Low-Sensitivity Functions from Unambiguous Certificates

Shalev Ben-David[*1], **Pooya Hatami**[†2], **and Avishay Tal**[‡3]

1 **MIT, Cambridge, USA**
shalev@mit.edu
2 **DIMACS, Piscataway and IAS, Princeton, USA**
pooyahat@math.ias.edu
3 **IAS, Princeton, USA**
avishay.tal@gmail.com

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 2.22 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 ($\mathrm{UC}_{\min}$). We also 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 $\mathrm{s}(f)$.

Along the way, we give a power 1.22 separation between certificate complexity and one-sided unambiguous certificate complexity, improving the power 1.128 separation due to Göös [20]. As a consequence, we obtain an improved $\Omega(\log^{1.22} n)$ lower-bound on the co-nondeterministic communication complexity of the Clique vs. Independent Set problem.

1998 ACM Subject Classification F.1.3 Computation by Abstract Devices, Complexity Measures and Classes

Keywords and phrases Boolean functions, decision tree complexity, query complexity, sensitivity conjecture

Digital Object Identifier 10.4230/LIPIcs.ITCS.2017.28

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 $\mathrm{Q}(f) \le$

* Partially supported by NSF.
† Partially supported by the National Science Foundation under agreement No. CCF-1412958.
‡ Supported by the Simons Collaboration on Algorithms and Geometry, and by the National Science Foundation grant No. CCF-1412958.

$\mathrm{R}(f) \leq \mathrm{D}(f) \leq \mathrm{Q}(f)^6$. In contrast, no polynomial relationship connecting sensitivity to these measures is known, despite much interest (this problem was first posed by [31]. For a survey, see [26]. For recent progress, see [8, 13, 6, 4, 7, 9, 18, 39, 24, 25, 41]).

Until recently, the best known separation between sensitivity and any of these other measures was quadratic. Tal [41] showed a power 2.11 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 $\mathrm{C}(f) = \tilde{\Omega}(\mathrm{s}(f)^{2.22})$.

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. [14, 17, 37, 11, 27, 23, 20, 21, 16, 5]), 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 $\alpha \in \mathbb{R}^+$, 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.*

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 [2]) have low $\mathrm{UC}_{\min}$; in particular, one of the functions in [2] already has a quadratic separation between $\mathrm{Q}(f)$ and $\mathrm{UC}_{\min}(f)$, giving a cubic separation between $\mathrm{Q}(f)$ and $\mathrm{s}(f)$.

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

To separate $\mathrm{C}(f)$ from $\mathrm{s}(f)$, we will use a function f with a significant gap between $\mathrm{C}(f)$ and $\mathrm{UC}_{\min}(f)$. Göös [20], as part of the proof of his exciting $\omega(\log n)$ lower-bound for communication complexity of clique versus independent set problem, gave a construction of a function f such that $\mathrm{C}(f) \geq \mathrm{UC}_{\min}(f)^\alpha$ for $\alpha \approx 1.128$. Using Göös's function [20] would give a family of functions with $\mathrm{C}(f) = \Omega(\mathrm{s}(f)^{2.128})$. We show that it is possible to obtain an even better separation (Theorem 4 below), leading to the following separation between $\mathrm{C}(f)$ and $\mathrm{s}(f)$.

▶ **Corollary 3.** *There is a family of functions with $\mathrm{C}(f) = \Omega(\mathrm{s}(f)^{2.22})$.*

New separation between C and $\mathrm{UC}_{\min}$

It is known that $\mathrm{C}(f) \leq \mathrm{UC}_{\min}(f)^2$ (e.g., [20]), and analogously in the communication complexity world $\mathbf{coNP}^{cc}(f) \leq \mathbf{UP}^{cc}(f)^2$ ([43]). Next, we discuss a polynomial separation between C and $\mathrm{UC}_{\min}$ due to [20] that uses function composition.

Throughout the years, Boolean function composition was used extensively to separate different complexity measures; a non-exhaustive list includes [1, 3, 12, 19, 28, 32, 33, 34, 42, 36, 38, 40, 41]. The natural idea is to exhibit some constant separation between any two measures: $M(f)$ and $N(f)$ (i.e., $M(f) < N(f)$ for a constant size function f) and then to prove that $M(f^k) \leq M(f)^k$ and $N(f^k) \geq N(f)^k$, for any $k \in \mathbb{N}$. This yields an infinite family of functions with polynomial separation between M and N, as $N(f^k) \geq M(f^k)^{\log N(f)/\log M(f)}$.

However, this approach does not work straightforwardly in an attempt to separate $\mathrm{UC}_{\min}$ from C, since it is not necessarily true that $\mathrm{UC}_{\min}(f^k) \leq \mathrm{UC}_{\min}(f)^k$. [20] overcomes this barrier by considering gadgets over a larger alphabet where the letters of the alphabet are weighted. He constructs such a gadget using projective planes, and further shows how to compose gadgets over a weighted alphabet in a way that behaves multiplicatively for both $\mathrm{UC}_{\min}$ and C. Finally, he shows how to simulate the weights and the larger alphabet with a Boolean function. The gadget f_k constructed by Göös satisfies $\mathrm{C}(f_k) = k^2 - k + 1$ and $\mathrm{UC}_{\min}(f_k) = \frac{k(k+1)}{2}$, whenever $k-1$ is a prime power. The optimum separation is obtained when $k = 8$, giving a separation exponent of $\log(57)/\log(36) \geq 1.128$.

Since $\mathrm{C}(f_k) \approx k^2$ and $\mathrm{UC}_{\min}(f_k) \approx k^2/2$ and the separation exponent is

$$\log(\mathrm{C}(f_k))/\log(\mathrm{UC}_{\min}(f_k)) \approx \log(k^2)/\log(k^2/2),$$

it seems that one should try to take k as small as possible. However, the additive terms affect smaller k's more significantly, making the optimum attained at $k = 8$. This motivated us to try and reduce the weights in other ways, in order to improve the exponent. To do so, we introduce *fractional weights*. The argument of Göös as is does not allow fractional weights, and in particular when Booleanizing the function, it seems inherent to use integer weights. We overcome this difficulty by considering fractional weights in intermediate steps of the construction, and then round them up at the end to get integral weights. We obtain the following separation.

▶ **Theorem 4** ($\mathrm{UC}_{\min}(f)$ vs $\mathrm{C}(f)$ - Improved)**.** *There exists an infinite family of Boolean functions* $f_n : \{0,1\}^n \to \{0,1\}$ *such that* $\mathrm{C}(f_n) \geq \tilde{\Omega}\left(\mathrm{UC}_{\min}(f_n)^{\frac{\log(38/3)}{\log(8)}}\right) \geq \Omega(\mathrm{UC}_{\min}(f_n)^{1.22})$.

Using the lifting theorem of Göös et al. [22] (see also [20, Appendix A]), Theorem 4 implies the following

▶ **Theorem 5** ($\mathbf{UP}^{cc}(f)$ vs $\mathbf{coNP}^{cc}(f)$)**.** *There exists an infinite family of Boolean functions* $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *such that* $\mathbf{coNP}^{cc}(f_n) \geq \Omega(\mathbf{UP}^{cc}(f_n)^{1.22})$.

Hence, the exponent between $\mathbf{coNP}^{cc}$ and $\mathbf{UP}^{cc}$ is somewhere between 1.22 and 2. We conjecture the latter to be tight. Moreover, we get as a corollary an improved lower-bound for the conondeterministic communication complexity of the Clique vs Independent Set problem.

▶ **Corollary 6.** *There is a family of graphs* G *such that*

$$\mathbf{coNP}^{cc}(\mathrm{CIS}_G) \geq \Omega(\log^{1.22} n).$$

We refer the reader to [20] for a discussion on the Clique vs Independent Set problem that shows how Theorem 5 implies Corollary 6.

Limitations of Theorem 1

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 7** ([28, Corollary 3.2])**.** *If there exists a family of functions with* $\mathrm{RC}(f) \geq \Omega(\mathrm{s}(f)^{2+\alpha})$*, then there exists a family of functions with* $\mathrm{bs}(g) \geq \Omega(\mathrm{s}(g)^{2+\alpha-o(1)})$.

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

We show that the factor of 2 in Theorem 8 is necessary. In Appendix A we strengthen this theorem to show that $\mathrm{RC}(f)$ also lower bounds one-sided conical junta degree.

Organization

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 prove Theorem 4, from which Corollary 3 follows. In Section 5, 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 8.

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 $\mathbf{Pr}[A(x) = f(x)] \geq 2/3$ 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 $\mathrm{Q}(f) \leq \mathrm{R}(f) \leq \mathrm{D}(f)$. For more details on these measures, see the survey by Buhrman and de Wolf [15].

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, $x_i^B = x_i$ 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 $\mathrm{s}_x(f)$ 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 [1] (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 [1] and [28].

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 $\epsilon = 1/3$. [10] 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 to 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

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

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

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

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

[10] showed $\mathrm{D}(f) \leq \mathrm{bs}(f)\,\mathrm{C}(f)$, and [31] showed $\mathrm{C}(f) \leq \mathrm{bs}(f)^2$. From this we conclude that $\mathrm{D}(f) \leq \mathrm{C}(f)^2$ and $\mathrm{D}(f) \leq \mathrm{bs}(f)^3$. [28] showed $\sqrt{\mathrm{RC}(f)} = O(\widetilde{\deg}(f))$; thus

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

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 [1]), $\mathrm{D}(f) \leq \mathrm{bs}(f)\deg(f) \leq \deg(f)^3$ (due to [30]), and $\deg^{+}(f) \leq \mathrm{UC}(f)$ (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 $\widetilde{\deg}^{+}_{\min}(f) \geq \widetilde{\deg}(f)$, which follows from the fact that $\widetilde{\deg}(f) \leq \widetilde{\deg}^{+}_{1}(f)$ and that $\widetilde{\deg}(f)$ is invariant under negating f. Similarly, $\deg(f) \leq \deg^{+}_{\min}(f)$. We also have

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

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 $\mathrm{D}(f) \leq \mathrm{UC}_{\min}(f)^2$. The analogous statement in communication complexity was shown by [43]. The query complexity version of the proof can be found in [20].

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 [41] that was used to give a power 2.115 separation between $\mathrm{D}(f)$ and $\mathrm{s}(f)$.

▶ **Definition 9** (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 10** (Desensitization). *Let f' be the desensitized version of $f : \{0,1\}^n \to \{0,1\}$. Then $\mathrm{s}_0(f') = 1$ and $\mathrm{UC}_1(f') \leq 3\,\mathrm{UC}_1(f)$. 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 $M(f') \geq M(f)$.

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 $p_x p_x p_x \subseteq xyz$. Since $p_x \in U$, we have $p_x p_x p_x \in U'$. Finally, if $ppp, qqq \in U'$ with $ppp \neq qqq$, then $p \neq q$ 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 $\max_{ppp \in U'} |ppp| = 3 \cdot \max_{p \in U} |p| = 3 \cdot \mathrm{UC}_1(f)$, so $\mathrm{UC}_1(f') \leq 3 \cdot \mathrm{UC}_1(f)$.

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 $\alpha \in \mathbb{R}^+$, 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 10, we have $\mathrm{s}_0(f') \leq 1$ and $\mathrm{s}_1(f') \leq \mathrm{UC}_1(f') \leq 3\,\mathrm{UC}_{\min}(f)$, and also $\mathrm{D}(f') \geq \mathrm{D}(f)$. 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 [19], for R it can be found in [21], and for Q it follows from a general composition theorem [35, 29]. 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 [2]. 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 BSUM_n. [2] showed that $\mathrm{Q}(\mathrm{BSUM}_n) = \tilde{\Omega}(n)$, and every input has a certificate with $O(\log^3 n)$ ones.

Consider the function $\hat{f} := \mathrm{BSUM}_{\mathrm{UC}_{\min}(f)} \circ f'$. We have $\mathrm{Q}(\hat{f}) = \mathrm{Q}(\mathrm{BSUM}_{\mathrm{UC}_{\min}(f)})\mathrm{Q}(f') = \tilde{\Omega}(\mathrm{UC}_{\min}(f)\mathrm{Q}(f))$. We now analyze the sensitivity of $\hat{f}$. Fix an input z to $\hat{f} = \mathrm{BSUM}_{\mathrm{UC}_{\min}(f)} \circ f'$. This input consists of $\mathrm{UC}_{\min}(f)$ inputs to f', which, when evaluated, form an input y to $\mathrm{BSUM}_{\mathrm{UC}_{\min}(f)}$. Note that some of the inputs to f' correspond to sensitive bits of y (with respect to $\mathrm{BSUM}_{\mathrm{UC}_{\min}(f)}$); 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 and Corollary 3.

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

Proof. By Theorem 1, it suffices to construct a family of functions with $\mathrm{Q}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^2)$. Our function will be a cheat sheet function $\mathrm{BKK}_{\mathrm{CS}}$ from [2] that quadratically separates quantum query complexity from exact degree. This function has quantum query complexity quadratically larger than $\mathrm{UC}_{\min}$, as shown in [5]. ◀

▶ **Corollary 3.** *There is a family of functions with* $\mathrm{C}(f) = \Omega(\mathrm{s}(f)^{2.22})$.

Proof. In Theorem 4, we construct a family of functions with $\mathrm{C}(f) = \tilde{\Omega}(\mathrm{UC}_{\min}(f)^{\frac{\log(38/3)}{\log(8)}})$. Thus, by Theorem 1, we can construct a family of functions with $\mathrm{C}(f) = \tilde{\Omega}(\mathrm{s}(f)^{1+\frac{\log(38/3)}{\log(8)}}) = \Omega(\mathrm{s}(f)^{2.22})$. ◀

4 Improved separation between UC_1 and C

In this section we prove Theorem 4, building on the proof by [20]. Our main contribution is to show how to adapt the argument in [20] to allow for fractional weights. We finally give a fractional weighting scheme that leads to our improved separation. We observe that in order to obtain our final result, one can just take Göös's construction and reweigh it in the end. Nonetheless, we include the full details here to show that any gadget with a separation between UC_1 and C implies an asymptotic separation (which was not explicit in [20]).

Throughout the section, Σ and Γ will denote finite sets that correspond to input and output alphabets of our functions. We shall assume that 0 is not in Σ, and will discuss functions $f : (\{0\} \cup \Sigma)^n \to \Gamma$ where 0 is a special symbol treated differently than others.

4.1 Certificates and Weighted-Certificates for Large-Alphabet Functions

We generalize the definition of certificates from Boolean functions to functions with arbitrary input and output alphabets.

▶ **Definition 11** (Multi-valued Certificates, Simple Certificates)**.** A certificate for a function $f : (\{0\} \cup \Sigma)^n \to \Gamma$ is a cartesian product of sets $S_1 \times S_2 \times \ldots S_n$ where each $S_i \subseteq \{0\} \cup \Sigma$ is a non-empty set and such that all $y \in S_1 \times S_2 \times \ldots S_n$ have the same f-value.

A simple certificate for f is a certificate where each S_i is either: (i) $\{0\} \cup \Sigma$, or (ii) S_i contains exactly one element, and this element is from Σ (i.e., not the 0 element).[1]

We define the size of a certificate as the number of i's such that $S_i \neq (\{0\} \cup \Sigma)$. For $x \in (\{0\} \cup \Sigma)^n$, we denote by $\mathrm{C}(f, x)$ the size of the smallest certificate for f which contains x.

For a set $T \subseteq \Gamma$ we say that $S_1 \times \ldots \times S_n$ certifies that "$f(\cdot) \in T$" if this is true for any $y \in S_1 \times \ldots \times S_n$. When $T = \Gamma \setminus \{i\}$ we write "$f(\cdot) \neq i$" for shorthand.

▶ **Definition 12** (Weight Schemes, Certificate Weights)**.** Let $w : \Sigma \to \mathbb{R}^+$ be a non-negative weight function. A weight scheme is a mapping, w, associating positive real numbers to non-empty subsets of $\{0\} \cup \Sigma$ such that:

1. If $S = \{i\}$, for some $i \in \Sigma$, then the weight of S is $w(i)$.
2. If $S = (\{0\} \cup \Sigma)$, then the weight of S is 0.
3. If $0 \in S$ an $S \neq (\{0\} \cup \Sigma)$, then the weight of S is $\max_{i \in \Sigma \setminus S}\{w(i)\}$. (In particular, if $S = \{0\}$ then the weight of S is $\max_{i \in \Sigma}\{w(i)\}$.)

(Note that we did not specify the weight of sets S of at least two elements which do not contain 0, as they will not be used in our analysis.)

The weight of a certificate $S_1 \times \ldots \times S_n$ is simply $\sum_{i=1}^{n} w(S_i)$. For a function $f : (\{0\} \cup \Sigma)^n \to \Gamma$ and an input $x \in (\{0\} \cup \Sigma)^n$ we define the certificate complexity $\mathrm{C}((f, w), x)$ to be the minimal weight of a certificate $S_1 \times \ldots \times S_n$ for f according to w, such that $x \in S_1 \times \ldots \times S_n$.

▶ **Definition 13** (Realization of Weight Schemes)**.** The weight-scheme defined by an integer-valued weight function $w : \Sigma \to \mathbb{N}$ is realized by $g_w : (\{0\} \cup \Sigma)^m \to (\{0\} \cup \Sigma)$ if:

- **(i)** For $i \in \Sigma$, there exists a collection of unambiguous certificates of size-$(w(i))$ for "$g_w(\cdot) = i$",
- **(ii)** $g_w(0^m) = 0$, and
- **(iii)** In order to prove "$g_w(0^m) \in S$" it is required to expose at least $w(S)$ coordinates of 0^m.

▶ **Lemma 14** (Weight-Scheme Implementation, [20])**.** *Let $w : \Sigma \to \mathbb{N}$ be an integer-valued weight function. Then, there exists a weight scheme associating natural numbers to non-empty subsets of $\{0\} \cup \Sigma$ that can be realized by a function $g_w : (\{0\} \cup \Sigma)^m \to (\{0\} \cup \Sigma)$ where $m = \max_i\{w_i\}$.*

[1] Note that a certificate for "$f(x) = 1$" for a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is always simple.

Proof. We define $g_w(x) = i$ iff the symbol i appears in the first $w(i)$ coordinates and i is the first non-zero symbol to appear in the string. We set $g_w(x) = 0$ if there is no such $i \in \Sigma$. (ii) holds trivially. For (i) note that the decision tree that queries the first $w(i)$ coordinates induces an unambiguous collection of certificates for "$g_w(\cdot) = i$". For (iii) we may assume without loss of generality that $S \neq (\{0\} \cup \Sigma)$ as otherwise the claim is trivial. Since we are proving that "$g_w(0^m) \in S$" and indeed $g_w(0^m) = 0$ it is required that $0 \in S$. It remains to show that it is required to expose the first $\max_{i \in \Sigma \setminus S} w(i)$ coordinates of the input to g_w. Let i be the element in $\Sigma \setminus S$ with maximal weight. Indeed, if one coordinate in the first $w(i)$ coordinates was not exposed, then it is still possible that $g_w(\cdot) = i$, as all coordinates that were exposed are equal to 0 and there is an unexposed position in the first $w(i)$ coordinates that might be marked with i. ◀

4.2 Composing Functions over Large Alphabet with Fractional Weights

Most of the results below are generalizations of arguments from [20]. However, since unlike [20] we deal with fractional weights, in addition to the total weight, we also need to take into account the number of coordinates in the intermediate certificates.

Let $f : (\{0\} \cup \Sigma)^N \to \{0, 1\}$, and let $w : \Sigma \to \mathbb{R}^+$. We treat the pair (f, w) as a "weighted function". Let $\mathcal{C}$ be an unambiguous collection of simple 1-certificates of size-s and weight at most W for (f, w). Let Σ_0 be a finite set that does not contain 0 and $w_0 : \Sigma_0 \to \mathbb{R}^+$. We define $(\tilde{f}, \tilde{w})$, where $\tilde{f} : (\{0\} \cup \Sigma \times \Sigma_0)^N \to (\{0\} \cup \Sigma_0)$ as follows. Denote by $\pi_1(x)$ and $\pi_2(x)$ the projection of $x \in (\{0\} \cup \Sigma \times \Sigma_0)^N$ to its $(\{0\} \cup \Sigma)^N$ coordinates and its $(\{0\} \cup \Sigma_0)^N$ coordinates respectively. The value of $\tilde{f}(x)$ is defined as follows.

> If $f(\pi_1(x)) = 0$, then set $\tilde{f}(x) := 0$. Otherwise, let $\mathcal{T} \in \mathcal{C}$ be the unique certificate for "$f(\cdot) = 1$" on $\pi_1(x)$. Read the corresponding coordinates of $\mathcal{T}$ from $\pi_2(x)$ and if all of them are equal to some $i \in \Sigma_0$, then set $\tilde{f}(x) := i$; otherwise set $\tilde{f}(x) := 0$.

Let $\tilde{w} : \Sigma \times \Sigma_0 \to \mathbb{R}^+$ be defined as $\tilde{w}(\sigma, i) = w(\sigma) \cdot w_0(i)$. The following lemma shows useful bounds on the certificates of the new function $\tilde{f}$ according to $\tilde{w}$.

▶ **Lemma 15** (From Boolean to Larger Output Alphabet). *Let $\tilde{f}$, f, $\tilde{w}$, w and w_0 be defined as above. Then,*

(B1) *There is an unambiguous collection of simple size-s certificates for "$\tilde{f}(\cdot) = i$" with weight at most $w_0(i) \cdot W$ according to $\tilde{w}$.*

(B2) *The certificate complexity of "$\tilde{f}(0^N) \neq i$" with respect to $\tilde{w}$ is at least $w_0(i) \cdot \mathrm{C}((f, w), 0^N)$.*

Proof.

(B1) The unambiguous collection of simple 1-certificates for f corresponds to unambiguous collection of simple i-certificates for $\tilde{f}$ by checking that each queried symbol has its Σ_0-part equals i. The weight of each certificate in the collection is at most $w_0(i) \cdot W$ as each coordinate weighs $w_0(i)$ times its "original" weight.

(B2) Fix $i \in \Sigma_0$. Assume we have a certificate for "$\tilde{f}(0^n) \neq i$". This is a cartesian product $S_1 \times \ldots \times S_N$ such that each S_i contains the 0 symbol and under which $\forall x \in S_1 \times \ldots \times S_N$ it holds that $\tilde{f}(x) \neq i$. Take $\hat{f}$ to be $\tilde{f}$ restricted only to input alphabet $\{0\} \cup (\Sigma \times \{i\})$. Then $S'_1 \times \ldots \times S'_n$ where $S'_j = S_j \cap (\{0\} \cup (\Sigma \times \{i\}))$ is a certificate for "$\hat{f}(0^N) \neq i$". Using property 3 in Definition 12, we show that $w(S'_j) \leq w(S_j)$. We consider two cases. If $S'_j = \{0\} \cup (\Sigma \times \{i\})$, then $w(S'_j) = 0 \leq w(S_j)$. Otherwise,

$$w(S'_j) = \max_{\sigma \in (\Sigma \times \{i\}) \setminus S'_j} w(\sigma) \leq \max_{\sigma \in (\Sigma \times \Sigma_0) \setminus S_j} w(\sigma) = w(S_j).$$

However, proving that "$\hat{f}(0^N) = 0$" is equivalent to proving that "$f(0^N) = 0$", except for the reweighing. Since each coordinate weighs according to $\tilde{w}$ at least $w_0(i)$ times its weight according to w, the weight of the certificate $S_1 \times \ldots \times S_n$ is at least $w_0(i) \cdot C((f,w),0^N)$. ◀

▶ **Lemma 16** (Composition Lemma). *Let $h : (\{0\} \cup [k])^n \to \{0,1\}$ with $h(0^n) = 0$, and let $w_0 : [k] \to \mathbb{R}^+$ such that (h, w_0) has an unambiguous collection of simple 1-certificates of size-k and (fractional) weight u, however any certificate for "$h(0^n) = 0$" is of (fractional) weight v.*

Let $\tilde{f}$ and $\tilde{w}$ be as defined above. Let $f' : (\{0\} \cup \Sigma \times [k])^{n \times N} \to \{0,1\}$ be defined by $f' = h \circ \tilde{f}$, and $w' : (\{0\} \cup \Sigma \times [k]) \to \mathbb{N}$ be equal to $\tilde{w}$. Then,

(A1) *(f', w') has an unambiguous collection of simple certificates 1-certificates with size at most sk and weight at most $u \cdot W$.*

(A2) $\mathrm{C}((f', w'), 0^{Nn}) \geq v \cdot \mathrm{C}((f,w), 0^N)$.

Proof.

(A1) Take the unambiguous collection $\mathcal{C}$ of simple 1-certificates for h of size-k and (fractional) weight u. For any certificate $\mathcal{T}$ from $\mathcal{C}$ replace the verification that some coordinate equals i with the simple certificate that the relevant N-length input of $\tilde{f}$ belongs to $\tilde{f}^{-1}(i)$. The cost of each such certificate to $\tilde{f}$ will be at most $W \cdot w_0(i)$ according to $\tilde{w} \equiv w'$. Thus, the overall cost will be $W \cdot u$, and the certificates will be of size at most sk. It is easy to verify that these certificates are unambiguous, since unambiguous collections of simple certificates are closed under composition.

(A2) Let $\mathcal{T}$ be a certificate for "$f'(0^{N \cdot n}) = 0$" of minimal weight (according to w'), and let $w_{\mathcal{T}}$ be its weight. Let $\mathcal{T}_1, \ldots, \mathcal{T}_n$ be the substrings of $\mathcal{T}$ of length N according to the composition of $h \circ \tilde{f}$. By Lemma 15[B1], if $\mathcal{T}_i$ certifies that "$\tilde{f}(0^N) \neq j$", then it costs at least $w_0(j) \cdot \mathrm{C}((f,w),0^N)$. We construct a certificate $\mathcal{H}$ for h from $\mathcal{T}$. If $\mathcal{T}_i$ certifies that $\tilde{f}(0^N) \neq j$ then $(\mathcal{H})_i \neq j$. More formally, let $\mathcal{H} = S_1 \times \ldots \times S_n$, where for $i \in [n]$ the set S_i consists of $\{0\}$ union with all j such that $\mathcal{T}_i$ *does not* certify that $\tilde{f}(0^N) \neq j$. Suppose by contradiction that $\mathcal{H}$ does not certify that "$h(0^n) = 0$". Then, there exists an input $y \in S_1 \times \ldots \times S_n$ (i.e., an input consistent with $\mathcal{H}$) such that $h(y) = 1$. Thus, there exist inputs $x^{(1)}, \ldots, x^{(n)}$ each of length N such that $\tilde{f}(x^{(i)}) = y_i$ and $\mathcal{T}_i$ is consistent with $x^{(i)}$, which shows that $\mathcal{T}$ is not a certificate for $h \circ \tilde{f}_{\tilde{w}}$. Thus, $\mathcal{H}$ is a certificate for $h(0^n) = 0$, and we get that

$$w_{\mathcal{T}} \geq w_0(\mathcal{H}) \cdot \mathrm{C}((f,w),0^N) = v \cdot \mathrm{C}((f,w),0^N).$$ ◀

Next, we show how to take any "gadget" h – a function over a constant number of symbols – with some gap between the $\mathrm{UC}_1(h)$ and $\mathrm{C}(h, 0^n)$, and convert it into an infinite family of functions with a polynomial separation between UC_1 and C.

▶ **Theorem 17** (From Gadgets to Boolean Unweighted Separations). *Let $u, v \in \mathbb{R}$, $k \in \mathbb{N}$ be constants such that $1 \leq k \leq u < v$. Let $h : (\{0\} \cup [k])^n \to \{0,1\}$ with $h(0^n) = 0$, and let $w_0 : [k] \to \mathbb{R}^+$ such that (h, w_0) has an unambiguous collection of simple 1-certificates of size-k and (fractional) weight u, however any certificate for "$h(0^n) = 0$" is of (fractional) weight v.*

Then, there exists an infinite family of Boolean functions $\{h'_m\}_{m \in \mathbb{N}}$ with

1. $\mathrm{UC}_1(h'_m) \leq \mathrm{poly}(m) \cdot u^m$
2. $\mathrm{C}(h'_m) \geq v^m$
3. *h'_m is defined over $\mathrm{poly}(m) \cdot \exp(O(m))$ many bits.*

Proof. We start by defining a sequence of weighted functions $\{(h_m, w_m)\}_{m\in\mathbb{N}}$ over large alphabet size with a polynomial gap between UC_1 and C. We then convert these functions into unweighted Boolean functions with the desired properties.

We take $h_1 := h$ and $w_1 := w_0$. For $m \geq 2$ we take (h_m, w_m) to be the composition of (h, w_0) with $(\tilde{h}_{m-1}, \tilde{w}_{m-1})$. Let $\Sigma_m = [k]^m$. Then, $h_m : (\{0\} \cup \Sigma_m)^{n^m} \to \{0,1\}$ and $w_m : (\{0\} \cup \Sigma_m) \to \mathbb{R}^+$. Using Lemma 16, we have that

(i) The maximal weight in w_m is at most $(w_{0,max})^m$, where $w_{0,max} := \max_i\{w_0(i)\}$.
(ii) There exists an unambiguous collection of simple 1-certificates of size k^m and weight at most u^m for (h_m, w_m).
(iii) $\mathrm{C}((h_m, w_m), \vec{0}) \geq v^m$.

Making Weights Integral

First, we modify the weights so that they will be integral. We take $w'_m(\cdot)$ to be $\lceil w_m(\cdot)\rceil$. Taking ceiling on the weights may only increase the certificate complexities. Thus, $\mathrm{C}((h_m, w'_m), \vec{0}) \geq v^m$. On the other hand, the weight of any certificate may only increase additively by its size, hence $\mathrm{UC}_1((h_m, w'_m)) \leq u^m + k^m \leq 2u^m$.

Eliminating Weights

Next, we convert the weighted function (h_m, w'_m) to an unweighted Boolean function h'_m with similar UC_1 and C complexities. First, we remove the weights by applying Lemma 14 (using the fact that w'_m is integer-valued). We define $h''_m = h_m \circ g_{w'_m}$. Lemma 14 implies that

$$\mathrm{C}(h''_m) \geq \mathrm{C}((h_m, w'_m)) \geq v^m$$

and

$$\mathrm{UC}_1(h''_m) \leq \mathrm{UC}_1((h_m, w'_m)) \leq 2 \cdot u^m.$$

Booleanizing

To make the inputs of the function h''_m Boolean we repeat the argument of Göös [20]. If f is a function $f : \Sigma^N \to \{0,1\}$, we may always convert it to a boolean function by composing it with some surjection $g_\Sigma : \{0,1\}^{\lceil \log|\Sigma|\rceil} \to \Sigma$. The following naive bounds will suffice for our purposes:

$$\mathcal{C}(f) \leq \mathcal{C}(f \circ g_\Sigma) \leq \mathcal{C}(f) \cdot \lceil \log|\Sigma|\rceil \quad \text{forall } \mathcal{C} \in \{\mathrm{UC}_1, \mathrm{C}\}. \tag{1}$$

In our final alphabet $\Sigma = \{0\} \cup [k]^m$, thus $h'_m = h''_m \circ g_\Sigma$ is a Boolean function with

$$\mathrm{C}(h'_m) \geq \mathrm{C}(h''_m) \geq v^m$$

and

$$\mathrm{UC}_1(h'_m) \leq \mathrm{UC}_1(h''_m) \cdot \lceil \log|\Sigma|\rceil \leq 2 \cdot u^m \cdot O(m \log k).$$

Input Length

The input length of h_m is n^m. By lemma 14, the input length of h''_m is at most $n^m \cdot (w^m_{0,max}+1)$. Thus the input length to h'_m is at most

$$O(\log(|\Sigma|) \cdot (n \cdot w_{0,max})^m) = O(m \cdot \log(k) \cdot (n \cdot w_{0,max})^m)$$ ◀

4.3 Gadgets Based on Projective Planes

We will use a reweighed version of the function constructed by Göös [20] based on projective planes as our gadget. Let us first recall the definition of a projective plane.

▶ **Definition 18** (Projective plane). A projective plane is a k-uniform hyper-graph with $n = k^2 - k + 1$ edges and n nodes with the following properties.

- Each node is incident on exactly k edges.
- For every two nodes, there exists a unique edge containing both.
- Every two edges intersect on exactly one node.

Given a projective plane, it follows from Hall's theorem that it is possible to assign an ordering to the edges incident to each vertex in a way that for each edge, its assigned order for each of its nodes is different. Namely, for each i, there are no two nodes for which their i-th incident edge is the same.

It is well-known that projective planes exist for every k such that $k-1$ is a prime power. Göös [20] introduced the following function $f : (\{0\} \cup \Sigma)^n \to \{0,1\}$ based on a projective plane, with $\Sigma = [k]$. We think of the inputs of f as a sequence of pointers, one for each node, where 0 is the Null pointer, and $i \in [k]$ is a pointer to the i-th edge on which the node is incident on. We set $f(x) = 1$ if there is an edge of the projective plane such that all its nodes point to it, and $f(x) = 0$ otherwise.

We will be interested in showing a gap between the certificate complexity of "$f(0^n) = 0$" and $\mathrm{UC}_1(f)$. However, the function as is, allows a certificate of size k for "$f(0^n) = 0$" matching its $\mathrm{UC}_1(f)$. One certificate for "$f(0^n) = 0$" is to pick an arbitrary edge of the projective plane, and certify that all its nodes have the Null pointer. This certifies "$f(0^n) = 0$" as every two edges in a projective plane intersect on a node. An unambiguous collection of size k certificates consists of picking for each edge all its nodes and ensuring that they point to that edge. This collection is unambiguous using the same property that every two edges intersect on one node.

In order to obtain a gadget with a gap between UC_1 and C, Göös introduced weights on the input alphabet of f. Each element $i \in \Sigma$ is assigned a weight $w(i)$, where the weights are intended to carry the following meaning: For every $i \in \Sigma$ it costs $w(i)$ for a certificate to assure that "$x_j = i$", and moreover 0 has the special property that it costs $\max_{i \in \Sigma} w(i)$ to assure that "$x_j = 0$" (as in Definition 12). In [20] each $i \in [k]$ is assigned a weight $w(i) = i$. Göös [20] implemented this weighting scheme specifically for the case when $w(i) := i$ via a weighting gadget $g_w : (\{0\} \cup \Sigma)^k \to (\{0\} \cup \Sigma)$ (as done in Lemma 14) and considering $f \circ g_w$. Our improvement comes from considering a different weighting scheme with fractional weights.

▶ **Claim 19** (Reweighing the Projective Plane). *Let f be defined as above, and let $w(i) := \frac{i}{(k+1)/2}$. Then, (f, w) has an unambiguous collection of simple 1-certificates of size k and weight k. Moreover, any certificate for $f(0^n) = 0$ is of weight at least $\frac{k^2-k+1}{(k+1)/2}$*

Proof. Göös [20, Claims 6 and 7] showed that with respect to the weight-function $w'(i) = i$, the function f has an unambiguous collection of simple 1-certificates of size-k and weight $(k \cdot (k+1))/2$. However, any certificate for "$f(0^n) = 0$" is of weight at least $k^2 - k + 1$.

From this, it is immediate that with respect to $w \equiv \frac{w'}{(k+1)/2}$, f has an unambiguous collection of simple 1-certificates of size-k and (fractional) weight $\frac{(k\cdot(k+1))/2}{(k+1)/2} = k$. However, any certificate for 0^n is of weight at least $\frac{k^2-k+1}{(k+1)/2}$. ◀

4.4 Putting Things Together

Given a gadget (h, w_0) such that h has unambiguous collection of simple 1-certificates of size-k and (fractional) weight u, however any certificate for 0^n is of (fractional) weight v, with $v > u > 1$ and $u \geq k$, Theorem 17 gives a polynomial separation between C and UC_1:

$$\mathrm{C}(h'_m) \geq v^m = (u^m)^{\log(v)/\log(u)} \geq \widetilde{\Omega}\left(\mathrm{UC}_1(h'_m)^{\log(v)/\log(u)}\right) . \tag{2}$$

We take h to be the projective plane function f described in Section 4.3 with $k = 8$, $n = k^2 - k + 1 = 57$ and weight function $w_0(i) = \frac{i}{(k+1)/2}$. By Claim 19, we have that with respect to w_0, h has an unambiguous collection of simple 1-certificates of size-k and weight $k = 8$. However, any certificate for 0^n is of weight $\frac{k^2-k+1}{(k+1)/2} = 38/3$. Plugging these values in Equation (2) we get a better separation:

$$\mathrm{C}(h'_m) \geq \widetilde{\Omega}\left(\mathrm{UC}_1(h'_m)^{\frac{\log(38/3)}{\log(8)}}\right) \geq \Omega(\mathrm{UC}_1(h'_m)^{1.22}) , \tag{3}$$

where the input length is $N \leq \mathrm{poly}(m) \cdot \exp(O(m))$. The lifting theorem of [22, 20] incurs a loss factor of $\log(N) = O(m)$ in the separation, however this is negligible compared to the $\mathrm{poly}(m) \cdot u^m$ versus v^m separation.

4.5 Further Improvements

Since our theorem is general in transforming a fractional weighted gadget into a polynomial separation, it is enough to only improve the gadget construction in order to improve the UC_1 vs C exponent. Indeed, even using the same gadget (the projective plane function of Göös) we can consider different weight function. Using computer search it seems that such reweighing is indeed better than our choice of w_0. However, the improvement is mild and currently we do not have a humanly verifiable proof for the lower bound on the certificate complexity of 0^n under the reweighing. Indeed, Göös relied on the fact that the weights were $w'(i) = i$ in order to present a simple proof of his lower bound on the certificate complexity of "$h(0^n) = 0$" according to w'. It seems though (we have verified this using computer-search for small values of k) that the best weights are attained by taking $w'(i) = i + 1$ and then reweighing by multiplying all weights by the constant $\alpha = \frac{1}{(k+3)/2}$, so that the unambiguous certificates for h will be of weights k. We leave proving a lower bound under this weight function as an open problem.

5 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, by [28], it suffices to provide a family of functions for which $\mathrm{RC}(f) \gg \mathrm{UC}_{\min}(f)$ (as explained in Section 5.1). In Section 5.2, we show that even separating $\mathrm{RC}(f)$ from $\mathrm{UC}_{\min}(f)$ is impossible: we have $\mathrm{RC}(f) \leq 2\,\mathrm{UC}_{\min}(f) - 1$. 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 [20] showed a separation between $\mathrm{C}(f)$ and $\mathrm{UC}_{\min}(f)$.

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

[28] showed that a separation between $\mathrm{s}(f)$ and $\mathrm{RC}(f)$ implies an equal separation between $\mathrm{s}(f)$ and $\mathrm{bs}(f)$ (see Theorem 7). The key insight is that $\mathrm{bs}(f)$ becomes $\mathrm{RC}(f)$ when the function is composed enough times; this was observed by [40] and by [19]. 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 $\mathrm{bs}(f) \approx \mathrm{RC}(f)$.

5.2 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 using our paradigm, as we now show. Actually, we can prove an even stronger statement, namely that $\mathrm{RC}(f) \leq (2\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - 1)/(1-4\epsilon)$. We note that this implies Theorem 8, because when $\epsilon = 0$, we have

$$\mathrm{RC}(f) \;\leq\; 2\,\mathrm{avdeg}^{+}_{\min}(f) - 1 \;\leq\; 2\,\mathrm{deg}^{+}_{\min}(f) - 1 \;\leq\; 2\,\mathrm{UC}_{\min}(f) - 1.$$

This stronger statement says that one-sided conical junta degree is lower bounded by two-sided randomized certificate complexity, which helps clarify the hierarchy of lower bounds for randomized algorithms.

The proof of the relationship $\mathrm{RC}(f) \leq (2\widetilde{\mathrm{avdeg}}^{+,\epsilon}_{\min}(f) - 1)/(1-4\epsilon)$ is somewhat technical; we leave it for Appendix A, and provide a cleaner proof (of $\mathrm{RC}(f) \leq 2\,\mathrm{UC}_{\min}(f) - 1$) below. One interesting thing to note about it is that it holds for partial functions as well, as 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 $\mathrm{bs}(f) \leq 2\,\mathrm{UC}_{\min}(f)$.

▶ **Lemma 20.** *For all non-constant $f : \{0,1\}^n \to \{0,1\}$, we have $\mathrm{bs}(f) \leq 2\,\mathrm{UC}_{\min}(f) - 1$.*

Proof. Without loss of generality, we have $\mathrm{UC}_{\min}(f) = \mathrm{UC}_1(f)$. We also have $\mathrm{bs}_1(f) \leq \mathrm{C}_1(f) \leq \mathrm{UC}_1(f)$, so it remains to show that $\mathrm{bs}_0(f) \leq 2\,\mathrm{UC}_1(f) - 1$. 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 $B_1, B_2, \ldots, B_{\mathrm{bs}(f)}$ 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 $i \neq j$, 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 $i \neq j$, 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 $i \neq j$, 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 $p_{j_1}, p_{j_2}, \ldots, p_{j_{(\mathrm{bs}(f)-1)/2}}$ 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 $|p_i| \geq \mathrm{bs}(f)/2 + 1/2$, so $\mathrm{bs}(f) \leq 2\,\mathrm{UC}_{\min}(f) - 1$. ◀

We now generalize this lemma from bs to RC, proving Theorem 8. A further strengthening of the result can be found in Appendix A.

▶ **Theorem 8.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. Then* $\mathrm{RC}(f) \leq 2\,\mathrm{UC}_{\min}(f) - 1$.

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

We prove the theorem using the characterization of $\mathrm{RC}(f)$ as the fractional block sensitivity of f. Let $B_1, B_2, \ldots, B_m$ be minimal sensitive blocks of 0^n. Let $a_1, \ldots, a_m$ be weights assigned to blocks $B_1, \ldots, B_m$ such that

$$\sum_j a_j = \mathrm{RC}(f) \quad \text{, and} \quad \forall i \in [n] : \sum_{j : i \in B_j} a_j \leq 1 \,.$$

Let U be an unambiguous collection of 1-certificates for f, each of size at most $\mathrm{UC}_1(f)$. For each $i \in [m]$, 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). Next, we show that if $i \neq j$, then p_i and p_j are different. Assume by contradiction that $p_i = p_j$, then p_i is a partial assignment that satisfy both $\vec{0}^{B_i}$ and $\vec{0}^{B_j}$, hence it must satisfy $\vec{0}^{B_i \cap B_j}$, but this means that $f(\vec{0}^{B_i \cap B_j}) = 1$ which contradicts the fact that both B_i and B_j are minimal sensitive blocks for $\vec{0}$.

We established that for any $i \neq j$, the partial assignments 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 weighted graph on vertex set $[m]$ as follows. For each $i, j \in [m]$ with $i \neq j$, we draw an arc from i to j with weight $a_i \cdot a_j$, if p_i has a 0 bit in a location where p_j has a 1 bit. It follows that for each pair $i, j \in [m]$ with $i \neq j$, we either have an arc from i to j or else we have an arc from j to i (or both). The total weight of the arcs in this graph is

$$\begin{aligned}
\sum_{i<j} a_i \cdot a_j \cdot (|p_i^{-1}(1) \cap p_j^{-1}(0)| + |p_i^{-1}(0) \cap p_j^{-1}(1)|) &\geq \sum_{i<j} a_i \cdot a_j \\
&= \frac{1}{2} \cdot (\sum_i a_i)^2 - \frac{1}{2} \cdot \sum_i a_i^2 \\
&\geq \frac{1}{2} \cdot (\sum_i a_i)^2 - \frac{1}{2} \cdot \sum_i a_i \quad (a_i \leq 1) \\
&\geq \frac{1}{2} \cdot (\mathrm{RC}(f)^2 - \mathrm{RC}(f))
\end{aligned}$$

Note that by symmetry, the LHS equals

$$\sum_i a_i \cdot \sum_{j \neq i} a_j \cdot |p_i^{-1}(0) \cap p_j^{-1}(1)|.$$

Since $\sum_i a_i = \mathrm{RC}(f)$, by averaging,

$$\exists i : \ \frac{1}{2}(\mathrm{RC}(f) - 1) \leq \sum_{j \neq i} a_j \cdot |p_i^{-1}(0) \cap p_j^{-1}(1)|. \tag{4}$$

Next, we get a lower bound on $|p_i^{-1}(0)|$ from Eq. (4).

$$\begin{aligned}
\frac{1}{2}(\mathrm{RC}(f)-1) &\le \sum_{j\neq i} a_j \cdot |p_i^{-1}(0)\cap p_j^{-1}(1)| \\
&= \sum_{k:p_i(k)=0} \sum_{j:p_j(k)=1} a_j \\
&\le \sum_{k:p_i(k)=0} \sum_{j:k\in B_j} a_j && (p_j \text{ is consistent with } \vec{0}^{B_j}) \\
&\le |p_i^{-1}(0)|. && (\textstyle\sum_{j:k\in B_j} a_j \le 1 \text{ for all } k)
\end{aligned}$$

We showed that p_i has at least $(\mathrm{RC}(f)-1)/2$ zero bits. It must also have at least one 1 bit. Thus $|p_i| \ge \mathrm{RC}(f)/2 + 1/2$, so $\mathrm{RC}(f) \le 2\,\mathrm{UC}_{\min}(f) - 1$. ◀

We note that the relationships in Lemma 20 and Theorem 8 are tight.[2] Let k be any non-negative integer, we construct a function f on $n = 2k+1$ variables with $\mathrm{s}(f) = \mathrm{bs}(f) = \mathrm{RC}(f) = n$ and $\mathrm{UC}_{\min}(f) \le k+1$. This shows that the inequalities $\mathrm{bs}(f) \le 2\,\mathrm{UC}_{\min}(f) - 1$ and $\mathrm{RC}(f) \le 2\,\mathrm{UC}_{\min}(f) - 1$ are both tight for all values of $\mathrm{UC}_{\min}(f)$. We define the function f by describing a set of partial assignments $p_0, \ldots, p_{n-1}$ such that $f(x) = 1$ if and only if $\exists i : p_i \subseteq x$. Let $p = 0^k 1 *^k$. The assignments $p_0, \ldots, p_{n-1}$ are all possible cyclic-shifts of p, namely for $0 \le i \le k$, $p_i = 0^{k-i} 1 *^k 0^i$ and for $k+1 \le i \le 2k$ we have $p_i = *^{2k+1-i} 0^k 1 *^{i-1-k}$. It is easy to verify that any two different partial assignments p_i and p_j are not consistent with one another. Hence, $p_0, \ldots, p_{n-1}$ is an unambiguous collection of 1-certificates for f, each of size $k+1$, exhibiting that $\mathrm{UC}_{\min}(f) \le k+1$. On the other hand, $f(0) = 0$ and for all $i \in [n]$, we have $f(e_i) = 1$, showing that f has sensitivity n on the all-zeros input. Overall, we showed that $\mathrm{s}(f) = \mathrm{bs}(f) = \mathrm{RC}(f) = n = 2k+1$ while $\mathrm{UC}_{\min}(f) \le k$.

Acknowledgements. We would like to thank Mika Göös and Robin Kothari for many helpful discussions and for comments on a preliminary draft. We also thank the anonymous referees of ITCS for their comments.

References

1. Scott Aaronson. Quantum certificate complexity. *Journal of Computer and System Sciences*, 74(3):313–322, 2008. Computational Complexity 2003. doi:10.1016/j.jcss.2007.06.020.
2. Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. *To appear in Proceedings of STOC 2016. arXiv preprint*, 2015. arXiv:1511.01937.
3. Andris Ambainis. Polynomial degree vs. quantum query complexity. *J. Comput. Syst. Sci.*, 72(2):220–238, 2006.
4. 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. doi:10.1007/978-3-662-43948-7_9.
5. Andris Ambainis, Martins Kokainis, and Robin Kothari. Nearly optimal separations between communication (or query) complexity and partitions. In *31st Conference on*

[2] We thank Mika Göös for helping to simplify this construction.

Computational Complexity (CCC 2016), volume 50 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:14, 2016. doi:10.4230/LIPIcs.CCC.2016.4.

6 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. doi:10.1007/978-3-662-44465-8_4.

7 Andris Ambainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs. Sensitivity versus certificate complexity of boolean functions. *arXiv preprint*, 2015. arXiv:1503.07691.

8 Andris Ambainis and Xiaoming Sun. New separation between s(f) and bs(f). *arXiv preprint*, 2011. arXiv:1108.3494.

9 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. doi:10.1007/978-3-319-17142-5_12.

10 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. doi:10.1145/502090.502097.

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

12 Shalev Ben-David and Robin Kothari. Randomized query complexity of sabotaged and composed functions. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 60:1–60:14, 2016.

13 Meena Boppana. Lattice variant of the sensitivity conjecture. *arXiv preprint*, 2012. arXiv:1207.1824.

14 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.

15 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.

16 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:10.1016/j.tcs.2016.05.006.

17 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.

18 Justin Gilmer, Michal Koucký, 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.

19 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. doi:10.1007/s00493-014-3189-x.

20 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.

21 Mika Göös, T.S. Jayram, Toniann Pitassi, and Thomas Watson. Randomized communication vs. partition number. *Electronic Colloquium on Computational Complexity (ECCC)* TR15-169, 2015.

22 Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles are nonnegative juntas. In *Symposium on Theory of Computing (STOC), 2015*, pages 257–266, 2015.

23 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.

24 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. doi:10.1145/2840728.2840738.

25 Parikshit Gopalan, Rocco Servedio, Avishay Tal, and Avi Wigderson. Degree and sensitivity: tails of two distributions. *arXiv preprint*, 2016. arXiv:1604.07432.

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

27 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. doi:10.4230/LIPIcs.APPROX-RANDOM.2015.915.

28 Raghav Kulkarni and Avishay Tal. On fractional block sensitivity. *Chicago J. Theor. Comput. Sci.*, 2016, 2016.

29 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. doi:10.1109/FOCS.2011.75.

30 Gatis Midrijanis. Exact quantum query complexity for total boolean functions. *arXiv preprint*, 2004. arXiv:quant-ph/0403168.

31 Noam Nisan. Crew prams and decision trees. *SIAM Journal on Computing*, 20(6):999–1007, 1991. doi:10.1137/0220062.

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

33 Ryan O'Donnell and Li-Yang Tan. A composition theorem for the fourier entropy-influence conjecture. In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*, pages 780–791, 2013.

34 Ryan O'Donnell, John Wright, Yu Zhao, Xiaorui Sun, and Li-Yang Tan. A composition theorem for parity kill number. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 144–154, 2014.

35 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. doi:10.1137/1.9781611973082.44.

36 Michael E. Saks and Avi Wigderson. Probabilistic boolean decision trees and the complexity of evaluating game trees. In *FOCS*, pages 29–38, 1986. doi:10.1109/SFCS.1986.44.

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

38 Alexander A. Sherstov. Making polynomials robust to noise. *Theory of Computing*, 9:593–615, 2013.

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

40 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.

41 Avishay Tal. On the sensitivity conjecture. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 38:1–38:13, 2016.

42 Ingo Wegener and Laszlo Zádori. A note on the relations between critical and sensitive complexity, 1988.
43 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.

A Lower Bound for Approximate Non-Negative Degree

Here we show that the lower bound in Theorem 8 holds even for one-sided average approximate non-negative degree, the smallest version of conical junta degree. This is saying that conical juntas, in all their forms, give a more powerful lower bound technique for randomized algorithms than $\mathrm{RC}(f)$.

▶ **Theorem 21.** *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

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

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

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

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

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

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 $\mathcal{M} := \{B \in \mathcal{B} : \forall B' \subset B, B' \notin \mathcal{B}\}$ 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 $\sum_{B\in\mathcal{M}} a_B = \mathrm{RC}_y(f)$ 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 $B \in \mathcal{B}$. Thus, 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.

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

where the second line follows because $a_{B_1} \leq 1$ 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

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

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

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

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 $p \not\subseteq y$ imply that the support of p is not disjoint from B_1. Finally, we get

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

as desired. ◀