Block Sensitivity of Minterm-Transitive Functions

Andrew Drucker[*]

Abstract

Boolean functions with a high degree of symmetry are interesting from a complexity theory perspective: extensive research has shown that these functions, if nonconstant, must have high complexity according to various measures. In recent work of this type, Sun (2007) gave lower bounds on the block sensitivity of nonconstant Boolean functions invariant under a transitive permutation group. Sun showed that all such functions satisfy $bs(f) = \Omega(N^{1/3})$. He also showed that there exists such a function for which $bs(f) = O(N^{3/7} \ln N)$. His example belongs to a subclass of transitively invariant functions called "minterm-transitive" functions, defined by Chakraborty (2005).

We extend these results in two ways. First, we show that nonconstant minterm-transitive functions satisfy $bs(f) = \Omega(N^{3/7})$. Thus Sun's example has nearly minimal block sensitivity for this subclass. Second, we improve Sun's example: we exhibit a minterm-transitive function for which $bs(f) = O(N^{3/7} \ln^{1/7} N)$.

1 Introduction

Boolean functions, like other objects in mathematics, can be classified according to the symmetries they possess. A natural notion of symmetry arises when we consider permutations of the input variables. Given a function $f : \{0,1\}^N \to \{0,1\}$ and a permutation σ on $[N] = \{1, \ldots, N\}$, we say that f is invariant under σ if permuting the input variables according to σ never affects the value of f. For every function f it is easily seen that the set of permutations under which f is invariant forms a group under the composition operation. This group is called the *invariance group* of f.

One class of "highly symmetric" functions are those whose invariance group is *transitive*: a permutation group Γ is transitive if for each $i, j \in [N]$ there is a $\pi \in \Gamma$ such that $\pi(i) = j$. Transitively invariant Boolean functions (also called *weakly symmetric* functions) are a natural, important class which includes graph properties and symmetric functions. They are of particular interest in computational complexity theory: several decades of research have shown that certain classes of (nonconstant) transitively invariant Boolean functions have high "complexity" in several senses. For example, symmetric functions on N inputs have randomized query complexity $\Omega(N)$, quantum query complexity $\Omega(\sqrt{N})$ [BBC+98], and sensitivity $\Omega(N)$; graph properties on n-vertex graphs have deterministic query complexity $\Omega(n)$, quantum query complexity $\Omega(n^{1/2})$ [SYZ04], and sensitivity $\Omega(n)$ [Tur84]. In each case the lower bound obtained is best-possible for the function class in question (except for a log-factor gap between upper and lower bounds in the case of [SYZ04]).

For general transitively invariant functions, the deterministic and quantum query complexities have also been pinpointed fairly precisely [SYZ04]. However, the sensitivity and block sensitivity of these functions are less well understood. In particular, it is open whether such functions have sensitivity $s(f) = N^{\Omega(1)}$. A version of this question was first asked in 1984 by Turan [Tur84], who gave an affirmative answer for the case of graph properties.

[*] EECS, MIT. Email: adrucker@mit.edu. Supported by a DARPA YFA grant of Scott Aaronson.

Partial progress on Turan's question was made by Chakraborty, who in [Cha05] defined a special class of transitively invariant functions called *minterm-transitive functions* (see Section 2.2 for the definition). Although they are of restricted form, these functions are of interest because, in contrast to graph properties and symmetric functions, they place no restriction on the type of transitive invariance group associated with the Boolean function. Chakraborty showed that for such functions $s(f) = \Omega(N^{1/3})$, and he also constructed an example for which this bound is tight. This is the lowest sensitivity known for any transitively invariant function.

In subsequent work, Sun [Sun07] showed that for general transitively invariant functions, the block sensitivity $bs(f)$ satisfies $bs(f) = \Omega(N^{1/3})$. Sun also gave an example of a transitively invariant (in fact minterm-transitive) function for which $bs(f) = O(N^{3/7} \ln N)$.

In this paper, we extend Sun's results in two directions. First, we show in Section 3 that for minterm-transitive functions, $bs(f) = \Omega(N^{3/7})$. While this does not close the gap in our knowledge for general transitively invariant functions, it in a sense explains why Sun's upper bound took the form it did. To prove this result, we build on Sun's approach of selecting random permutations from the invariance group for f to find disjoint sensitive blocks (related ideas were used earlier in [Cha05, RV76]). In a novel step, we use the "deletion method" of probabilistic combinatorics [AS08, Chap. 3] to create a large collection of sensitive blocks with "low overlap". We then apply a method, specific to minterm-transitive functions, to pass from an input with many, low-overlap sensitive blocks to an input with many disjoint sensitive blocks.

Second, we improve Sun's upper-bound example, by presenting (in Section 4) a family of minterm-transitive functions for which $bs(f) = O(N^{3/7} \ln^{1/7} N)$. We follow the same basic approach used by Sun [Sun07] to construct his example, but we improve part of the construction, using a powerful inequality from probability theory due to Janson and Suen [Jan98]. We introduce this inequality in Section 2.3.

2 Preliminaries

For convenience, in what follows we will always regard an N-bit string as having coordinates indexed by $\mathbb{Z}_N$, the integers mod N. We let S_N denote the symmetric group of permutations over $\mathbb{Z}_N$ under the composition operation.

2.1 Sensitivity and block sensitivity

Given a string $x \in \{0,1\}^N$ and a set $B \subseteq \mathbb{Z}_N$ (also referred to as a "block"), define x^B as the string whose ith bit is $\overline{x_i}$ if $i \in B$, and x_i otherwise. Let $x^i := x^{\{i\}}$ denote the string x with its ith bit flipped.

For any Boolean function $f : \{0,1\}^N \to \{0,1\}$ and $x \in \{0,1\}^N$, say that $B \subseteq \mathbb{Z}_N$ is a *sensitive block for* x if $f(x^B) \neq f(x)$. Define $bs(f;x)$ as the largest d for which there exist d disjoint sensitive blocks $B_1, \ldots, B_d \subseteq \mathbb{Z}_N$ for x. For $b \in \{0,1\}$, define the *b-block sensitivity* of f, or $bs_b(f)$, as $\max_{x \in f^{-1}(b)} bs(f;x)$. Define the *block sensitivity* $bs(f) = \max(bs_0(f), bs_1(f))$. Block sensitivity was first defined by Nisan in [Nis91].

Block sensitivity is a variant of a measure called sensitivity (originally called "critical complexity"), defined earlier in [CDR86] . The *sensitivity* of f, denoted $s(f)$, is defined identically to $bs(f)$, except we restrict attention to sensitive blocks of size 1. Thus we have $s(f) \leq bs(f)$; it is open whether $bs(f)$ can be upper-bounded by some polynomial in $s(f)$.

2.2 Patterns, permutations, and invariance

Define a *pattern* as a string $p \in \{0,1,*\}^N$. Define the *domain* of p as $\text{dom}(p) := \{i \in \mathbb{Z}_N : p_i \in \{0,1\}\}$. We say that p is *defined on* i if $i \in \text{dom}(p)$. Say that two patterns p, p' *agree* if for all $i \in \mathbb{Z}_N$, $p_i \in \{0,1\} \Rightarrow$

$p'_i \in \{p_i, *\}$. Note that this condition is symmetric in p, p'.

For a pattern p and a permutation $\sigma \in S_N$, define the *σ-shift of p*, denoted $\sigma(p)$, as the pattern given by $\sigma(p)_i := p_{\sigma^{-1}(i)}$. Similarly, for a subset $B \subseteq \mathbb{Z}_N$, define the σ-shifted set $\sigma(B) := \{\sigma(b) : b \in B\}$.

Given a permutation group $\Gamma \leq S_N$, we say a Boolean function f is *invariant under* Γ if for all $x \in \{0,1\}^N$ and $\sigma \in \Gamma$, $f(x) = f(\sigma(x))$. A permutation group Γ is called *transitive* if for all $i, j \in \mathbb{Z}_N$ there exists $\sigma \in \Gamma$ such that $\sigma(i) = j$. An important example of a transitive permutation group is the family of cyclic shifts of the coordinates, which we denote by $\mathcal{T} = \{t_j\colon t_j(i) = i + j \mod N\}_{j \in \mathbb{Z}_N}$. We say a Boolean function f is *transitively invariant* if it is invariant under some transitive group Γ. We say f is *cyclically invariant* if it is invariant under $\mathcal{T}$.

Given a pattern p and $\Gamma \leq S_N$, define the *(Γ, p)-pattern matching problem* $f^{\Gamma,p} : \{0,1\}^n \to \{0,1\}$ by

$$f^{\Gamma,p}(x) = 1 \quad \Leftrightarrow \quad \exists \sigma \in \Gamma : x \text{ agrees with } \sigma(p).$$

Equivalently, $f^{\Gamma,p}(x) = 1 \Leftrightarrow \exists \sigma \in \Gamma$ such that $\sigma(x)$ agrees with p. A function $f : \{0,1\}^n \to \{0,1\}$ is called *minterm-transitive* if there exists a transitive group Γ and pattern p such that $f = f^{\Gamma,p}$. The function f is called *minterm-cyclic* if in addition we may take $\Gamma = \mathcal{T}$. Note that transitive pattern-matching functions are transitively invariant, and minterm-cyclic functions are cyclically invariant. Both of these subclasses were defined in [Cha05], where the terminology is explained.

2.3 A probabilistic inequality

The key tool in our construction of a minterm-transitive function with low block sensitivity is a probabilistic inequality from a paper of Janson [Jan98]. This inequality reformulates an earlier result of Suen [Sue90], which in turn generalizes another, earlier result of Janson; see [Jan98] and [AS08, Sec. 8.7] for details. Roughly speaking, the inequality upper-bounds the probability that a family of 0/1-valued random variables sums to zero, provided the expected value of their sum is large enough and they are "mostly independent". We set up and state this inequality next; it will be used only in Section 4.

Let $\{I_i\}_{i \in \mathcal{I}}$ be a finite family of 0/1-valued random variables on some probability space Ω. Let G be an undirected graph with vertex set $\mathcal{I}$ and edges indicated by $\sim$. Say that G is a *dependency graph* if the following two conditions hold: First, for all i we must have $i \nsim i$. Second, if A, B are disjoint sets in $\mathcal{I}$ and $i \nsim j$ for each pair $(i,j) \in A \times B$, then the family $\{I_i\}_{i \in A}$ must be independent of the family $\{I_j\}_{j \in B}$.

For Theorem 1 below, suppose G is such a dependency graph for $\mathcal{I}$. Given $i \in \mathcal{I}$, let $q_i := \mathbb{E}[I_i]$, and let $\mu := \mathbb{E}\left[\sum_{i \in \mathcal{I}} I_i\right] = \sum_{i \in \mathcal{I}} q_i$. Let $\delta_i := \sum_{j: i \sim j} q_j$. Let $\delta := \max_i \delta_i$, and let $\Delta := \sum_{\{i,j\}: i \sim j} \mathbb{E}\left[I_i I_j\right]$, where the sum is over unordered pairs. Observe that δ and Δ measure in a sense the "level of dependence" among the family. Then we have:

Theorem 1. *[Jan98, Theorem 2]* $\Pr[\sum_{i \in \mathcal{I}} I_i = 0] \leq e^{-\mu + \Delta e^{2\delta}}$.

3 Lower bound for minterm-transitive functions

In this section we prove:

Theorem 2. *If $f : \{0,1\}^N \to \{0,1\}$ is a nonconstant minterm-transitive function, then $bs(f) = \Omega(N^{3/7})$.*

The following easy observation is due to [RV76], and has been used repeatedly in the study of transitively invariant functions [Cha05, Sun07].

Lemma 3. *[RV76] If $\Gamma \subseteq S_N$ is a transitive group of permutations, $i \in \mathbb{Z}_N$ is any index, and σ is a uniformly chosen element of Γ, then $\sigma(i)$ is uniformly distributed over $\mathbb{Z}_N$.*

We will use the following combinatorial lemma:

Lemma 4. *Let $B \subseteq \mathbb{Z}_N$ be of size at most $N^{3/7}$, and let $\Gamma \leq S_N$ be a transitive permutation group. If N is sufficiently large, there exists a $T \geq N^{3/7}/2$ and group elements $\Sigma = \{\sigma_1, \ldots, \sigma_T\} \subseteq \Gamma$ such that for each $i \in \mathbb{Z}_N$, there are at most 3 indices $j \leq T$ for which $i \in \sigma_j(B)$.*

Note that there is no requirement that the σ_j all be distinct.

Proof of Lemma 4. Our approach is as follows: first we select T_0 permutations σ_j independently at random from Γ, where $T_0 := \lceil N^{3/7} \rceil$. Some indices i may be contained in 4 or more of the shifted sets $\sigma_j(B)$, but we argue that with nonzero probability, we can discard at most $N^{3/7}/2$ of the permutations in our collection to "repair" every such index i.

So let $\sigma_1, \ldots, \sigma_{T_0}$ be independent and uniform from Γ. For each $i \in \mathbb{Z}_N$, say i is "bad" if $i \in \sigma_j(B)$ for at least 4 trials $j \leq T_0$. We upper-bound the probability that i is bad. First, for any fixed trial, Lemma 3 tells us that $\Pr[i \in \sigma_j(B)] = |B|/N$. Independence of the trials implies that for any fixed 4-tuple of distinct trials $(j_1, j_2, j_3, j_4) \in [T_0]$, the probability that i is in the shifted set on each of the 4 trials is $(|B|/N)^4$. Then by a union bound,

$$\Pr[i \text{ is bad}] \leq \binom{T_0}{4} \left(\frac{|B|}{N}\right)^4 < \frac{(T_0|B|)^4}{24N^4} \leq \frac{((N^{3/7}+1)N^{3/7})^4}{24N^4} < \frac{N^{-4/7}}{23},$$

the last step holding if N is sufficiently large. Summing over all $i \in \mathbb{Z}_N$, the *expected* number of bad indices is less than $N^{3/7}/23$. By Markov's bound, the probability that there are $N^{3/7}/10$ bad indices is less than $1/2$.

Now say that $i \in \mathbb{Z}_N$ is "terrible" if $i \in \sigma_j(B)$ for at least 7 indices $j \leq T_0$. By reasoning similar to the above, the expected number of terrible indices is at most

$$N \cdot \binom{T_0}{7} \left(\frac{|B|}{N}\right)^7 < N \cdot \frac{(N^{-1/7})^7}{7! - 1} < 1/2,$$

for sufficiently large N. So the probability that *any* terrible index appears is less than 1/2, and we find that with positive probability there are no terrible indices and fewer than $N^{3/7}/10$ bad indices.

Take any such outcome, specified by a sequence $\sigma_1, \ldots, \sigma_{T_0}$. For each bad index $i \in \mathbb{Z}_N$, delete from the collection some set of 3 permutations σ_j such that $i \in \sigma_j(B)$ (some such deletions may count towards more than one bad index). The total number of permutations deleted is less than $3 \cdot (N^{3/7}/10) < N^{3/7}/2$. The remaining collection has size greater than $N^{3/7}/2$ and (since there were no terrible indices) satisfies the Lemma's conclusion. □

Proof of Theorem 2. Take any nonconstant minterm-transitive function $f = f^{\Gamma,p} : \{0,1\}^N \to \{0,1\}$, where Γ is a transitive group and p a pattern. Let $B := \{i : p_i \in \{0,1\}\}$; as f is nonconstant, B is nonempty. Without loss of generality we may assume that the number of 1-entries in p is at least $|B|/2$. Let $x \in \{0,1\}^N$ be the string that agrees with p and equals 0 on coordinates where p is undefined. Note that $f(x) = 1$, while $f(x^i) = 0$ for any i such that $p_i = 1$. Thus $bs(f) \geq bs(f; x) \geq |B|/2$.

If $|B| > N^{3/7}$, then $bs(f) > N^{3/7}/2$. Let us assume now that $|B| \leq N^{3/7}$. In this case, Lemma 4 applies to B: there exist group elements $\Sigma = \{\sigma_1, \ldots, \sigma_T\} \subseteq \Gamma$, with $T \geq N^{3/7}/2$, satisfying Lemma 4's conclusions. Let $\Sigma(p) := \{\sigma_j(p) : \sigma_j \in \Sigma\}$ denote our distinguished (multi-)set of shifted patterns, and let

$$\mathcal{B}_\Sigma := \{B_j = \text{dom}(\sigma_j(p)) : j \in [T]\}$$

denote the corresponding collection of domains. Note that $B_j = \sigma_j(B)$.

At most three patterns $\sigma_j(p) \in \Sigma(p)$ from our collection are defined on any index $i \in \mathbb{Z}_N$, so for each i we can select a value $v_i \in \{0,1\}$ such that *at most* one $\sigma_j(p)$ that is defined on i disagrees with the setting v_i there. Let $v := (v_i)_{i \in \mathbb{Z}_N}$. Now consider the following algorithm:

1. Initialize $x \in \{0,1\}^N$ to any value such that $f(x) = 0$.
2. If there exists some $i \in \mathbb{Z}_N$ such that $x_i \neq v_i$, and such that $f(x^i) = 0$, pick such an i arbitrarily and set $x \leftarrow x^i$; otherwise halt.
3. Repeat Step 2.

Note that $f(x) = 0$ for every value of x during the algorithm's run. Note also that the algorithm must halt, since each step reduces the number of disagreements between x and v. Now we ask the following question: looking at the final value of x when the algorithm halts, for how many indices i does x_i still disagree with v_i? Call these indices "stubborn".

First, suppose there are at least $N^{3/7}/12$ stubborn indices. Since the algorithm halted, it must be the case that $f(x^i) = 1 \neq f(x)$ for each such stubborn index i, and thus $bs(f) \geq bs(f; x) \geq N^{3/7}/12$.

On the other hand, suppose there are fewer than $N^{3/7}/12$ stubborn indices. As each index $i \in \mathbb{Z}_N$ appears in at most 3 sets from $\mathcal{B}_\Sigma$, fewer than $N^{3/7}/4$ sets from $\mathcal{B}_\Sigma$ contain *any* stubborn index. If $B_j \in \mathcal{B}_\Sigma$ contains no stubborn indices, call it "stubborn-free"; so, there are more than $T - N^{3/7}/4 \geq N^{3/7}/4$ stubborn-free sets B_j.

For each $B_j \in \mathcal{B}_\Sigma$, define the "disagreement set" $D_j := \{i : (\sigma_j(p))_i \in \{0,1\} \wedge x_i \neq (\sigma_j(p))_i\} \subseteq B_j$. Each D_j is nonempty, since $f(x) = 0$ and $f = f^{\Gamma,p}$. Also, $f(x^{D_j}) = 1$. Observe that if B_j is stubborn-free, and $i \in D_j$, then $\sigma_j(p)_i \neq v_i$, so $\sigma_j(p)$ is the *only* pattern in $\Sigma(p)$ that disagrees with x at i. Thus if $j \neq j'$ and $B_j, B_{j'}$ are stubborn-free, $D_j \cap D_{j'} = \emptyset$. It follows that $bs(f; x)$ is at least the number of stubborn-free sets $B_j \in \mathcal{B}_\Sigma$, which we've seen is at least $N^{3/7}/4$.

Combining all of our cases, we find that $bs(f) = \Omega(N^{3/7})$. □

4 An improved upper-bound example

Sun [Sun07] gave an example of a minterm-cyclic function with block sensitivity $O(N^{3/7} \ln N)$. This was the lowest block sensitivity known for any nonconstant transitively invariant function. In this section we prove the following result, improving on Sun's example:

Theorem 5. *There exist a family of nonconstant, minterm-transitive (in fact minterm-cyclic) functions* $f_N : \{0,1\}^N \to \{0,1\}$, *such that* $bs(f_N) = O(N^{3/7} \ln^{1/7} N)$.

Most of our proof follows the outline of Sun's, but for completeness we give a self-contained presentation. Before defining the pattern p we will use to define $f_N = f^{\mathcal{T},p}$, we give two lemmas (both from [Sun07]) for upper-bounding the block sensitivity of such functions.

Lemma 6. *[Sun07] For any* $f = f^{\mathcal{T},p}, bs_1(f) \leq |\mathrm{dom}(p)|$.

Proof. If $f(x) = 1$, then some shift $t_{j_0}(p)$ of p agrees with x. Given any collection of disjoint blocks $\{B_k\}_{k \in [d]}$ satisfying $f(x^{B_k}) = 0$, for every $k \in [d]$ there must some $i \in \mathrm{dom}(t_{j_0}(p))$ belonging uniquely to B_k. Thus $d \leq |\mathrm{dom}(t_{j_0}(p))| = |\mathrm{dom}(p)|$. □

Obtaining an upper bound on $bs_0(f)$ takes a bit more work. We give some preparatory definitions. By a *4-set* in $\mathbb{Z}_N$ we mean a subset of $\mathbb{Z}_N$ of size 4. If A is a 4-set, say that pattern *p contains a balanced shifted copy of A* if there exists a cyclic shift t_j such that the shifted pattern $t_j(p)$ satisfies $\mathrm{dom}(t_j(p)) \supseteq A$, and $t_j(p)$ equals 0 on some two of the coordinates in A and equals 1 on the other two.

Lemma 7. *[Sun07] For any $f = f^{\mathcal{T},p}$, if $bs_0(f) \geq d$ then there exists a set $S \subseteq \mathbb{Z}_N$ of size d, such that there is no 4-set $A \subseteq S$ for which p contains a balanced shifted copy of A.*

Proof. Say $bs_0(f) \geq d$; then there exists an input x and d disjoint subsets $B_1, \ldots, B_d \subseteq \mathbb{Z}_N$ such that $f(x^{B_k}) = 1 \neq f(x)$, for $k \in [d]$. Thus for each $k \in [d]$, there exists $j(k) \in \mathbb{Z}_N$ such that x^{B_k} agrees with $t_{j(k)}(p)$. We claim these indices are all distinct. For suppose $k \neq k'$ yet $j(k) = j(k')$. Then both of $B_k, B_{k'}$ contain each of the (nonempty set of) coordinates on which $t_{j(k)}(p)$ disagrees with x. But this contradicts the fact that $B_k \cap B_{k'} = \emptyset$. Thus the indices $j(1), \ldots, j(d)$ are indeed distinct.

Let $S := \{-j(k) : k \in [d]\}$. We claim that if A is any 4-set contained in S, then p contains no balanced shifted copy of A. For suppose to the contrary there exists some $j^* \in \mathbb{Z}_N$ and distinct indices $k_1, k_2, k_3, k_4 \in [d]$, such that (letting $p' := t_{j^*}(p)$) we have:

1. the distinct indices $-j(k_1), -j(k_2), -j(k_3), -j(k_4)$ are in the domain of p';
2. $p'_{-j(k_1)} = p'_{-j(k_2)} = 0$ while $p'_{-j(k_3)} = p'_{-j(k_4)} = 1$. Equivalently, $p_{-j(k_1)-j^*} = p_{-j(k_2)-j^*} = 0$ and $p_{-j(k_3)-j^*} = p_{-j(k_4)-j^*} = 1$ (here, index arithmetic is mod N).

Recall that x^{B_k} agrees with $t_{j(k)}(p)$ for $k \in [d]$; in particular, for $k \in \{k_1, k_2, k_3, k_4\}$ we have $(t_{j(k)}(p))_{-j^*} \in \{x^{B_k}_{-j^*}, *\}$, i.e.,

$$p_{-j(k)-j^*} \in \{x^{B_k}_{-j^*}, *\}.$$

But we have seen that for $k \in \{k_1, k_2\}$ the left-hand side equals 0, and for $k \in \{k_3, k_4\}$ the left-hand side equals 1. Thus the index $-j^*$ must be contained in exactly *two* of the sets $B_{k_1}, \ldots, B_{k_4}$, contradicting the disjointness of these sets. Thus p contains no balanced shifted copy of any 4-set $A \subseteq S$, as claimed. □

We can now explain our strategy (following [Sun07]) to prove Theorem 5: we build a pattern $p \in \{0, 1, *\}^N$ with "small" domain, so that $bs_1(f^{\mathcal{T},p})$ is small by Lemma 6. We choose p such that for any "sufficiently large" $S \subseteq \mathbb{Z}_N$, p contains a balanced shifted copy of some 4-set $A \subseteq S$; this will bound $bs_0(f^{\mathcal{T},p})$ by Lemma 7.

Our pattern p will have all of its 0/1 entries on $\{0, 1, \ldots, 2K-2\}$, where $K = K_N < N/2$ is a parameter. In this we are following [Sun07], with some further optimization in our setting of K. The key properties we need in p are provided by the following Lemma:

Lemma 8. *For sufficiently large K, there is a pattern p with $\mathrm{dom}(p) \subseteq \{0, 1, \ldots, 2K-2\}$ that contains a shifted balanced copy of every 4-set $A \subseteq \{0, 1, \ldots, K-1\}$, and satisfies $|\mathrm{dom}(p)| \leq 3K^{3/4} \ln^{1/4} K$.*

Note that the "sufficiently large" requirement in Lemma 8 is independent of N. This Lemma resembles [Sun07, Lemma 2], but uses a different construction and improves its parameters. Sun defined a pattern p by randomly assigning 0/1 values to a collection of translates of an explicit set; by contrast, we use a fully probabilistic construction. We defer the proof of Lemma 8.

Proof of Theorem 5. Set $K := \lceil N^{4/7} / \ln^{1/7} N \rceil$. Fix a pattern p as guaranteed by Lemma 8 (for each sufficiently large N). Let $f^{\mathcal{T},p}$ be the corresponding minterm-cyclic pattern-matching problem. First, by Lemma 6,

$$bs_1(f^{\mathcal{T},p}) \leq 3K^{3/4}(\ln K)^{1/4} = O\left(N^{\frac{4}{7}\cdot\frac{3}{4}}(\ln N)^{-\frac{1}{7}\cdot\frac{3}{4}} \cdot (\ln N)^{1/4}\right) = O\left(N^{3/7} \ln^{1/7} N\right),$$

since $\frac{1}{4} - \frac{3}{28} = \frac{1}{7}$.

To upper-bound $bs_0(f^{\mathcal{T},p})$, let $S \subseteq \mathbb{Z}_N$ be any set of size $d := \lceil 4N^{3/7} \ln^{1/7} N \rceil \geq 4N/K$. Following [Sun07], if we pick an interval $[a, a+K-1]$ (mod N) by choosing $a \in \mathbb{Z}_N$ uniformly at random, the expected number of elements of S in the interval is at least $K \cdot (4N/K)/N = 4$. Thus there exists some such interval which contains at least 4 elements of S. Let $A \subseteq S$ be these 4 elements. Since A is contained in an interval of length K, Lemma 8 tells us that p contains a balanced shifted copy of A.

As S was an arbitrary set of size d, it follows from Lemma 7 that $bs_0(f^{\mathcal{T},p}) < d = O(N^{3/7} \ln^{1/7} N)$, and hence that $bs(f^{\mathcal{T},p}) = O(N^{3/7} \ln^{1/7} N)$. This proves Theorem 5. □

Proof of Lemma 8. We construct p as follows. For each $0 \leq i \leq 2K-2$, we independently set p_i, where for $b \in \{0,1\}$ we have $\Pr[p_i = b] = ((\ln K)/K)^{1/4}$; with the remaining probability we set $p_i = *$. If $p_i = b \in \{0,1\}$ we say that p "colors" i with the color b.

Now we prepare to apply Theorem 1 from Section 2.3. Fix any 4-set $A \subseteq \{0,1,\ldots,K-1\}$. For $0 \leq i < K$, let I_i be the event that $A+i$ is contained in the domain of p and receives a balanced coloring by p (note that $A+i \subseteq \{0,1,\ldots 2K-2\}$). We define $i \sim j$ to hold iff $i \neq j$ and $(A+i) \cap (A+j) \neq \emptyset$. Note that this defines a valid dependency graph, since I_i depends only on the restriction of p to the indices of $A+i$ and p is chosen according to a product measure. We will use Theorem 1 to upper-bound the probability that $\sum_{0 \leq i < K} I_i = 0$; then we will simply take a union bound over all possible choices of A.

First, let us compute μ for our family of random variables. Note that each translate $A+i$ can be given a balanced coloring by p in $\binom{4}{2} = 6$ ways, and that each such coloring has probability $((\ln K)/K)^{1/4})^4 = (\ln K)/K$. Thus $q_i = 6(\ln K)/K$ and $\mu = 6 \ln K$.

Now we bound δ and Δ. Note that each translate $A+i$ overlaps with at most 3 others, so that $\delta = O(\max_i q_i) = o(1)$. Also, for each pair $A+i, A+j$ of overlapping translates, there are certainly fewer than $\binom{4}{2}^2 = 36$ colorings of $(A+i) \cup (A+j)$ that make both translates balanced. Any such coloring has probability at most $((\ln K)/K)^{1/4})^5$ of occurring, since $|(A+i) \cup (A+j)| \geq 5$. The number of such pairs $i \sim j$ is $O(K)$; thus,

$$\Delta = \sum_{\{i,j\}: i \sim j} \mathbb{E}[I_i I_j] \leq O\left(K \cdot (\ln^{5/4} K)/K^{5/4}\right) = o(1).$$

Theorem 1 then tells us that $\Pr\left[\sum_i I_i = 0\right] \leq e^{-6 \ln K + o(1)} = (1+o(1))K^{-6}$. This is less than K^{-4} for large enough K.

There are $\binom{K}{4} < K^4/24$ 4-sets $A \subseteq \{0,1,\ldots,K-1\}$, so for large enough K, the probability that p fails to contain a balanced shifted copy of any such A is, by a union bound, at most $1/24$. Also, the expected domain size of p is $K \cdot 2((\ln K)/K)^{1/4} = 2K^{3/4} \ln^{1/4} K$. Using Markov's inequality, the probability that $|\mathrm{dom}(p)| > 3K^{3/4} \ln^{1/4} K$ is less than $2/3$. By a union bound we conclude that with nonzero probability, p contains a balanced shifted copy of each 4-set $A \subseteq \{0,1,\ldots,K-1\}$, and simultaneously $|\mathrm{dom}(p)| \leq 3K^{3/4} \ln^{1/4} K$. This proves Lemma 8 (and completes the proof of Theorem 5). □

5 Open Problems

It is natural to wonder if the parameters in Lemma 8 can be improved further to remove the log factor entirely. (If so, we suspect a non-probabilistic approach is needed.) This would yield a tight bound of $\Theta(N^{3/7})$ for the minimum achievable block sensitivity for nonconstant minterm-transitive functions.

More broadly, we still hope for a better understanding of the sensitivity and block sensitivity of general transitively invariant functions. The main open problem in this area is whether for such functions $s(f) = N^{\Omega(1)}$; it is unresolved even for the special case of cyclically invariant functions.

References

[AS08] N. Alon and J. H. Spencer. *The Probabilistic Method.* Wiley-Interscience, third edition, 2008.

[BBC$^+$98] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *FOCS*, pages 352–361, 1998.

[CDR86] Stephen Cook, Cynthia Dwork, and Rüdiger Reischuk. Upper and lower time bounds for parallel random access machines without simultaneous writes. *SIAM J. Comput.*, 15(1):87–97, 1986.

[Cha05] Sourav Chakraborty. On the sensitivity of cyclically-invariant boolean functions. In *IEEE Conference on Computational Complexity*, pages 163–167, 2005.

[Jan98] Svante Janson. New versions of suen's correlation inequality. *Random Struct. Algorithms*, 13(3-4):467–483, 1998.

[Nis91] Noam Nisan. Crew prams and decision trees. *SIAM J. Comput.*, 20(6):999–1007, 1991.

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

[Sue90] Stephen Suen. A correlation inequality and a poisson limit theorem for nonoverlapping balanced subgraphs of a random graph. *Random Struct. Algorithms*, 1(2):231–242, 1990.

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

[SYZ04] Xiaoming Sun, Andrew Chi-Chih Yao, and Shengyu Zhang. Graph properties and circular functions: How low can quantum query complexity go? In *IEEE Conference on Computational Complexity*, pages 286–293, 2004.

[Tur84] György Turán. The critical complexity of graph properties. *Inf. Process. Lett.*, 18(3):151–153, 1984.