On the sensitivity of cyclically-invariant Boolean functions

Sourav Chakraborty

To cite this version:

Sourav Chakraborty. On the sensitivity of cyclically-invariant Boolean functions. Discrete Mathematics and Theoretical Computer Science, DMTCS, 2011, Vol. 13 no. 4 (4), pp.51–60. hal-00990492

HAL Id: hal-00990492
https://hal.inria.fr/hal-00990492

Submitted on 13 May 2014

On the sensitivity of cyclically-invariant Boolean functions

Sourav Chakraborty[1]†

[1] *Chennai Mathematical Institute, Chennai, India*

received 29th July 2010, revised 17th May 2011, accepted 20th May 2011.

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.

Keywords: sensitivity, cyclically invariant functions

1 Introduction

Cook, Dwork and Reischuk Cook et al. (1986) originally introduced sensitivity as a simple combinatorial complexity measure for Boolean functions providing lower bounds on the time needed by a CREW PRAM. Nisan Nisan (1991) 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. So far the quadratic gap found by Rubinstein Rubinstein (1995) is the largest known. But for an arbitrary Boolean function the best known upper bound on block sensitivity in terms of sensitivity is exponential. H.-U. Simon Simon (1983) 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 Kenyon and Kutin (2004) 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 Nisan (1991) 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

†Email: `sourav@cmi.ac.in`. Major part of the work was done when the author was a graduate student in University of Chicago. Some of the results in this paper appeared in Chakraborty (2005)

(Example 2.15) 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 Turán (1984) 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 Turán (1984) 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 Kenyon and Kutin (2004) 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 class of Boolean functions called the minterm-transitive functions (Definition 2.14). This class of function is a subclass of the class of functions *invariant under some transitive group* (Definition 2.8) and 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 $\Omega(\sqrt{n})$. We also show that for this class of functions the sensitivity and block sensitivity is quadratically related. Our lower bound results generalizes to some bigger classes of Boolean functions (Section 5).

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 supp(x) as $\{i \mid x_i = 1\}$. Weight of x, denoted wt(x), is $|\text{supp}(x)|$, *i.e.*, number of 1s in x.

Definition 2.1 The *sensitivity* of f on the word x is defined 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 by $bs(f)$, is $\max_x bs(f, x)$.

	Best known lower bound on sensitivity†	Least sensitivity for which an example is known
General Functions	$(\frac{1}{2}\log m - \frac{1}{2}\log\log m + \frac{1}{2})$	$\frac{1}{2}\log n + \frac{1}{4}\log\log n + O(1)$
Symmetric Functions	$\lceil\frac{n+1}{2}\rceil$	$\lceil\frac{n+1}{2}\rceil$
Monotone Functions	$(\frac{1}{2}\log m - \frac{1}{2}\log\log m + \frac{1}{2})$	$\frac{1}{2}\log n + \frac{1}{4}\log\log n + O(1)$
Graph Properties on graphs with vertex set V	$\lfloor\frac{\lvert V\rvert}{2}\rfloor$	$(\lvert V\rvert - 1)$
Cyclically Invariant Functions	$(\frac{1}{2}\log n - \frac{1}{2}\log\log n + \frac{1}{2})$	$\Theta(n^{1/3})$
Minterm Transitive Functions	$(2n)^{1/3}$	$\Theta(n^{1/3})$

† For the lower bounds m denotes the number of relevant indices. An index i is said to be relevant for f if there exist $x \in \{0,1\}^n$ such that $f(x) \neq f(x^i)$.

Tab. 1: Current knowledge about sensitivity of some classes of Boolean functions

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 be 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 if p has k' ones then no minterm of $\mathcal{F}$ can have less than k' ones. 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 $1 \le i, j \le n$ 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 Rubinstein (1995). 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* $B_1, \dots, B_k$ *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 Simon (1983) 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 Turán (1984) proved that non-trivial graph properties have sensitivity $\Omega(\sqrt{m})$.

A function f is called *monotone* if $f(x) \leq f(y)$ whenever $\mathrm{supp}(x) \subseteq \mathrm{supp}(y)$. NisanNisan (1991) 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 Kenyon and Kutin (2004) 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.

Recently Sun Sun (2006) proved that for functions that are invariant under some transitive group action the block sensitivity is at least $n^{1/3}$ and they gave an example of a function that has block sensitivity $O(n^{3/7}\log n)$.

Table 1 gives a list of classes of Boolean functions and the current knowledge of sensitivity for these classes of functions.

3 Cyclically Invariant Function with Sensitivity $\Theta(n^{1/3})$

In this section we will construct a cyclically invariant Boolean function which has sensitivity $\Theta(n^{1/3})$. We will also construct 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 $g(y) = 1$.

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 3.3: (a) Let x be the following word:

$$(110^{k-2}(111110^{k-5})^{k-2}111110^{k-8}111)0^{n-k^2}$$

Note that $f(x) = 1$. Also it is easy to see that on this input x 1-sensitivity of f is at least $(6k-2)$.

Now let $x \in \{0,1\}^n$ be such that $f(x) = 1$. Now $f(x) = 1$ implies that some cyclic shift of x contains a contiguous substring z of length k^2 such that $g(z) = 1$. 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 $s^1(f) \leq 6k-2$.

Combined with the lower bound $s^1(f) \geq 6k-2$ we conclude $s^1(f) = \Theta(k)$.

(b) Let $\lfloor \frac{n}{k^2} \rfloor = m$ and $r = (n - k^2 m)$. Let x be

$$(1\underline{0}0^{k-2}(111110^{k-5})^{k-2}111110^{k-8}111)^m 0^r$$

Note that $f(x) = 0$. 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 $s^0(f) \geq \frac{n}{k^2} - 1$.

Now let $x \in \{0,1\}^n$ and assume $f(x) = 0$ while $f(x^i) = 1$ for some $1 \leq i \leq n$. By definition, the 0-sensitivity of f is the number of such i. For each such i there exists a contiguous substring z_i of length k^2 of some cyclic shift of x^i such that $g(z_i) = 1$. 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 $\mathcal{R}$ we note that 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 have at most three 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 $s^0(f) \geq \frac{n}{k^2}$ we conclude that $s^0(f) = \Theta(\frac{n}{k^2})$. □

Proof of Theorem 3.1:: From Claim 3.3 it follows $s(f) = \max\left\{\Theta(k), \Theta(\frac{n}{k^2})\right\}$. 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 Turán (1984) (see the Introduction) in the negative. In Kenyon and Kutin (2004), 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 $\Omega(\sqrt{n})$. Since our example for Theorem 3.1 is also a minterm-transitive function, so our example is the best one can hope for with minterm-transitive functions.

4 Lower Bound on Sensitivity for Some Classes of Boolean Functions

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 $s^1(f) \geq \frac{k}{2}$.*

Proof: Let y be the minterm defining f. Without loss of generality $\mathrm{wt}(y) \geq \frac{k}{2}$. 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 $s(f,x) \geq \frac{k}{2}$. Hence $s^1(f) \geq \frac{k}{2}$. □

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 disjoint G-shifts of S. Since T is maximal, T hits all G-shifts of S, that is, for all $\pi \in G$ we have $T \cap S^\pi \neq \emptyset$. Let H_{ij} be the subset of G that sends the 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, that is

$$|\{\pi \in G \mid j \in S^\pi\}| \leq \sum_{i=1}^{k} |H_{ij}|.$$

Since G is transitive, for all i and j we have $|H_{ij}| \leq \frac{|G|}{n}$. Therefore $\forall j$, $\sum_{i=1}^{k} |H_{ij}| \leq k\frac{|G|}{n}$. That is each bit position j

$$|\{\pi \in G \mid j \in S^\pi\}| \leq k\frac{|G|}{n}.$$

But there are $|G|$ elements in G. So we must have $|T| \geq \frac{n}{k}$. 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 *Let $f : \{0,1\}^n \to \{0,1\}$ be a non-constant Boolean function invariant under a transitive group G. Let $S \subseteq [n]$ and let $p : S \to \{0,1\}$ be a 1-certificate of f. If the support of p has size k (i.e. $|S| = k$), then $s^0(f) \geq \frac{n}{k^2}$.*

Proof: By Lemma 4.3 we can have $\frac{n}{k^2}$ disjoint G-shifts of p. The union of these disjoint G-shifts of p defines a partial assignment. Let $\hat{S} = \{s_1, s_2, ..., s_r\}$ 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 the function f is not a constant function, there exists a word z such that $f(z) = 0$. The i-th bit of z is denoted by z_i. We define,

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

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 p. But from Lemma 4.3 we know that z^T contains $\frac{n}{k^2}$ disjoint G-shifts of p. So $|(T\backslash P)|$ is at least $\frac{n}{k^2}$ and thus $s^0(f) \geq s(f, z^P) = \frac{n}{k^2}$. □

Corollary 4.5 *If $f \in D_G(n,k)$ then $s^0(f) \geq \frac{n}{k^2}$.*

Proof of Theorem 4.1: From the Lemma 4.2 and Corollary 4.5 we obtain,

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

This implies $s(f) \geq (2n)^{1/3}$.

Now since $s^0(f)$ and $s^1(f)$ cannot be smaller than 1, it follows from the Lemma 4.2 and Lemma 4.5 that

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

So $s^0(f)s^1(f) \geq \sqrt{n}$. □

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 4.6 *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 be the word for which the block sensitivity is $bs(f)$. Also let us assume that $k \geq 2$ as if the size of the minterm is 1 then then the function becomes trivial with $s(f) = bs(f) = n$.

If $f(x) = 1$ then x must have at least one minterm. And then any sensitive block must touch that minterm. In that case $bs(f)$ is at most the size of the minterm, that is k. On the other hand since f is minterm-transitive so $s(f)$ is at least the $k/2$ (from Lemma 4.2). And so if $f(x) = 1$ then

$$s(f) \geq k/2 \geq bs(f)/2 \geq bs(f)/k.$$

Now lets consider the case when $f(x) = 0$. 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 $(k-1)$ other blocks. By Turan's theorem of independence number of sparse graphs we obtain $\frac{bs(f)}{k}$ blocks such that if we switch any block a minterm will be formed that does not intersects any other block. Let the union of these blocks be B.

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

Proof: Follows from Theorem 4.6 and Lemma 4.2. □

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

5 Generalization of the Results and Open Problems

Note that Lemma 4.4 holds for any function invariant under some transitive group. But unfortunately the proof of Lemma 4.2 does not generalizes for all functions closed under some transitive group action. But the proof of Lemma 4.2 uses the fact that all the minterms of the Boolean function have more than $k/2$ number of 0 or all of them more than $k/2$ number of 1. Thus for functions having that property we can prove a similar lemma and hence for these kind of functions the sensitivity is also $\Omega(n^{1/3})$.

For the proof of Theorem 4.6 the fact that is used is that all the minterms are of support less than k. So if a Boolean function, f, that is invariant under some transitive group, has all minterms of size k and weight at least (or at most) k/c for some constant c then the sensitivity of the function is $\Omega(n^{1/3})$

and $bs(f) = O(s(f)^2)$. In particular it is still open whether the best gap between sensitivity and block sensitivity of cyclically invariant functions is quadratic.

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 $s(f) = \Omega(n^c)$ 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

S. Chakraborty. On the sensitivity of cyclically invariant boolean functions. *Computational Complexity Conference (CCC)*, 2005.

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.

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

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

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

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.

X. Sun. Block sensitivity of weakly symmetric functions. *Proceedings of Theory and Applications of Models of Computation*, pages 339–344, 2006.

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