Electronic Colloquium on Computational Complexity, Report No. 84 (2016)

Low-Sensitivity Functions from Unambiguous Certificates

Shalev Ben-David
MIT
shalev@mit.edu

Abstract

We provide new query complexity separations against sensitivity for total Boolean functions: a power 3 separation between deterministic (and even randomized or quantum) query complexity and sensitivity, and a power 2.1 separation between certificate complexity and sensitivity. We get these separations by using a new connection between sensitivity and a seemingly unrelated measure called one-sided unambiguous certificate complexity ($\mathrm{UC}_{\min}$). Finally, we show that $\mathrm{UC}_{\min}$ is lower-bounded by fractional block sensitivity, which means we cannot use these techniques to get a super-quadratic separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$.

1 Introduction

Sensitivity is one of the simplest complexity measures of a Boolean function. For $f : \{0,1\}^n \to \{0,1\}$ and $x \in \{0,1\}^n$, the sensitivity of x is the number of bits of x that, when flipped, change the value of $f(x)$. The sensitivity of f, denoted $\mathrm{s}(f)$, is the maximum sensitivity of any input x to f. Sensitivity lower bounds other important measures in query complexity, such as deterministic query complexity $\mathrm{D}(f)$, randomized query complexity $\mathrm{R}(f)$, certificate complexity $\mathrm{C}(f)$, and block sensitivity $\mathrm{bs}(f)$ (see Section 2 for definitions). $\sqrt{\mathrm{s}(f)}$ is a lower bound on quantum query complexity $\mathrm{Q}(f)$.

Despite its simplicity, sensitivity has remained mysterious. The other measures are polynomially related to each other: we have $\mathrm{bs}(f) \le \mathrm{C}(f) \le \mathrm{D}(f) \le \mathrm{bs}(f)^3$ and $\mathrm{Q}(f) \le \mathrm{R}(f) \le \mathrm{D}(f) \le \mathrm{Q}(f)^6$. In contrast, no polynomial relationship connecting sensitivity to these measures is known, despite much interest (this problem was posed by [Nis91]. For a survey, see [HKP11]. For recent progress, see [AS11, Bop12, AP14, ABG+14, APV15, AV15, GKS15, Sze15, GNS+16, GSTW16, Tal16]).

Until recently, the best known separation between sensitivity and any of these other measures was quadratic. Tal [Tal16] showed a power 2.1 separation between $\mathrm{D}(f)$ and $\mathrm{s}(f)$. In this work, we improve this to a power 3 separation, and also show functions for which $\mathrm{Q}(f) = \tilde{\Omega}(\mathrm{s}(f)^3)$ and $\mathrm{C}(f) = \tilde{\Omega}(\mathrm{s}(f)^{2.1})$.

We do this by exploiting a new connection between sensitivity and a measure called one-sided unambiguous certificate complexity, which we denote by $\mathrm{UC}_{\min}(f)$. This measure, and particularly its two-sided version $\mathrm{UC}(f)$ (which is sometimes called subcube complexity), has received significant attention in previous work (e.g. [BOH90, FKW02, Sav02, Bel06, KRS15, GPW15, Göö15, GJPW15, CKLS16, AKK16]), in part because it corresponds to partition number in communication complexity. Intuitively, $\mathrm{UC}_{\min}(f)$ is similar to (one-sided) certificate complexity, except that the certificates are required to be *unambiguous*: each input must be consistent with only one certificate. For a formal definition, see Section 2.5.

We prove the following theorem.

Theorem 1. *For any $\alpha \in \mathrm{R}^+$, if there is a family of functions with $\mathrm{D}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^{1+\alpha})$, then there is a family of functions with $\mathrm{D}(f) = \tilde{\Omega}(\mathrm{s}(f)^{2+\alpha})$. The same is true if we replace $\mathrm{D}(f)$ by $\mathrm{bs}(f), \mathrm{C}(f), \mathrm{R}(f), \mathrm{Q}(f)$, and many other measures.*

ISSN 1433-8092

Theorem 1 can be generalized from sensitivity $\mathrm{s}(f)$ to bounded-size block sensitivity $\mathrm{bs}_{(k)}(f)$ (block sensitivity where each block is restricted to have size at most k). However, there is a constant factor loss that depends on k.

We observe that cheat sheet functions (as defined in [ABK15]) have low $\mathrm{UC}_{\min}$; in particular, one of the functions in [ABK15] already has a quadratic separation between $\mathrm{Q}(f)$ and $\mathrm{UC}_{\min}(f)$, giving a cubic separation between $\mathrm{Q}(f)$ and $\mathrm{s}(f)$. To separate $\mathrm{C}(f)$ from $\mathrm{s}(f)$, we use Göös's function [Göö15], which gives a 1.1 separation between $\mathrm{C}(f)$ and $\mathrm{UC}_{\min}(f)$. This gives us the following corollary.

Corollary 2. *There is a family of functions with $\mathrm{Q}(f) = \tilde{\Omega}(\mathrm{s}(f)^3)$, and one with $\mathrm{C}(f) = \Omega(\mathrm{s}(f)^{2.128})$.*

We note that $\mathrm{UC}_{\min}(f)$ upper bounds $\deg(f)$, so this technique cannot be used to get super-quadratic separations between $\deg(f)$ and $\mathrm{s}(f)$. A natural question is whether we can use Theorem 1 to get a super-quadratic separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$. To do so, it would suffice to separate $\mathrm{bs}(f)$ from $\mathrm{UC}_{\min}(f)$. It would even suffice to separate randomized certificate complexity $\mathrm{RC}(f)$ (a measure larger than $\mathrm{bs}(f)$) from $\mathrm{UC}_{\min}(f)$, because of the following theorem.

Theorem 3 (Follows from [Tal13] and independently [GSS16])**.** *A power $2+\alpha$ separation between $\mathrm{RC}(f)$ and $\mathrm{s}(f)$ implies a power $2+\alpha-o(1)$ separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$.*

Unfortunately, we show that separating $\mathrm{RC}(f)$ from $\mathrm{UC}_{\min}(f)$ is impossible. We conclude that Theorem 1 cannot be used to super-quadratically separate $\mathrm{bs}(f)$ from $\mathrm{s}(f)$.

Theorem 4. *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. Then $\mathrm{RC}(f) \le 2\,\mathrm{UC}_{\min}(f)$.*

In fact, we prove a strengthened version of Theorem 4 regarding non-negative approximate degree $\widetilde{\deg}^{+}_{\min}(f)$, a measure upper bounded by $\mathrm{UC}_{\min}(f)$. We show $\widetilde{\deg}^{+}_{\min}(f) = \Omega(\mathrm{RC}(f))$, strengthening a result of [GJPW15] that showed $\widetilde{\deg}^{+}_{\min}(\mathrm{AND}_n) = \Omega(n)$. The $\mathrm{RC}(f)$ lower bound even holds for the (one-sided) average approximate non-negative degree $\widetilde{\mathrm{avdeg}}^{+}_{\min}(f)$ introduced by [GJ15], which we define in Section 2.6. We also show that the factor of 2 in Theorem 4 is neccessary.

In Section 2, we briefly define the many complexity measures mentioned here, and discuss the known relationships between them. In Section 3, we prove Theorem 1 and Corollary 2. In Section 4, we discuss a failed attempt to get a new separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$, and in the process we prove Theorem 3 and Theorem 4.

2 Preliminaries

2.1 Query Complexity

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. Let A be a deterministic algorithm that computes $f(x)$ on input $x \in \{0,1\}^n$ by making queries to the bits of x. The worst-case number of queries A makes (over choices of x) is the query complexity of A. The minimum query complexity of any deterministic algorithm computing f is the deterministic query complexity of f, denoted by $\mathrm{D}(f)$.

We define the bounded-error randomized (respectively quantum) query complexity of f, denoted by $\mathrm{R}(f)$ (respectively $\mathrm{Q}(f)$), in an analogous way. We say an algorithm A computes f with bounded error if $\Pr[A(x) = f(x)] \ge 2/3$ for all $x \in \{0,1\}^n$, where the probability is over the internal randomness of A. Then $\mathrm{R}(f)$ (respectively $\mathrm{Q}(f)$) is the minimum number of queries required by any randomized (respectively quantum) algorithm that computes f with bounded error. It is clear that $\mathrm{Q}(f) \le \mathrm{R}(f) \le \mathrm{D}(f)$. For more details on these measures, see the survey by Buhrman and de Wolf [BdW02].

2.2 Partial Assignments and Certificates

A partial assignment is a string $p \in \{0,1,*\}^n$ representing partial knowledge of a string $x \in \{0,1\}^n$. Two partial assignments are consistent if they agree on all entries where neither has a $*$. We will identify p with the set $\{(i,p_i) : p_i \neq *\}$. This allows us to write $p \subseteq x$ to denote that the string x is consistent with the partial assignment p. We observe that if p and q are consistent partial assignments, then $p \cup q$ is also a partial assignment. The size of a partial assignment p is $|p|$, the number of non-$*$ entries in p. The support of p is the set $\{i \in [n] : p_i \neq *\}$.

Fix a Boolean function $f : \{0,1\}^n \to \{0,1\}$. We say a partial assignment p is a certificate (with respect to f) if $f(x)$ is the same for all strings $x \supseteq p$. If $f(x) = 0$ for such strings, we say p is a 0-certificate; otherwise, we say p is a 1-certificate. We say p is a certificate for the string x if p is consistent with x. We use $\mathrm{C}_x(f)$ to denote the size of the smallest certificate for x. We then define the certificate complexity of f as $\mathrm{C}(f) := \max_{x\in\{0,1\}^n} \mathrm{C}_x(f)$. We also define the one-sided measures $\mathrm{C}_0(f) := \max_{x\in f^{-1}(0)} \mathrm{C}_x(f)$ and $\mathrm{C}_1(f) := \max_{x\in f^{-1}(1)} \mathrm{C}_x(f)$.

2.3 Sensitivity and Block Sensitivity

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and let $x \in \{0,1\}^n$ be a string. A block is a subset of $[n]$. If B is a block, we denote by x^B the string we get from x by flipping the bits in B; that is, $x^B_i = x_i$ if $i \notin B$, and $x^B = 1 - x_i$ if $i \in B$. For a bit i, we also use x^i to denote $x^{\{i\}}$.

We say that a block B is sensitive for x (with respect to f) if $f(x^B) \neq f(x)$. We say a bit i is sensitive for x if the block $\{i\}$ is sensitive for x. The maximum number of disjoint blocks that are all sensitive for x is called the block sensitivity of x (with respect to f), denoted by $\mathrm{bs}_x(f)$. The number of sensitive bits for x is called the sensitivity of x, denoted by $\mathrm{s}_x(f)$. Clearly, $\mathrm{bs}_x(f) \geq \mathrm{s}_x(f)$, since $\mathrm{s}_x(f)$ is has the same definition as $\mathrm{bs}_x(f)$ except the size of the blocks is restricted to 1.

We now define the measures $\mathrm{s}(f)$, $\mathrm{s}_0(f)$, and $\mathrm{s}_1(f)$ analogously to $\mathrm{C}(f)$, $\mathrm{C}_0(f)$, and $\mathrm{C}_1(f)$. That is, $\mathrm{s}(f)$ is the maximum of $\mathrm{s}_x(f)$ over all x, $\mathrm{s}_0(f)$ is the maximum where x ranges over 0-inputs to f, and $\mathrm{s}_1(f)$ is the maximum over 1-inputs. We define $\mathrm{bs}(f)$, $\mathrm{bs}_0(f)$, and $\mathrm{bs}_1(f)$ similarly.

2.4 Fractional Block Sensitivity

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and let $x \in \{0,1\}^n$ be a string. Note that the support of any certificate p of x must have non-empty intersection with every sensitive block B of x; this is because otherwise, x^B would be consistent with p, which is a contradiction since $f(x^B) \neq f(x)$.

Note further that any subset S of $[n]$ that intersects with all sensitive blocks of x gives rise to a certificate x_S for x. This is because if x_S was not a certificate, there would be an input $y \supseteq x_S$ with $f(y) \neq f(x)$. If we write $y = x^B$, where B is the set of bits where x and y disagree, then B would be a sensitive block that is disjoint from S, which contradicts our assumption on S.

This means the certificate complexity $\mathrm{C}_x(f)$ of x is the hitting number for the set system of sensitive blocks of x (that is, the size of the minimum set that intersects all the sensitive blocks). Furthermore, the block sensitivity $\mathrm{bs}_x(f)$ of x is the packing number for the same set system (i.e. the maximum number of disjoint sets in the system). It is clear that the hitting number is always larger than the packing number, because if there are k disjoint sets we need at least k domain elements in order to have non-empty intersection with all the sets.

Moreover, we can define the fractional certificate complexity of x as the fractional hitting number of the set system; that is, the minimum amount of non-negative weight we can distribute among the domain elements $[n]$ so that every set in the system gets weight at least 1 (where the weight of a set is the sum of the weights of its elements). We can also define the fractional block sensitivity of

x as the fractional packing number of the set system; that is, the maximum amount of non-negative weight we can distribute among the sets (blocks) so that every domain element gets weight at most 1 (where the weight of a domain element is the sum of the weights of the sets containing that element).

It is not hard to see that the fractional hitting and packing numbers are the solutions to dual linear programs, which means they are equal. We denote them by $\mathrm{RC}_x(f)$ for "randomized certificate complexity", following the original notation as introduced by Aaronson [Aar08] (we warn that our definition differs by a constant factor from Aaronson's original definition). We define $\mathrm{RC}(f)$, $\mathrm{RC}_0(f)$, and $\mathrm{RC}_1(f)$ in the usual way. For more properties of $\mathrm{RC}(f)$, see [Aar08] and [KT13].

2.5 Unambiguous Certificate Complexity

Fix $f : \{0,1\}^n \to \{0,1\}$. We call a set of partial assignments U an unambiguous collection of 0-certificates for f if

1. Each partial assignment in U is a 0-certificate (with respect to f)
2. For each $x \in f^{-1}(0)$, there is some $p \in U$ with $p \subseteq x$
3. No two partial assignments in U are consistent.

We then define $\mathrm{UC}_0(f)$ to be the minimum value of $\max_{p\in U} |p|$ over all choices of such collections U. We define $\mathrm{UC}_1(f)$ analogously, and set $\mathrm{UC}(f) := \max\{\mathrm{UC}_0(f), \mathrm{UC}_1(f)\}$. We also define the one-sided version, $\mathrm{UC}_{\min}(f) := \min\{\mathrm{UC}_0(f), \mathrm{UC}_1(f)\}$.

2.6 Degree Measures

A polynomial q in the variables $x_1, x_2, \ldots, x_n$ is said to represent the function $f : \{0,1\}^n \to \{0,1\}$ if $q(x) = f(x)$ for all $x \in \{0,1\}^n$. q is said to ϵ-approximate f if $q(x) \in [0, \epsilon]$ for all $x \in f^{-1}(0)$ and $q(x) \in [1-\epsilon, 1]$ for all $x \in f^{-1}(1)$. The degree of f, denoted by $\deg(f)$, is the minimum degree of a polynomial representing f. The ϵ-approximate degree, denoted by $\widetilde{\deg}^{\epsilon}(f)$, is the minimum degree of a polynomial ϵ-approximating f. We will omit ϵ when $\epsilon = 1/3$. [BBC+01] showed that $\mathrm{D}(f) \geq \deg(f)$, $\mathrm{R}(f) \geq \widetilde{\deg}(f)$, and $\mathrm{Q}(f) \geq \widetilde{\deg}(f)/2$.

We also define non-negative variants of degree. For each partial assignment p we identify a polynomial $p(x) := (\Pi_{i:\, p_i=1} x_i)\,(\Pi_{i:\, p_i=0}(1-x_i))$. We note that $p(x) = 1$ if $p \subseteq x$ and $p(x) = 0$ otherwise, and also that the degree of $p(x)$ is $|p|$. We say a polynomial is non-negative if it is of the form $\sum_p w_p p(x)$, where $w_p \in \mathbb{R}^+$ are non-negative weights. For such a sum, define its degree as $\max_{p:\, w_p>0} |p|$. Define its average degree as the maximum over $x \in \{0,1\}^n$ of $\sum_{p:\, p\subseteq x} w_p|p|$. We note that if a non-negative polynomial q satisfies $|q(x)| \in [0,1]$ for all $x \in \{0,1\}^n$, then the average degree of q is at most its degree. Moreover, if all the monomials in q have the same size and $q(x) = 1$ for some $x \in \{0,1\}^n$, the degree and average degree of q are equal.

We define the non-negative degree of f as the minimum degree of a non-negative polynomial representing f. We note that this is a one-sided measure, since it may change when f is negated; we therefore denote it by $\deg_1^+(f)$, and use $\deg_0^+(f)$ for the degree of a non-negative polynomial representing the negation of f. We let $\deg^+(f)$ be the maximum of the two, and let $\deg_{\min}^+(f)$ be the minimum. We also define $\mathrm{avdeg}_1^+(f)$ as the minimum average degree of a non-negative polynomial representing f, with the other corresponding measures defined analogously. Finally, we define the approximate variants of these, denoted by (for example) $\widetilde{\deg}_1^{+,\epsilon}(f)$, in a similar way, except the polynomials need only ϵ-approximate f.

2.7 Known Relationships

2.7.1 Two-Sided Measures

We describe some of the known relationships between these measures. To start with, we have

$$\mathrm{s}(f) \le \mathrm{bs}(f) \le \mathrm{RC}(f) \le \mathrm{C}(f) \le \mathrm{UC}(f) \le \mathrm{D}(f),$$

where the last inequality holds because for each deterministic algorithm A, the partial assignments defined by the input bits A examines when run on some $x \in \{0,1\}^n$ form an unambiguous collection of certificates. We also have

$$\widetilde{\deg}(f) \le 2\,\mathrm{Q}(f), \quad \widetilde{\deg}^+(f) \le \mathrm{R}(f), \quad \deg^+(f) \le \mathrm{D}(f),$$

with $\widetilde{\deg}(f) \le \widetilde{\deg}^+(f) \le \deg^+(f)$ and $\mathrm{Q}(f) \le \mathrm{R}(f) \le \mathrm{D}(f)$.

[BBC+01] showed $\mathrm{D}(f) \le \mathrm{bs}(f)\,\mathrm{C}(f)$, and [Nis91] showed $\mathrm{C}(f) \le \mathrm{bs}(f)^2$. From this we conclude that $\mathrm{D}(f) \le \mathrm{C}(f)^2$ and $\mathrm{D}(f) \le \mathrm{bs}(f)^3$. [KT13] showed $\sqrt{\mathrm{RC}(f)} = O(\widetilde{\deg}(f))$; thus

$$\mathrm{D}(f) \le \mathrm{bs}(f)^3 \le \mathrm{RC}(f)^3 = O(\widetilde{\deg}(f)^6) = O(\mathrm{Q}(f)^6),$$

so the above measures are polynomially related (with the exception of sensitivity). Other known relationships are $\mathrm{RC}(f) = O(\mathrm{R}(f))$ (due to [Aar08]), $\mathrm{D}(f) \le \mathrm{bs}(f)\deg(f) = O(\deg(f)^3)$ (due to [Mid04]), and $\deg^+(f) \le \mathrm{UC}(f)$ (since we can get a polynomial representing f by summing up the polynomials corresponding to unambiguous 1-certificates of f).

2.7.2 One-Sided Measures

One-sided measures such as $\mathrm{C}_1(f)$ are not polynomially related to the rest of the measures above, as can be seen from $\mathrm{C}_1(\mathrm{OR}_n) = 1$. This makes them less interesting to us. On the other hand, the one sided measures $\deg^+_{\min}(f)$, $\widetilde{\deg}^+_{\min}(f)$, and $\mathrm{UC}_{\min}(f)$ are polynomially related to the rest. An easy way to observe this is to note that $\widetilde{\deg}^+_{\min}(f) \ge \widetilde{\deg}(f)$, which follows from the fact that $\widetilde{\deg}(f) \le \widetilde{\deg}^+_1(f)$ and that $\widetilde{\deg}(f)$ is invariant under negating f. Similarly, $\deg(f) \le \deg^+_{\min}(f)$. We also have

$$\widetilde{\deg}^+_{\min}(f) \le \deg^+_{\min}(f) \le \mathrm{UC}_{\min}(f),$$

where the last inequality holds since we can form a non-negative polynomial representing f by summing up the polynomials corresponding to a set of unambiguous 1-certificates.

An additional useful inequality is $\mathrm{D}(f) \le \mathrm{UC}_{\min}(f)^2$. The analogous statement in communication complexity was shown by [Yan91]. The query complexity version of the proof can be found in [Göö15].

3 Sensitivity and Unambiguous Certificates

We start by defining a transformation that takes a function f and modifies it so that $\mathrm{s}_0(f)$ decreases to 1. This transformation might cause $\mathrm{s}_1(f)$ to increase, but we will argue that it will remain upper bounded by $3\,\mathrm{UC}_1(f)$. We will also argue that other measures, such as $\mathrm{D}(f)$, do not decrease. This transformation is motivated by the construction of [Tal16] that was used to give a power 2.1 separation between $\mathrm{D}(f)$ and $\mathrm{s}(f)$.

Definition 5 (Desensitizing Transformation)**.** *Let $f : \{0,1\}^n \to \{0,1\}$. Let U be an unambiguous collection of 1-certificates for f, each of size at most $\mathrm{UC}_1(f)$. For each $x \in f^{-1}(1)$, let $p_x \in U$ be the unique certificate in U consistent with x. The desensitized version of f is the function $f' : \{0,1\}^{3n} \to \{0,1\}$ defined by $f'(xyz) = 1$ if and only if $f(x) = f(y) = f(z) = 1$ and $p_x = p_y = p_z$.*

The following lemma illustrates key properties of f'.

Lemma 6 (Desensitization)**.** *Let f' be the desensitized version of $f : \{0,1\}^n \to \{0,1\}$. Then $\mathrm{s}_0(f') = 1$ and $\mathrm{UC}_1(f') \le 3\,\mathrm{UC}_1(f)$. Also, for any complexity measure*

$$M \in \{\mathrm{D}, \mathrm{R}, \mathrm{Q}, \mathrm{C}, \mathrm{C}_0, \mathrm{C}_1, \mathrm{bs}, \mathrm{bs}_0, \mathrm{bs}_1, \mathrm{RC}, \mathrm{RC}_0, \mathrm{RC}_1, \mathrm{UC}, \mathrm{UC}_0, \mathrm{UC}_1, \mathrm{UC}_{\min}, \deg, \deg^+, \widetilde{\deg}, \widetilde{\deg}^+\},$$

we have $M(f') \ge M(f)$.

Proof. We start by upper bounding $\mathrm{s}_0(f')$. Consider any 0-input xyz to f' which has at least one sensitive bit. Pick a sensitive bit i of this input; without loss of generality, this bit is inside the x part of the input. Since flipping i changes xyz to a 1-input for f', we must have $f(x^i) = f(y) = f(z) = 1$ and $p_{x^i} = p_y = p_z$. In particular, it must hold that $f(y) = f(z) = 1$ and $p_y = p_z$. Let $p := p_y$, so $p = p_z$ and $p = p_{x^i}$. Since $f(xyz) = 0$, it must be the case that x is not consistent with p. Since p is consistent with x^i, it must be the case that p and x disagree exactly on the bit i.

Now, it's clear that xyz cannot have any sensitive bits inside the y part of the input, because then x would not be consistent with p_z. Similarly, xyz cannot have sensitive bits in the z part of the input. Any sensitive bits inside the x part of the input must make x consistent with p; but x disagrees with p on bit i, so this must be the only sensitive bit. It follows that the sensitivity of xyz is at most 1, as desired. We conclude that $\mathrm{s}_0(f') = 1$.

Next, we upper bound UC_1. Define $U' := \{ppp : p \in U\} \subseteq \{0,1,*\}^{3n}$. We show that this is an unambiguous collection of 1-certificates for f'. First, note that for $p \in U$, if $ppp \subseteq xyz$, then $f(x) = f(y) = f(z) = 1$ and $p_x = p_y = p_z = p$, so $f'(xyz) = 1$. Thus U' is a set of 1-certificates. Next, if xyz is a 1-input for f', then $f(x) = f(y) = f(z) = 1$ and $p_x = p_y = p_z$, which means $p_xp_xp_x \subseteq xyz$. Since $p_x \in U$, we have $p_xp_xp_x \in U'$. Finally, if $ppp, qqq \in U'$ with $ppp \ne qqq$, then $p \ne q$ and $p, q \in U$, which means p and q are inconsistent. This means ppp and qqq are inconsistent. This concludes the proof that U' is an unambiguous collection of 1-certificates for f'. We have $\max_{ppp \in U'} |ppp| = 3 \max_{p \in U} |p| = 3\,\mathrm{UC}_1(f)$, so $\mathrm{UC}_1(f') \le 3\,\mathrm{UC}_1(f)$.

Finally, we show that almost all complexity measures do not decrease in the transition from f to f'. To see this, note that we can restrict f' to the promise that all inputs come from the set $\{xyz \in \{0,1\}^{3n} : x = y = z\}$. Under this promise, the function f' is simply the function f with each input bit occurring 3 times. But tripling input bits in this way does not affect the usual complexity measures (among the measures defined in Section 2, sensitivity is the only exception), and restricting to a promise can only cause them to decrease. This means that f' has higher complexity than f under almost any measure. ☐

We now prove Theorem 1, which we restate here for convenience.

Theorem 1. *For any $\alpha \in \mathrm{R}^+$, if there is a family of functions with $\mathrm{D}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^{1+\alpha})$, then there is a family of functions with $\mathrm{D}(f) = \tilde{\Omega}(\mathrm{s}(f)^{2+\alpha})$. The same is true if we replace $\mathrm{D}(f)$ by $\mathrm{bs}(f), \mathrm{C}(f), \mathrm{R}(f), \mathrm{Q}(f)$, and many other measures.*

Proof. Fix $f : \{0,1\}^n \to \{0,1\}$ from the family for which $\mathrm{D}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^{1+\alpha})$. By negating f if necessary, assume $\mathrm{UC}_1(f) = \mathrm{UC}_{\min}(f)$. Apply the desensitizing transformation to get f'. By Lemma 6, we have $\mathrm{s}_0(f') \le 1$ and $\mathrm{s}_1(f') \le \mathrm{UC}_1(f') \le 3\,\mathrm{UC}_{\min}(f)$, and also $\mathrm{D}(f') \ge \mathrm{D}(f)$. We now consider the function $\hat{f} := \mathrm{OR}_{3\,\mathrm{UC}_{\min}(f)} \circ f'$. It is not hard to see that $\mathrm{s}_0(\hat{f}) \leq 3\,\mathrm{UC}_{\min}(f)$ and $\mathrm{s}_1(\hat{f}) = \mathrm{s}_1(f') \leq 3\,\mathrm{UC}_{\min}(f)$, so $\mathrm{s}(\hat{f}) \leq 3\,\mathrm{UC}_{\min}(f)$.

We now analyze $\mathrm{D}(\hat{f})$. We have $\mathrm{D}(f') \geq \mathrm{D}(f)$; since deterministic query complexity satisfies a perfect composition theorem, we have

$$\mathrm{D}(\hat{f}) = \mathrm{D}(\mathrm{OR}_{3\,\mathrm{UC}_{\min}(f)})\,\mathrm{D}(f') \geq 3\,\mathrm{UC}_{\min}(f)\,\mathrm{D}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^{2+\alpha}) = \tilde{\Omega}(\mathrm{s}(\hat{f})^{2+\alpha}).$$

This concludes the proof for deterministic query complexity.

For other measures, we need the following properties: first, that the measure is invariant under negating the function (so that we can assume $\mathrm{UC}_{\min}(f) = \mathrm{UC}_1(f)$ without loss of generality); second, that the measure satisfies a composition theorem, at least in the case that the outer function is OR; and finally, that the measure is large for the OR function. We note that the measures C, bs, RC, R, and Q all satisfy a composition theorem of the form $M(\mathrm{OR} \circ g) \geq \Omega(M(\mathrm{OR})M(g))$; for the first three measures, this can be found in [GSS16], for R it can be found in [GJPW15], and for Q it follows from a general composition theorem [Rei11, LMR+11]. Moreover, $\mathrm{bs}(\mathrm{OR}_n) = \mathrm{C}(\mathrm{OR}_n) = \mathrm{RC}(\mathrm{OR}_n) = n$ and $\mathrm{R}(\mathrm{OR}_n) = \Omega(n)$. This completes the proof for these measures; for Q, we will have to work harder, since $\mathrm{Q}(\mathrm{OR}_n) = \Theta(\sqrt{n})$.

For quantum query complexity, the trick will be to use the function "Block k-sum" defined in [ABK15]. It has the property that all inputs have certificates that use very few 0 bits. Actually, we'll swap the 0s and 1s so that all inputs have certificates that use very few 1 bits. When $k = \log n$ (where n the size of the input), we denote this function by $\textsc{BSum}_n$. [ABK15] showed that $\mathrm{Q}(\textsc{BSum}_n) = \tilde{\Omega}(n)$, and every input has a certificate with $O(\log^3 n)$ ones.

Consider the function $\hat{f} := \textsc{BSum}_{\mathrm{UC}_{\min}(f)} \circ f'$. We have $\mathrm{Q}(\hat{f}) = \mathrm{Q}(\textsc{BSum}_{\mathrm{UC}_{\min}(f)})\,\mathrm{Q}(f') = \tilde{\Omega}(\mathrm{UC}_{\min}(f)\,\mathrm{Q}(f))$. We now analyze the sensitivity of $\hat{f}$. Fix an input z to $\hat{f} = \textsc{BSum}_{\mathrm{UC}_{\min}(f)} \circ f'$. This input consists of $\mathrm{UC}_{\min}(f)$ inputs to f', which, when evaluated, form an input y to $\textsc{BSum}_{\mathrm{UC}_{\min}(f)}$. Note that some of the inputs to f' correspond to sensitive bits of y (with respect to $\textsc{BSum}_{\mathrm{UC}_{\min}(f)}$); the sensitive bits of z are then simply the sensitive bits of those inputs. Now, consider the certificate of y that uses only $O(\log^3 \mathrm{UC}_{\min}(f))$ bits that are 1. Since it is a certificate, it must contain all the sensitive bits of y; thus at most $O(\log^3 \mathrm{UC}_{\min}(f))$ of the 1 bits of y are sensitive. It follows that the number of sensitive bits of z is at most $\mathrm{UC}_{\min}(f)\,\mathrm{s}_0(f') + O(\log^3 \mathrm{UC}_{\min}(f))\,\mathrm{s}_1(f') = \tilde{O}(\mathrm{UC}_{\min}(f))$. This concludes the proof. ☐

It is not hard to see that the same approach can yield separations against bounded-size block sensitivity (where the blocks are restricted to have size at most k). To do this, we need the desensitizing construction to repeat the inputs $2k+1$ times instead of 3 times. Instead of increasing to $3\,\mathrm{UC}_{\min}(f)$, the bounded-size block sensitivity would increase to $(2k+1)\,\mathrm{UC}_{\min}(f)$, and the deterministic query complexity would increase to $(2k+1)\,\mathrm{D}(f)$. When k is constant, we get the same asymptotic separations as for sensitivity.

We now construct separations against $\mathrm{UC}_{\min}$. This proves Corollary 2.

Corollary 2. *There is a family of functions with* $\mathrm{Q}(f) = \tilde{\Omega}(\mathrm{s}(f)^3)$, *and one with* $\mathrm{C}(f) = \Omega(\mathrm{s}(f)^{2.128})$.

Proof. We need to construct a family of functions with $\mathrm{C}(f) = \Omega(\mathrm{UC}_{\min}(f)^{1.128})$, and another family with $\mathrm{Q}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^2)$; Theorem 1 will then finish the argument. The former was constructed in [Göö15]. For the latter, our function will be a cheat sheet function $\mathrm{BKK}_{\mathrm{CS}}$ from [ABK15] that quadratically separates quantum query complexity from exact degree. This function has quantum query complexity quadratically larger than $\mathrm{UC}_{\min}$, as shown in [AKK16]. ☐

4 Attempting a Super-Quadratic Separation vs. Block Sensitivity

In this section, we describe why attempting to use Theorem 1 to get a super-quadratic separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$ fails. In the process, we show some new lower bounds for $\mathrm{UC}_{\min}(f)$ and even for the one-sided non-negative degree measures.

One approach for the desired super-quadratic separation is to find a family of functions for which $\mathrm{bs}(f) \gg \mathrm{UC}_{\min}(f)$. In fact, we show that it suffices to provide a family of functions for which $\mathrm{RC}(f) \gg \mathrm{UC}_{\min}(f)$, a strictly easier task. We prove this in Section 4.1. In Section 4.2, we show that even separating $\mathrm{RC}(f)$ from $\mathrm{UC}_{\min}(f)$ is impossible: we have $\mathrm{RC}(f) \leq 2\,\mathrm{UC}_{\min}(f)$. This means our techniques do not give anything new for this problem. This is perhaps surprising, since $\mathrm{RC}(f)$ is similar to $\mathrm{C}(f)$, yet [Göö15] showed a separation between $\mathrm{C}(f)$ and $\mathrm{UC}_{\min}(f)$.

4.1 A Separation Against $\mathrm{RC}(f)$ is Sufficient

We now explain why a separation between $\mathrm{s}(f)$ and $\mathrm{RC}(f)$ implies an equal separation between $\mathrm{s}(f)$ and $\mathrm{bs}(f)$, proving Theorem 3. The key insight is that $\mathrm{bs}(f)$ becomes $\mathrm{RC}(f)$ when the function is composed enough times; this was observed by [Tal13] and by [GSS16]. This means that if we start with a function separating $\mathrm{s}(f)$ and $\mathrm{RC}(f)$ and compose it enough times, we should get a function with the same separation between $\mathrm{s}(f)$ and $\mathrm{RC}(f)$, but with the additional property that $\mathrm{bs}(f) \approx \mathrm{RC}(f)$.

To prove this, we need to get a handle on how $\mathrm{s}(f)$, $\mathrm{bs}(f)$, and $\mathrm{RC}(f)$ behave under composition. We cite [Tal13] for this, but similar results appear in [GSS16]. Tal showed the following results, which give us the composition properties we need. In the statements below, we use f^k to denote the composition of f with itself k times.

Definition 7. *$f : \{0,1\}^n \to \{0,1\}$ is in $(\mathrm{RC}, 0)$-good form if $\mathrm{RC}_{0^n}(f) = \mathrm{RC}(f)$ and $f(0^n) = 0$.*

Lemma 8 ([Tal13])**.** *For any function $f : \{0,1\}^n \to \{0,1\}$, there is a function $\tilde{f} : \{0,1\}^n \to \{0,1\}$ which is in $(\mathrm{RC}, 0)$-good form and satisfies $\mathrm{RC}(\tilde{f}) = \mathrm{RC}(f), \mathrm{bs}(\tilde{f}) = \mathrm{bs}(f), \mathrm{s}(\tilde{f}) = \mathrm{s}(f)$.*

Theorem 9 ([WZ88])**.** *For any $f : \{0,1\}^n \to \{0,1\}$ and any $k \in \mathbb{N}$, we have $\mathrm{s}(f^k) \leq \mathrm{s}(f)^k$.*

Theorem 10 ([Tal13])**.** *For any $f : \{0,1\}^n \to \{0,1\}$ and any $k \in \mathbb{N}$, we have $\mathrm{bs}(f^k) \geq \frac{\mathrm{RC}(f^k)}{25n^2 2^n}$.*

Theorem 11 ([Tal13])**.** *For any $f : \{0,1\}^n \to \{0,1\}$ in $(\mathrm{RC}, 0)$-good form, $\mathrm{RC}(f^k) = \mathrm{RC}(f)^k$.*

Using these ingredients, we now prove Theorem 3, which we restate here for convenience.

Theorem 3 (Follows from [Tal13] and independently [GSS16])**.** *A power $2+\alpha$ separation between $\mathrm{RC}(f)$ and $\mathrm{s}(f)$ implies a power $2+\alpha-o(1)$ separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$.*

Proof. The result follows from a simple recursive composition. The only catch is that recursive composition can amplify even constant factors, so we must be careful not to destroy the separation by composing too much. To be very explicit, we will assume that we're starting with a family of functions satisfying $\mathrm{RC}(f) \geq \mathrm{s}(f)^{2+\alpha-\phi(\mathrm{s}(f))}$, where ϕ is a function that approaches 0. For example, we can represent the constant factor loss $\mathrm{RC}(f) \geq \mathrm{s}(f)^{2+\alpha}/10$ by setting $\phi(\mathrm{s}(f)) = (\log_{10} \mathrm{s}(f))^{-1}$.

Fix a family $\{f_\ell\}_{\ell=1}^{\infty}$ of Boolean functions $f_\ell : \{0,1\}^{n_\ell} \to \{0,1\}$ with $\lim_{\ell\to\infty} \mathrm{s}(f_\ell) = \infty$ and $\mathrm{RC}(f_\ell) \geq \mathrm{s}(f_\ell)^{2+\alpha-\phi(\mathrm{s}(f))}$, with $\lim_{n\to\infty} \phi(n) = 0$. By using Lemma 8 if necessary, we can assume f_ℓ is in $(\mathrm{RC}, 0)$-good form for all ℓ.

We now define $g_\ell := f_\ell^{\psi(\ell)}$, where $\psi(\ell) := 25n_\ell^2 2^{n_\ell}$. Now, $\mathrm{s}(g_\ell) \leq \mathrm{s}(f_\ell)^{\psi(\ell)}$ by Theorem 9, and $\mathrm{bs}(g_\ell) \geq \frac{\mathrm{RC}(f_\ell)^{\psi(\ell)}}{25n_\ell^2 2^{n_\ell}}$ by Theorem 10 and Theorem 11. Thus $\mathrm{bs}(g_\ell) \geq \frac{\mathrm{RC}(f_\ell)^{\psi(\ell)}}{\psi(\ell)}$, so $\psi(\ell) \leq$

$\frac{\log \mathrm{bs}(g_\ell)+\log\psi(\ell)}{\log \mathrm{RC}(f_\ell)} \le \log \mathrm{bs}(g_\ell)+\log\psi(\ell)$. This means $\psi(\ell)-\log\psi(\ell)\le \log \mathrm{bs}(g_\ell)$, which gives $\psi(\ell)\le 2\log \mathrm{bs}(g_\ell)$. This means $\mathrm{bs}(g_\ell)\ge \frac{\mathrm{RC}(f_\ell)^{\psi(\ell)}}{2\log \mathrm{bs}(g_\ell)}$, so

$$2\,\mathrm{bs}(g_\ell)\log \mathrm{bs}(g_\ell) \ge \mathrm{RC}(f_\ell)^{\psi(\ell)} \ge \mathrm{s}(f_\ell)^{(2+\alpha-\phi(\mathrm{s}(f_\ell)))\psi(\ell)} \ge \mathrm{s}(g_\ell)^{2+\alpha-\phi(\mathrm{s}(f_\ell))}.$$

Since $\mathrm{s}(f_\ell)$ goes to infinity as ℓ goes to infinity, it also goes to infinity as $\mathrm{s}(g_\ell)$ goes to infinity. Thus $\phi(\mathrm{s}(f_\ell))=o(1)$ in terms of the parameter $\mathrm{s}(g_\ell)$. We conclude that $\mathrm{bs}(g_\ell)\ge \mathrm{s}(g_\ell)^{2+\alpha-o(1)}$, as desired. □

4.2 But $\mathrm{RC}(f)$ Lower Bounds $\mathrm{UC}_{\min}(f)$

We would get a super-quadratic separation between $\mathrm{bs}(f)$ and $\mathrm{s}(f)$ if we had a super-linear separation between $\mathrm{RC}(f)$ and $\mathrm{UC}_{\min}(f)$. Unfortunately, this is impossible, as we now show. Actually, we'll prove the stronger statement $\mathrm{RC}(f) \le 2\,\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f)/(1-4\epsilon)$. We note that this implies Theorem 4, because when $\epsilon=0$, we have

$$\mathrm{RC}(f)\le 2\,\mathrm{avdeg}^{+}_{\min}(f)\le 2\deg^{+}_{\min}(f)\le 2\,\mathrm{UC}_{\min}(f).$$

The proof of the relationship $\mathrm{RC}(f) \le 2\,\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f)/(1-4\epsilon)$ is somewhat technical. One interesting thing to note about it is that it holds for partial functions as well, so long as the definition of $\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f)$ requires the approximating polynomial to evaluate to at most 1 on the entire Boolean hypercube.

Before providing the proof, we'll provide a warm up proof that $\mathrm{bs}(f)\le 2\,\mathrm{UC}_{\min}(f)$.

Lemma 12. *For all non-constant $f:\{0,1\}^n\to\{0,1\}$, we have $\mathrm{bs}(f)\le 2\,\mathrm{UC}_{\min}(f)-1$.*

Proof. Without loss of generality, we have $\mathrm{UC}_{\min}(f)=\mathrm{UC}_1(f)$. We also have $\mathrm{bs}_1(f)\le \mathrm{C}_1(f)\le \mathrm{UC}_1(f)$, so it remains to show that $\mathrm{bs}_0(f)\le 2\,\mathrm{UC}_1(f)-1$. Also without loss of generality, we assume that the block sensitivity of 0^n is $\mathrm{bs}(f)$ and that $f(0^n)=0$.

Let $B_1,B_2,\dots,B_{\mathrm{bs}(f)}$ be disjoint sensitive blocks of 0^n. Let U be an unambiguous collection of 1-certificates for f, each of size at most $\mathrm{UC}_1(f)$. For each $i\in[\mathrm{bs}(f)]$, we have $f(\vec{0}^{B_i})=1$, so there is some 1-certificate $p_i\in U$ such that p_i is consistent with $\vec{0}^{B_i}$. Since p_i is a 1-certificate, it is not consistent with $\vec{0}$, so it has a 1 bit (which must have index in B_i). Now, if $i\ne j$, the certificate p_i has a 1 inside B_i and only 0 or $*$ symbols outside B_i, and the certificate B_j has a 1 inside B_j and only 0 or $*$ symbols outside B_j; thus p_i and p_j are different. Since U is an unambiguous collection, p_i and p_j must conflict on some bit (with one of them assigning 0 and the other assigning 1), or else there would be an input consistent with both.

We construct a directed graph on vertex set $[\mathrm{bs}(f)]$ as follows. For each $i,j\in[\mathrm{bs}(f)]$ with $i\ne j$, we draw an arc from i to j if p_i has a 0 bit in a location where p_j has a 1 bit. It follows that for each pair $i,j\in[\mathrm{bs}(f)]$ with $i\ne j$, we either have an arc from i to j or else we have an arc from j to i (or both). The number of arcs in this graph is at least $\mathrm{bs}(f)(\mathrm{bs}(f)-1)/2$, so the average out degree is at least $(\mathrm{bs}(f)-1)/2$. Hence there is some vertex i with out degree at least $(\mathrm{bs}(f)-1)/2$. But this means p_i conflicts with $(\mathrm{bs}(f)-1)/2$ other certificates $p_{j_1},p_{j_2},\dots,p_{j_{(\mathrm{bs}(f)-1)/2}}$ with p_i having a bit 0 and p_{j_k} having a 1-bit; however, two different certificates p_{j_x} and p_{j_y} cannot both agree on a 1 bit, since the 1 bits of p_{j_x} must come from block B_{j_x} and the blocks are disjoint. This means p_i has at least $(\mathrm{bs}(f)-1)/2$ zero bits. It must also have at least one 1 bit. Thus $|p_i|\ge \mathrm{bs}(f)/2+1/2$, so $\mathrm{bs}(f)\le 2\,\mathrm{UC}_{\min}(f)-1$. □

We note that the relationship in Lemma 12 is tight. To see this, consider the function $f : \{0,1\}^3 \to \{0,1\}$ defined by $f(x) = 1$ if and only if $x_1 = x_2 = x_3$. The sensitivity of this function is 3, but $\mathrm{UC}_0(f) = 2$, because an unambiguous set of 0-certificates is $\{01*, *01, 1*0\}$.

We can even construct an infinite set of functions for which the factor of 2 in Lemma 12 is tight, using ideas from [Göö15]. To see this, let $f : (\{0\} \cup [k])^n \to \{0,1\}$ be the colored projective plane function defined in [Göö15], where $n = k^2 - k + 1$ and $k - 1$ is a prime power. This function f is defined as follows. Let H be the projective plane on $k^2 - k + 1$ points (so it has $k^2 - k + 1$ lines, with k points per line and k lines per point). For each point in H, pick an ordering of the k lines passing through it, and for each line in H, pick an ordering of the k points it contains; moreover, we require that if point P is the i-th point on line L, then line L is the i-th line containing point P. Such commuting orderings are known to exist. Now, in an input x to f, each point in H gets a number in $\{0\} \cup [k]$, and $f(x) = 1$ if and only if there is a line L whose points numbered exactly by their ordering in L.

Next, let $g : \{0,1\}^k \to \{0\} \cup [k]$ be a weight gadget defined by $g(0^k) = 0$, and otherwise $g(x)$ is the position of the first 1 bit in x. Consider the composed function $f \circ g$. It is not hard to see that $\mathrm{UC}_1(f \circ g) = 1 + 2 + \ldots + k = k(k+1)/2$, since we can unambiguously certify 1-inputs to f by showing the appropriate line (which has k points), and we can unambiguously certify that a point has number i by showing the first i bits of the gadget g. We also have $\mathrm{bs}_{\vec{0}}(f \circ g) \geq k^2 - k + 1$, because starting from the $\vec{0}$ input, we can satisfy a line by flipping the points on it to the appropriate number (by flipping a single bit in the gadget g for that point). Moreover, since no two lines give the same number to a point, no two of these blocks will overlap. Hence the block sensitivity is at least the number of lines, which is $k^2 - k + 1$. As $k \to \infty$, this is a factor of 2 larger than $\mathrm{UC}_{\min}(f \circ g)$.

We now prove the more general theorem using the same rough idea as we used for Lemma 12.

Theorem 13. *Let $f : \{0,1\}^n \to \{0,1\}$ be a non-constant function, and let $\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f)$ denote the minimum average degree of a non-negative polynomial that approximates either f or its negation with error at most ϵ (see Section 2.6 for definitions). If $\epsilon < 1/4$, we have $\mathrm{RC}(f) \leq \frac{2\,\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - 1}{1 - 4\epsilon}$.*

Proof. Let q be the non-negative approximating polynomial with average degree $\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f)$. Without loss of generality, we assume q approximates f rather than its negation. We can write $q \equiv \sum_{p \in \{0,1,*\}} w_p p$, so for any $x \in \{0,1\}^n$, we have

$$q(x) = \sum_{p \in \{0,1,*\}} w_p p(x) = \sum_{p\colon p \subseteq x} w_p,$$

where recall that w_p are non-negative weights given to partial assignments. This means for all $x \in \{0,1\}^n$, we know that

$$\left| f(x) - \sum_{p\colon p \subseteq x} w_p \right| \leq \epsilon, \qquad \sum_{p\colon p \subseteq x} w_p \leq 1, \qquad \text{and} \qquad \sum_{p\colon p \subseteq x} w_p |p| \leq \widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f).$$

Now, consider the input $y \in \{0,1\}^n$ for which $\mathrm{RC}_y(f) = \mathrm{RC}(f)$. There are two cases: either y is a 0-input, or else y is a 1-input. If y is a 1-input, we use the fractional certificate complexity interpretation of $\mathrm{RC}_y(f)$: the value $\mathrm{RC}_y(f)$ is the minimum amount of weight that can be distributed to the bits of y such that every sensitive block of y contains bits of total weight at least 1. We assign to bit $i \in [n]$ the weight

$$\frac{1}{1 - 2\epsilon} \sum_{p\colon p \subseteq y, p_i \neq *} w_p.$$

Then each sensitive block $B \subseteq [n]$ for y satisfies $f(y^B) = 0$, so the sum of w_p over all $p \subseteq y$ that have support disjoint from B must be at most ϵ. Since the sum of w_p over all $p \subseteq y$ is at least $1-\epsilon$, there must be weight at least $1-2\epsilon$ assigned to partial assignments consistent with p whose support overlaps B. It follows that the total weight given to the bits in B is at least 1, which means this weighting is feasible. This means the total weight upper bounds $\mathrm{RC}_y(f)$, so

$$\mathrm{RC}(f) = \mathrm{RC}_y(f) \leq \frac{1}{1-2\epsilon} \sum_{i\in[n]} \sum_{p:\, p\subseteq y,\, p_i\neq *} w_p = \frac{1}{1-2\epsilon} \sum_{p:\, p\subseteq y} w_p|p| \leq \frac{\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f)}{1-2\epsilon}.$$

It remains to deal with the case where y is a 0-input. In this case, we use the fractional block sensitivity interpretation of $\mathrm{RC}_y(f)$: the value of $\mathrm{RC}_y(f)$ is the maximum amount of weight that can be distributed to the sensitive blocks of y such that every bit of y lies inside blocks of total weight at most 1. Without loss of generality, we can assume only minimal sensitive blocks are assigned weight (minimal sensitive blocks are sensitive blocks such that all their proper subsets are not minimal).

Let $\mathcal{B} := \{B \subseteq [n] : f(y^B) \neq f(y)\}$ be the set of sensitive blocks of y, and let $\mathcal{M} := \{B \in \mathcal{B} : \forall B' \in \mathcal{B}, B' \subseteq B \Rightarrow B' = B\}$ be the set of minimal sensitive blocks of y. Let $\{a_B\}_{B\in\mathcal{M}}$ with $a_B \in \mathbb{R}^+$ be the optimal weighting of the minimal sensitive blocks. This means $\sum_{B\in\mathcal{B}} a_B = \mathrm{RC}_y(f)$ and $\sum_{B\ni i} a_B \leq 1$ for all $i \in [n]$.

We have $\sum_{p\subseteq y} w_p \leq \epsilon$ and $\sum_{p\subseteq y^B} w_p \geq 1-\epsilon$ for all $B \in \mathcal{B}$, which means that each $B \in \mathcal{B}$ overlaps partial assignments p of y of total weight at least $1-2\epsilon$. For any $B_1, B_2 \in \mathcal{M}$ with $B_1 \neq B_2$, we can write

$$2-2\epsilon \leq \sum_{p\subseteq y^{B_1}} w_p + \sum_{p\subseteq y^{B_2}} w_p = \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y^{B_1\cup B_2}} w_p + \sum_{p\subseteq y^{B_2}:\, p\not\subseteq y^{B_1\cup B_2}} w_p + \sum_{p\in G} w_p + \sum_{p\in H} w_p,$$

where $G := \{p : p \subseteq y^{B_1},\, p \subseteq y^{B_1\cup B_2}\}$ and $H := \{p : p \subseteq y^{B_2},\, p \subseteq y^{B_1\cup B_2}\}$. The last two sums are equal to $\sum_{p\in G\cup H} w_p + \sum_{p\in G\cap H} w_p$. We have $\sum_{p\in G\cup H} w_p \leq \sum_{p\subseteq y^{B_1\cup B_2}} w_p \leq 1$. Also, any $p \in G\cap H$ satisfies $p \subseteq y^{B_1\cap B_2}$. Since $B_1 \neq B_2$ and they are both minimal sensitive blocks, we have $f(y^{B_1\cap B_2}) = 0$, so $\sum_{G\cap H} w_p \leq \sum_{p\subseteq y^{B_1\cap B_2}} w_p \leq \epsilon$. It follows that

$$\sum_{p\subseteq y^{B_1}:\, p\not\subseteq y^{B_1\cup B_2}} w_p + \sum_{p\subseteq y^{B_2}:\, p\not\subseteq y^{B_1\cup B_2}} w_p \geq 1-3\epsilon.$$

Note that the above sums are over disjoint sets, since if $p \subseteq y^{B_1}$ and $p \not\subseteq y^{B_1\cup B_2}$, then p must disagree with y^{B_2} on some bit inside B_2. If we split out the parts of the sums for which $p \subseteq y$, we get

$$\sum_{p\subseteq y} w_p + \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p + \sum_{p\subseteq y^{B_2}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p \geq 1-3\epsilon.$$

Since $f(y) = 0$, the first sum is at most ϵ, so

$$\sum_{p\subseteq y^{B_1}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p + \sum_{p\subseteq y^{B_2}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p \geq 1-4\epsilon.$$

We now write the following.

$$\begin{aligned}
\mathrm{RC}(f)^2 - \mathrm{RC}(f) &= \sum_{B_1\in\mathcal{M}} a_{B_1} \sum_{B_2\in\mathcal{M}} a_{B_2} - \sum_{B_1\in\mathcal{M}} a_{B_1} \\
&\le \sum_{B_1\in\mathcal{M}} a_{B_1} \sum_{B_2\in\mathcal{M}} a_{B_2} - \sum_{B_1\in\mathcal{M}} a_{B_1}^2 \\
&= \sum_{B_1\in\mathcal{M}} a_{B_1} \sum_{B_2\neq B_1} a_{B_2} \\
&\le \frac{1}{1-4\epsilon} \sum_{B_1\in\mathcal{M}} a_{B_1} \sum_{B_2\neq B_1} a_{B_2} \left(\sum_{p\subseteq y^{B_1}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p + \sum_{p\subseteq y^{B_2}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p \right) \\
&= \frac{2}{1-4\epsilon} \sum_{B_1\in\mathcal{M}} a_{B_1} \sum_{B_2\neq B_1} a_{B_2} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p,
\end{aligned}$$

where the second line follows because $a_{B_1} \le 1$ for all $B_1 \in \mathcal{M}$.

Note that $\sum_{B_1\in\mathcal{M}} a_{B_1} = \mathrm{RC}(f)$, so if we divide both sides by $\mathrm{RC}(f)$, the last line becomes a weighted average. It follows that there exists some minimal block B_1 such that

$$\begin{aligned}
\mathrm{RC}(f) - 1 &\le \frac{2}{1-4\epsilon} \sum_{B_2\neq B_1} a_{B_2} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y,\, p\not\subseteq y^{B_1\cup B_2}} w_p \\
&= \frac{2}{1-4\epsilon} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y} w_p \sum_{B_2\neq B_1 : p\not\subseteq y^{B_1\cup B_2}} a_{B_2}.
\end{aligned}$$

Examine the inner summation above. Note that $y^{B_1\cup B_2} = (y^{B_1})^{B_2\setminus B_1}$. Since $p \subseteq y^{B_1}$, the condition $p \not\subseteq y^{B_1\cup B_2}$ is equivalent to the support of p having non-empty intersection with $B_2 \setminus B_1$. Using $\mathrm{supp}(p)$ to denote the support of p, we have

$$\begin{aligned}
\mathrm{RC}(f) - 1 &\le \frac{2}{1-4\epsilon} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y} w_p \sum_{i\in\mathrm{supp}(p)\setminus B_1} \sum_{B_2\in\mathcal{M}:\, i\in B_2} a_{B_2} \\
&\le \frac{2}{1-4\epsilon} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y} w_p \sum_{i\in\mathrm{supp}(p)\setminus B_1} 1 \\
&= \frac{2}{1-4\epsilon} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y} w_p |\mathrm{supp}(p)\setminus B_1| \\
&\le \frac{2}{1-4\epsilon} \sum_{p\subseteq y^{B_1}:\, p\not\subseteq y} w_p (|p|-1) \\
&\le \frac{2}{1-4\epsilon} \widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - \frac{2}{1-4\epsilon} \sum_{p\subseteq y^{B_1}:p\not\subseteq y} w_p \\
&\le \frac{2}{1-4\epsilon} \widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - \frac{2}{1-4\epsilon} \left(\sum_{p\subseteq y^{B_1}} w_p - \sum_{p\subseteq y} w_p \right) \\
&\le \frac{2}{1-4\epsilon} \widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - \frac{2}{1-4\epsilon} (1-\epsilon-\epsilon) \\
&\le \frac{2}{1-4\epsilon} \widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - \frac{2-4\epsilon}{1-4\epsilon},
\end{aligned}$$

where the second line follows because the sum of a_B over all blocks $B \in \mathcal{M}$ containing a given element $i \in [n]$ is at most 1, and the fourth line follows because the conditions $p \subseteq y^{B_1}$ and $p \nsubseteq y$ imply that the support of p is not disjoint from B_1. Finally, we get

$$\mathrm{RC}(f) \le \frac{2}{1-4\epsilon}\,\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - \frac{1}{1-4\epsilon} = \frac{2\,\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - 1}{1-4\epsilon},$$

as desired. □

Acknowledgements

I thank Robin Kothari for many helpful discussions and for comments on a preliminary draft. Work partially supported by NSF.

References

[Aar08] Scott Aaronson. Quantum certificate complexity. *Journal of Computer and System Sciences*, 74(3):313–322, 2008. Computational Complexity 2003. arXiv:1506.04719, doi:10.1016/j.jcss.2007.06.020. [pp. 4, 5]

[ABG+14] Andris Ambainis, Mohammad Bavarian, Yihan Gao, Jieming Mao, Xiaoming Sun, and Song Zuo. Tighter relations between sensitivity and other complexity measures. In *Automata, Languages, and Programming: 41st International Colloquium, ICALP 2014, Proceedings, Part I*, pages 101–113. Springer, 2014. arXiv:1411.3419, doi:10.1007/978-3-662-43948-7_9. [p. 1]

[ABK15] Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. *To appear in Proceedings of STOC 2016. arXiv preprint* arXiv:1511.01937, 2015. [pp. 2, 7]

[AKK16] Andris Ambainis, Martins Kokainis, and Robin Kothari. Nearly optimal separations between communication (or query) complexity and partitions. In *31st Conference on Computational Complexity (CCC 2016)*, volume 50 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:14, 2016. arXiv:1512.01210, doi:10.4230/LIPIcs.CCC.2016.4. [pp. 1, 7]

[AP14] Andris Ambainis and Krišjānis Prūsis. A tight lower bound on certificate complexity in terms of block sensitivity and sensitivity. In *Mathematical Foundations of Computer Science (MFCS 2014)*, pages 33–44. Springer, 2014. arXiv:1402.5078, doi:10.1007/978-3-662-44465-8_4. [p. 1]

[APV15] Andris Ambainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs. Sensitivity versus certificate complexity of boolean functions. *arXiv preprint* arXiv:1503.07691, 2015. [p. 1]

[AS11] Andris Ambainis and Xiaoming Sun. New separation between s(f) and bs(f). *arXiv preprint* arXiv:1108.3494, 2011. [p. 1]

[AV15] Andris Ambainis and Jevgēnijs Vihrovs. Size of sets with small sensitivity: A generalization of simon's lemma. In *Theory and Applications of Models of Computation (TAMC 2015)*, pages 122–133. Springer, 2015. arXiv:1406.0073, doi:10.1007/978-3-319-17142-5_12. [p. 1]

[BBC+01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald De Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001. arXiv:quant-ph/9802049, doi:10.1145/502090.502097. [pp. 4, 5]

[BdW02] Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002. doi:10.1016/S0304-3975(01)00144-X. [p. 2]

[Bel06] Aleksandrs Belovs. Non-intersecting complexity. In *SOFSEM 2006: Theory and Practice of Computer Science*, pages 158–165. Springer, 2006. doi:10.1007/11611257_13. [p. 1]

[BOH90] Yigal Brandman, Alon Orlitsky, and John Hennessy. A spectral lower bound technique for the size of decision trees and two-level and/or circuits. *IEEE Transactions on Computers*, 39(2):282–287, 1990. doi:10.1109/12.45216. [p. 1]

[Bop12] Meena Boppana. Lattice variant of the sensitivity conjecture. *arXiv preprint* arXiv:1207.1824, 2012. [p. 1]

[CKLS16] Sourav Chakraborty, Raghav Kulkarni, Satyanarayana V Lokam, and Nitin Saurabh. Upper bounds on fourier entropy. *Theoretical Computer Science*, pages 771–782, 2016. Computing and Combinatorics 2015, TR13-052. doi:http://dx.doi.org/10.1016/j.tcs.2016.05.006. [p. 1]

[FKW02] Ehud Friedgut, Jeff Kahn, and Avi Wigderson. Computing graph properties by randomized subcube partitions. In *Randomization and approximation techniques in computer science (RANDOM 2002)*, pages 105–113. Springer, 2002. doi:10.1007/3-540-45726-7_9. [p. 1]

[GJ15] Mika Göös and TS Jayram. A composition theorem for conical juntas. *Electronic Colloquium on Computational Complexity (ECCC)* TR15-167, 2015. [p. 2]

[GJPW15] Mika Göös, T.S. Jayram, Toniann Pitassi, and Thomas Watson. Randomized communication vs. partition number. *Electronic Colloquium on Computational Complexity (ECCC)* TR15-169, 2015. [pp. 1, 2, 7]

[GKS15] Justin Gilmer, Michal Kouckỳ, and Michael E Saks. A new approach to the sensitivity conjecture. In *Conference on Innovations in Theoretical Computer Science (ITCS 2015)*, pages 247–254. ACM, 2015. doi:10.1145/2688073.2688096. [p. 1]

[GNS+16] Parikshit Gopalan, Noam Nisan, Rocco A Servedio, Kunal Talwar, and Avi Wigderson. Smooth boolean functions are easy: Efficient algorithms for low-sensitivity functions. In *Conference on Innovations in Theoretical Computer Science (ITCS 2016)*, pages 59–70. ACM, 2016. arXiv:1508.02420, doi:10.1145/2840728.2840738. [p. 1]

[Göö15] Mika Göös. Lower bounds for clique vs. independent set. In *Foundations of Computer Science (FOCS 2015)*, pages 1066–1076. IEEE, 2015. TR15-012. doi:10.1109/FOCS.2015.69. [pp. 1, 2, 5, 7, 8, 10]

[GPW15] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. In *Foundations of Computer Science (FOCS 2015)*, pages 1077–1088. IEEE, 2015. TR15-050. doi:10.1109/FOCS.2015.70. [p. 1]

[GSS16] Justin Gilmer, Michael Saks, and Sudarshan Srinivasan. Composition limits and separating examples for some boolean function complexity measures. *Combinatorica*, pages 1–47, 2016. CCC 2013. arXiv:1306.0630, doi:10.1007/s00493-014-3189-x. [pp. 2, 7, 8]

[GSTW16] Parikshit Gopalan, Rocco Servedio, Avishay Tal, and Avi Wigderson. Degree and sensitivity: tails of two distributions. *arXiv preprint* arXiv:1604.07432, 2016. [p. 1]

[HKP11] Pooya Hatami, Raghav Kulkarni, and Denis Pankratov. Variations on the sensitivity conjecture. *Theory of Computing, Graduate Surveys*, 4:1–27, 2011. arXiv:1011.0354, doi:10.4086/toc.gs.2011.004. [p. 1]

[KRS15] Robin Kothari, David Racicot-Desloges, and Miklos Santha. Separating decision tree complexity from subcube partition complexity. In *Approximation, Randomization, and Combinatorial Optimization (RANDOM 2015)*, volume 40, pages 915–930. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015. arXiv:1504.01339, doi:10.4230/LIPIcs.APPROX-RANDOM.2015.915. [p. 1]

[KT13] Raghav Kulkarni and Avishay Tal. On fractional block sensitivity. *Electronic Colloquium on Computational Complexity (ECCC)* TR13-168, 2013. [pp. 4, 5]

[LMR+11] Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Špalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Foundations of Computer Science (FOCS 2011)*, pages 344–353, 2011. arXiv:1011.3020, doi:10.1109/FOCS.2011.75. [p. 7]

[Mid04] Gatis Midrijanis. Exact quantum query complexity for total boolean functions. *arXiv preprint* arXiv:quant-ph/0403168, 2004. [p. 5]

[Nis91] Noam Nisan. Crew prams and decision trees. *SIAM Journal on Computing*, 20(6):999–1007, 1991. doi:10.1137/0220062. [pp. 1, 5]

[Rei11] Ben W Reichardt. Reflections for quantum query algorithms. In *Proceedings of the twenty-second annual ACM-SIAM symposium on Discrete Algorithms (SODA 2011)*, pages 560–569. SIAM, 2011. arXiv:1005.1601, doi:10.1137/1.9781611973082.44. [p. 7]

[Sav02] Petr Savicky. On determinism versus unambiquous nondeterminism for decision trees. *Electronic Colloquium on Computational Complexity (ECCC)* TR02-009, 2002. [p. 1]

[Sze15] Mario Szegedy. An $O(n^{0.4732})$ upper bound on the complexity of the gks communication game. *arXiv preprint* arXiv:1506.06456, 2015. [p. 1]

[Tal13] Avishay Tal. Properties and applications of boolean function composition. In *Innovations in Theoretical Computer Science (ITCS 2013)*, pages 441–454, 2013. TR12-163. doi:10.1145/2422436.2422485. [pp. 2, 8]

[Tal16] Avishay Tal. On the sensitivity conjecture. *Electronic Colloquium on Computational Complexity (ECCC)* TR16-062, 2016. [pp. 1, 5]

[WZ88] Ingo Wegener and Laszlo Zádori. A note on the relations between critical and sensitive complexity, 1988. [p. 8]

[Yan91] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *Journal of Computer and System Sciences*, 43(3):441–466, 1991. STOC 1988. doi:10.1016/0022-0000(91)90024-Y. [p. 5]

ECCC ISSN 1433-8092

http://eccc.hpi-web.de