Quadratically Tight Relations for Randomized Query Complexity

Rahul Jain1,2 · Hartmut Klauck1,3 · Srijita Kundu1 · Troy Lee1,3 · Miklos Santha1,4 · Swagato Sanyal1,3 · Jevgēnijs Vihrovs5

Published online: 10 August 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
In this work we investigate the problem of quadratically tightly approximating the randomized query complexity of Boolean functions $R(f)$. The certificate complexity $C(f)$ is such a complexity measure for the zero-error randomized query complexity $R_0(f)$: $C(f) \leq R_0(f) \leq C(f)^2$. In the first part of the paper we introduce a new complexity measure, expectational certificate complexity $EC(f)$, which is also a quadratically tight bound on $R_0(f)$: $EC(f) \leq R_0(f) = O(EC(f)^2)$. For $R(f)$, we prove that $EC^{2/3} \leq R(f)$. We then prove that $EC(f) \leq C(f) \leq EC(f)^2$ and show that there is a quadratic separation between the two, thus $EC(f)$ gives a tighter upper bound for $R_0(f)$. The measure is also related to the fractional certificate complexity $FC(f)$ as follows: $FC(f) \leq EC(f) = O(FC(f)^{3/2})$. This also connects to an open question by Aaronson whether $FC(f)$ is a quadratically tight bound for $R_0(f)$, as $EC(f)$ is in fact a relaxation of $FC(f)$. In the second part of the work, we investigate whether the corruption bound $corr_\epsilon(f)$ quadratically approximates $R(f)$. By Yao’s theorem, it is enough to prove that the square of the corruption bound upper bounds the distributed query complexity $D_\mu^\epsilon(f)$ for all input distributions $\mu$. Here, we show that this statement holds for input distributions in which the various bits of the input are distributed independently. This is a natural and interesting subclass of distributions, and is also in the spirit of the input distributions studied in communication complexity in which the inputs to the two communicating parties are statistically independent. Our result also improves upon a result of Harsha et al. (2016), who proved a similar weaker statement. We also note that a similar statement in the communication complexity is open.

Keywords Query complexity · Randomized algorithms · Certificate complexity · Fractional block sensitivity · Corruption bound

This article is part of the Topical Collection on Computer Science Symposium in Russia (2018)

Jevgēnijs Vihrovs
jevgenijs.vihrovs@lu.lv

Extended author information available on the last page of the article.
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 \( f : \{0,1\}^n \rightarrow \{0,1\} \) 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 produced 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 [6] 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 [2]. In this work, we focus on characterizing the bounded-error and zero-error randomized query complexity measures, denoted by \( R(f) \) and \( \text{R}_0(f) \), respectively. More specifically, we study measures that could quadratically approximate the randomized query complexity for all Boolean functions.

The following measures are known to lower bound \( \text{R}_0(f) \): block sensitivity \( \text{bs}(f) \), fractional certificate complexity \( \text{FC}(f) \) (also known as fractional block sensitivity \( \text{fbs}(f) \), [13]), and certificate complexity \( C(f) \). They are related as follows:

\[
\text{bs}(f) \leq \text{fbs}(f) = \text{FC}(f) \leq C(f).
\]

Let \( D(f) \) denote the deterministic query complexity of \( f \). It is known that \( \text{R}_0(f) \leq D(f) \leq C(f)^2 \), and the TRIBES function (an AND of \( \sqrt{n} \) ORs on \( \sqrt{n} \) bits) demonstrates that this upper bound is tight, \( C(\text{TRIBES}) = \sqrt{n} \) and \( \text{R}_0(\text{TRIBES}), D(\text{TRIBES}) = \Theta(n) \) [10]. It is also known that \( \text{R}_0(f) = O(\text{bs}(f)^3) = O(\text{FC}(f)^3) \) [4, 12]. A quadratic separation between \( \text{R}_0(f) \) and \( \text{FC}(f) \) is also achieved by TRIBES. Aaronson posed a question whether \( \text{R}_0(f) = O(\text{FC}^2(f)) \) holds [1] (stated in terms of the randomized certificate complexity \( \text{RC}(f) \), which later has been shown to be equivalent to \( \text{FC}(f) \) [7]). A positive answer to this question would imply that \( \text{R}_0(f) = O(\deg(f)^4) = O(\text{Q}(f)^4) \) [2], where \( \deg(\cdot) \) and \( \text{Q}(\cdot) \) stand for approximate polynomial degree and quantum query complexity respectively.

One approach to showing \( \text{R}_0(f) \leq \text{FC}(f)^2 \) is to consider the natural generalization of the proof \( D(f) \leq C(f)^2 \) to the randomized case; the analysis of this algorithm, however, has met some unresolved obstacles [11]. We define a new complexity measure \( \text{EC}(f) \) that is specifically designed to avert these problems and is of a similar form to \( \text{FC}(f) \). We show that \( \text{EC} \) gives a quadratically tight bound for \( \text{R}_0 \):

\[
\text{EC}(f) \leq \text{FC}(f) \leq C(f).
\]
Theorem 1 For all total Boolean functions $f$, 

$$EC(f) \leq R_0(f) \leq O(EC(f)^2).$$

In fact, FC($f$) is a relaxation of EC($f$), and we show that FC($f$) $\leq$ EC($f$) $\leq$ C($f$). Moreover, we show that EC($f$) lies closer to FC($f$) than C($f$) does: FC($f$) $\leq$ EC($f$) $\leq$ FC($f$)$^{3/2}$, while FC($f$) $\leq$ C($f$) $\leq$ FC($f$)$^2$ [7, 13]. While we don’t know whether EC($f$) is a lower bound on $R(f)$, EC($f$) $\leq$ FC($f$)$^{3/2}$ together with $R(f) = \Omega(FC(f))$ [7, 13] gives $R(f) = \Omega(EC(f)^{2/3})$.

As mentioned earlier, C($f$)$^2$ bounds $R_0(f)$ from above. But for specific functions, EC($f$)$^2$ can be an asymptotically tighter upper bound than C($f$)$^2$. We demonstrate that by showing that the same example that provides a quadratic separation between C($f$) and FC($f$) [7] also gives C($f$) $= \Omega(EC(f)^2)$. This is the widest separation possible between EC($f$) and C($f$), because C($f$) $\leq$ $R_0(f) = O(EC(f)^2)$.

In the second part of the paper, we investigate whether the query corruption bound corr$_e$($f$) quadratically approximates $R(f)$. By Yao’s Minimax Principle (see Fact 4), it is sufficient to show that the distributional query complexity $D_{\mu}^{4\epsilon} (f)$ is upper bounded by the square of corr$_e$($f$) for all distributions $\mu$. We show that this holds for the bitwise product distributions, where the distributional query complexity can be upper bounded by the product of the minimum product query corruption bound corr$_{\min, \epsilon}$($f$) and the block sensitivity bs($f$) (see Definition 10 and Section 2 (Fig. 1)).

Theorem 2 Let $\epsilon \in [0, 1/8)$ and $\mu$ a product distribution over the inputs. Then

$$D_{4\epsilon}^{\mu} (f) = O(corr_{\min, \epsilon}^x (f) \cdot bs(f)).$$

![Fig. 1 Lower bounds on $R_0(f)$ and $R(f)$](image_url)
We then show that $\text{bs}(f) \leq \text{corr}_\epsilon(f)$, thus $D_{4\epsilon}(f) = O(\text{corr}_\epsilon(f)^2)$ (Theorem 8), as we have $\text{corr}_{\min,\epsilon}(f) \leq \text{corr}_\epsilon(f)$.

We contrast Theorem 2 with the past work by Harsha, Jain and Radhakrishnan [8], who showed that for product distributions, the distributional query complexity is bounded above by the square of the smooth corruption bound (which is equivalent to the relaxed partition bound) corresponding to inverse polynomial error. Theorem 8, a consequence of Theorem 2, improves upon their result, firstly by upper bounding the distributional complexity with the 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. Thus Theorem 8 resolves a question that was open after the work of Harsha et al. The analogous question in communication complexity from their paper is still open.

Theorem 2 also bounds distributional query complexity in terms of the partition bound $\text{prt}(\cdot)$ of Jain and Klauck [10]. The following theorem follows from Theorems 2, 7 and Lemma 5.

**Theorem 3** Let $\epsilon \in \left[0, \frac{1}{16}\right)$ and $\mu$ a product distribution over the inputs. Then

$$D_{8\epsilon}(f) = O(\text{prt}_\epsilon(f)^2).$$

Jain and Klauck showed that $\text{prt}(f)$ is a powerful lower bound on $R(f)$. In the same work, $\text{prt}(f)$ was used to give a tight $\Omega(n)$ lower bound on $R(f)$ for the TRIBES function on $n$ bits. The authors proved that $\text{prt}(f)$ is asymptotically larger than $\text{FC}(f)$. This implies that $R(f) = O(\text{prt}(f)^3)$, since $R(f) = O(\text{bs}(f)^3)$. While a quadratic separation between $R(f)$ and $\text{prt}(f)$ is known [3], it is open whether $R(f) = O(\text{prt}(f)^2)$. Theorem 3 proves a distributional version of this quadratic relation, for the special case in which the input is sampled from a product distribution, i.e., a distribution where the input bits are independently distributed. We remark here that Harsha, Jain and Radhakrishnan [8] proved in their work that $D_{1/3}(f) = O(\text{prt}_{1/3}(f)^2 \cdot (\log \text{prt}_{1/3}(f))^2)$; Theorem 3 achieves poly-logarithmic improvement over this bound. Once again, an analogous statement for an arbitrary distribution together with the Minimax Principle will imply that $R(f) = O(\text{prt}(f)^2)$.

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 [6]. For the rest of this paper, $f$ is any total Boolean function on $n$ bits, $f : \{0, 1\}^n \rightarrow \{0, 1\}$. 

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

The zero-error randomized query complexity $R_0(f)$ is defined as

$$\min_{A} \max_{x} \mathbb{E}_r[C(A, x, r)],$$

where $A$ is any randomized algorithm such that for all $x \in \{0, 1\}^n$, we have $\Pr_r[A(x, r) = f(x)] = 1$.

The one-sided error randomized query complexity $R_1^\epsilon(f)$ is defined as $\min_{A} C(A)$, where $A$ is any randomized algorithm such that for every $x$ such that $f(x) = 0$, we have $\Pr_r[A(x, r) = 1] \leq \epsilon$, and for all $x$ such that $f(x) = 1$, we have $\Pr_r[A(x, r) = 1] = 1$. Similarly we define $R_1^\epsilon(f)$.

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

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 $D_\mu^\epsilon(f)$ is the minimum number of queries made in the worst case (over inputs) by a deterministic query algorithm $A$ for which $\Pr_{x \sim \mu}[A(x) = f(x)] \geq 1 - \epsilon$.

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

Fact 4 (Minimax Principle) For any Boolean function $f$, $R_\epsilon(f) = \max_{\mu} D_\mu^\epsilon(f)$.

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 (Assignment) 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 $A$, 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 $A$.

Definition 5 (Certificate Complexity) 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 $C(f, x)$ of
on $x$ is the size of the shortest $f(x)$-certificate that is consistent with $x$. The certificate complexity of $f$ is defined as $C(f) = \max_{x \in \{0, 1\}^n} C(f, x)$. The $b$-certificate complexity of $f$ is defined as $C^b(f) = \max_{x : f^{-1}(b)} C(f, x)$.

**Definition 6 (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 $s(f, x)$ 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 $s(f) = \max_{x \in \{0, 1\}^n} s(f, x)$.

The block sensitivity $bs(f, x)$ 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 $bs(f) = \max_{x \in \{0, 1\}^n} bs(f, x)$.

**Definition 7 (Fractional Certificate Complexity)** The fractional certificate complexity $FC(f, x)$ of $f$ on $x \in \{0, 1\}^n$ is defined as the optimal value of the following linear program:

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

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 $FC(f) = \max_{x \in \{0, 1\}^n} FC(f, x)$. The fractional $b$-certificate complexity of $f$ is defined as $FC^b(f) = \max_{x : f^{-1}(b)} FC(f, x)$.

**Definition 8 (Fractional Block Sensitivity)** Let $B = \{B \mid f(x) \neq f(x^B)\}$ be the set of sensitive blocks of $x$. The fractional block sensitivity $fbs(f, x)$ of $f$ on $x$ is defined as the optimal value of the following linear program:

$$
\begin{align*}
\text{maximize} & \quad \sum_{B \in \mathcal{B}} u_x(B) \\
\text{subject to} & \quad \forall i \in [n] : \sum_{B \in \mathcal{B}} u_x(B) \leq 1.
\end{align*}
$$

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 $fbs(f) = \max_{x \in \{0, 1\}^n} fbs(f, x)$.

Fractional certificate complexity and fractional block sensitivity were discovered independently by Tal [13] and Gilmer, Saks and Srinivasan [7]. The linear programs $FC(f, x)$ and $fbs(f, x)$ are duals of each other, hence their optimal solutions are equal and $FC(f) = fbs(f)$.

### 3 Expectational Certificate Complexity

In this section, we give the results for the expectational certificate complexity. The measure is motivated by the well-known $D(f) \leq C^0(f)C^1(f)$ deterministic query algorithm which was independently discovered several times [5, 9, 14]. 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 $R(f) \leq FC^0(f)FC^1(f)$, 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 1 ([11], 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 a feasible solution for the $FC(f)$ 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 9 (Expectational Certificate Complexity)** The *expectational certificate complexity* $EC(f)$ of $f$ is defined as the optimal value of the following program:

$$\minimize \max_x \sum_{i=1}^n w_x(i) \quad \text{s.t.} \quad \sum_{i: x_i \neq y_i} w_x(i)w_y(i) \geq 1 \quad \forall x, y \text{ s.t. } f(x) \neq f(y),$$

$$0 \leq w_x(i) \leq 1 \text{ for all } x \in \{0, 1\}^n, i \in [n].$$

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** $EC(f) \leq R_0(f) \leq O(EC(f)^2)$.

**Proof** The first inequality follows from Lemma 4 and $C(f) \leq R_0(f)$.

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

---

© Springer
Proposition 1 For any $b \in \{0, 1\}$, we have $R_b^b(f) \leq \lceil EC(f)^2/\epsilon \rceil$.

The second inequality of Theorem 1 follows from Proposition 1 by standard arguments of ZPP = RP $\cap$ coRP.

Proof of Proposition 1 We prove the proposition for $b = 0$. The case $b = 1$ is similar.

Let $\{w_x\}_{x \in \{0, 1\}^n}$ be an optimal solution to the EC($f$) program. We say that an input $y$ is consistent with the queries made by $A$ 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 $A$.

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

1. Repeat $\lceil EC(f)^2/\epsilon \rceil$ 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 $A$ always performs at most $\lceil EC(f)^2/\epsilon \rceil$ queries. We prove the correctness of the algorithm in Appendix A.

3.2 Relation with the Fractional Certificate Complexity

Lemma 2 $FC(f) \leq EC(f)$.

Proof We show that a feasible solution $\{w_x\}_x$ for EC($f$) is also feasible for 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 3 $EC(f) = O(FC(f) \sqrt{s(f)})$.

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

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

© Springer
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

$$1 \leq \sum_{i \in B} v_x(i) = \sum_{i \in B, v_x(i) \geq 1/3s(f)} v_x(i) + \sum_{i \in B, v_x(i) \geq 1/3s(f)} v_x(i) \leq \frac{1}{3} + \sum_{i \in B, v_x(i) \geq 1/3s(f)} v_x(i).$$

The second line follows because $|B| \leq s(f)$, as $B$ is a minimal sensitive block and therefore every index in $B$ is sensitive. Rearranging the last inequality, we have

$$\sum_{i \in B, v_x(i) \geq 1/3s(f)} v_x(i) \geq \frac{2}{3s(f)} + \sum_{i \in B, v_x(i) \geq 1/3s(f)} v_x(i).$$

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

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

The second inequality holds by Lemma 1.

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:

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

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

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

Corollary 1  $\text{EC}(f) = O(\text{FC}(f)^{3/2}) = O(R(f)^{3/2})$.

3.3 Relation with the Certificate Complexity

Lemma 4  $\text{EC}(f) \leq C(f)$.

Proof  We construct a feasible solution $\{w_x\}_x$ for $\text{EC}(f)$ from $C(f)$. 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, $w_x(i)w_y(i) \geq 1$. The value of this solution is $\max_x \sum_{i \in [n]} w_x(i) = \max_x C(f, x) = C(f)$.  

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

Theorem 5 (\cite{7}, Theorem 32)  For every $n \in \mathbb{N}$ sufficiently large, there is a function $f : \{0, 1\}^{n^2} \to \{0, 1\}$ such that $\text{FC}(f) = O(n)$ and $C(f) = \Omega(n^2)$.  

Springer
Their construction for $f$ is as follows. First a function $g : \{0, 1\}^n \rightarrow \{0, 1\}$ is exhibited such that $\text{FC}_0^0(g) = \Theta(1)$, $\text{C}_0^0(g) = \Theta(n)$ and $\text{FC}_1^1(g) = \text{C}_1^1(g) = n$. The function $f : \{0, 1\}^{n^2} \rightarrow \{0, 1\}$ is defined as a composition $\text{OR}(g(x^{(1)}), \ldots, g(x^{(n)})$. This gives $\text{FC}(f) = \max \{n \text{FC}_0^0(g), \text{FC}_1^1(g)\} = \Theta(n)$ and $\text{C}(f) \geq n \text{C}_0^0(g) = \Theta(n^2)$ (both properties follow by Proposition 31 in their paper).

Let us construct a feasible solution $w$ for $\text{EC}(f)$. 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 $\text{FC}(f)$. 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 $\sum_{i=1}^{n^2} w_x(i) = \text{FC}(f, x) = O(n)$.

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 $g(x^{(j)}) = 0$. Let $x'$ be an input such that $x'(j) = x^{(j)}$, and $x'(k) = y^{(k)}$ for all $k \neq j$. Then $f(x') = 1$. By construction,

$$\sum_{i : x_i \neq y_i} w_x(i)w_y(i) = \sum_{i : x'_i \neq y_i} w_{x'}(i)w_{y}(i) = \sum_{i : x'_i \neq y_i} w_y(i) \geq 1.$$ 

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

### 4 Minimum Query Corruption Bound and Partition Bound

In this section, we prove upper bounds on the distributional query complexity $D^\mu_{\leq \epsilon}$, where $\mu$ is bitwise product distribution on the inputs. We first consider the query corruption bound and minimum query corruption bound.

**Definition 10 (Query Corruption Bound and Minimum Query Corruption Bound for product distributions)** Let $\epsilon \in [0, 1]$ and $\mu : \{0, 1\}^n \rightarrow [0, 1]$ 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

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

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

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

The query corruption bound of $f$ is defined as $\text{corr}_{\epsilon}(f) = \max_{\mu} \max_{\mu} \text{corr}_{\epsilon}^{b, \mu}(f)$, where $\mu$ ranges over all distributions on $\{0, 1\}^n$. Define the **minimum query corruption bound** of $f$ for product distributions by $\text{corr}_{\epsilon}^{\mu, \mu}(f) = \max_{\mu} \min_{\mu} \text{corr}_{\epsilon}^{b, \mu}(f)$, where $\mu$ ranges over all product distributions on $\{0, 1\}^n$.
4.1 Upper Bound in Terms of the Corruption Bound and Block Sensitivity

In this subsection, we give a deterministic algorithm that achieves the bound of Theorem 2 (restated below).

**Theorem 2** Let $\epsilon \in [0, 1/8)$ and $\mu$ a product distribution over the inputs. Then
\[
D^\mu_{4\epsilon}(f) = O(\text{corr}^\times_{\min, \epsilon}(f) \cdot \text{bs}(f)).
\]

In the algorithm, we will work with restrictions of probability distributions. Let $\eta$ be a probability distribution over $\{0, 1\}^n$, $x \in \{0, 1\}^n$ be an $n$-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 $y \in \{0, 1\}^n$
\[
\eta|_{x_Q}(y) = \begin{cases} \frac{\eta(y)}{\sum_{z: \forall i \in Q, z_i = x_i} \eta(z)} & \text{if } \forall i \in Q, y_i = x_i, \\ 0 & \text{otherwise}. \end{cases}
\]

**Algorithm 2** The deterministic query algorithm $B$.

**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 $\eta^{(i)}$.
   (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 $t_b = 2\text{bs}(f)$, return $b$.
   (f) $\eta^{(i+1)} \leftarrow \eta^{(i)}|_{x_Q}$.
   (g) $i \leftarrow i + 1$.

We analyze the correctness and performance of the algorithm in Appendix B.

4.2 Quadratic Upper Bound in Terms of the Partition Bound

In this subsection, we show that the partition bound is a quadratic upper bound on the distributional query complexity. We prove Theorem 3 (restated below).

**Theorem 3** Let $\epsilon \in \left[0, \frac{1}{16}\right)$ and $\mu$ a product distribution over the inputs. Then
\[
D^\mu_{8\epsilon}(f) = O(\text{prt}_\epsilon(f)^2).
\]

We reproduce the definition of the partition bound by Jain and Klauck [10]. 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 11 (Partition Bound)** For $\epsilon \in [0, 1]$, the $\epsilon$-partition bound of $f$, denoted $\text{prt}_\epsilon(f)$, is given by the logarithm to base 2 of the optimal value of the following linear program:

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

$$
\forall x : \sum_{z,A \ni x} w_{z,A} = 1,
$$

$$
\forall z, A : w_{z,A} \geq 0.
$$

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 6 ([10], Theorem 3)**

1. $R_{\epsilon}(f) \geq \frac{1}{2} \text{prt}_\epsilon(f)$ for any $\epsilon \in [0, 1]$.
2. $R_{1/3}(f) \leq D(f) = O(\text{prt}_{1/3}(f)^3)$.

The best known separation between $D(f)$ and $\text{prt}(f)$ is quadratic [3]. 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 7 ([10], Theorem 3)** For any error parameter $\epsilon \in [0, 1/2)$,

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

We show that the minimum query corruption bound lower-bounds the partition bound (see Appendix C 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 [10].

**Lemma 5** For any error parameter $\epsilon \in (0, 1/2)$,

$$
corr_{\text{min, 2}\epsilon}^\times(f) \leq \text{prt}_\epsilon(f) + \log(1/\epsilon).
$$

Theorem 3 now follows, combining Theorems 2, 7 and Lemma 5 together.

---

1Jain and Klauck in their paper defined $\text{prt}_\epsilon(f)$ to be the value of the linear program, instead of the logarithm of the value of the program.
4.3 Quadratic Upper Bound in Terms of the Corruption Bound

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

**Theorem 8** Let $\epsilon \in [0, 1/8)$ and $\mu$ a product distribution over the inputs. Then

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

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

**Lemma 6** For any $\epsilon \in [0, 1)$, $\text{fbs}(f) \leq \text{corr}_\epsilon(f)$.

5 Open Problems

**Expectational vs. Fractional Certificate** What is the largest separation between the two measures? Is the upper bound $\text{EC}(f) \leq \text{FC}(f)^{3/2}$ tight? Any smaller upper bound would improve the $\text{R}(f) \leq \text{FC}(f)^3$ upper bound. Our attempts in finding a function where $\text{EC}(f)$ is asymptotically larger than $\text{FC}(f)$ so far have been unsuccessful. As evident by the proof of the quadratic separation between $\text{EC}(f)$ and $\text{C}(f)$, such an example would need to have $\text{FC}(f) = o(\text{C}(f))$ for both $z \in \{0, 1\}$. Examples of separations between $\text{FC}(f)$ and $\text{C}(f)$ given in [1] and [7] do not satisfy these properties.

**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 complexity. Can the argument of $D(f) \leq C(f)^2$ 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.

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.

Appendix A: Analysis of Algorithm 1

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 $A$ 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 $\lceil EC(f)^2/\epsilon \rceil$ iterations with probability at least $1 - \epsilon$. (For notational convenience, in what follows we will drop the ceilings and assume $EC(f)^2/\epsilon$ is an integer.)

Define a random variable $T_k$ as

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

Let $T = \sum_{k=1}^{EC(f)^2/\epsilon} T_k$. As $\sum_{i \in [n]} w_x(i) \leq EC(f)$ by definition, $T > EC(f)$ implies that $A$ has terminated before point 2. Then it has returned 0, and the answer is correct. Let $p = \Pr[T > EC(f)]$. 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 $\mathbb{E}[T]$.

1. The maximum possible value of $T$ is at most

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

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

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

$$\mathbb{E}[T_k] = \Pr[\mathcal{E}_k] \cdot \frac{1}{EC(f)} + \Pr[\overline{\mathcal{E}}_k] \cdot \mathbb{E}[w_x(i_k) | \overline{\mathcal{E}}_k]$$

$$\geq \Pr[\mathcal{E}_k] \cdot \frac{1}{EC(f)} + \Pr[\overline{\mathcal{E}}_k] \cdot \sum_{i: x_i \neq y_i} w_x(i) \mu_y(i)$$

$$= \Pr[\mathcal{E}_k] \cdot \frac{1}{EC(f)} + \Pr[\overline{\mathcal{E}}_k] \cdot \sum_{i: x_i \neq y_i} w_x(i) w_y(i) / \sum_{i \in [n]} w_y(i)$$

$$\geq \Pr[\mathcal{E}_k] \cdot \frac{1}{EC(f)} + \Pr[\overline{\mathcal{E}}_k] \cdot \frac{1}{EC(f)}$$

$$= \frac{1}{EC(f)},$$

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 $A$. 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 $\sum_{i \in [n]} w_y(i) \leq EC(f)$. By the linearity of expectation, we have that $\mathbb{E}[T] = \sum_{k=1}^{EC(f)^2/\epsilon} \mathbb{E}[T_k] \geq EC(f)/\epsilon$.

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

Appendix B: Analysis of Algorithm 2

Proof of Theorem 2 We analyze the correctness and performance of the algorithm for inputs sampled according to \( \mu \).

For each \( i = 2, \ldots, 4bs(f) \), define \( T^{(i)} \) to be the event that \( B \) 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 exclusive or),

\[
U \oplus s := \{ y \in \{0, 1\}^n : \forall j \in Q_{A^{(i)}}, y_j = A_j^{(i)} \oplus s_j \text{ and } \exists z \in U \text{ s.t. } \forall j \notin Q_{A^{(i)}}, y_j = z_j \}.
\]

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

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

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

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

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

Proposition 2 For every \( i \) and \( s \in \{0, 1\}^{Q_{A^{(i)}}} \), \( Pr[x \in E^{(i)} \oplus s \mid T^{(i)}, x \in A^{(i)} \oplus s] \leq \epsilon \).

Proof Condition on the events \( T^{(i)}, x \in A^{(i)} \oplus s \). Furthermore, condition on \( x_{L^{(i)}} \).

Notice that under this conditioning, the distribution of the input \( x \) is \( \eta^{(i)} = \mu |_{x_{\overline{L^{(i)}}}} \).

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 proposition follows. \( \square \)

In particular, Proposition 2 implies that for all \( i = 1, \ldots, 4bs(f) \),

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

Since \( B \) runs for at most \( 4bs(f) - 1 < 4bs(f) \) steps, by (1), linearity of expectation and Markov’s inequality we have that

\[
Pr[|i \mid X^{(i)} = 1] \geq bs(f)] \leq 4\epsilon. \tag{2}
\]
For $i$ such that $T^{(i)}$ occurs, define $S^{(i)} := \{ j \in Q_{A^{(i)}} \mid x_j \neq A^{(i)}(j) \}$. The following proposition will play a central role in our analysis.

**Proposition 3** Let $i_1 < i_2$. For each $i \in \{i_1, i_2\}$, let $T^{(i)}$ happen and $X^{(i)} = 0$. Then $f(x^{S^{(i)}}) = b^{(i)}$, $S^{(i_1)} \cap S^{(i_2)} = \emptyset$. 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 $S^{(i_1)} \cap S^{(i_2)} = \emptyset$, 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 $B$ terminates at iteration $i$. We will bound the probability that $B$ errs.

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

Next, condition on the event that $B$ terminates at step 2e, and $t_0 = 2bs(f)$ (the case $t_1 = 2bs(f)$ is symmetrical). By (2), $|\{i \mid X^{(i)} = 1\}| \geq bs(f)$ with probability at most $4\epsilon$. Condition on $|\{i \mid X^{(i)} = 1\}| < bs(f)$. Then $B$ outputs 0. We claim that $f(x) = 0$ with probability 1. Towards a contradiction, assume that $f(x) = 1$. As $t_0 = 2bs(f)$ and $|\{i \mid X^{(i)} = 1\}| < bs(f)$, then in at least $2bs(f) - (bs(f) - 1) = bs(f) + 1$ iterations $j \leq i$, $b^{(j)} = 0$ and $X^{(j)} = 0$. By Proposition 3, the blocks $S^{(j)}$ for those $j$ iterations are sensitive for $x$ and are disjoint. Since any input can have at most $bs(f)$ sensitive blocks, we have the desired contradiction.

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

**Appendix C: Proof of Lemma 5**

**Proof** Let $c = \text{prt}_c(f)$. 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,

$$\sum_{z,A: |A| > c + \log(1/\epsilon)} w_{z,A} \leq \epsilon.$$  \hfill (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 $\text{corr}_{2^c}^{1/\mu}(f) \leq c + \log(1/\epsilon)$. 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 (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,

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

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

Dividing (6) by (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,

\[
\text{corr}_{\mu, 2\epsilon}^\mu(f) \leq \text{corr}_{1\epsilon}^\mu(f) \leq |A| \leq \text{prt}_{\epsilon}(f) + \log(1/\epsilon).
\]

Note that in (5), a better upper bound of simply \( \epsilon \) follows from the first primal constraint of the partition bound LP. This results in a slightly better error \( \epsilon_{1-\epsilon} < 2\epsilon \) for \( \epsilon < 1/2 \). Thanks to the anonymous reviewer for pointing this out.

**Appendix D: Proof of Lemma 6**

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

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

Let $A$ be the shortest $\epsilon$-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 $B_i \cap Q_A \neq \emptyset$, thus

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

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

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

Therefore,

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

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

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

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

References

1. Aaronson, S.: Quantum certificate complexity. J. Comput. Syst. Sci. 74(3), 313–322 (2008)
2. Aaronson, S., Ben-David, S., Kothari, R.: Separations in query complexity using cheat sheets. In: Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing, STOC’16, pp. 863–876. ACM, New York (2016)
3. Ambainis, A., Kokainis, M., Kothari, R.: Nearly optimal separations between communication (or query) complexity and partitions. In: Proceedings of the 31St Conference on Computational Complexity, CCC’16, pp. 4:1–4:14. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Germany (2016)
4. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM 48(4), 778–797 (2001)
5. Blum, M., Impagliazzo, R.: Generic oracles and oracle classes. In: Proceedings of the 28th annual symposium on foundations of computer science, SFCS’87, pp. 118–126. IEEE Computer Society, Washington (1987)
6. Buhrman, H., de Wolf, R.: Complexity measures and decision tree complexity: a survey. Theor. Comput. Sci. 288(1), 21–43 (2002)
7. Gilmer, J., Saks, M., Srinivasan, S.: Composition limits and separating examples for some Boolean function complexity measures. Combinatorica 36(3), 265–311 (2016)
8. Harsha, P., Jain, R., Radhakrishnan, J.: Partition bound is quadratically tight for product distributions. In: 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016), vol. 55 of Leibniz International Proceedings in Informatics (LIPIcs), pp. 135:1–135:13, Dagstuhl, Germany. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik (2016)
9. Hartmanis, J., Hemachandra, L.A.: One-way functions, robustness, and non-isomorphism of NP-complete sets. In: Proceedings of 2nd Structure in Complexity Theory, pp. 160–173 (1987)
10. Jain, R., Klauck, H.: The partition bound for classical communication complexity and query complexity. In: Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity, CCC’10, pp. 247–258. IEEE Computer Society, Washington (2010)
11. Kulkarni, R., Tal, A.: On fractional block sensitivity. Chicago Journal Of Theoretical Computer Science 8, 1–16 (2016)
12. Nisan, N.: Crew prams decision trees. In: Proceedings of the twenty-first annual ACM symposium on theory of computing, STOC’89, pp. 327–335. ACM, New York (1989)
13. Tal, A.: Properties and applications of Boolean function composition. In: Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS’13, pp. 441–454. ACM, New York (2013)
14. Tardos, G.: 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)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Rahul Jain\(^1\),\(^2\) · Hartmut Klauck\(^1\),\(^3\) · Srijita Kundu\(^1\) · Troy Lee\(^1\),\(^3\) · Miklos Santha\(^1\),\(^4\) · Swagato Sanyal\(^1\),\(^3\) · Jevgēnijs Vihrovs\(^5\)

\(^1\) Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore, Singapore 117543
\(^2\) MajuLab, UMI 3654, Singapore, Singapore
\(^3\) SPMS, Nanyang Technological University, 21 Nanyang Link, Singapore, Singapore 637371
\(^4\) IRIF, Université Paris Diderot, CNRS, 75205 Paris, France
\(^5\) Centre for Quantum Computer Science, Faculty of Computing, University of Latvia, Raiņa 19, Riga, Latvia, LV-1586