Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 384 (2007) 87–91
Theoretical Computer Science
www.elsevier.com/locate/tcs

Block sensitivity of weakly symmetric functions

Xiaoming Sun*

Center for Advanced Study, Tsinghua University, Beijing 100084, China

Abstract

Block sensitivity, which was introduced by Nisan [Noam Nisan, CREW PRAMs and decision trees, SIAM Journal on Computing 20 (6) (1991) 999–1007. Earlier version in STOC'89], is one of the most useful measures of Boolean functions. In this paper we investigate the block sensitivity of weakly symmetric functions (functions invariant under some transitive group action). We prove a $\Omega(N^{1/3})$ lower bound for the block sensitivity of weakly symmetric functions. We also construct a weakly symmetric function which has block sensitivity $\tilde{O}(N^{3/7})$.

Keywords: Boolean functions; Block sensitivity; Weakly symmetric functions

1. Introduction

For a Boolean function $f : \{0,1\}^N \to \{0,1\}$, the *block sensitivity* of f on input x is the maximum number b such that there are pair-wise disjoint subsets $B_1, \ldots, B_b$ of $[N]$ for which $f(x) \neq f(x^{(B_i)})$; here $x^{(B_i)}$ is the input obtained by flipping all the bits x_j that $j \in B_i$. We call each B_i a block. The *block sensitivity* of f, denoted by $bs(f)$, is $\max_x bs(f, x)$.

Nisan [5] introduced the concept of block sensitivity and proved tight bounds for computing f on a CREW PRAM in terms of $bs(f)$. It has been shown that block sensitivity is polynomially related to many other measures of complexity, such as decision tree complexity [5], polynomial degree [6], and quantum query complexity [1]. The relationship between block sensitivity and sensitivity complexity is still open. For more information about these complexity measures, see [2] for an excellent survey.

A Boolean function f is called *weakly symmetric* (or *transitive*) if there exists a transitive group[1] $\Gamma \subseteq S_N$ such that for all $\sigma \in \Gamma$, $f(x_1 \ldots x_N) = f(x_{\sigma(1)} \ldots f_{\sigma(N)})$. For example, symmetric functions, graph properties, and cyclically invariant functions are all weakly symmetric functions.

Much research have been done on different complexity measures of weakly symmetric functions. It is known that the certificate complexity $C(f) \geq \sqrt{N}$ (see [4] for example). Since the decision tree complexity $D(f) \geq C(f)$, so

* Corresponding address: Institute for Theoretical Computer Science (ITCS), Tsinghua University, FIT 1-203, 100084 Beijing, China. Tel.: +86 10 62792230.
E-mail address: xiaomings@tsinghua.edu.cn.

[1] A group $\Gamma \subseteq S_N$ is called *transitive* if $\forall i, j \in [N], \exists \sigma \in \Gamma, \sigma(i) = j$.

0304-3975/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2007.05.020

$D(f) = \Omega(\sqrt{N})$, and this bound is tight. Turán [9] proved that for graph property the sensitivity $s(f) = \Omega(\sqrt{N})$ and he conjectured that it is also true for weakly symmetric functions. Recently Chakraborty [3] disproved this conjecture by giving a certain class of cyclically invariant functions with sensitivity complexity $\Theta(N^{1/3})$. Sun, Yao, and Zhang [8] proved the quantum query complexity $Q(f) = \Omega(N^{1/4})$ for weakly symmetric functions. They also showed that this bound is tight (up to log N factor).

Nisan [6] showed that $bs(f) = \Omega(\sqrt{C(f)})$; this combined with $C(f) \geq \sqrt{N}$ implies $bs(f) = \Omega(N^{1/4})$ for weakly symmetric function. No better lower bound is known about block sensitivity. In this paper our main results are the following theorems:

Theorem 1. *For any nontrivial weakly symmetric function f, $bs(f) \geq N^{1/3}$.*

Theorem 2. *There exists a cyclically invariant function f such that $bs(f) = O(N^{3/7} \log N)$.*

2. Proof of Theorem 1

The following lemma [7] is used in the proof of Theorem 1. We denote by $w(x)$ the number of 1's in input x, and by $\sigma(x)$ the input $x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(N)}$.

Lemma 1 (*Rivest and Vuillemin [7]*). *If $\Gamma \subseteq S_N$ is transitive, then for any $x \in \{0,1\}^N$ and any $i \in \{1,\ldots,N\}$,*

$$w(x) \cdot |\{\sigma(x) : \sigma \in \Gamma\}| = N \cdot |\{\sigma(x) : \sigma \in \Gamma, \sigma(x)_i = 1\}|. \tag{1}$$

In order to make the paper self-contained, we give a proof of Lemma 1 here.

Proof. Consider a $|\{\sigma(x) : \sigma \in \Gamma\}| \times N$ matrix; each row is an element in $\{\sigma(x)|\sigma \in \Gamma\}$. The left side of Eq. (1) counts the number of 1's in the matrix by rows. Since Γ is transitive, each column of the matrix contains the same number of 1's. Therefore, the right side of Eq. (1) counts the number of 1's in the matrix by columns. Thus Eq. (1) holds. □

Corollary 1. *For any $x, y \in \{0,1\}^N$, if $w(x) \cdot w(y) < N$, then there exists a $\sigma \in \Gamma$, such that*

$$\{i \in [N] : \sigma(x)_i = 1\} \cap \{j \in [N] : y_j = 1\} = \emptyset.$$

Proof. Suppose that for any $\sigma \in \Gamma$,

$$\{i \in [N] : \sigma(x)_i = 1\} \cap \{j \in [N] : y_j = 1\} \neq \emptyset,$$

so

$$|\{i \in [N] : \sigma(x)_i = 1\} \cap \{j \in [N] : y_j = 1\}| \geq 1. \tag{2}$$

Let Γ' be the minimum subgroup of Γ such that $\{\sigma(x) : \sigma \in \Gamma'\} = \{\sigma(x) : \sigma \in \Gamma\}$; then, summing up Eq. (2) over all $\sigma \in \Gamma'$, we have

$$\sum_{\sigma \in \Gamma'} |\{i : \sigma(x)_i = 1\} \cap \{j : y_j = 1\}| \geq |\Gamma'| = |\{\sigma(x) : \sigma \in \Gamma\}|. \tag{3}$$

But on the other hand,

$$\begin{aligned} \sum_{\sigma \in \Gamma'} |\{i : \sigma(x)_i = 1\} \cap \{j : y_j = 1\}| &= \sum_{i : y_i = 1} |\{\sigma(x) : \sigma \in \Gamma', \sigma(x)_i = 1\}| \\ &= \sum_{i : y_i = 1} |\{\sigma(x) : \sigma \in \Gamma, \sigma(x)_i = 1\}| \\ &= w(y) \cdot |\{\sigma(x) : \sigma \in \Gamma, \sigma(x)_i = 1\}|. \end{aligned} \tag{4}$$

By Lemma 1 we know

$$|\{\sigma(x) : \sigma \in \Gamma, \sigma(x)_i = 1\}| = \frac{w(x) \cdot |\{\sigma(x) : \sigma \in \Gamma\}|}{N},$$

thus Eq. (4) implies that

$$\sum_{\sigma\in\Gamma'} |\{i : \sigma(x)_i = 1\} \cap \{j : y_j = 1\}| = w(y) \cdot \frac{w(x)|\{\sigma(x) : \sigma \in \Gamma\}|}{N}. \tag{5}$$

Combine inequality (3) with inequality (5), we obtain $w(x)w(y) \geq N$, which contradicts the hypothesis. □

Now the proof of Theorem 1 is as follows:

Proof of Theorem 1. Let f be a nontrivial weakly symmetric function. The transitive permutation group is Γ. We denote $\mathbf{0} = 00...0$. Without loss of generality, we assume that $f(\mathbf{0}) = 0$. Let B be a minimal subset such that $f(\mathbf{0}^{(B)}) = 1$, i.e. for any proper subset $B' \subset B$, we have $f(\mathbf{0}^{(B')}) = 0$. Thus flipping any x_i where $i \in B$ changes the value of $f(\mathbf{0}^{(B)})$. Therefore $bs(f, \mathbf{0}^{(B)}) \geq |B|$. If $|B| \geq N^{1/3}$; it is done, since $bs(f) \geq bs(f, \mathbf{0}^{(B)})$. In the following, we assume that $|B| < N^{1/3}$.

Since $w(\mathbf{0}^{(B)}) = |B| < N^{1/3}$, $w(\mathbf{0}^{(B)})w(\mathbf{0}^{(B)}) < N^{2/3} < N$, according to Corollary 1 there exists a $\sigma \in \Gamma$, that

$$\{i \in [N] : \sigma(\mathbf{0}^{(B)})_i = 1\} \cap \{i \in [N] : (\mathbf{0}^{(B)})_i = 1\} = \emptyset.$$

i.e. $\sigma(B) \cap B = \emptyset$, where $\sigma(B)$ denotes the set $\{\sigma(b) : b \in B\}$. Let $B_1 = B$, $B_2 = \sigma(B)$. Since

$$w(\mathbf{0}^{(B_1\cup B_2)})w(\mathbf{0}^{(B)}) = 2|B| \times |B| < 2N^{2/3} < N,$$

from Corollary 1 there exists a $\sigma' \in \Gamma$, $\sigma'(B) \cap (B_1 \cup B_2) = \emptyset$. Let $B_3 = \sigma'(B)$, then $B_3 \cap B_1 = B_3 \cap B_2 = \emptyset$. By repeating this argument, finally we can obtain $B_1, B_2, \ldots, B_{N^{1/3}}$, such that for each B_i, there exists a $\sigma_i \in \Gamma$ that $B_i = \sigma_i(B)$, and $\forall i \neq j$, $B_i \cap B_j = \emptyset$.

Now let us consider that $bs(f, \mathbf{0})$: $\{B_1, \ldots, B_{N^{1/3}}\}$ are pair-wise disjoint subsets, and for $i = 1, \ldots, N^{1/3}$,

$$f(\mathbf{0}^{(B_i)}) = f(\mathbf{0}^{(\sigma_i(B))}) = f(\sigma_i(\mathbf{0}^{(B)})) = f(\mathbf{0}^{(B)}) \neq f(\mathbf{0}),$$

the third "=" is due to the invariance of f under the group action of Γ, so $bs(f, \mathbf{0}) \geq N^{1/3}$. Therefore $bs(f) \geq N^{1/3}$. □

3. Proof of Theorem 2

We firstly construct a partial assignment which has a nice property, and then use it as the 1-certificate to define the Boolean function f.

Lemma 2. *For any large k, there exists a partial assignment $p : S \to \{0, 1\}$, $S \subseteq [100k^4 \log k]$, $|S| = O(k^3 \log k)$, such that for any four distinct integers $i_1, i_2, i_3, i_4 \in [k^4]$, there exist $s_1, s_2, s_3, s_4 \in S$ such that*

(1) $s_{j_1} - s_{j_2} = i_{j_1} - i_{j_2}$ $(\forall j_1, j_2 = 1, 2, 3, 4)$*;*

(2) *the multiset $\{p(s_1), p(s_2), p(s_3), p(s_4)\}$ contains two 0's and two 1's.*

We meet the requirement (1) by a combinatorial design, and then use probabilistic arguments to show that we can assign $\{0, 1\}$ to the set to satisfy (2).

Proof. We represent numbers under base-k and use $[d_j, \ldots, d_0]_k$ to denote the number $d_j k^j + \cdots + d_1 k + d_0$. Let

$$\begin{aligned}
S_4 &= \{s = [s_3, s_2, s_1, 0]_k : s_2, s_1 = 0, 1, \ldots, k, s_3 = 0, \ldots, k+1\},\\
S_3 &= \{s = [s_3, s_2, 0/1, s_0] : s_2, s_0 = 0, 1, \ldots, k, s_3 = 0, \ldots, k+1\},\\
S_2 &= \{s = [s_3, 0/1, s_1, s_0] : s_1, s_0 = 0, 1, \ldots, k, s_3 = 0, \ldots, k+1\},\\
S_1 &= \{s = [0, s_2, s_1, s_0] : s_2, s_1, s_0 = 0, 1, \ldots, k\}.
\end{aligned}$$

The third bit of S_1 and the second bit of S_2 are 0 or 1; 1 will be used to handle the possible carrying of the addition.

Define $\widetilde{S} = S_1 \cup S_2 \cup S_3 \cup S_4$, then $\widetilde{S} \subseteq [2k^4]$ and $|\widetilde{S}| = O(k^3)$. For any $i_1 < i_2 < i_3 < i_4 \in [k^4]$, let $a = i_2 - i_1$, $b = i_3 - i_1$, $c = i_4 - i_1$, then $1 \leq a < b < c \leq k^4 - 1$. Write a, b, c under base-k: $a = [a_3a_2a_1a_0]_k$, $b = [b_3b_2b_1b_0]_k$, $c = [c_3c_2c_1c_0]_k$, where $0 \leq a_i, b_i, c_i \leq (k-1)$, $i = 1, 2, 3, 4$. Now we pick $s_1 = [0, k - a_2, k - b_1, k - c_0]_k$, by the definition of S_i, $s_1 \in S_1$, and it is easy to check that

$$s_2 = s_1 + a \in S_2, s_3 = s_1 + b \in S_3, \text{ and } s_4 = s_1 + c \in S_4.$$

Thus

$$s_1, s_2, s_3, s_4 \in \widetilde{S}, \text{ and } s_{j_1} - s_{j_2} = i_{j_1} - i_{j_2} \ (j_1, j_2 = 1, 2, 3, 4).$$

Now we define $S = \cup_{j=0}^{50\log k-1}(j \cdot 2k^4 + \widetilde{S})$, i.e. by repeating set $\widetilde{S}$ $50\log k$ times. It is clear that $S \subseteq [100k^4 \log k]$ and $|S| = O(k^3 \log k)$.

We claim that if we randomly assign $\{0, 1\}$ to each $s \in S$, then with high probability it will satisfy (2): We call an assignment "bad" if there exists $i_1, i_2, i_3, i_4 \in [k^4]$ such that the assignment of the related elements $s_1, s_2, s_3, s_4 \in S$ is not $\{0, 0, 1, 1\}$. For any fixed $\{i_1, i_2, i_3, i_4\}$, the probability that a random assignment of $\widetilde{S}$ is "bad" is $1-3/8 = 5/8$. Thus the probability that all the $50\log k$ copies of $\widetilde{S}$ are "bad" is $(\frac{5}{8})^{50\log k} < \frac{1}{k^{25}}$. Therefore,

$$\Pr(\text{a random assignment of } S \text{ is bad}) \leq \binom{k^4}{4}\frac{1}{k^{25}} \ll 1.$$

So there exists an assignment to satisfy (2). □

Proof of Theorem 2. By setting $k = N^{1/7}$ in Lemma 2 we obtain a partial assignment $p : S \to \{0, 1\}$, $S \in [100N^{4/7}\log N]$ and $|S| = O(N^{3/7}\log N)$. For any $x \in \{0, 1\}^N$, define its j-shift $SH_j(x) = (x_{j+1}, \ldots, x_N, x_1, \ldots, x_j)$, $j = 0, 1, \ldots, N-1$. For a set B, we use $SH_j(B)$ to represent the set $\{b + j : b \in B\}$, here "+" is modular N.

Now we define our function $f : \{0, 1\}^N \to \{0, 1\}$,

$$f(x) = 1 \Leftrightarrow \exists j, SH_j(x) \text{ satisfies the partial assignment } p, \text{ i.e. } (SH_j(x))_i = p(i), \forall i \in S.$$

By the definition we know that f is cyclically invariant. Next, we prove that for any input x, $bs(f, x) \leq O(N^{3/7}\log N)$. We separate the two cases $f(x) = 1$ or $f(x) = 0$:

(i) $f(x) = 1$. By definition there is a j_0 that $SH_{j_0}(x)$ satisfies the partial assignment p. With loss of generality, we assume that $j_0 = 0$ (because, for cyclically invariant functions, $bs(f, x) = bs(f, SH_j(x))$), i.e. $x_i = p(i)$ for any $i \in S$. Now let $B_1, \ldots, B_{bs(f,x)}$ be the maximum pair-wise disjoint subsets that $f(x) \neq f(x^{(B_l)})$, $l = 1, \ldots, bs(f, x)$. Then each B_l must contain at least one bit in the partial assignment p, otherwise flipping the block B_l will not change the value of $f(x)$. Thus $B_l \cap S \neq \emptyset$. But $B_1, \ldots, B_{bs(f,x)}$ are pair-wise disjointed, therefore $bs(f, x) \leq |S| = O(N^{3/7}\log N)$.

(ii) $f(x) = 0$. Let $B_1, \ldots, B_{bs(f,x)}$ be the maximum pair-wise disjoint subsets that $f(x^{(B_l)}) = 1$, $l = 1, \ldots, bs(f, x)$. By the definition of function f, for each B_l, there must be a j_l that $SH_{j_l}(x^{(B_l)})$ satisfies partial assignment p. Since $SH_{j_l}(x^{(B_l)}) = (SH_{j_l}(x))^{(SH_{j_l}(B_l))}$ and $B_1, \ldots, B_{bs(f,x)}$ are pair-wise disjointed, $j_1, \ldots, j_{bs(f,x)}$ must be distinct. With loss of generality, we assume that $j_1 < j_2 < \cdots < j_{bs(f,x)}$. We claim that $bs(f, x) \leq 4N^{3/7}$:

Suppose the opposite, i.e. $bs(f, x) > 4N^{3/7}$. Since $j_l \in [N]$, there exists an interval with length $N^{4/7}$ which contains at least four j_l. With loss of generality, we assume that $j_1, j_2, j_3, j_4 \in [c - N^{4/7}, c)$ for some $c \in [N]$. Then $c - j_i \in [N^{4/7}]$, $i = 1, 2, 3, 4$. Now we use the property of S: there exists $s_1, s_2, s_3, s_4 \in S$,

$$s_2 - s_1 = (c - j_2) - (c - j_1), s_3 - s_1 = (c - j_3) - (c - j_1), s_4 - s_1 = (c - j_4) - (c - j_1),$$

i.e.

$$s_1 + j_1 = s_2 + j_2 = s_3 + j_3 = s_4 + j_4, \tag{6}$$

and multiset $\{p(s_1), p(s_2), p(s_3), p(s_4)\} = \{0, 0, 1, 1\}$. Let $t = s_1 + j_1$. For $i = 1, 2, 3, 4$, $SH_{j_i}(x^{(B_i)})$ satisfying partial assignment p implies that

$$(SH_{j_i}(x^{(B_i)}))_{s_i} = p(s_i),$$

i.e.

$$(x^{(B_i)})_{j_i+s_i} = p(s_i), i = 1, 2, 3, 4. \tag{7}$$

Combine Eq. (6) with (7) we obtain

$$(x^{(B_i)})_t = p(s_i), i = 1, 2, 3, 4.$$

But $\{p(s_1), p(s_2), p(s_3), p(s_4)\}$ contains two 0's and two 1's, and no matter what x_t is, there must exist two blocks B_i which contain the index t. This contradicts to the disjointness of B_i.

Combining (i) with (ii), we conclude that $bs(f, x) = O(N^{3/7} \log N)$. □

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China Grant 60603005, 60553001, and the National Basic Research Program of China Grant 2007CB807900, 2007CB807901.

References

[1] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, Ronald de Wolf, Quantum lower bounds by polynomials, Journal of the ACM 48 (4) (2001) 778–797. Earlier version in FOCS'98.

[2] Harry Buhrman, Ronald de Wolf, Complexity measures and decision tree complexity: A survey, Theoretical Computer Science 288 (1) (2002) 21–43.

[3] Sourav Chakraborty, On the sensitivity of cyclically-invariant boolean functions, in: IEEE Conference on Computational Complexity, 2005, pp. 163–167.

[4] L. Lovasz, N. Young, Lecture notes on evasiveness of graph properties, Technical Report, TR 317-91, Princeton University, 1994.

[5] Noam Nisan, CREW PRAMs and decision trees, SIAM Journal on Computing 20 (6) (1991) 999–1007. Earlier version in STOC'89.

[6] Noam Nisan, Mario Szegedy, On the degree of Boolean functions as real polynomials, Computational Complexity 4 (4) (1994) 301–313. Earlier version in STOC'92.

[7] R. Rivest, J. Vuillemin, On recognizing graph properties from adjacency matrices, Theoretical Computer Science 3 (1976) 371–384.

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

[9] György Turán, The critical complexity of graph properties, Information Processing Letters 18 (3) (1984) 151–153.