On the Sensitivity of Cyclically-Invariant Boolean Functions

Sourav Chakraborty
University of Chicago
sourav@cs.uchicago.edu

Abstract

In this paper we construct a cyclically invariant Boolean function whose sensitivity is $\Theta(n^{1/3})$. This result answers two previously published questions. Turán (1984) asked if any Boolean function, invariant under some transitive group of permutations, has sensitivity $\Omega(\sqrt{n})$. Kenyon and Kutin (2004) asked whether for a "nice" function the product of 0-sensitivity and 1-sensitivity is $\Omega(n)$. Our function answers both questions in the negative.

We also prove that for minterm-transitive functions (a natural class of Boolean functions including our example) the sensitivity is $\Omega(n^{1/3})$. Hence for this class of functions sensitivity and block sensitivity are polynomially related.

1. Introduction

Cook, Dwork and Reischuk [1] originally introduced sensitivity as a simple combinatorial complexity measure for Boolean functions providing lower bounds on the time needed by a CREW PRAM. Nisan [3] introduced the concept of block sensitivity and demonstrated the remarkable fact that block sensitivity and CREW PRAM complexity are polynomially related. Whether block sensitivity and sensitivity are polynomially related is still an open question.

The largest known gap between them is quadratic, as shown by Rubinstein [4]. But for an arbitrary Boolean function the best known upper bound on block sensitivity in terms of sensitivity is exponential. H.-U. Simon [5] gave the best possible lower bound on sensitivity in terms of the number of effective variables. From that it follows that block sensitivity of a function f is $O(s(f)4^{s(f)})$, where $s(f)$ is the sensitivity of the function f. Kenyon and Kutin [2] gave the best known upper bound on block sensitivity in terms of sensitivity; their bound is $O\left(\frac{e}{\sqrt{2\pi}}e^{s(f)}\sqrt{s(f)}\right)$.

Nisan pointed out [3] that for *monotone* Boolean functions sensitivity and block sensitivity are equal.

A natural direction in the study of the gap between sensitivity and block sensitivity is to restrict attention to Boolean functions with symmetry. We note that a slight modification of Rubinstein's construction (Example 2.13) gives a Boolean function, invariant under the cyclic shift of the variables, which still shows the quadratic gap between sensitivity and block sensitivity. Turán pointed out [6] that for *symmetric* functions (functions invariant under all permutations of the variables), block sensitivity is within a factor of two of sensitivity. For any non-trivial *graph property* (the $n = \binom{V}{2}$ variables indicate the adjacency relation among the V vertices), Turán [6] proved that sensitivity is at least $V = \Theta(\sqrt{n})$ and therefore the gap is at most quadratic. In the same paper he also asked the following question:

Problem (Turán, 1984): *Does a lower bound of similar order hold still if we generalize graph properties to Boolean functions invariant under a transitive group of permutations?*

In Section 3 we give a cyclically invariant function with sensitivity $\Theta(n^{1/3})$. This example gives a negative answer to Turán's question.

Kenyon and Kutin [2] observed that for "nice" functions the product of 0-sensitivity and 1-sensitivity tends to be linear in the input length. Whether this observation extends to all "nice" functions was given as a (vaguely stated) open problem in that paper. In Section 3 we also construct a cyclically invariant Boolean function for which the product of 0-sensitivity and 1-sensitivity is $\Theta(\sqrt{n})$. Thus our function also gives a counterexample to Kenyon and Kutin's suggestion.

In Section 2.1 we define a natural class of Boolean functions called the minterm-transitive functions. It contains our new functions (that we give in Section 3). In Section 4 we prove that for minterm-transitive functions sensitivity is $\Omega(n^{1/3})$ (where n is the input size) and the product of 0-sensitivity and 1-sensitivity is $\Omega(\sqrt{n})$. Thus for this class of functions sensitivity and block sensitivity are polynomially related.

2. Preliminaries

2.1. Definitions

We use the notation $[n] = \{1, 2, 3, ..., n\}$. Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function. We call the elements of $\{0,1\}^n$ "words." For any word x and $1 \leq i \leq n$ we denote by x^i the word obtained by switching the ith bit of x. For a word x and $A \subseteq [n]$ we use x^A to denote the word obtained from x by switching all the bits in A. For a word $x = x_1, x_2, ..., x_n$ we define $\mathrm{supp}(x)$ as $\{i \mid x_i = 1\}$. Weight of x, denoted $\mathrm{wt}(x)$, is $|\mathrm{supp}(x)|$, *i.e.*, number of 1s in x.

Definition 2.1 The *sensitivity* of f on the word x is defines as the number of bits on which the function is sensitive: $s(f,x) = |\{i : f(x) \neq f(x^i)\}|$.

We define the *sensitivity* of f as $s(f) = \max\{s(f,x) : x \in \{0,1\}^n\}$

We define *0-sensitivity* of f as $s^0(f) = \max\{s(f,x) : x \in \{0,1\}^n, f(x) = 0\}$

We define *1-sensitivity* of f as $s^1(f) = \max\{s(f,x) : x \in \{0,1\}^n, f(x) = 1\}$.

Definition 2.2 The *block sensitivity* $bs(f,x)$ of a function f on an input x is the maximum number of disjoint subsets $B_1, B_2, ..., B_r$ of $[n]$ such that for all j, $f(x) \neq f(x^{B_j})$.

The *block sensitivity* of f, denoted $bs(f)$, is $\max_x bs(f,x)$.

Definition 2.3 A *partial assignment* is a function $p : S \to \{0,1\}$ where $S \subseteq [n]$. We call S the support of this partial assignment. The weight of a partial assignment is the number of elements in S that are mapped to 1. We call x a (full) assignment if $x : [n] \to \{0,1\}$. (Note than any word $x \in \{0,1\}^n$ can be thought of as a full assignment.) We say $p \subseteq x$ if x is an extension of p, *i.e.*, the restriction of x to S denoted $x|_S = p$.

Definition 2.4 A *1-certificate* is a partial assignment, $p : S \to \{0,1\}$, which forces the value of the function to 1. Thus if $x|_S = p$ then $f(x) = 1$.

Definition 2.5 If $\mathcal{F}$ is a set of partial assignments then we define $m_\mathcal{F} : \{0,1\}^n \to \{0,1\}$ as $m_\mathcal{F}(x) = 1 \iff (\exists p \in \mathcal{F})$ such that $(p \subseteq x)$.

Note that each member of $\mathcal{F}$ is a 1-certificate for $m_\mathcal{F}$ and $m_\mathcal{F}$ is the unique smallest such function. (Here the ordering is pointwise, *i.e.*, $f \leq g$ if for all x we have $f(x) \leq g(x)$).

Definition 2.6 A *minterm* is a minimal 1-certificate, that is, no sub-assignment is a 1-certificate.

Definition 2.7 Let $S \subseteq [n]$ and let $\pi \in S_n$. Then we define S^π to be $\{\pi(i) \mid i \in S\}$.

Let G be a permutation group acting on $[n]$. Then the sets S^π, where $\pi \in G$, are called the *G-shifts* of S. If $p : S \to \{0,1\}$ is a partial assignment then we define $p^\pi : S^\pi \to \{0,1\}$ as $p^\pi(i) = p(\pi^{-1}i)$.

Definition 2.8 Let G be a subgroup of S_n, *i.e.*, a permutation group acting on $[n]$. A function $f : \{0,1\}^n \to \{0,1\}$ is said to be *invariant under the group G* if for all permutations $\pi \in G$ we have $f(x^\pi) = f(x)$ for all $x \in \{0,1\}^n$.

Definition 2.9 Let $x = x_1 x_2 ... x_n \in \{0,1\}^n$ be a word. Then for $0 < \ell < n$, we denote by $cs_\ell(x)$ the word $x_{\ell+1}x_{\ell+2}...x_n x_1 x_2 ... x_\ell$, *i.e.*, the *cyclic shift* of the variables of x by ℓ positions.

Definition 2.10 A function $f : \{0,1\}^n \to \{0,1\}$ is called *cyclically invariant* if $f(x) = f(cs_1(x))$ for all $x \in \{0,1\}^n$.

Note that a cyclically invariant function is invariant under the group of cyclic shifts.

Proposition 2.11 *Let G be a permutation group. Let $p : S \to \{0,1\}$ be a partial assignment and let $\mathcal{F} = \{p^\pi \mid \pi \in G\}$. Then p is a minterm for the function $m_\mathcal{F}$.*

The function $m_\mathcal{F}$ will be denoted p^G. Note that the function p^G is invariant under the group G. When G is the group of cyclic shifts we denote the function p^{cyc}. The function p^{cyc} is cyclically invariant.

Proof of Proposition 2.11: If p has k zeros then for any word x with fewer than k zeros $m_\mathcal{F}(x) = 0$, since all the element of $\mathcal{F}$ has same number of 1s and 0s. But if q is a 1-certificate with fewer than k zeros we can have a word x by extending q to a full assignment by filling the rest with 1s, satisfying $f(x) = 1$ (since $q \subseteq x$). But x contains fewer than k zeros, a contradiction. So no minterm of $m_\mathcal{F}$ has fewer than k zeros.

Similarly no minterm of $\mathcal{F}$ has weight less than p. So no proper sub-assignment of p can be a 1-certificate. Hence p is a minterm of $m_\mathcal{F}$. ■

Definition 2.12 Let G be a permutation group on $[n]$. G is called *transitive* if for all $1 \leq i, j \leq n$ there exists a $\pi \in G$ such that $\pi(i) = j$.

Definition 2.13 Let $C(n,k)$ be the set of Boolean functions f on n variables such that there exists a partial assignment $p : S \to \{0,1\}$ with support $k (\neq 0)$ for which $f = p^{cyc}$. Let $C(n) = \cup_{k=1}^n C(n,k)$. We will call the functions in $C(n)$ **minterm-cyclic**. These are the simplest cyclically invariant functions.

Definition 2.14 Let G be a permutation group on $[n]$. We define $D_G(n,k)$ (for $k \neq 0$) to be the set of Boolean functions f on n variables such that there exists a partial assignment $p : S \to \{0,1\}$ with support k for which $f = p^G$. We define $D_G(n)$ to be $\cup_{k=1}^n D_G(n,k)$. This is a class of simple G-invariant Boolean functions. We define $D(n)$ to be $\cup_G D_G(n)$ where G ranges over all transitive groups. We call these functions **minterm-transitive**. Note that the class of minterm-cyclic functions is a subset of the class of minterm-transitive functions.

2.2. Previous Results

The largest known gap between sensitivity and block sensitivity is quadratic, given by Rubinstein [4]. Although Rubinstein's example is not cyclically invariant, the following slight modification is cyclically invariant with a similar gap between sensitivity and block sensitivity.

Example 2.15 *Let $g : \{0,1\}^k \to \{0,1\}$ be such that $g(x) = 1$ iff x contains two consecutive ones and the rest of the bits are 0. In function $f' : \{0,1\}^{k^2} \to \{0,1\}$ the variables are divided into groups $B_1, \ldots, B_k$ each containing k variables. $f'(x) = g(B_1) \vee g(B_2) \vee \cdots \vee g(B_k)$. Using f' we define the function $f : \{0,1\}^{k^2} \to \{0,1\}$ as $f(x) = 1$ iff $f(x') = 1$ for some x' which is a cyclic shift of x. The sensitivity of f is $2k$ while the block sensitivity is $\lfloor \frac{k^2}{2} \rfloor$.*

Hans-Ulrich Simon [5] proved that for any function f we have $s(f) \geq (\frac{1}{2}\log n - \frac{1}{2}\log\log n + \frac{1}{2})$, where n is the number of effective variables (the ith variable is effective if there exist some word x for which $f(x) \neq f(x^i)$). This bound is tight. Although for various restricted classes of functions better bounds are known.

Let $f : \{0,1\}^m \to \{0,1\}$ be a Boolean function that takes as input the adjacency matrix of a graph G and evaluates to 1 iff the graph G has a given property. So the input size m is $\binom{|V|}{2}$ where $|V|$ is the number of vertices in the graph G. Also $f(G) = f(H)$ whenever G and H are isomorphic as graphs. Such a function f is called a *graph property*. György Turán [6] proved that non-trivial graph properties have sensitivity $\Omega(\sqrt{m})$.

A function f is called *monotone* if $f(x) \leq f(y)$ whenever $\text{supp}(x) \subseteq \text{supp}(y)$. Nisan[3] pointed out that for monotone functions sensitivity and block sensitivity are the same.

In the definition of block sensitivity (Definition 2.2) if we restrict the block size to be at most ℓ then we obtain the concept of ℓ-block sensitivity of the function f, denoted $s_\ell(f)$. In [2] Kutin and Kenyon introduced this definition and proved that $bs_\ell(f) \leq c_\ell s(f)^\ell$ where c_ℓ is a constant depending on ℓ.

3. The new functions

In this section we will construct a cyclically invariant Boolean function which has sensitivity $\Theta(n^{1/3})$ and a cyclically invariant function for which the product of 0-sensitivity and 1-sensitivity is $\Theta(\sqrt{n})$.

Theorem 3.1 *There is a cyclically invariant function, $f : \{0,1\}^n \to \{0,1\}$, such that, $s(f) = \Theta(n^{1/3})$.*

Theorem 3.2 *There is a cyclically invariant function, $f : \{0,1\}^n \to \{0,1\}$, such that, $s^0(f)s^1(f) = \Theta(\sqrt{n})$.*

For proving the above theorems we will first define an auxiliary function g on k^2 variables ($k^2 \leq n$). Then we use g to define our new minterm-cyclic function f on n variables. If we set $k = \lfloor n^{1/3} \rfloor$, Theorem 3.1 will follow. Theorem 3.2 follows by setting $k = \lfloor \sqrt{n} \rfloor$.

3.1. The auxiliary function

We first define $g : \{0,1\}^{k^2} \to \{0,1\}$ where $k^2 \leq n$. We divide the input into k blocks of size k each. We define g by a regular expression.

$$g(z) = 1$$
$$\Updownarrow$$
$$z \in \underbrace{110^{k-2}}_{k}\underbrace{(11111(0+1)^{k-5})}_{k}{}^{k-2}\ \underbrace{11111(0+1)^{k-8}111}_{k}$$

We call this regular expression $\mathcal{R}$.

In other words, let $z \in \{0,1\}^{k^2}$ and let $z = z_1 z_2 ... z_k$, where each $z_i \in \{0,1\}^k$ for all $1 \leq i \leq k$, *i.e.*, z is broken up into k blocks of size k each. Then $g(z) = 1$ iff $z_1 = (11\underbrace{00...0}_{k-2})$ and for all $2 \leq j \leq k$ the first five bits of z_j are 1 and also the last 3 bits of z_k are 1. Note that g does not depend on the rest of the bits.

3.2. The new function

Now we define the function f using the auxiliary function g. Let $x|_{[m]}$ denote the word formed by the first m bits of x. Let us set

$$f(x) = 1 \iff \exists \ell \text{ such that } g\left(cs_\ell(x)|_{[k^2]}\right) = 1.$$

In other words, viewing x as laid out on a cycle, $f(x) = 1$ iff x contains a contiguous substring y of length k^2 on which $g(y) = 1$.

In other words, let $z \in \{0,1\}^{k^2}$ and let $z = z_1 z_2 ... z_k$, where each $z_i \in \{0,1\}^k$ for all $1 \leq i \leq k$, *i.e.*, z is broken up into k blocks of size k each. Then $g(z) = 1$ iff $z_1 = (11\underbrace{00...0}_{k-2})$ and for all $2 \leq j \leq k$ the first five bits of z_j are 1 and also the last 3 bits of z_k are 1. Note that g does not depend on the rest of the bits.

3.3. Properties of the new function

It follows directly from the definition that f is a cyclically invariant Boolean function.

It is important to note that the function g is so defined that the value of g on input z depends only on $(6k-2)$ bits of z.

Also note that the pattern defining g is so chosen that if $g(z)=1$ then there is exactly one set of consecutive $(k-2)$ zeros in z and no other set of consecutive $(k-4)$ zeros.

Claim 3.3 *The function f has (a) 1-sensitivity $\Theta(k)$ and (b) 0-sensitivity $\Theta(\frac{n}{k^2})$*

Proof of Claim: (a) Let x be a word such that the first k^2 bits are of the form (1) and the rest of the bits are 0. Now clearly $f(x)=1$. Also it is easy to see that on this input x 1-sensitivity of f is $(6k-2)$ and therefore $s^1(f)=\Omega(k)$.

Now let $x \in \{0,1\}^n$ be such that $f(x)=1$ and there exists $1 \le i \le n$ such that $f(x^i)=0$. But $f(x)=1$ implies that some cyclic shift of x contains a contiguous substring z of length k^2 of the form (1) (i. e., $g(z)=1$). But since g depends only on the values of $(6k-2)$ positions so one of those bits has to be switched so that f evaluates to 0. Thus $s^1(f)=O(k)$.

Combined with the lower bound $s^1(f)=\Omega(k)$ we conclude $s^1(f)=\Theta(k)$.

(b) Let $\lfloor \frac{n}{k^2} \rfloor = m$ and $r = (n-k^2m)$. Let $x = (1\underline{0}0^{k-2}(111110^{k-5})^{k-2}111110^{k-8}111)^m0^r$. Then $f(x)=0$ since no partial assignment of the form (1) exists in x. But if we switch any of the underlined zero the function evaluates to 1. Note that the function is not sensitive on any other bit. So on this input x the 0-sensitivity of f is $m=\lfloor \frac{n}{k^2} \rfloor$ and therefore $s^0(f)=\Omega(\frac{n}{k^2})$.

Now let $x \in \{0,1\}^n$ and assume $f(x)=0$ while $f(x^i)=1$ for some $1 \le i \le n$. By definition, the 0-sensitivity of f is the number of such values of i. For each such i there exists a partial assignment $z_i \subseteq x^i$ of the form $\mathcal{R}$ (defined in Section 3.1). So z_i is a contiguous substring of x^i (or some cyclic shift of x^i) of length k^2. Now consider the $z_i^i \subseteq x$ (recall z_i^i denotes the partial assignment obtained by switching the ith bit of z_i). Due to the structure of the pattern $\mathcal{R}$ z_i has exactly one set of consecutive $(k-2)$ zeros. So z_i^i either has exactly one set of consecutive $(k-1)$ zeros or exactly one set of consecutive $(k-2)$ zeros or exactly one set of consecutive $(k-2)$ bits with at most one of the bits being 1 while the remaining bits are zero. So the supports of any two z_i^i either have at least (k^2-1) positions in common or they have at most two positions in common (since the pattern $\mathcal{R}$ begins and ends with 11). Hence the number of distinct z_i^i is at most $\Theta(\frac{n}{k^2})$. Hence we have $s^0(f)=O(\frac{n}{k^2})$.

Combined with the lower bound $s^0(f)=\Omega(\frac{n}{k^2})$ we conclude that $s^0(f)=\Theta(\frac{n}{k^2})$. ∎

Proof of Theorem 3.1: From Claim 3.3 it follows $s(f) = \max\left\{\Theta(k), \Theta(\frac{n}{k^2})\right\}$ (since $s(f)=\max s^0(f), s^1(f)$). So if we set $k=\lfloor n^{1/3} \rfloor$ we obtain $s(f)=\Theta(n^{1/3})$. ∎

Proof of Theorem 3.2: From Claim 3.3 we obtain $s^0(f)s^1(f) = \Theta(\frac{n}{k})$. So if we set $k=\lfloor\sqrt{n}\rfloor$ we have $s^0(f)s^1(f)=\Theta(\sqrt{n})$. ∎

Theorem 3.1 answers Turán's problem [6] (see the Introduction) in the negative. In [2], Kenyon and Kutin asked whether $s^0(f)s^1(f)=\Omega(n)$ holds for all "nice" functions f. Although they do not define "nice," arguably our function in Theorem 3.2 is nice enough to answer the Kenyon-Kutin question in the negative.

In the next section we prove that for a minterm-transitive function, sensitivity is $\Omega(n^{1/3})$ and the product of 0-sensitivity and 1-sensitivity is $\Omega(\sqrt{n})$. Hence our examples are tight.

4. Minterm-transitive functions have sensitivity $\Omega(n^{1/3})$

Theorem 4.1 *If f is a minterm-transitive function on n variables then $s(f)=\Omega(n^{1/3})$ and $s^0(f)s^1(f)=\Omega(\sqrt{n})$.*

To prove this theorem we will use the following three lemmas. Since f is a minterm-transitive function, *i. e.*, $f \in D(n)$, we can say $f \in D_G(n,k)$ for some transitive group G and some $k \neq 0$.

Lemma 4.2 *If $f \in D_G(n,k)$ then $s^1(f) \ge \frac{k}{2}$.*

Proof: Let y be the minterm defining f. Without loss of generality $\mathrm{wt}(y) \ge \frac{k}{2}$. Let us extend y to a full assignment x by assigning zeros everywhere outside the support of y. Then switching any 1 to 0 changes the value of the function from 1 to 0. So we obtain $s(f,x) \ge \frac{k}{2}$. Hence $s^1(f) \ge \frac{k}{2}$. ∎

Lemma 4.3 *If S is a subset of $[n]$, $|S|=k$ then there exist at least $\frac{n}{k^2}$ disjoint G-shifts of S.*

Proof: Let T be a maximal union of G-shifts of S. Since T is maximal T hits all G-shifts of S. Let H_{ij} be the subgroup of G that sends ith bit of the minterm to the bit position j. So the bit position j can at most hit $\sum_{i=1}^{k}|H_{ij}|$ many G-shifts of S. Since G is transitive for all i and j we have $|H_{ij}| \le \frac{|G|}{n}$. Therefore $\forall j$, $\sum_{i=1}^{k}|H_{ij}| \le k\frac{|G|}{n}$. That is each bit position hits at most $k\frac{|G|}{n}$ many G-shifts of S. But there are $|G|$ different G-shifts of S. So we must have $|T| \ge \frac{n}{k}$. Hence T must be a union of at least $\frac{n}{k^2}$ disjoint G-shifts of S. And this proves the lemma. ∎

Lemma 4.4 *If $f \in D_G(n,k)$ then $s^0(f)=\Omega(\frac{n}{k^2})$.*

Proof: Let y be the minterm defining f. By Lemma 4.3 we can have $\Omega(\frac{n}{k^2})$ disjoint G-shifts of y. The union of these disjoint G-shifts of y defines a partial assignment. Let $S = \{s_1, s_2, ..., s_r\}$ be the support of the partial assignment. And let Y_{s_i} be the value of the partial assignment in the s_i-th entry.

Since $k \neq 0$ the function f is not a constant function. Thus there exists a word z such that $f(z) = 0$. The i-th bit of z is denoted by z_i. We define,

$$T = \{j \,|\, z_j \neq Y_{s_m}, s_m = j\}$$

Now let $P \subseteq T$ be a maximal subset of T such that $f(z^P) = 0$. Since P is maximal, if we switch any other bit in $T \backslash P$ the value of the function f will change to 1.

So $s(f, z^P) \geq |(T \backslash P)|$. Now since $f(z^P) = 0$ we note that z^P does not contain any G-shift of y. But from Lemma 4.3 we know that z^T contains $\Omega(\frac{n}{k^2})$ disjoint G-shifts of y. So $|(T \backslash P)|$ is $\Omega(\frac{n}{k^2})$ and thus $s^0(f) \geq s(f, z^P) = \Omega(\frac{n}{k^2})$. ■

Proof of Theorem 4.1: From the Lemma 4.2 and Lemma 4.4 we obtain,

$$s(f) = \max\{s^0(f), s^1(f)\} = \max\left\{\Omega\left(\frac{n}{k^2}\right), \frac{k}{2}\right\}.$$

This implies $s(f) = \Omega(n^{1/3})$.

Now since $s^0(f)$ and $s^1(f)$ cannot be smaller than 1, it follows from the Lemma 4.2 and 4.4 that

$$s^0(f)s^1(f) = \max\left\{\Omega\left(\frac{n}{k}\right), \frac{k}{2}\right\}.$$

So $s^0(f)s^1(f) = \Omega(\sqrt{n})$. ■

The new function we looked at in Theorem 3.1 is minterm-transitive and has sensitivity $\Theta(n^{\frac{1}{3}})$. Thus this lower bound on sensitivity is tight for minterm-transitive functions. Similarly for the function in Theorem 3.2 the product of 0-sensitivity and 1-sensitivity is tight.

We can even give tight upper bound on block sensitivity for minterm-transitive functions in terms of sensitivity.

Theorem 4.5 *For a minterm-transitive function $f : \{0,1\}^n \to \{0,1\}$ we have $s(f) \geq \frac{bs(f)}{k}$, where k is the size of the minterm.*

Proof: Let x is the word for which the block sensitivity is $bs(f)$. Now let the minimal blocks be $B_1, B_2, \cdots, B_{bs(f)}$. By definition $f(x^{B_i}) \neq f(x)$. That means x^{B_i} has at least one minterm. Choose any minterm. Now that minterm can intersect at most k of the blocks. Drop those blocks from the set of blocks. Do it for all the blocks. Finally at least $\frac{bs(f)}{k}$ of the blocks are left. Let the union of these blocks be B. The blocks have the property that if we switch any block a minterm will be formed that does not intersects any other block.

Now let $A \subset B$ be the maximal set such that $f(x^A) = f(x)$. So x^A has sensitivity more than $B \backslash A$. And $B \backslash A$ must have have at least one bit from all the blocks because if any block is switched fully then a minterm is formed because the minterm does not intersect any other block. So $|B \backslash A| \geq \frac{(bs(f)}{k}$. Hence $s(f, x^A) \geq \frac{bs(f)}{k}$. ■

Corollary 4.6 *For miniterm-transitive function, $bs(f) \leq s(f)^2$.*

Hence for minterm-transitive functions, sensitivity and block sensitivity does not have a gap of more than quadratic. And this is tight.

5. Open Problems

The main question in this field is still open: Are sensitivity and block sensitivity polynomially related? Can the gap between them be more than quadratic? The following variant of Turán's question remains open:
Problem: If f is a Boolean function invariant under a transitive group of permutations then is it true that $s(f) \geq n^c$ for some constant $c > 0$?

Acknowledgements

I thank László Babai and Sandy Kutin for giving me lots of useful ideas and suggestions. I also thank Nanda Raghunathan for helpful discussions. Sandy Kutin helped me simplify the proof of Lemma 4.4.

References

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

[2] C. Kenyon and S. Kutin. Sensitivity, block sensitivity, and ℓ-block sensitivity of boolean functions. *Information and Computation*, 189(1):43–53, 2004.

[3] N. Nisan. Crew prams and decision trees. *SIAM J. Comput.*, 20(6):999–1070, 1991.

[4] D. Rubinstein. Sensitivity vs. block sensitivity of boolean functions. *Combinatorica*, 15(2):297–299, 1995.

[5] H.-U. Simon. A tight $\omega(\log\log n)$-bound on the time for parallel ram's to compute nondegenerated boolean functions. *FCT, Lecture notes in Comp. Sci*, 4(158), 1983.

[6] G. Turán. The critical complexity of graph properties. *Inform. Process. Lett.*, 18:151–153, 1984.