs}(f)}.$$

Therefore,

$$\frac{\mathsf{corr}_\epsilon(f)}{\mathsf{fbs}(f)} \geq \frac{\mathsf{corr}_\epsilon^{b,\mu}(f)}{\mathsf{fbs}(f)} \geq \frac{|A|}{\mathsf{fbs}(f)} \geq \frac{1-\epsilon-c}{(1-\epsilon)(1-c)} = \frac{1-\epsilon-c}{1-\epsilon-c+\epsilon c}.$$

Since the above relation is true for every $c$, we have,

$$\frac{\mathsf{corr}_\epsilon(f)}{\mathsf{fbs}(f)} \geq \lim_{c\to 0} \frac{1-\epsilon-c}{1-\epsilon-c+\epsilon c} = 1.$$

Thus we have $\mathsf{corr}_\epsilon(f) \geq \mathsf{fbs}(f)$. □



ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il