Electronic Colloquium on Computational Complexity, Comment 1 on Report No. 168 (2013)

On Fractional Block Sensitivity

Raghav Kulkarni* Avishay Tal†

November 29, 2013

Abstract

In this paper we study the *fractional block sensitivity* of Boolean functions. Recently, Tal [Tal13] and Gilmer, Saks, and Srinivasan [GSS13] independently introduced this complexity measure, denoted by $\mathrm{fbs}(f)$, and showed that it is equal (up to a constant factor) to the *randomized certificate complexity*, denoted by $\mathrm{RC}(f)$, which was introduced by Aaronson [Aar03]. In this paper, we relate the fractional block sensitivity to other complexity measures such as sensitivity $s(f)$ and approximate degree $\widetilde{\deg}(f)$. As a consequence we obtain the following results:

1. We show that $\widetilde{\deg}(f) = \Omega(\sqrt{\mathrm{RC}(f)})$, solving an open question posed by Aaronson [Aar03]. This also implies that $\widetilde{\deg}(f) = \Omega(\mathrm{QC}(f))$, where $\mathrm{QC}(f)$ is the quantum certificate complexity of f. As both $\widetilde{\deg}(f)$ and $\mathrm{QC}(f)$ serve as lower bounds for the *bounded error quantum query complexity*, this shows that $\widetilde{\deg}(f)$ is always a tighter lower bound compared to $\mathrm{QC}(f)$.
2. (a) We show that every transitive function on n variables must have $\mathrm{RC}(f) = \Omega(n^{1/2})$, $\mathrm{QC}(f) = \Omega(n^{1/4})$ and $\widetilde{\deg}(f) = \Omega(n^{1/4})$, and note that all these bounds are tight. This is a strengthening of the previous lower bounds given by [SYZ04] and [Sun07].
   (b) We show that Chakraborty's [Cha11] example of a transitive function with $s(f) = O(n^{1/3})$ is optimal unless there is better than quadratic separation between the block sensitivity and the sensitivity.
3. Using fractional block sensitivity, we show that the *zero error randomized decision tree complexity*, $R_0(f)$, is upper bounded by $O(R_2(f)^2 \cdot \log R_2(f))$ where $R_2(f)$ is the *two-sided bounded error randomized decision tree complexity* of f. This improves the previous best relation between these two complexity measures given by Midrijanis [Mid05] of $R_0(f) = O(R_2(f)^2 \cdot \log n)$ (where n is the number of variables).
4. We show that the (non-negative weight) adversary methods to lower bound the *bounded error quantum query complexity* of f can not give better bounds than $\sqrt{\mathrm{RC}^0(f)\mathrm{RC}^1(f)}$. This refines the earlier bound of $\sqrt{\mathrm{C}^0(f)\mathrm{C}^1(f)}$ by Spalek and Szegedy [SS06] and strengthens the so called *certificate complexity barrier* to its randomized analogue.

*Centre for Quantum Technologies, Singapore Email: kulraghav@gmail.com

†The Weizmann Institute of Science, Rehovot, Israel. Email: avishay.tal@weizmann.ac.il. Research supported by an Adams Fellowship of the Israel Academy of Sciences and Humanities, by an Israel Science Foundation grant and by the Israeli Centers of Research Excellence (I-CORE) program.

ISSN 1433-8092

1 Introduction

The study of Boolean functions has become an integral part of theoretical computer science. Several complexity measures associated to Boolean functions have been extensively studied over decades. The one that is relevant to this paper is called the *decision tree complexity*. The decision tree model a.k.a. query model is perhaps the simplest model of computation. This model, perhaps due to its simplicity and fundamental nature, has been widely explored.

Fix a Boolean function $f : \{0,1\}^n \to \{0,1\}$. A deterministic decision tree D_f for f takes $x = (x_1, \ldots, x_n)$ as an input and determines the value of $f(x_1, \ldots, x_n)$ using queries of the form " is $x_i = 1$? ". Let $C(D_f, x)$ denote the cost of the computation, that is the number of queries made by D_f on input x. The *deterministic decision tree complexity* of f is defined as $D(f) = \min_{D_f} \max_x C(D_f, x)$. There are several complexity measures that are closely related to the decision tree complexity, for example: the *sensitivity, block sensitivity, and certificate complexity*. There are also randomized and quantum analogues of the decision tree complexity (see [BdW02] for an excellent survey on this subject). Although the exact relations between these measures are yet to be completely understood, all of them (with the notable exception of the sensitivity) are known to be polynomially related to each other. Whether or not the sensitivity is polynomially related to the decision tree complexity remains an outstanding open question [NS94].

The purpose of this paper is to study a relatively less studied complexity measure called *fractional block sensitivity*. This measure was recently introduced by Tal [Tal13] and Gilmer, Saks, and Srinivasan [GSS13] independently. Both showed that up to a constant factor, it is in fact equal to the so called *randomized certificate complexity* defined by Aaronson [Aar03]. In this paper we relate fractional block sensitivity to other complexity measures associated to the decision tree complexity such as sensitivity, block sensitivity, certificate complexity, approximate degree etc.

Fractional Block Sensitivity

To set notations for the rest of this paper, if M is some complexity measure (such as $s, \mathrm{bs}, \mathrm{fbs}, \mathrm{FC}, \mathrm{RC}, \mathrm{QC}, \mathrm{C}$) defined over a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and a point $x \in \{0,1\}^n$ on the Boolean hypercube, then we say that the complexity measure M of the function f, $M(f)$, is simply $\max_x M(f,x)$. We also denote $M^0(f) = \max_{x:f(x)=0} M(f,x)$ and $M^1(f)$ analogously.

A Boolean function f: $\{0,1\}^n \to \{0,1\}$ is said to be sensitive on the i^{th} bit of input $x = (x_1, \ldots, x_n)$ if $f(x_1, \ldots, x_{i-1}, 1 - x_i, x_{i+1}, \ldots, x_n) \neq f(x)$. The *sensitivity* of f on input x, denoted by $s(f,x)$ is the number of sensitive bits of f on x. $s(f), s^0(f), s^1(f)$ are defined as described above.

A block $B \subseteq \{1, 2, \ldots, n\}$ is said to be sensitive on an input x if $f(x \oplus B) \neq f(x)$, where $x \oplus B$ denotes the string obtained by flipping the values of all x_i such that $i \in B$. The *block sensitivity* of f on input x, denoted by $\mathrm{bs}(f,x)$, is the maximum number of pairwise disjoint blocks that are sensitive on x. One may express $\mathrm{bs}(f,x)$ as the optimum value of an integer program. For every potential block $B \subseteq \{1, 2, \ldots, n\}$ we have $y_B \in \{0,1\}$. The integer program is given as follows:

maximize $\sum_B y_B$	subject to: $(\forall i) \sum_{B:i \in B} y_B \leq 1$

The fractional block sensitivity of f on input x, denoted by $\mathrm{fbs}(f,x)$ is the optimum value of the relaxation of the above by allowing $0 \leq y_B \leq 1$. The fractional block sensitivity of f is now defined as: $\max_x \mathrm{fbs}(f,x)$. This relaxation exhibits some nice properties, such as being *submultiplicative under composition*, that the block sensitivity does not have [Tal13].

Related Work

We point out to two recent related works on fractional block sensitivity. Tal [Tal13] introduced the complexity measure and proved interesting composition properties. Independently, Gilmer, Saks and Srinivasan [GSS13] exhibited some limiting behavior of fractional block sensitivity and other complexity measures. In both works, it was noted that

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

where $\mathrm{C}(f), \mathrm{FC}(f)$ are the certificate complexity and the fractional certificate complexity of f, correspondingly. In fact, this holds locally for any input

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

As noted in both works, it turns out that this "new" complexity measure ($\mathrm{fbs}(f)$ or alternatively $\mathrm{FC}(f)$) is actually equal up to a constant to a previously known complexity measure defined by Aaronson [Aar03] called *randomized certificate complexity*, and denoted by $\mathrm{RC}(f)$. Aaronson studied this complexity measure and its quantum analogue, $\mathrm{QC}(f)$, establishing the tight relation $\mathrm{QC}(f) = \Theta(\sqrt{\mathrm{RC}(f)})$ for any Boolean function. $\mathrm{RC}(f)$ and $\mathrm{QC}(f)$ serve as lower bounds for the two-sided bounded error *randomized decision tree complexity* ($R_2(f)$) and *quantum query complexity* ($Q_2(f)$) correspondingly.

Both [Tal13, GSS13] considered composition of Boolean functions, where the composition of $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ is a function $f \circ g : \{0,1\}^{nm} \to \{0,1\}$ obtained by substituting each variable in f with a copy of g on a disjoint set of m variables. Both showed that taking a constant size function f and performing repeated compositions of f to itself, one gets a sequence of functions whose block sensitivity and fractional block sensitivity behaves the same asymptotically (see Claim 2.7 for a precise formulation). While this behavior seems to indicate that bs and fbs are the same up to a constant factor for any Boolean function, it turns out to be false as [GSS13] exhibit polynomial gaps between the two.[1] [2]

The fact that using composition alone can not separate between bs and fbs seems like a negative result, indicating this technique is just not strong enough to show certain results which can be proven using other methods. However, it turns out that this behavior can be turned into a positive result showing new relations between fractional block sensitivity and other complexity measures such as *degree* and *approximate degree*, as we exhibit in this work.

Our Results

1.1 $\mathrm{fbs}(f)$ vs $\widetilde{\deg}(f)$

Building upon the behavior of fbs and bs to composition and a recent result by Sherstov [She12] we show that the fractional block sensitivity can be at most quadratically larger than the approximate degree.

Theorem 1.1. *(restatement of Theorem 3.4)* $\mathrm{fbs}(f) = O(\widetilde{\deg}(f)^2)$.

[1] They also exhibit an optimal quadratic gap between fbs and C, which is in fact also an optimal gap between bs and C.

[2] In this work, we give a different example which exhibits a polynomial gap between block sensitivity and fractional block sensitivity.

This extends a result by Nisan and Szegedy [NS94] who showed $bs(f) = O(\widetilde{\deg}(f)^2)$. Since randomized certificate complexity is of the same order as the fractional block sensitivity, this solves an open problem posed by Aaronson [Aar03].

Corollary 1.2. $\widetilde{\deg}(f) = \Omega(\sqrt{\mathrm{RC}(f)})$.

By Aaronson's relation $\mathrm{QC}(f) = \Theta(\sqrt{\mathrm{RC}(f)})$ we get as an immediate corollary

Corollary 1.3. $\widetilde{\deg}(f) = \Omega(\mathrm{QC}(f))$.

Since both $\widetilde{\deg}(f)$ and $\mathrm{QC}(f)$ serve as lower bounds for $Q_2(f)$, this shows that $\widetilde{\deg}(f)$ is always a tighter lower bound compared to $\mathrm{QC}(f)$. Ambainis [Amb99] shows that almost all functions have $\widetilde{\deg}(f) = \Omega(n)$ whereas Aaronson [Aar03] shows that for all functions $\mathrm{QC}(f) = O(\sqrt{n})$. Hence, there are (many) functions where $\mathrm{QC}(f)$ is much smaller than $\widetilde{\deg}(f)$.

1.2 fbs of Transitive Functions

The effect of symmetry on the complexity of Boolean functions has been a recurrent theme in the literature. In particular, transitive functions such as graph properties and cyclically invariant functions have received considerable attention in the past (see for instance [SYZ04], [Cha11]; and further references there). In this paper we study: how small can the fractional block sensitivity of transitive functions be? We show the following:

Theorem 1.4. *(restatement of Theorem 4.4) Let $f : \{0,1\}^n \to \{0,1\}$ be a non constant transitive-function then* $\mathrm{fbs}(f) \geq \max\{s(f), n/s(f)\} \geq \sqrt{n}$.

The $\sqrt{n}$ lower bound on fbs is tight as demonstrated by the function $\vee_{i=1}^{\sqrt{n}} \wedge_{i=1}^{\sqrt{n}} x_{ij}$. Our theorem has the following two consequences worth mentioning:

$\widetilde{\deg}(f)$ of Transitive Functions

Corollary 1.5. *Let $f : \{0,1\}^n \to \{0,1\}$ be a non-constant transitive Boolean function then* $\mathrm{RC}(f) = \Omega(n^{1/2})$ *and* $\widetilde{\deg}(f) = \Omega(\mathrm{QC}(f)) = \Omega(n^{1/4})$.

This improves the previous known bound of $\Omega(n^{1/6})$ by Sun [Sun07]. Since approximate degree forms a lower bound on the quantum query complexity, this also gives a qualitative refinement of the $\Omega(n^{1/4})$ lower bound on the quantum query complexity of transitive functions obtained by Sun, Yao, and Zhang [SYZ04]. Moreover: this refinement is strict since there are transitive functions where approximate degree is much smaller than the quantum query complexity (see Section 5 in [Amb06]). Our $\Omega(n^{1/4})$ bound on approximate degree of transitive functions is tight as demonstrated by an example in [SYZ04] with $\widetilde{O}(n^{1/4})$ quantum query complexity. A related question that is open is what is the approximate degree of monotone transitive functions? It is believed that their quantum query complexity is $\Omega(n^{1/3})$ since their randomized query complexity is $\Omega(n^{2/3})$ and at most quadratic gap is expected between the two. Proving that $\widetilde{\deg}(f) = \Omega(n^{1/3})$ for monotone transitive functions will prove the desired lower bound on quantum query complexity. The lowest known bound for approximate degree of a monotone transitive function is $O(\sqrt{n})$, given by the OR function on n variables.

Sensitivity of Transitive Functions

The relation of sensitivity to other complexity measures [NS94] is a notorious problem, as is the problem of determining the minimal sensitivity achievable by transitive functions. Chakraborty [Cha11] gave an example of a transitive function with $s(f) = O(n^{1/3})$. The only lower bound known is $\Omega(\log n)$. No one has yet succeeded in finding a transitive function with sensitivity $o(n^{1/3})$. In this context, we hope that the following observation sheds some light.

Corollary 1.6. *Any transitive Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $s(f) = n^\alpha$ implies an $(1-\alpha)/\alpha$ exponent separating between* bs *and* s.

In particular if $\alpha < 1/3$ this will give a better than quadratic separation between block sensitivity and sensitivity. It is conjectured that block sensitivity and sensitivity are quadratically related. This suggests that Chakraborty's example might, in fact, be optimal!

1.3 $R_0(f)$ vs $R_2(f)$

In the randomized decision tree complexity there are at least three variants of randomized computation (as in other models): zero-error (a.k.a. Las Vegas), one sided error, and two-sided error (a.k.a. Monte Carlo), denoted by $R_0(f), R_1(f)$ and $R_2(f)$ respectively. By definition $R_2(f) \leq R_1(f) \leq R_0(f) \leq D(f)$. Nisan [Nis89] showed that $D(f) = O(R_2(f)^3)$ and $D(f) = O(R_1(f)^2)$. In [Mid05], Midrijanis established the relation to $R_0(f) = O(R_2(f)^2 \cdot \log(n))$. We follow this proof and improve its bound.

Recall that the block sensitivity of f on x is the maximal number of disjoint blocks $B \subseteq [n]$ such that $f(x) \neq f(x \oplus B)$. What if we got rid of the disjointness condition? denote by $\mathrm{nbs}(f)$ the number of flipping blocks (not necessarily disjoint) which are minimal with respect to set inclusion. Each such block, B, is of size at most $s(f)$, since f has sensitivity $\geq |B|$ on $x \oplus B$ when B is a minimal flipping block. So a first order estimate is $\mathrm{nbs}(f) \leq n^{s(f)}$. Midrijanis shows that $R_0(f) = O(R_2(f) \cdot \log \mathrm{nbs}(f))$, and then uses the above upper bound on $\mathrm{nbs}(f)$ to get the desired connection between $R_0(f)$ and $R_2(f)$. We refine the upper bound on $\mathrm{nbs}(f)$ to the tight estimate $\mathrm{nbs}(f) \leq \mathrm{fbs}(f)^{s(f)}$, which in turn yields the following result:

Theorem 1.7. *(restatement of Theorem 5.3)* $R_0(f) = O(R_2(f)^2 \cdot \log(R_2(f)))$

1.4 Tighter Limitations of Quantum Adversary

In [SS06], Spalek and Szegedy showed that seven seemingly different adversary methods, each giving lower bounds on the quantum query complexity, are in fact equivalent. One of the methods is the so called minimax method, denoted by $\mathrm{MM}(f)$. They show that this method can not give a lower bound better than $\sqrt{\mathrm{C}^0(f)\mathrm{C}^1(f)}$. We can refine their result by replacing the certificate complexity with the randomized certificate complexity.

Theorem 1.8. *(restatement of Theorem 6.4)* $\mathrm{MM}(f) \leq O\left(\sqrt{\mathrm{RC}^0(f)\mathrm{RC}^1(f)}\right)$

Since the randomized certificate complexity may be strictly smaller than certificate complexity, this gives a tighter limitation of the quantum adversary methods.

2 Preliminaries

Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. We say that a block $B \subseteq [n]$ is a *minimal flipping block* for $f : \{0,1\}^n \to \{0,1\}$ on $x \in \{0,1\}^n$ if $f(x \oplus B) \neq f(x)$, and for every proper subset of B, $A \subset B$ we have $f(x) = f(x \oplus A)$. In other words, B is a flipping block minimal to set inclusion.

2.1 Measures Equivalent to The Fractional Block Sensitivity

A 0-certificate for an input x such that $f(x) = 0$ is a partial assignment $S \to \{0,1\}$ for the subset S of variables, consistent with x, such that for any y that is consistent with the assignment $f(y) = 0$. Similarly one can define a 1-certificate. The minimum cardinality of such an S is the certificate complexity of f on x, denoted by $\mathrm{C}(f, x)$.

Next, we define a fractional version of the certificate complexity.

Definition 2.1 (Fractional Certificate)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and $W : [n] \to \mathbb{R}^+$ be a (non-negative) weight function on the coordinates. For any two points $x, y \in \{0,1\}^n$ we denote the W-weighted hamming distance between x and y as*

$$\mathrm{Dist}(W, x, y) = \sum_{i : x_i \neq y_i} W(i) \ .$$

W is a fractional certificate *for f on $x \in \{0,1\}^n$ if for any $y \in \{0,1\}^n$ such that $f(x) \neq f(y)$ we have $\mathrm{Dist}(W, x, y) \geq 1$. The fractional certificate complexity of f on x, denoted by $\mathrm{FC}(f, x)$,is the minimal $\sum_i W(i)$ of such W.*

It is easy to verify that this is indeed a relaxation of certificate complexity: given a certificate S for f on x we can assign weight 1 to each $i \in S$ and weight 0 otherwise. This yields a feasible fractional certificate for f on x, hence $\mathrm{FC}(f, x) \leq \mathrm{C}(f, x)$.

Aaronson [Aar03] defined a randomized version of the certificate complexity.

Definition 2.2 (Randomized Certificate)**.** *A randomized verifier for input x is a randomized algorithm that, on input y in the domain of f (i) accepts with probability 1 if $y = x$, and (ii) rejects with probability at least $1/2$ if $f(y) \neq f(x)$. The algorithm can behave arbitrarily on other case: $y \neq x$ but $f(y) = f(x)$. Then $\mathrm{RC}(f, x)$ is the minimum expected number of queries used by a randomized verifier for x. We can similarly define the quantum analogue $\mathrm{QC}(f, x)$ by allowing quantum algorithm instead of randomized.*

2.2 Some Useful Properties of fbs and Other Measures

Every Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be represented as a unique multilinear polynomial over $\mathbb{R}$. Let $\deg(f)$ denote the degree of this polynomial. Given an ϵ we denote by $\widetilde{\deg}_\epsilon(f)$ the minimal degree of a multilinear polynomial $g : \{0,1\}^n \to \mathbb{R}$ such that for all x, $|f(x) - g(x)| \leq \epsilon$. We denote $\widetilde{\deg}_{1/3}(f)$ by $\widetilde{\deg}(f)$.

Theorem 2.3 (bs vs. deg, [NS94], improved in [Tal13])**.** *Let f be a Boolean function, then*

1. $\mathrm{bs}(f) \leq \deg(f)^2$
2. $\mathrm{bs}(f) \leq 6 \cdot \widetilde{\deg}_{1/3}(f)^2$

We define the composition of two Boolean functions.

Definition 2.4 (Function Composition)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^m \to \{0,1\}$, then the function composition of f and g, $f \circ g : \{0,1\}^{nm} \to \{0,1\}$ is defined as follows:*

$$(f \circ g)\left(x_1^1, x_2^1, \ldots, x_m^n\right) \triangleq f\left(g\left(x_1^1, x_2^1, \ldots, x_m^1\right), \ldots, g\left(x_1^n, x_2^n \ldots, x_m^n\right)\right)$$

We define the repeated composition of a Boolean function to itself.

Definition 2.5 (Function Powering)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ and $k \in \mathbb{N}$, then the kth power of f denoted by f^k is defined recursively by $f^1 \triangleq f$ and $f^k \triangleq f \circ (f^{k-1})$ for $k > 1$.*

Lemma 2.6 (Function Composition Properties, [Tal13])**.** *Let $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^m \to \{0,1\}$ be Boolean functions, then the following hold:*

1. $\deg(f \circ g) = \deg(f) \cdot \deg(g)$
2. $s(f \circ g) \leq s(f) \cdot s(g)$
3. $\mathrm{fbs}(f \circ g) \leq \mathrm{fbs}(f) \cdot \mathrm{fbs}(g)$
4. *for $z \in \{0,1\}$, if $f(z^n) = g(z^m) = z$ then* $\mathrm{fbs}(f \circ g, z^{nm}) \geq \mathrm{fbs}(f, z^n) \cdot \mathrm{fbs}(g, z^m)$

Tal shows in [Tal13] (Gilmer et al. [GSS13] have a similar independent result) that taking a constant size Boolean function and composing it to itself many times yields a sequence of functions with constant ratio between bs and fbs.

Claim 2.7 (Constant Gap, [Tal13])**.** *Let $f : \{0,1\}^n \to \{0,1\}$ then for any integer $\ell \in \mathbb{N}$ the ratio $\mathrm{fbs}(f^\ell)/\mathrm{bs}(f^\ell)$ is at most $c(n) = 25 \cdot n^2 \cdot 2^n$ i.e. independent of ℓ.*

3 Approximate Degree and Fractional Block Sensitivity

In this section we show that approximate degree can be at most quadratically smaller than the fractional block sensitivity.

Lemma 3.1. *Let M be any measure such that $\forall f, g : M(f \circ g) \leq M(f) \cdot M(g)$. Then any bound of the form $\forall f : \mathrm{bs}(f) \leq M(f)^\alpha$ for some constant $\alpha > 0$ implies the same bound on* fbs*, namely $\forall f : \mathrm{fbs}(f) \leq M(f)^\alpha$.*

Proof. Assume by contradiction that there exists an $f : \{0,1\}^n \to \{0,1\}$ such that $\mathrm{fbs}(f) \geq M(f)^\alpha + 1$. Let $\epsilon = 1/M(f)^\alpha$, then $\epsilon > 0$ and we have $\mathrm{fbs}(f) \geq M(f)^\alpha \cdot (1+\epsilon)$ Without loss of generality suppose that $\mathrm{fbs}(f) = \max_x \mathrm{fbs}(f, x)$ is realized at 0^n and $f(0^n) = 0$. By repeatedly applying Lemma 2.6 we have $\mathrm{fbs}(f^\ell) \geq \mathrm{fbs}(f)^\ell$. Overall, we get

$$\begin{aligned}
\mathrm{bs}(f^\ell) &\geq \frac{1}{c(n)} \cdot \mathrm{fbs}(f^\ell) && \text{(Claim 2.7)} \\
&\geq \frac{1}{c(n)} \cdot \mathrm{fbs}(f)^\ell && (\mathrm{fbs}(f^\ell) \geq \mathrm{fbs}(f)^\ell) \\
&\geq \frac{1}{c(n)} \cdot (M(f)^\alpha \cdot (1+\epsilon))^\ell && \text{(contradiction assumption)} \\
&= \frac{1}{c(n)} \cdot \left(M(f)^\ell\right)^\alpha \cdot (1+\epsilon)^\ell \\
&\geq \frac{1}{c(n)} \cdot M(f^\ell)^\alpha \cdot (1+\epsilon)^\ell . && \text{(assumption on } M)
\end{aligned}$$

Choosing a large enough ℓ, one can guarantee $\frac{1}{c(n)} \cdot (1+\epsilon)^\ell > 2$ and this is a contradiction. □

Corollary 3.2. *1.* $\forall f : \mathrm{fbs}(f) \leq \deg(f)^2$

2. If there exists a constant $\alpha > 0$ *such that* $\forall f : \mathrm{bs}(f) \leq s(f)^\alpha$ *then* $\forall f : \mathrm{fbs}(f) \leq s(f)^\alpha$

Proof. By Lemma 2.6 both deg and s fulfill the requirements in Lemma 3.1, so 2 follows immediately. As for 1, by Theorem 2.3 we have $\forall f : \mathrm{bs}(f) \leq \deg(f)^2$ hence $\forall f : \mathrm{fbs}(f) \leq \deg(f)^2$. □

In order to prove a similar bound on fbs with approximate degree, we need to understand the behaviour of approximate degree with respect to composition. The following theorem by Sherstov is useful in this context (recall that we are denoting $\widetilde{\deg}_{1/3}(f)$ by $\widetilde{\deg}(f)$.).

Theorem 3.3 ([She12])**.** $\widetilde{\deg}(f \circ g) = \Theta(\widetilde{\deg}(f) \cdot \widetilde{\deg}(g))$.

Theorem 3.4. *There is a universal constant* c *such that for any Boolean function* $\mathrm{fbs}(f) \leq c \cdot \widetilde{\deg}(f)^2$.

Proof. Let c_1 be a universal constant such that for any Boolean functions f, g we have $\widetilde{\deg}(f \circ g) \leq c_1 \cdot \widetilde{\deg}(f) \cdot \widetilde{\deg}(g)$ and $\mathrm{bs}(f) \leq \left(c_1 \cdot \widetilde{\deg}(f)\right)^2$. The existence of c_1 is guaranteed by Theorems 3.3 and 2.3. Define $M(f) \triangleq c_1 \cdot \widetilde{\deg}(f)$. Then M is a complexity measure for which $\mathrm{bs}(f) \leq M(f)^2$ and $M(f \circ g) \leq M(f) \cdot M(g)$ since

$$M(f \circ g) = c_1 \cdot \widetilde{\deg}(f \circ g) \leq c_1 \cdot c_1 \cdot \widetilde{\deg}(f) \cdot \widetilde{\deg}(g) = M(f) \cdot M(g) \ .$$

Applying Lemma 3.1 we get that

$$\forall f : \mathrm{fbs}(f) \leq M(f)^2 = (c_1)^2 \cdot \widetilde{\deg}(f)^2 \ ,$$

which completes the proof. □

We note that Theorem 3.4 is tight up to the constant factor as the OR_n function gives $\mathrm{fbs}(\mathrm{OR}_n) = n$ and $\widetilde{\deg}(\mathrm{OR}_n) = \Theta(\sqrt{n})$. See [NS94] for a proof.

4 Transitive Boolean Functions

Definition 4.1. *Let* $f : \{0,1\}^n \to \{0,1\}$ *be a Boolean function and* $\sigma \in S_n$ *a permutation, we say that* f *is invariant under* σ *if* $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ *for all* $x \in \{0,1\}^n$.

An easy observation is that the permutations under which f is invariant form a subgroup of S_n. We say a subgroup $\Gamma \subseteq S_n$ is transitive if $\forall i, j \in [n]$, $\exists \sigma \in \Gamma : \sigma(i) = j$. We say a function f is *transitively-invariant* or *transitive* if the invariant permutations of f are a transitive subgroup of S_n. We say that f is *cyclically invariant* or *cyclic* if f is invariant under the left cyclic shift permutation $(2, 3, \ldots, n, 1)$. In particular, any cyclic function is transitive.

We state a useful property of such subgroups:

Lemma 4.2 ([RV76])**.** *If* $\Gamma \subseteq S_n$ *is a transitive subgroup, then for any* $S \subseteq [n]$ *and any* $i \in [n]$ *we have*

$$|S| \cdot |\{\sigma(S) \ : \ \sigma \in \Gamma\}| = n \cdot |\{\sigma(S) \ : \ \sigma \in \Gamma, i \in \sigma(S)\}|$$

where $\sigma(S) = \{\sigma(x) : x \in S\}$.

Claim 4.3. *Let $f : \{0,1\}^n \to \{0,1\}$ be any non constant transitive-function; then* $\mathrm{fbs}(f, 0^n) \geq n/s(f)$.

Proof. Let B be a minimal block flipping the value of f at 0^n, i.e., any proper subset of B does not flip the value of f at 0^n. The cardinality of B is at most $s(f)$, since otherwise we have more than $s(f)$ sensitive coordinates on the input $\mathbf{1}_B$. Take the blocks $\mathcal{B} = \{\sigma(B) \ : \sigma \in \Gamma\}$ (there might be less than $|\Gamma|$ such blocks as this is a set), and assign each such block a weight of $w \triangleq \frac{n}{|B|\cdot|\mathcal{B}|}$. Then, by Lemma 4.2 the number of blocks containing a coordinate $i \in [n]$ is exactly $|B| \cdot |\mathcal{B}|/n$. Hence, the total weight of blocks containing i is exactly 1. The total weight is $|\mathcal{B}| \cdot w = n/|B| \geq n/s(f)$ and this is a lower bound for the fractional block sensitivity at 0^n. □

This immediately yields the following:

Theorem 4.4. *Let $f : \{0,1\}^n \to \{0,1\}$ be any non constant transitive-function; then* $\mathrm{fbs}(f) \geq \sqrt{n}$.

Proof. $\mathrm{fbs}(f) \geq \max\{s(f), n/s(f)\} \geq \sqrt{n}$. □

Corollary 4.5. *There is a family of cyclically invariant Boolean functions such that*

$$\mathrm{fbs}(f) = \Omega(\mathrm{bs}(f)^{4/3}).$$

Proof. In [Sun07] Sun gives a probabilistic construction of a family of cyclically invariant functions (which is in particular a family of transitive functions) for which $\mathrm{bs}(f) = O(n^{3/7} \cdot \log(n))$. In [Dru11], Drucker improved this construction to give a family of cyclically invariant f's for which $\mathrm{bs}(f) = O(n^{3/7} \cdot \log(n)^{1/7})$. In [Ama11], Amano improved this construction to give a family of cyclically invariant f's for which $\mathrm{bs}(f) = O(n^{3/7})$. Thus, using claim 4.3, we get that $\mathrm{fbs}(f) \geq n/s(f) \geq n/\mathrm{bs}(f) \geq \Omega(n^{4/7})$. This gives a separation between bs and fbs as $\mathrm{fbs}(f) \geq \Omega(\mathrm{bs}(f)^{4/3})$. □

Corollary 4.6. *Any transitive Boolean function $f : \{0,1\}^n \to \{0,1\}$ with $s(f) = n^\alpha$ implies an $(1-\alpha)/\alpha$ exponent separating between* bs *and* s. *In particular if $\alpha < 1/3$ this will give a better than quadratic separation between block sensitivity and sensitivity.*

Proof. By Claim 4.3, $\mathrm{fbs}(f) \geq n/s(f) = n^{1-\alpha}$ and by Corollary 3.2, this gives a $(1-\alpha)/\alpha$ exponent separating bs and s. □

One can get a slightly more general result: the existence of a transitive function f for which $s^0(f) \cdot s^1(f) \cdot s(f) = o(n)$ implies a quadratic separation between block sensitivity and sensitivity. This is true since given such a function f, one can construct a transitive function $g : \{0,1\}^m \to \{0,1\}$ with $s(g) = o(m^{1/3})$ by composing $\mathrm{OR}_{s^1(f)/s^0(f)} \circ f$ in the case where $s^1(f) \geq s^0(f)$, or $\mathrm{AND}_{s^0(f)/s^1(f)} \circ f$ if $s^0(f) \geq s^1(f)$. The existence of such a function g implies the mentioned separation by Corollary 4.6.

5 The Number of Minimal Flipping Blocks

Consider a Boolean function $f : \{0,1\}^n \to \{0,1\}$ and a point $x \in \{0,1\}^n$. Recall that $\mathrm{nbs}(f,x)$ counts the number of flipping blocks for f on x which are minimal with respect to set inclusion. Given a parameter k, we will count how many minimal blocks of size k flip the value of f on x, and denote this number by $\mathrm{nbs}_k(f,x)$. Clearly $\mathrm{nbs}_1(f,x) = s(f,x)$ and $\mathrm{nbs}_k(f,x) \leq \binom{n}{k}$ by definition. In addition, $\mathrm{nbs}(f,x) = \sum_{i=1}^{s(f)} \mathrm{nbs}_k(f,x)$ by the fact that a minimal flipping block can be of size at most $s(f)$. We give the following estimate on nbs_k which is independent of n.

Claim 5.1. $\mathrm{nbs}_k(f,x) \le \mathrm{fbs}(f,x) \cdot \mathrm{nbs}_{k-1}(f)$

Proof. Let $N := \mathrm{nbs}_k(f,x)$ be the number of minimal flipping blocks $B \subseteq [n]$ of size k. For any such block B and any $i \in B$ the block $B - \{i\}$ is a minimal flipping block of size $k-1$ for $x \oplus \{i\}$. Note that for a fixed $i \in [n]$, if i is contained in $B_1, B_2, \dots B_t$ then all blocks $B_1 - \{i\}, \dots, B_t - \{i\}$ are different minimal flipping blocks for f on $x \oplus \{i\}$, each of size $k-1$. By definition their number is at most $\mathrm{nbs}_{k-1}(f, x \oplus \{i\}) \le \mathrm{nbs}_{k-1}(f)$. Thus, putting weight $1/\mathrm{nbs}_{k-1}(f)$ for all blocks $B \subseteq [n]$ of size k gives a feasible solution to the fractional block sensitivity linear program of f on x. The value of this solution is $\frac{N}{\mathrm{nbs}_{k-1}(f)}$, hence

$$\mathrm{fbs}(f,x) \ge \frac{N}{\mathrm{nbs}_{k-1}(f)} \; . \qquad \square$$

Corollary 5.2. $\mathrm{nbs}_k(f,x) \le \prod_{i=1}^{k} \mathrm{fbs}(f) \le \mathrm{fbs}(f)^k$

We note that this bound is *tight* since taking the function $f = \wedge_{i=1}^{k} \vee_{i=1}^{k} x_{ij}$, we have $\mathrm{fbs}(f) = s(f) = k$, while $\mathrm{nbs}_k(f,0) = k^k$.

Midrijanis showed that for any Boolean function $f : \{0,1\}^n \to \{0,1\}$ it holds that $R_0(f) = O(R_2(f) \cdot \log \mathrm{nbs}(f))$ deriving the upper bound $R_0(f) = O(R_2(f)^2 \cdot \log n)$. We improve this bound by the improved bound on $\mathrm{nbs}_k(f)$.

Theorem 5.3. $R_0(f) = O(R_2(f)^2 \cdot \log(R_2(f)))$

Proof. Assume without loss of generality that $\mathrm{fbs}(f) \ge 2$ as any function with $\mathrm{fbs}(f) < 2$ depends only on at most one variable, and the statement of the theorem is true for such functions. Corollary 5.2 implies

$$\mathrm{nbs}(f) = \sum_{k=1}^{s(f)} \mathrm{nbs}_k(f) \le \sum_{k=1}^{s(f)} \mathrm{fbs}(f)^k \le 2 \cdot \mathrm{fbs}(f)^{s(f)} \; .$$

Using Midrijanis' relation $R_0(f) = O(R_2(f) \cdot \log \mathrm{nbs}(f))$ gives $R_0(f) = O(R_2(f) \cdot s(f) \cdot \log(\mathrm{fbs}(f)))$. Since $s(f) \le \mathrm{fbs}(f) = O(R_2(f))$ we get

$$R_0(f) = O(R_2(f)^2 \cdot \log(R_2(f))) \; . \qquad \square$$

6 Tighter Limitations of Quantum Adversary Method

The next lemma by Blum and Impagliazzo states that every 0-certificate and 1-certificate intersect. This lemma is crucial for the proof that $\mathrm{D}(f) \le \mathrm{C}^0(f) \cdot \mathrm{C}^1(f)$.

Lemma 6.1 ([BI87])**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, $x, y \in \{0,1\}^n$ points on the Boolean hypercube such that $f(x) = 0$ and $f(y) = 1$. Let $S, T \subseteq [n]$ be certificates for x, y respectively, then there is a coordinate $i \in S \cap T$ such that $x_i \ne y_i$.*

The following lemma is a generalization of Lemma 6.1 to the case of fractional certificates.

Lemma 6.2 (Relaxed intersection of fractional certificates)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, $x, y \in \{0,1\}^n$ points on the Boolean hypercube such that $f(x) = 0$ and $f(y) = 1$. Let $W_x, W_y : [n] \to \mathbb{R}^+$ be fractional certificates for f on x and y respectively, then*

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

Proof. Let $z \in \{0,1\}^n$ be the point defined by

$$z_i = \begin{cases} y_i & \text{if } W_x(i) < W_y(i) \\ x_i & \text{otherwise,} \end{cases}$$

for $i \in [n]$. Then the W_x hamming distance between x and z is

$$\mathrm{Dist}(W_x, x, z) = \sum_{i:W_x(i)<W_y(i) \text{ and } x_i \neq y_i} W_x(i)$$

and this is at most $\sum_{i:x_i \neq y_i} \min\{W_x(i), W_y(i)\}$. Similarly,

$$\mathrm{Dist}(W_y, y, z) \leq \sum_{i:x_i \neq y_i} \min\{W_x(i), W_y(i)\} \,.$$

By the definition of fractional certificate, one of $\mathrm{Dist}(W_x, x, z)$, $\mathrm{Dist}(W_y, y, z)$ must be at least 1, hence $\sum_{i:x_i \neq y_i} \min\{W_x(i), W_y(i)\} \geq 1$. □

6.1 The Quantum Adversary Bound and Fractional Certificate Complexity

In this section we show that the following measure which lower bounds the quantum query complexity is limited by the fractional certificate complexity.

Definition 6.3 (Minimax over probability distributions)**.** *Let $S \subseteq \{0,1\}^n$, and let $f : S \to \{0,1\}$ be a partial function. Let $p : S \times [n] \to \mathbb{R}$ denote a set of probability distributions, that is $p_x(i) \geq 0$ and $\sum_i p_x(i) = 1$ for every $x \in S$. Then*

$$\mathrm{MM}(f) = \min_p \max_{x,y:f(x)\neq f(y)} \frac{1}{\sum_{i:x_i \neq y_i} \sqrt{p_x(i) p_y(i)}}$$

We adapt the proof of Spalek and Szegedy that $\mathrm{MM}(f) \leq \sqrt{\mathrm{C}^0(f)\mathrm{C}^1(f)}$ for total functions ([SS06], Theorem 3.2) to show that $\mathrm{MM}(f) \leq \sqrt{\mathrm{FC}^0(f)\mathrm{FC}^1(f)}$, using Lemma 6.2. We also include an improved bound for partial functions.

Theorem 6.4. *Let $S \subseteq \{0,1\}^n$ and let $f : S \to \{0,1\}$ be a non constant function.*

1. *If $S = \{0,1\}^n$, then $\mathrm{MM}(f) \leq \sqrt{\mathrm{FC}^0(f)\mathrm{FC}^1(f)}$.*
2. *If $S \subset \{0,1\}^n$, and $\mathrm{FC}^0(f) \geq \mathrm{FC}^1(f)$ then $\mathrm{MM}(f) \leq 2\sqrt{n\mathrm{FC}^1(f)}$.*

Proof. We begin with the case of total functions, i.e. $S = \{0,1\}^n$. For any $x \in \{0,1\}^n$, fix some arbitrary minimal certificate W_x for f on x, and distribute the probability $p_x(i)$ proportional to the weights given by W_x. Namely,

$$p_x(i) = \frac{W_x(i)}{|W_x|} \,, \tag{1}$$

for $i \in [n]$ where $|W_x| = \sum_i W_x(i)$. Since MM is the minimum over all probability distributions,

$$\mathrm{MM}(f) \leq \max_{x,y:f(x)\neq f(y)} \frac{1}{\sum_{i:x_i\neq y_i} \sqrt{p_x(i)p_y(i)}} \tag{2}$$

Plugging (1) into (2) gives

$$\begin{aligned}
\mathrm{MM}(f) &\leq \max_{x,y:f(x)\neq f(y)} \frac{\sqrt{|W_x||W_y|}}{\sum_{i:x_i\neq y_i} \sqrt{W_x(i)W_y(i)}} \\
&\leq \max_{x,y:f(x)\neq f(y)} \frac{\sqrt{|W_x||W_y|}}{\sum_{i:x_i\neq y_i} \min\{W_x(i), W_y(i)\}} && (\min\{a,b\} \leq \sqrt{ab} \text{ for } a,b \geq 0) \\
&\leq \max_{x,y:f(x)\neq f(y)} \frac{\sqrt{\mathrm{FC}^0(f)\mathrm{FC}^1(f)}}{\sum_{i:x_i\neq y_i} \min\{W_x(i), W_y(i)\}} && (\text{optimality of } W_x, W_y) \\
&\leq \sqrt{\mathrm{FC}^0(f)\mathrm{FC}^1(f)} && (\text{Lemma 6.2})
\end{aligned}$$

which completes the proof of the first part of the theorem.

Now we deal with partial functions.[3] For any $x \in \{0,1\}^n$, fix some arbitrary minimal certificate W_x for f on x, and put

$$q_x(i) = \frac{1}{2n} + \frac{1}{2} \cdot \frac{W_x(i)}{|W_x|} \,,$$

for $i \in [n]$ where $|W_x| = \sum_i W_x(i)$. This is the average between the uniform distribution and p_x from Equation 1. Since MM is the minimum over all probability distributions,

$$\mathrm{MM}(f) \leq \max_{x,y:f(x)\neq f(y)} \frac{1}{\sum_{i:x_i\neq y_i} \sqrt{q_x(i)q_y(i)}} \tag{3}$$

Take any x and y such that $f(x) = 1$ and $f(y) = 0$, then

$$\begin{aligned}
\sum_{i:x_i\neq y_i} \sqrt{q_x(i)q_y(i)} &\geq \sum_{i:x_i\neq y_i} \sqrt{\frac{W_x(i)}{2|W_x|} \cdot \frac{1}{2n}} && (\text{by definition of } q) \\
&\geq \sqrt{\sum_{i:x_i\neq y_i} \frac{W_x(i)}{2|W_x|} \cdot \frac{1}{2n}} && (\textstyle\sum_i \sqrt{a_i} \geq \sqrt{\sum_i a_i}) \\
&\geq \sqrt{\frac{1}{2|W_x|} \cdot \frac{1}{2n}} && (\text{by definition of FC}) \\
&\geq \sqrt{\frac{1}{4\mathrm{FC}^1(f) \cdot n}} \,.
\end{aligned}$$

Plugging this into Equation (3) completes the proof. □

[3] Note that Lemma 6.2 does not hold for partial functions as we needed f to be defined on z.

7 Open Ends

The relation of fractional block sensitivity with certificate complexity was tightly understood by Gilmer et al. [GSS13]. In this paper the relation of fractional block sensitivity with approximate degree (and with degree) was tightly understood. However, tightly relating fractional block sensitivity to other complexity measures remains open. We highlight some of these questions.

Relation to randomized decision tree complexity Aaronson posed in [Aar03] the question of whether or not $R(f) \leq \mathrm{RC}^0(f) \cdot \mathrm{RC}^1(f)$, where $R(f)$ is the randomized decision tree complexity. Trying to adapt Blum and Impagliazzo's argument from [BI87] to the randomized case seems promising since we generalized Lemma 6.1 (which was crucial for Blum and Impagliazzo's proof) to the randomized analogue. However, our attempts to do so have failed so far.

Relation to block sensitivity The relation of fractional block sensitivity with block sensitivity was partially understood in [GSS13]. They gave a family of functions where $\mathrm{fbs}(f) = \Theta\left(\mathrm{bs}(f)^{3/2}\right)$ which complements the known relation $\mathrm{fbs}(f) \leq \mathrm{C}(f) \leq \mathrm{bs}(f)^2$ for any Boolean function. Determining the right exponent in the range $[3/2, 2]$ remains open.

Relation to sensitivity Lemma 3.1 shows that for any constant α it holds that $\forall f : \mathrm{bs}(f) \leq s(f)^\alpha$ iff $\forall f : \mathrm{fbs}(f) \leq s(f)^\alpha$. Thus, understanding the relation between block sensitivity and sensitivity is essentially the same as understanding the relation between fractional block sensitivity and sensitivity.

8 Acknowledgments

We thank Scott Aaronson and Andrew Drucker for helpful discussions.

References

[Aar03] S. Aaronson. Quantum certificate complexity. In *IEEE Conference on Computational Complexity*, pages 171–178, 2003.

[Ama11] K. Amano. Minterm-transitive functions with asymptotically smallest block sensitivity. *Inf. Process. Lett.*, 111(23-24):1081–1084, 2011.

[Amb99] A. Ambainis. A note on quantum black-box complexity of almost all boolean functions. *Inf. Process. Lett.*, 71(1):5–7, 1999.

[Amb06] A. Ambainis. Polynomial degree vs. quantum query complexity. *J. Comput. Syst. Sci.*, 72(2):220–238, 2006.

[BdW02] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey. *Theor. Comput. Sci.*, 288(1):21–43, 2002.

[BI87] M. Blum and R. Impagliazzo. Generic oracles and oracle classes (extended abstract). In *FOCS*, pages 118–126, 1987.

[Cha11] S. Chakraborty. On the sensitivity of cyclically-invariant boolean functions. *Discrete Mathematics & Theoretical Computer Science*, 13(4):51–60, 2011.

[Dru11] A. Drucker. Block sensitivity of minterm-transitive functions. *Theor. Comput. Sci.*, 412(41):5796–5801, 2011.

[GSS13] J. Gilmer, M. Saks, and S. Srinivasan. Composition limits and separating examples for some boolean function complexity measures. In *IEEE Conference on Computational Complexity*, 2013.

[Mid05] G. Midrijanis. On randomized and quantum query complexities. *arXiv preprint quant-ph/0501142*, 2005.

[Nis89] N. Nisan. Crew prams and decision trees. In *STOC*, pages 327–335, 1989.

[NS94] N. Nisan and M. Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4:301–313, 1994.

[RV76] R. L. Rivest and J. Vuillemin. On recognizing graph properties from adjacency matrices. *Theor. Comput. Sci.*, 3(3):371–384, 1976.

[She12] A. A. Sherstov. Making polynomials robust to noise. In H. J. Karloff and T. Pitassi, editors, *STOC*, pages 747–758. ACM, 2012.

[SS06] R. Spalek and M. Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2(1):1–18, 2006.

[Sun07] X. Sun. Block sensitivity of weakly symmetric functions. *Theor. Comput. Sci.*, 384(1):87–91, 2007.

[SYZ04] X. Sun, A. C. Yao, and S. Zhang. Graph properties and circular functions: How low can quantum query complexity go? In *IEEE Conference on Computational Complexity*, pages 286–293, 2004.

[Tal13] A. Tal. Properties and applications of boolean function composition. In R. D. Kleinberg, editor, *ITCS*, pages 441–454. ACM, 2013.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de