# Tight Bounds on Sensitivity and Block Sensitivity of Some Classes of Transitive Functions * 

Siddhesh Chaubal ${ }^{\dagger} \quad$ Anna Gál ${ }^{\ddagger}$


#### Abstract

Nisan and Szegedy [18] conjectured that block sensitivity is at most polynomial in sensitivity for any Boolean function. Until a recent breakthrough of Huang [15], the conjecture had been wide open in the general case, and was proved only for a few special classes of Boolean functions. Huang's result [15] implies that block sensitivity is at most the 4th power of sensitivity for any Boolean function. It remains open if a tighter relationship between sensitivity and block sensitivity holds for arbitrary Boolean functions; the largest known gap between these measures is quadratic [20, 23, $9,12,4,10]$.

We prove tighter bounds showing that block sensitivity is at most 3rd power, and in some cases at most square of sensitivity for subclasses of transitive functions, defined by various properties of their DNF (or CNF) representation. Our results improve and extend previous results regarding transitive functions. We obtain these results by proving tight (up to constant factors) lower bounds on the smallest possible sensitivity of functions in these classes.

In another line of research, it has also been examined what is the smallest possible block sensitivity of transitive functions. Our results yield tight (up to constant factors) lower bounds on the block sensitivity of the classes we consider.


## 1 Introduction

The sensitivity $s(f)$ of a Boolean function $f$ is the maximum over all inputs $x$ of the number of coordinate positions $i$ such that changing the value of the $i$-th bit of $x$ changes the value of the function. The block sensitivity $b s(f)$ of a Boolean function $f$ is the maximum over all inputs $x$ of the number of disjoint blocks of positions such that changing the value of all bits of $x$ in any given block changes the value of the function. (See Section 2 for more formal definitions.) Nisan and Szegedy [18] conjectured that block sensitivity is at most polynomial in sensitivity for any Boolean function. A number of important complexity measures (such as

[^0]CREW PRAM complexity, certificate complexity, decision tree depth in various models and degree) are polynomially related to block sensitivity, and therefore to each other. See [8, 13] for a survey. Until a recent breakthrough by Huang [15], the best upper bounds on any of these measures were exponential in terms of sensitivity. The previous best upper bounds on block sensitivity in terms of sensitivity were by Ambainis et al. [3] giving $b s(f) \leq s(f) 2^{s(f)-1}$, and by He et al. [14] who gave a constant factor improvement to this bound. Huang [15] proved that the degree of a Boolean function $f$ is at most $s(f)^{2}$. This was further improved to show that the degree is at most the product of the 0 -sensitivity and 1 -sensitivity in $[17,1]$. Huang's result [15] implies that $b s(f) \leq s(f)^{4}$ for any Boolean function $f$. The best separation between sensitivity and block sensitivity remains quadratic [20, 23, 9, 12, 4, 10].

Despite a lot of attention to the problem, until Huang's result, the conjecture was verified only for a few special classes of Boolean functions, including some special classes of transitive functions, such as symmetric functions, graph properties and minterm-transitive functions. The following questions have been raised in connection to sensitivity and block sensitivity of transitive functions.

1. An intriguing aspect of transitive functions is that no examples of transitive functions are known on $n$ input bits with $o\left(n^{1 / 3}\right)$ sensitivity. Chakraborty [9] constructed a transitive function on $n$ variables with sensitivity $\Theta\left(n^{1 / 3}\right)$. It is implicit in a paper by Sun [22] that for a transitive function $f$ on $n$ variables, $b s(f) \cdot s(f)^{2} \geq n$. Together with Huang's result this gives that any transitive function $f$ on $n$ variables has $s(f) \geq \Omega\left(n^{1 / 6}\right)$. Previously, Chakraborty [9] proved that every minterm-transitive function $f$ on $n$ variables has $s(f) \geq \Omega\left(n^{1 / 3}\right)$. It remains open if the sensitivity of every transitive function is at least $\Omega\left(n^{1 / 3}\right)$.
2. Another intriguing question is that considering transitive functions with $f\left(0^{n}\right) \neq f\left(1^{n}\right)$, we don't even have any examples with $o\left(n^{1 / 2}\right)$ sensitivity. A remark in the survey [13] in combination with Huang's result [15] implies that any transitive function $f$ on $n$ variables where $n$ is a prime power and $f\left(0^{n}\right) \neq f\left(1^{n}\right)$ has sensitivity $s(f) \geq \Omega(\sqrt{n})$. However, this does not seem to directly imply a similar consequence for transitive functions with $f\left(0^{n}\right) \neq f\left(1^{n}\right)$ when $n$ is not a prime power, because for a transitive function, a subfunction obtained by fixing a subset of its bits is no longer necessarily transitive.
3. While it is still open if every transitive function has sensitivity $\Omega\left(n^{1 / 3}\right)$, Sun [22] proved that every transitive function has block sensitivity at least $n^{1 / 3}$. This resulted in further studies of what is the smallest possible block sensitivity of transitive functions. Drucker [11] showed that minterm-transitive functions must have block sensitivity at least $\Omega\left(n^{3 / 7}\right)$. This bound is tight for the class of minterm-transitive functions: Amano [2] constructed minterm-transitive functions with block sensitivity $O\left(n^{3 / 7}\right)$, improving constructions of Sun [22] and Drucker [11] by logarithmic factors. It remains open if transitive functions with block sensitivity o( $\left.n^{3 / 7}\right)$ exist.

### 1.1 Our Results

In this paper we settle the above questions for some special classes of transitive functions, significantly extending previous results about subclasses of transitive functions. For the classes we consider, we show that for functions $f$ on $n$ variables $s(f) \geq \Omega\left(n^{1 / 3}\right)$ which
implies $b s(f) \leq O\left(s(f)^{3}\right)$. In addition, we prove that the block sensitivity of functions on $n$ variables in all the classes we consider is at least $\Omega\left(n^{3 / 7}\right)$. Furthermore, under the additional assumption that $f\left(0^{n}\right) \neq f\left(1^{n}\right)$, we show that $s(f) \geq \Omega(\sqrt{n})$ for transitive functions $f$ represented by DNF (or CNF) such that the number of positive literals per term is the same up to constant factors. Previously this was not known to hold for arbitrary values of $n$, even for the special case of minterm-transitive functions.

Our lower bounds on both sensitivity and block sensitivity are tight up to constant factors for the corresponding classes.

We consider the following three subclasses of transitive functions.
Transitive Functions with Sparse DNF (or CNF) We consider transitive functions that can be represented by DNFs with up to $2^{n^{\frac{1}{2}-\epsilon}}$ terms, or by CNFs with up to $2^{n^{\frac{1}{2}-\epsilon}}$ clauses, for constant $\epsilon>0$. For any non-constant function $f$ of this form we prove that $s(f) \geq \Omega\left(\min \left\{n^{1 / 3}, n^{2 \epsilon}\right\}\right)$. In particular, setting $\epsilon=1 / 6$ gives the bound $s(f) \geq \Omega\left(n^{1 / 3}\right)$ for transitive functions represented by DNFs (or CNFs) of size up to $2^{n^{1 / 3}}$.

Comparing with previous results, we note that any DNF with at most $t$ terms is also a read- $t$ DNF. Thus, the results of [7] imply that non-constant functions represented by DNFs with at most $n^{\frac{1}{3}-\epsilon}$ terms have sensitivity $\Omega\left(n^{\epsilon}\right)$. Our results significantly improve this to DNFs with up to an exponential $2^{n^{\frac{1}{2}-\epsilon}}$ number of terms, in the case of transitive functions.

Transitive Functions Represented by DNF (or CNF) with a Not-Too-Frequent Variable We further extend these results to transitive functions represented by DNFs (or CNFs) of arbitrary sizes, as long as there exists a variable that appears at most $2^{n^{\frac{1}{2}-\epsilon}}$ times, for constant $\epsilon>0$. As above, setting $\epsilon=1 / 6$ gives $s(f) \geq \Omega\left(n^{1 / 3}\right)$.

Transitive Functions Represented by DNF (or CNF) with Approximately the Same Number of Positive Literals per Term

Next we consider transitive functions represented by DNF (or CNF) where the number of terms as well as the size of the terms (i.e. the width of the DNF) are arbitrary, but the number of positive literals in each term is the same up to constant factors. We prove for transitive functions $f$ on $n$ variables with this property that $s(f) \geq \Omega\left(n^{1 / 3}\right)$.

This class significantly extends the previously studied class of minterm-transitive functions. Roughly speaking, minterm-transitive functions have the property that all their 1 inputs are consistent with minterms that are equivalent to just one minterm, under permutations from the invariance group of the function. Chakraborty [9] proved that mintermtransitive functions $f$ on $n$ variables have $s(f) \geq \Omega\left(n^{1 / 3}\right)$, and he noted that his argument extends to the case when the number of positive literals as well as the sizes of each term are the same up to constant factors. Our contribution is to further extend the argument without making any assumptions about the sizes of the terms.

Tightness of Our Bounds As noted above, Chakraborty [9] gave an example of a transitive function on $n$ variables with sensitivity $\Theta\left(n^{1 / 3}\right)$, and Amano [2] gave an example of a transitive function on $n$ variables with block sensitivity $\Theta\left(n^{3 / 7}\right)$. Both functions are minterm-transitive, thus they can be represented by DNFs where each term has the same number of positive literals. On the other hand, both functions can be represented by DNFs with $n$ terms, thus they also belong to the other two classes of transitive functions that we
consider. This shows that our bounds $s(f) \geq \Omega\left(n^{1 / 3}\right)$ and $b s(f) \geq \Omega\left(n^{3 / 7}\right)$ are the best possible for these classes, up to constant factors.

We give a simple example of a minterm-transitive function $f$ on $n$ variables, with sensitivity $\Theta(\sqrt{n})$ such that $f\left(0^{n}\right) \neq f\left(1^{n}\right)$. This shows that our $\Omega(\sqrt{n})$ lower bound on sensitivity is tight up to constant factors for the corresponding class.

### 1.2 Our Techniques

First, we note that our arguments are independent of Huang's proof [15]. Instead, our results are based on new upper bounds on the minimum certificate size, that hold for arbitrary Boolean functions, not just transitive functions. We give two such bounds: one upper bounds the minimum certificate size by the sensitivity of the function and by the logarithm of the number of terms of the DNF (Lemma 5), the other relates the minimum certificate size to the number of occurrences of any given variable and the influence of that variable (Lemma 6). We note that relating the minimum certificate size to influence has been also used in [6] in a different context. These upper bounds allow us to take advantage of a result of Chakraborty [9] (see Corollary 1) which shows that for transitive functions, upper bounds on the minimum certificate size imply lower bounds on the sensitivity of the function.

We emphasize that our upper bounds on minimum certificate size hold for arbitrary Boolean functions, not just transitive functions. The part of our arguments that is specific to transitive functions, is using the fact that for transitive functions, upper bounds on minimum certificate size imply lower bounds on sensitivity, and the relationship between the influences of different variables of transitive functions.

We also provide a new, stronger tradeoff between sensitivity and the certificate size on two special inputs, $\left(0^{n}\right.$ and $\left.1^{n}\right)$, that holds for arbitrary transitive functions (Lemma 8). This allows us to obtain tight, $\Omega(\sqrt{n})$ lower bounds on the sensitivity of functions $f$ on $n$ variables in our third class, when $f\left(0^{n}\right) \neq f\left(1^{n}\right)$.

Finally, we observe that upper bounds on the minimum certificate size also provide lower bounds on block sensitivity of arbitrary transitive functions, (Lemma 11), with a stronger tradeoff than what follows from tradeoffs between sensitivity and minimum certificate size. This allows us to obtain tight, $\Omega\left(n^{3 / 7}\right)$ lower bounds on the block sensitivity of functions in all the classes we consider.

## 2 Preliminaries

Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a Boolean function. For $x \in\{0,1\}^{n}$ and $i \in[n]$ we denote by $x^{i}$ the input obtained by flipping the $i$-th bit of $x$. More generally, for $S \subseteq[n]$ we denote by $x^{S}$ the input obtained by flipping the bits of $x$ in all coordinates in the subset $S$.

Definition 1. Sensitivity The sensitivity $s(f, x)$ of a Boolean function $f$ on input $x$ is the number of coordinates $i \in[n]$ such that $f(x) \neq f\left(x^{i}\right)$. The 0 -sensitivity and 1-sensitivity of $f$ are defined as $s_{0}(f)=\max \{s(f, x): f(x)=0\}$ and $s_{1}(f)=\max \{s(f, x): f(x)=$
$1\}$, respectively. The sensitivity of $f$ is defined as $s(f)=\max \left\{s(f, x): x \in\{0,1\}^{n}\right\}=$ $\max \left\{s_{0}(f), s_{1}(f)\right\}$.
Definition 2. Block Sensitivity The block sensitivity bs $(f, x)$ of a Boolean function $f$ on input $x$ is the maximum number of pairwise disjoint subsets $S_{1}, \ldots, S_{k}$ of $[n]$ such that for each $i \in[k] f(x) \neq f\left(x^{S_{i}}\right)$. The 0 -block sensitivity and 1-block sensitivity of $f$ are defined as $b s_{0}(f)=\max \{b s(f, x): f(x)=0\}$ and $b s_{1}(f)=\max \{b s(f, x): f(x)=1\}$, respectively. The block sensitivity of $f$ is defined as $b s(f)=\max \left\{b s(f, x): x \in\{0,1\}^{n}\right\}=$ $\max \left\{b s_{0}(f), b s_{1}(f)\right\}$.

It is convenient to refer to coordinates $i \in[n]$ such that $f(x) \neq f\left(x^{i}\right)$ as sensitive bits for $f$ on $x$. Similarly, a subset $S \subseteq[n]$ is called a sensitive block for $f$ on $x$ if $f(x) \neq f\left(x^{S}\right)$.
Definition 3. Partial assignment Given an integer $n>0$, a partial assignment $\alpha$ is a function $\alpha:[n] \rightarrow\{0,1, \star\}$. A partial assignment $\alpha$ corresponds naturally to a setting of $n$ variables $\left(x_{1}, x_{2}, \ldots, x_{n}\right)$ to $\{0,1, \star\}$ where $x_{i}$ is set to $\alpha(i)$. The variables set to $\star$ are called unassigned or free, and we say that the variables set to 0 or 1 are fixed. We say that $x \in\{0,1\}^{n}$ agrees with $\alpha$ if $x_{i}=\alpha(i)$ for all $i$ such that $\alpha(i) \neq \star$. The size of a partial assignment $\alpha$ is defined as the number of fixed variables of $\alpha$.
Definition 4. Certificate For a function $f:\{0,1\}^{n} \rightarrow\{0,1\}$ and input $x \in\{0,1\}^{n}$ a partial assignment $\alpha$ is a certificate of $f$ on $x$ if $x$ agrees with $\alpha$ and any input $y$ agreeing with $\alpha$ satisfies $f(y)=f(x)$. A certificate $\alpha$ is a 1-certificate (resp. 0-certificate) if $f(x)=1$ (resp. $f(x)=0$ ), on inputs $x$ that agree with $\alpha$.
Definition 5. Minterms and Maxterms A certificate $\alpha$ is called minimal, if after changing any of its fixed variables to a free variable, the resulting partial assignment $\alpha^{\prime}$ is not a certificate, that is the function is not constant on inputs agreeing with $\alpha^{\prime}$. A minimal 1 -certificate is called a minterm, and a minimal 0 -certificate is called a maxterm.

Definition 6. Size and Weight of Certificates The size of a certificate $\alpha$, denoted by size $(\alpha)$ is defined as the size of the partial assignment $\alpha$. The weight of a certificate $\alpha$, denoted by wt $(\alpha)$, is the number of bits fixed to 1 by $\alpha$.
Definition 7. Certificate Complexity The certificate complexity $C(f, x)$ of a Boolean function $f$ on input $x$ is the size of the smallest certificate of $f$ on $x$. The 0 -certificate complexity and 1-certificate complexity of $f$ are defined as $C_{0}(f)=\max \{C(f, x): f(x)=0\}$ and $C_{1}(f)=\max \{C(f, x): f(x)=1\}$, respectively. The certificate complexity of $f$ is defined as $C(f)=\max \left\{C(f, x): x \in\{0,1\}^{n}\right\}=\max \left\{C_{0}(f), C_{1}(f)\right\}$.

It is also useful to consider the following definition of the smallest certificate size over all inputs. Note that this can be rephrased as the co-dimension of the largest subcube of the Boolean cube $\{0,1\}^{n}$ where $f$ is constant.

Definition 8. Minimum Certificate Size The minimum certificate size of a Boolean function $f:\{0,1\}^{n} \rightarrow\{0,1\}$ is defined as $C_{\min }(f)=\min \left\{C(f, x): x \in\{0,1\}^{n}\right\}$.

We will use the following lemma of Simon [21].
Lemma 1. [21](see also [5]) Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant Boolean function. Then $\left|f^{-1}(1)\right| \geq 2^{n-s_{1}(f)}$ and $\left|f^{-1}(0)\right| \geq 2^{n-s_{0}(f)}$.

### 2.1 Transitive Functions

Definition 9. Invariance Group $A$ Boolean function $f:\{0,1\}^{n} \rightarrow\{0,1\}$ is invariant under a permutation $\sigma:[n] \rightarrow[n]$, if for any $x \in\{0,1\}^{n}, f\left(x_{1}, \ldots, x_{n}\right)=f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)$. The set of all permutations under which $f$ is invariant forms a group, called the invariance group of $f$.

Definition 10. Transitive Function A Boolean function is transitive if its invariance group $\Gamma$ is transitive, that is, for each $i, j \in[n]$, there is a $\sigma \in \Gamma$ such that $\sigma(i)=j$.

For example, the set of all permutations on $n$ bits, denoted by $S_{n}$ is a transitive group of permutations. Another example of a transitive group of permutations is the set of all cyclic shifts on $n$ bits, denoted by $\operatorname{Shift}_{n}=\left\{\xi_{0}, \xi_{1}, \ldots, \xi_{n-1}\right\}$, where the permutation $\xi_{j}$ cyclically shifts the string by $j$ positions.

We need the following notation. For a partial assignment $\alpha:[n] \rightarrow\{0,1, *\}$ and a permutation $\sigma$ on $n$ bits we denote by $\sigma(\alpha)$ the partial assignment obtained by applying the partial assignment $\alpha$ to the bits permuted according to $\sigma$, that is $\sigma(\alpha)(\ell)=\alpha\left(\sigma^{-1}(\ell)\right)$ for $\ell \in[n]$.

Definition 11. Minterm-Transitive Function Let $\Gamma$ be a transitive group of permutations. A function $f:\{0,1\}^{n} \rightarrow\{0,1\}$ is minterm-transitive under $\Gamma$ if there exists a minterm $\alpha$ of $f$ such that $f(x)=1$ if and only if $x$ agrees with $\sigma(\alpha)$ for some $\sigma \in \Gamma$.
$A$ function is called minterm-transitive if it is minterm-transitive under some transitive group of permutations.

We will use the following observations of Chakraborty about transitive functions. Recall that $S_{n}$ denotes the group of all permutations on $n$ bits.

We use the following notation: for a set $S \subseteq[n]$ and a permutation $\sigma \in S_{n}$ we denote by $\sigma(S)$ the set $\{\sigma(i) \mid i \in S\}$.

Lemma 2 (4.3 in [9]). Let $\Gamma \subseteq S_{n}$ be a transitive group of permutations on $n$ bits. Then, for any $\emptyset \neq S \subseteq[n]$ with $|S|=k$, there exists $\hat{\Gamma} \subseteq \Gamma$ with $|\hat{\Gamma}| \geq \frac{n}{k^{2}}$ such that for any two permutations $\sigma_{1}, \sigma_{2} \in \hat{\Gamma}$ their images on $S$ are disjoint, that is $\sigma_{1}(S) \cap \sigma_{2}(S)=\emptyset$.

Lemma 3 (4.4 in [9]). Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function. Let $\alpha$ be a 1-certificate (resp. 0-certificate) for some $x \in\{0,1\}^{n}$, with size $(\alpha)=k>0$. Then, $s_{0}(f) \geq \frac{n}{k^{2}}\left(\right.$ resp. $\left.s_{1}(f) \geq \frac{n}{k^{2}}\right)$.

Since this lemma is crucial for our arguments, we include its proof.
Proof. [9] Let $\Gamma$ be the invariance group of $f$. Let $S$ be the set of bits fixed by $\alpha$, and let $\hat{\Gamma} \subseteq \Gamma$ with $|\hat{\Gamma}|=t \geq \frac{n}{k^{2}}$ be the set of permutations guaranteed by Lemma 2. For $\sigma_{i} \in \hat{\Gamma}$ let $\alpha_{i}:[n] \rightarrow\{0,1, *\}$ denote the partial assignment $\sigma_{i}(\alpha)$ obtained by applying the partial assignment $\alpha$ to the bits permuted according to $\sigma_{i}$, that is $\alpha_{i}(\ell)=\alpha\left(\sigma_{i}(\ell)\right)$ for $\ell \in[n]$. Then, for $1 \leq i \neq j \leq t$, we have that the set of bits fixed by $\alpha_{i}$ is disjoint from the set of bits fixed by $\alpha_{j}$.

Assume that $\alpha$ is a 1 -certificate for $f$ (the proof for a 0 -certificate is analogous). In this case note that for each $i \in[t], \alpha_{i}$ is a 1-certificate of $f$, since each $\sigma_{i}$ belongs to the invariance group of $f$.

Now, consider any 0 -input $z \in f^{-1}(0)$. $z$ must disagree with each 1 -certificate $\alpha_{i}$ in at least one bit. Let $T$ be the set of all bits $j$ such that $z$ disagrees in the bit $j$ with some certificate $\alpha_{i}$ for $i \in[t]$.

Now, let $P \subset T$ be a maximal subset of $T$ such that $f\left(z^{P}\right)=0$. Since $P$ is maximal, if we flip any other bit in $T \backslash P$, the value of the function will change to 1 . Therefore, $s_{0}(f) \geq|T \backslash P|$. Also, $z^{P}$ must still disagree with each 1-certificate $\alpha_{i}$ for $i \in[t]$, since $f\left(z^{P}\right)=0$. Therefore, $|T \backslash P| \geq t \geq \frac{n}{k^{2}}$, and we have $s_{0}(f) \geq \frac{n}{k^{2}}$.

Corollary 1. For a non-constant transitive function $f:\{0,1\}^{n} \rightarrow\{0,1\}$ we have:

$$
s(f)\left(C_{\min }(f)\right)^{2} \geq n
$$

We will also use the following observation of Sun [22].
Lemma 4. [22] Let $\Gamma \subseteq S_{n}$ be a transitive group of permutations on $n$ bits. For any $x, y \in\{0,1\}^{n}$, if $w t(x) \cdot w t(y)<n$, then there exists some $\sigma \in \Gamma$, such that $\sigma(x)$ and $y$ do not have any 1-s in the same position.

## 3 Lower Bounds on Sensitivity of Transitive Functions

### 3.1 Sparse DNF (or CNF)

In this section we prove lower bounds on the sensitivity of transitive functions that can be represented by DNFs with up to $2^{n^{\frac{1}{2}-\epsilon}}$ terms, or by CNFs with up to $2^{n^{\frac{1}{2}-\epsilon}}$ clauses, for constant $\epsilon>0$.

We start with a lemma that holds for any Boolean function, transitivity is not required.
Lemma 5. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant Boolean function. If $f$ can be represented by a DNF with $t$ terms, then $C_{\min }(f) \leq s_{1}(f)+\log t$, and if $f$ can be represented by a CNF with $t$ clauses, then $C_{\min }(f) \leq s_{0}(f)+\log t$.

Proof. We prove the statement about DNFs, the proof for CNFs is analogous. Let $f$ : $\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant Boolean function that can be represented by a DNF with $t$ terms. Notice that for each term of the DNF, we get a 1-certificate by fixing the variables that appear in the given term, to a value so that the term is satisfied, and leaving the remaining variables free. This means that the number of variables that participate in any given term must be at least $C_{\min }(f)$. Thus, the number of different inputs that satisfy a given term is at most $2^{n-C_{\min }(f)}$. This means that $\left|f^{-1}(1)\right| \leq t 2^{n-C_{\min }(f)}$. On the other hand, by Simon's Lemma (see Lemma 1 in Section 2) $\left|f^{-1}(1)\right| \geq 2^{n-s_{1}(f)}$. Combining these two inequalities implies the statement of the lemma.

We obtain the following theorem.
Theorem 1. Let $\epsilon>0$ and let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function that can be represented by a DNF with up to $2^{n^{\frac{1}{2}-\epsilon}}$ terms, or by a CNF with up to $2^{n^{\frac{1}{2}-\epsilon}}$ clauses. Then $s(f) \geq \Omega\left(\min \left\{n^{1 / 3}, n^{2 \epsilon}\right\}\right)$.

Proof. We prove the statement about DNFs, the proof for CNFs is analogous.
First note that it is enough to prove the statement for $0<\epsilon \leq 1 / 6$, since this will imply that $s(f) \geq \Omega\left(n^{1 / 3}\right)$ whenever $\epsilon \geq 1 / 6$.

Next, notice that if $s_{1}(f) \geq n^{\frac{1}{2}-\epsilon}$, and $\epsilon \leq 1 / 6$, then the statement obviously holds. Assume that $s_{1}(f)<n^{\frac{1}{2}-\epsilon}$. Then, by Lemma $5 C_{\min }(f) \leq 2 n^{\frac{1}{2}-\epsilon}$, and Corollary 1 implies that $s(f) \geq \Omega\left(n^{2 \epsilon}\right)$.

Remark 1. Setting $\epsilon=1 / 6$ gives $s(f) \geq \Omega\left(n^{1 / 3}\right)$ for transitive functions represented by DNFs (or CNFs) of size up to $2^{n^{1 / 3}}$.

### 3.2 DNF (or CNF) with a Not-Too-Frequent Variable

In this section we further extend the results of the previous section. We show that the same lower bounds for sensitivity hold for transitive functions represented by DNFs with an arbitrary number of terms, as long as there exists a variable that appears in no more than $2^{n^{\frac{1}{2}-\epsilon}}$ terms, for constant $\epsilon>0$. An analogous result holds considering CNFs.

We once again start with an observation that holds for arbitrary Boolean functions, not just transitive functions.

For a Boolean function $f:\{0,1\}^{n} \rightarrow\{0,1\}$, the influence of the $i$-th variable, denoted by $\operatorname{In} f_{i}(f)$ is defined as: $\operatorname{In} f_{i}(f)=\operatorname{Pr}_{x}\left[f(x) \neq f\left(x^{i}\right)\right]$ where the probability is taken over the uniform distribution on $\{0,1\}^{n}$.

Lemma 6. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a Boolean function that can be represented by a DNF (or CNF) such that its $i$-th variable appears in at most $k$ terms (resp. clauses) of the formula, for some $i \in[n]$. Then we have: $C_{\min }(f) \leq \log k+1-\log \operatorname{Inf} f_{i}(f)$

Proof. We prove the statement about DNFs, the proof for CNFs is analogous.
As we noted in the proof of Lemma 5, for each term of the DNF, we get a 1-certificate by fixing the variables that appear in the given term, to a value so that the term is satisfied, and leaving the remaining variables free. This means that the number of variables that participate in any given term must be at least $C_{\min }(f)$. Thus, the number of different inputs that satisfy a given term is at most $2^{n-C_{m i n}(f)}$.

Consider only those $k$ terms that include the variable $x_{i}$. The number of inputs satisfying at least one of these terms is at most $k 2^{n-C_{\min }(f)}$. Also, notice that each of the 1-inputs that are sensitive to the $i$-th bit must satisfy one of the terms that include the variable $x_{i}$. (Each 1-input must satisfy at least one term, and an input that is sensitive to $x_{i}$ cannot satisfy a term that does not depend on $x_{i}$.) Therefore, the number of 1-inputs that are sensitive to the $i$-th bit is at most $k 2^{n-C_{\min }(f)}$. On the other hand, the number of 1 -inputs that are
sensitive to the $i$-th bit equals $\operatorname{In} f_{i}(f) \cdot 2^{n-1}$. Thus, we get $\operatorname{In} f_{i}(f) \cdot 2^{n-1} \leq k 2^{n-C_{\min }(f)}$, and this gives the statement of the lemma.

We are ready to prove the following theorem for transitive functions.
Theorem 2. Let $\epsilon>0$ and let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function that can be represented by a DNF (or CNF) such that one of its variables appears in at most $2^{n^{\frac{1}{2}-\epsilon}}$ terms (resp. clauses) of the formula. Then $s(f) \geq \Omega\left(\min \left\{n^{1 / 3}, n^{2 \epsilon}\right\}\right)$.

Proof. We prove the statement about DNFs, the proof for CNFs is analogous. As before, it is enough to prove the statement for $0<\epsilon \leq 1 / 6$, since this will imply that $s(f) \geq \Omega\left(n^{1 / 3}\right)$ whenever $\epsilon \geq 1 / 6$.

Let $x_{i}$ be a variable that appears in at most $k=2^{n^{\frac{1}{2}-\epsilon}}$ terms of the DNF. It is known (see e.g. [19]) that for transitive $f, \operatorname{In} f_{i}(f)=\operatorname{In} f_{j}(f)$ for any $j \in[n]$, and thus $\operatorname{In} f_{i}(f)=$ $\max _{j \in[n]} \operatorname{In} f_{j}(f)$. By a theorem of Kahn, Kalai and Linial [16], $\max _{j \in[n]} I n f_{j}(f) \geq \Omega(p(1-$ $p) \log n / n)$, where $p$ is the probability that the function $f$ equals 1 . Then, by Lemma 6 we get $C_{\text {min }}(f) \leq \log k+1-\log \operatorname{In} f_{i}(f) \leq O\left(\log k+1+\log n+\log \frac{1}{p(1-p)}\right)$.

Notice that $\frac{1}{p(1-p)} \geq 2^{n^{\frac{1}{2}-\epsilon}}$ implies that $\min \left\{\left|f^{-1}(1)\right|,\left|f^{-1}(0)\right|\right\} \leq 2^{n+1-n^{\frac{1}{2}-\epsilon}}$. Then by Lemma $1, s(f) \geq \Omega\left(n^{\frac{1}{2}-\epsilon}\right)$, which is at least $\Omega\left(n^{2 \epsilon}\right)$ when $\epsilon \leq 1 / 6$.

Otherwise, $\frac{1}{p(1-p)}<2^{n^{\frac{1}{2}-\epsilon}}$, and we get $C_{\min }(f) \leq O\left(n^{\frac{1}{2}-\epsilon}\right)$. Then, Corollary 1 implies that $s(f) \geq \Omega\left(n^{2 \epsilon}\right)$.

Remark 2. Setting $\epsilon=1 / 6$ gives $s(f) \geq \Omega\left(n^{1 / 3}\right)$ for transitive functions represented by DNFs (or CNFs) such that one of the variables appears no more than $2^{n^{1 / 3}}$ times.

### 3.3 DNF (or CNF) with Approximately the Same Number of Positive Literals per Term

In this section we consider transitive functions represented by DNFs where the number of terms as well as the size of the terms (i.e. the width of the DNF) are arbitrary, but the number of positive literals in each term is approximately the same. In other words, we consider transitive functions $f$ such that the 1-inputs of $f$ can be covered by subcubes that correspond to minterms with approximately equal weights.

Note that minterm-transitive functions have this property, since all their minterms have exactly the same weight. However, a minterm-transitive function $f$ must have a single minterm $\alpha$ such that every 1 -input of $f$ agrees with either $\alpha$ or $\sigma(\alpha)$ for some $\sigma$ in the invariance group of $f$. Our condition allows $f$ to have a set $\Lambda=\left\{\alpha_{1}, \alpha_{2}, \ldots\right\}$ of an arbitrary number of different minterms, as long as they have approximately the same weight, and every 1-input of $f$ agrees with some $\alpha_{i} \in \Lambda$.

Note also that we allow the different minterms in $\Lambda$ to have different sizes, we only require that they have approximately equal weight. That is, we require that they each set approximately the same number of bits to 1 but they can set different numbers of bits to 0 .

Remark 3. Our arguments would also work if we require the number of bits fixed to 0 to be approximately the same in each minterm. Analogous results hold for maxterms and CNFs as well.

First we prove a simple lemma that holds for arbitrary Boolean functions, not just for transitive functions.

Lemma 7. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant Boolean function. Let $\Lambda=\left\{\alpha_{1}, \alpha_{2}, \ldots\right\}$ be a set of minterms of $f$ such that every 1 -input of $f$ agrees with some $\alpha_{i} \in \Lambda$. Let $\lambda_{1}$ denote the smallest number of 1-s fixed by any $\alpha_{i} \in \Lambda$, and let $\lambda_{0}$ denote the smallest number of 0-s fixed by any $\alpha_{i} \in \Lambda$. Then, $s_{1}(f) \geq \max \left\{\lambda_{1}, \lambda_{0}\right\}$.

Proof. First note that although $f$ may have minterms that are not included in the set $\Lambda$, every minterm of $f$ must fix at least $\lambda_{1}$ bits to 1 , and at least $\lambda_{0}$ bits to 0 . This follows because every 1-input of $f$ must agree with some minterm from $\Lambda$. This also means that every 1-input $x \in\{0,1\}^{n}$ must have at least $\lambda_{1}$ of its bits equal to 1 and at least $\lambda_{0}$ of its bits equal to 0 . Let $\beta_{1} \in \Lambda$ be the minterm that fixes exactly $\lambda_{1}$ bits to 1 . Let $y \in\{0,1\}^{n}$ be the input that agrees with $\beta_{1}$ on the bits fixed by $\beta_{1}$, and is 0 on every free bit of $\beta_{1}$. Then, $f(y)=1$, but changing any 1 bit of $y$ we obtain a 0 -input of $f$. Thus, $s(f, y) \geq \lambda_{1}$. Similarly, let $\beta_{0} \in \Lambda$ be the minterm that fixes exactly $\lambda_{0}$ bits to 0 . Let $z \in\{0,1\}^{n}$ be the input that agrees with $\beta_{0}$ on the bits fixed by $\beta_{0}$, and is 1 on every free bit of $\beta_{0}$. Then, $f(z)=1$, but changing any 0 bit of $z$, we obtain a 0 -input of $f$. Thus, $s(f, z) \geq \lambda_{0}$. This implies the statement.

Note that the number of minterms in the set $\Lambda$ can be arbitrarily large. An analogous statement considering sets of maxterms covering the 0 -inputs of $f$ gives a lower bound on $s_{0}(f)$.

We obtain the following theorem.
Theorem 3. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function. Assume that there is a set $\Lambda=\left\{\alpha_{1}, \alpha_{2}, \ldots\right\}$ of minterms of $f$ such that every 1 -input of $f$ agrees with some $\alpha_{i} \in \Lambda$. Let $w$ be the weight of the smallest weight minterm in $\Lambda$, and assume that for some constant $c$, $w t\left(\alpha_{i}\right) \leq c \cdot w$ for all $\alpha_{i} \in \Lambda$. Then $s(f)=\Omega\left(n^{1 / 3}\right)$.

Proof. Let $\alpha \in \Lambda$ be a minterm of $f$ that fixes the smallest number of bits to 0 among the minterms in $\Lambda$. Note that if size $(\alpha) \leq n^{1 / 3}$ then by Corollary 1, we have: $s(f) \geq \frac{n}{n^{2 / 3}} \geq n^{1 / 3}$. Thus, we can assume that $\operatorname{size}(\alpha)>n^{1 / 3}$.

Let $u$ denote the number of bits fixed to 0 by $\alpha$. We consider two cases.
Case 1. $u \geq \frac{\operatorname{size}(\alpha)}{2}$. Then, by Lemma $7, s_{1}(f) \geq u \geq \frac{\operatorname{size}(\alpha)}{2}>\frac{n^{1 / 3}}{2}$ and we are done.
Case 2. $u<\frac{\operatorname{size}(\alpha)}{2}$, and thus $w t(\alpha) \geq \frac{\operatorname{size}(\alpha)}{2}$. Then we have $n^{1 / 3}<\operatorname{size}(\alpha) \leq 2 \cdot w t(\alpha) \leq$ $2 c w$. By Lemma 7 this gives $s(f)=\Omega\left(n^{1 / 3}\right)$.

## A Stronger Tradeoff between Certificate Size and Sensitivity

Our bounds in the previous sections are based on using the tradeoff between minimum certificate size and sensitivity proved by Chakraborty (see Corollary 1). Next we observe that considering the certificate size of a transitive function on either the all 0 or all 1 string, one can obtain a stronger tradeoff between certificate size and sensitivity. More precisely, we prove the following lemma.

Lemma 8. For a non-constant transitive function $f:\{0,1\}^{n} \rightarrow\{0,1\}$,

$$
C\left(f, 0^{n}\right) \cdot s(f) \geq n \quad \text { and } \quad C\left(f, 1^{n}\right) \cdot s(f) \geq n
$$

Proof. We prove the first statement, the proof of the second statement is analogous. Let $B$ be a minimal block such that $f\left(0^{n}\right) \neq f\left(\left(0^{n}\right)^{B}\right)$. Since $B$ is minimal, $s(f) \geq|B|$.

Let $\alpha$ be a certificate of $f$ on the all zero input $0^{n}$. If size $(\alpha) \cdot|B|<n$, then, we apply Lemma 4 to the characteristic vectors of the set of bits that $\alpha$ fixes and the set $B$. This gives that there is a $\sigma \in \Gamma$ where $\Gamma$ is the invariance group of $f$, such that $\sigma(\alpha)$ and $B$ do not have any indices in common. But this gives a contradiction, since every certificate of $f$ on $0^{n}$ must intersect $B$. Thus, size $(\alpha) \cdot|B| \geq n$, which implies the statement.

Lower Bound on Sensitivity when $f\left(0^{n}\right) \neq f\left(1^{n}\right)$
We use Lemma 8 to obtain stronger lower bounds on the sensitivity of transitive functions with approximately equal weight minterms in their DNF representation, under the additional condition that $f\left(0^{n}\right) \neq f\left(1^{n}\right)$.

Theorem 4. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function, such that $f\left(0^{n}\right) \neq f\left(1^{n}\right)$. Assume that there is a set $\Lambda=\left\{\alpha_{1}, \alpha_{2}, \ldots\right\}$ of minterms of $f$ such that every 1 -input of $f$ agrees with some $\alpha_{i} \in \Lambda$. Let $w$ be the weight of the smallest weight minterm in $\Lambda$, and assume that for some constant $c, w t\left(\alpha_{i}\right) \leq c \cdot w$ for all $\alpha_{i} \in \Lambda$. Then $s(f)=\Omega(\sqrt{n})$.
Proof. First we consider the case when $f\left(0^{n}\right)=0$. Then, $f\left(1^{n}\right)=1$, and any DNF representing $f$ must include a term with only positive literals. For a given DNF representing $f$, let $w$ denote the smallest number of positive literals in any term. Then, by the condition of the Theorem, $C\left(f, 1^{n}\right) \leq c \cdot w$ for some constant $c$, and combining Lemma 8 with Lemma 7 we get that $s(f) \geq \Omega(\sqrt{n})$.

In the case when $f\left(0^{n}\right)=1$, any DNF for $f$ must include a term with only negative literals, and then our condition implies that the DNF uses only negative literals. That is, in this case the function must be anti-monotone, which implies that $s(f, x)=b s(f, x)=C(f, x)$ for every input $x$. Thus, $s(f) \geq C\left(f, 0^{n}\right)$. Since $f\left(1^{n}\right) \neq f\left(0^{n}\right), f$ is not constant, and we can apply Lemma 8 , which now directly gives $s(f) \geq \sqrt{n}$.

An example with sensitivity $\Theta(\sqrt{n})$ when $f\left(0^{n}\right) \neq f\left(1^{n}\right)$
We give a simple example of a minterm-transitive function $f$ on $n$ variables, with sensitivity $\Theta(\sqrt{n})$ such that $f\left(0^{n}\right) \neq f\left(1^{n}\right)$. This shows that our $\Omega(\sqrt{n})$ lower bound on sensitivity in Theorem 4 is tight up to constant factors for the corresponding class.

Define $f:\{0,1\}^{n} \rightarrow\{0,1\}$ to be a monotone function, with $n$ m interms $\alpha_{1}, \ldots, \alpha_{n}$, each fixing $\sqrt{n}$ bits to 1 as follows. The minterm $\alpha_{1}$ fixes the first consecutive $\sqrt{n}$ bits to 1 , and $\alpha_{i}$ for $i \in[n]$ is obtained by cyclically shifting $\alpha_{1}$ by $i-1$ positions.

Note that $f\left(0^{n}\right)=0$ and $f\left(1^{n}\right)=1$.
We now show that $s(f)=\Theta(\sqrt{n})$.

1. $s_{1}(f)=\sqrt{n}$ : Any 1 -input is consistent with a minterm of size $\sqrt{n}$, fixing a set of $\sqrt{n}$ bits to 1 . Therefore, $C_{1}(f)=\sqrt{n}=s_{1}(f)$, since $f$ is monotone.
2. $2 \sqrt{n}-4 \leq s_{0}(f) \leq 2 \sqrt{n}$ : Note that for any 0-input $x$, the sensitive bits of $x$ must be 0 -bits (because $f$ is monotone).
Any sensitive 0 -bit must be surrounded by a block of at least $(\sqrt{n}-1)$ consecutive 1 s , that is, for any sensitive 0 , if the number of consecutive 1 's on its left is $a$ and the number of consecutive 1 s on its right is $b$, then $a+b \geq \sqrt{n}-1$. So for every sensitive 0 -bit, there are $\sqrt{n}-11$-bits around it that ar e not sensitive.
Moreover, any 1 -bit can only contribute to surrounding at most 2 sensitive 0 -bits. Thus, denoting the number of sensitive 0 -bits by $n_{0}$ we have $n_{0}(\sqrt{n}-1) \leq 2\left(n-n_{0}\right)$, which gives that $s_{0}(f)$ is at most $2 \sqrt{n}$.
On the other hand, let $x=\left(1^{\left(\frac{\sqrt{n}}{2}\right)} 01^{\left(\frac{\sqrt{n}}{2}\right)} 0 \ldots\right)$. Then, $f(x)=0$ and $s_{0}(f) \geq s(f, x)=$ $2 \sqrt{n}-4$.

## 4 Lower Bounds on Block Sensitivity of Transitive Functions

We start with two Lemmas that follow from Drucker's work [11].
Lemma 9. (Implicit in Lemma 4 in [11]) Let $\Gamma \subseteq S_{n}$ be a transitive group of permutations on $n$ bits and let $5 \leq r \leq 15$ be an integer.
Then, for any $\emptyset \neq S \subseteq[n]$ with $|S| \leq n^{3 / r}$, there exists $\hat{\Gamma} \subseteq \Gamma$ with $|\hat{\Gamma}| \geq \frac{(16-r)}{12} \cdot n^{\left(1-\frac{4}{r}\right)}$ such that for each $i \in[n]$, there are at most 3 permutations $\sigma_{j} \in \hat{\Gamma}$ for which $i \in \sigma_{j}(S)$.

Lemma 10. (Implicit in the proof of Theorem 2 in [11]) For any non-constant function $f:\{0,1\}^{n} \rightarrow\{0,1\}$, if $f$ has a set of 1-certificates $\Lambda=\left\{\alpha_{1}, \ldots \alpha_{t}\right\}$ such that for any index $i \in[n]$, there exist at most three 1-certificates from $\Lambda$ fixing $i$, then $b s(f) \geq \frac{t}{4}$.

Combining the above two lemmas, we obtain the following tradeoff between the minimum certificate size and the block sensitivity of transitive functions.

Lemma 11. For any non-constant transitive function $f:\{0,1\}^{n} \rightarrow\{0,1\}$, and an integer $5 \leq r \leq 15$, if $C_{\min }(f) \leq O\left(n^{3 / r}\right)$, then $b s(f) \geq \Omega\left(n^{1-\frac{4}{r}}\right)$.

Proof. Let $\alpha$ be a 1-certificate of $f$ of size at most $n^{3 / r}$, and let $S_{\alpha}$ be the set of bits fixed by $\alpha$. By Lemma 9 , there exists $\hat{\Gamma} \subset \Gamma$ with $|\hat{\Gamma}| \geq \Omega\left(n^{1-\frac{4}{r}}\right)$, such that for each $i \in[n]$, there are at most 3 permutations $\sigma_{j} \in \hat{\Gamma}$ for which $i \in \bar{\sigma}_{j}\left(S_{\alpha}\right)$. Also notice that for every permutation $\sigma_{j} \in \hat{\Gamma} \subset \Gamma, \sigma_{j}(\alpha)$ is a 1-certificate of $f$. The set of 1-certificates $\left\{\sigma_{j}(\alpha) \mid \sigma_{j} \in \hat{\Gamma}\right\}$ satisfies the condition of Lemma 10 and thus we have that $b s(f) \geq \Omega\left(n^{1-\frac{4}{r}}\right)$.

Combining Lemma 11 with our arguments in the previous sections, we prove $\Omega\left(n^{3 / 7}\right)$ lower bounds on the block sensitivity of functions on $n$ bits in each of the classes we considered.

Theorem 5. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function. If $f$ can be represented by a DNF with at most $2^{n^{3 / 7}}$ terms, or with a CNF with at most $2^{n^{3 / 7}}$ clauses, then $b s(f) \geq \Omega\left(n^{3 / 7}\right)$.
Proof. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be represented by a DNF with at most $2^{\frac{n^{3 / 7}}{2}}$ terms.
We now have two cases:
Case 1: $C_{\text {min }}(f)<n^{3 / 7}$. In this case, we use Lemma 11 with $r=7$ to give $b s(f) \geq$ $\Omega\left(n^{3 / 7}\right)$.

Case 2: $C_{\min }(f) \geq n^{3 / 7}$. By Lemma 5, we have: $C_{\min }(f) \leq s_{1}(f)+\frac{n^{3 / 7}}{2}$. Thus we have $b s(f) \geq s_{1}(f) \geq \frac{n^{3 / 7}}{2}$ and we are done.

As before, we can extend this theorem to DNFs (or CNFs) with an arbitrary number of terms (resp. clauses) as long as there is at least one variable that is not used too many times.

Theorem 6. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a transitive function that can be represented by a DNF (or CNF) such that its $i$-th variable appears in at most $2^{n^{3 / 7}}$ terms (resp. clauses) of the formula, for some $i \in[n]$. Then we have: $b s(f) \geq \Omega\left(n^{3 / 7}\right)$

Proof. We prove the statement about DNFs, the proof for CNFs is analogous. Let $x_{i}$ be a variable that appears in at most $k=2^{\frac{n^{3 / 7}}{3}}$ terms of the DNF.

As noted before (see e.g. [19]), for transitive $f, \operatorname{In} f_{i}(f)=\operatorname{In} f_{j}(f)$ for any $j \in[n]$, and thus $\operatorname{In} f_{i}(f)=\max _{j \in[n]} \operatorname{In} f_{j}(f)$.

Recall that by a theorem of Kahn, Kalai and Linial [16],

$$
\max _{j \in[n]} \operatorname{In} f_{j}(f) \geq \Omega(p(1-p) \log n / n),
$$

where $p$ is the probability that the function $f$ equals 1 .
Then, by Lemma 6 , for large enough $n$ we get

$$
C_{\min }(f) \leq \log k+1-\log \operatorname{In} f_{i}(f) \leq \log k+1+\log n+\log \frac{1}{p(1-p)}
$$

Notice that if $\frac{1}{p(1-p)} \geq 2^{\frac{n^{3} / 7}{3}}$, that implies that $\min \left\{\left|f^{-1}(1)\right|,\left|f^{-1}(0)\right|\right\} \leq 2^{n+1-\frac{n^{3 / 7}}{3}}$. Then by Lemma $1, b s(f) \geq s(f) \geq \Omega\left(n^{3 / 7}\right)$.

Otherwise, $\frac{1}{p(1-p)}<2^{\frac{n^{3 / 7}}{3}}$, and, for large enough $n$, we get $C_{\text {min }}(f) \leq n^{3 / 7}$. Then, using Lemma 11 with $r=7$ gives $b s(f) \geq \Omega\left(n^{3 / 7}\right)$.

Finally, we consider the class of transitive functions represented by DNFs (or CNFs) where the number of positive literals in each term (resp. clause) is approximately equal.

Theorem 7. Let $f:\{0,1\}^{n} \rightarrow\{0,1\}$ be a non-constant transitive function. Assume that there is a set $\Lambda=\left\{\alpha_{1}, \alpha_{2}, \ldots\right\}$ of minterms of $f$ such that every 1 -input of $f$ agrees with some $\alpha_{i} \in \Lambda$. Let $w$ be the weight of the smallest weight minterm in $\Lambda$, and assume that for some constant $c, w t\left(\alpha_{i}\right) \leq c \cdot w$ for all $\alpha_{i} \in \Lambda$. Then $b s(f)=\Omega\left(n^{3 / 7}\right)$.

Proof. Let $\alpha \in \Lambda$ be a minterm of $f$ that fixes the smallest number of bits to 0 among the minterms in $\Lambda$. Note that if $\operatorname{size}(\alpha) \leq n^{3 / 7}$ then by Lemma 11, we have: $b s(f) \geq \Omega\left(n^{3 / 7}\right)$. Thus, we can assume that $\operatorname{size}(\alpha)>n^{3 / 7}$.

Let $u$ denote the number of bits fixed to 0 by $\alpha$. We consider two cases.
Case 1. $u \geq \frac{\operatorname{size}(\alpha)}{2}$. Then, by Lemma 7, $b s(f) \geq s_{1}(f) \geq u \geq \frac{\operatorname{size}(\alpha)}{2}>\frac{n^{3 / 7}}{2}$ and we are done.
Case 2. $u<\frac{\operatorname{size}(\alpha)}{2}$, and thus $w t(\alpha) \geq \frac{\operatorname{size}(\alpha)}{2}$. Then we have $n^{3 / 7}<\operatorname{size}(\alpha) \leq 2 \cdot w t(\alpha) \leq$ $2 c w$. By Lemma 7 this gives $b s(f) \geq s(f)=\Omega\left(n^{3 / 7}\right)$.

## Acknowledgements

We thank the anonymous referees for helpful comments.

## References

1. Scott Aaronson, Shalev Ben-David, Robin Kothari, and Avishay Tal. Quantum implications of huang's sensitivity theorem. Electronic Colloquium on Computational Complexity (ECCC), 27:66, 2020.
2. Kazuyuki Amano. Minterm-transitive functions with asymptotically smallest Block Sensitivity. Inf. Process. Lett., 111(23-24):1081-1084, 2011.
3. Andris Ambainis, Mohammad Bavarian, Yihan Gao, Jieming Mao, Xiaoming Sun, and Song Zuo. Tighter Relations between Sensitivity and Other Complexity Measures. In Proceedings of the 41 st International Colloquium on Automata, Languages, and Programming (ICALP), pages 101-113, 2014.
4. Andris Ambainis and Xiaoming Sun. New separation between $s(f)$ and $b s(f)$. Electronic Colloquium on Computational Complexity (ECCC), 18:116, 2011.
5. Andris Ambainis and Jevgēnijs Vihrovs. Size of Sets with Small Sensitivity: A Generalization of Simon's Lemma. In Proceedings of the 12th Annual Conference on Theory and Applications of Models of Computation (TAMC), pages 122-133, 2015.
6. Srinivasan Arunachalam, Sourav Chakraborty, Michal Koucký, Nitin Saurabh, and Ronald de Wolf. Improved bounds on Fourier entropy and Min-entropy. CoRR, abs/1809.09819, 2018.
7. Mitali Bafna, Satyanarayana V. Lokam, Sébastien Tavenas, and Ameya Velingker. On the Sensitivity Conjecture for Read-k Formulas. In 41 st International Symposium on Mathematical Foundations of Computer Science (MFCS), pages 16:1-16:14, 2016.
8. Harry Buhrman and Ronald De Wolf. Complexity Measures and Decision Tree Complexity: A Survey. Theoretical Computer Science, 288(1):21-43, 2002.
9. Sourav Chakraborty. On the Sensitivity of Cyclically-Invariant Boolean functions. Discrete Mathematics $\mathcal{F}$ Theoretical Computer Science, 13(4):51-60, 2011.
10. Siddhesh Chaubal and Anna Gál. New Constructions with Quadratic Separation between Sensitivity and Block Sensitivity. In Proceedings of the 38th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), pages 13:113:16, 2018.
11. Andrew Drucker. Block Sensitivity of Minterm-Transitive functions. Theor. Comput. Sci., 412(41):5796-5801, 2011.
12. Parikshit Gopalan, Rocco A. Servedio, Avishay Tal, and Avi Wigderson. Degree and Sensitivity: Tails of Two Distributions. CoRR, abs/1604.07432, 2016.
13. Pooya Hatami, Raghav Kulkarni, and Denis Pankratov. Variations on the Sensitivity Conjecture. Theory of Computing, Graduate Surveys, 4:1-27, 2011.
14. Kun He, Qian Li, and Xiaoming Sun. A tighter relation between sensitivity complexity and certificate complexity. Theoretical Computer Science, 762:1-12, 2019.
15. Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. Annals of Mathematics, 190(3):949-955, 2019.
16. Jeff Kahn, Gil Kalai, and Nathan Linial. The Influence of Variables on Boolean Functions. In 29th Annual Symposium on Foundations of Computer Science (FOCS), pages 68-80, 1988.
17. Sophie Laplante, Reza Naserasr, and Anupa Sunny. Sensitivity Lower Bounds from Linear Dependencies. In 45 th International Symposium on Mathematical Foundations of Co mputer Science (MFCS 2020), volume 170 of Leibniz International Proceedings in Informatics (LIPIcs), pages 62:1-62:14, 2020.
18. Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. Computational Complexity, 4(4):301-313, Dec 1994.
19. Ryan O'Donnell. Analysis of Boolean functions. Cambridge University Press, 2014.
20. David Rubinstein. Sensitivity vs. Block Sensitivity of Boolean functions. Combinatorica, 15(2):297-299, Jun 1995.
21. Hans-Ulrich Simon. A tight $\Omega(\log \log \mathrm{n})$-bound on the time for parallel RAM's to compute nondegenerated Boolean functions. Information and Control, 55(1):102-107, 1982.
22. Xiaoming Sun. Block Sensitivity of Weakly Symmetric Functions. In Proceedings of the Third International Conference on Theory and Applications of Models of Computation (TAMC), pages 339-344, 2006.
23. Madars Virza. Sensitivity versus Block Sensitivity of Boolean functions. Information Processing Letters, 111(9):433-435, 2011.

[^0]:    *A preliminary version of this paper appears in the Proceedings of LATIN 2020
    ${ }^{\dagger}$ University of Texas at Austin, Email: siddhesh@cs.utexas.edu
    ${ }^{\ddagger}$ University of Texas at Austin, Email: panni@cs.utexas.edu

