Information Processing Letters 111 (2011) 1081–1084

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Minterm-transitive functions with asymptotically smallest block sensitivity

Kazuyuki Amano *

Department of Computer Science, Gunma University, 1-5-1 Tenjin, Kiryu, Gunma 376-8515, Japan

ARTICLE INFO

Article history:
Received 1 July 2011
Received in revised form 12 September 2011
Accepted 13 September 2011
Available online 17 September 2011
Communicated by J. Torán

Keywords:
Computational complexity
Boolean functions
Block sensitivity
Minterm-transitive functions
Tight bounds

ABSTRACT

In this note, we give an explicit construction of a minterm-transitive Boolean function with block sensitivity $O(n^{3/7})$. This removes a log-factor from the previously known bounds by Xiaoming Sun [Block sensitivity of weakly symmetric functions, Theoret. Comput. Sci. 384 (1) (2007) 87–91] and by Andrew Drucker [Block sensitivity of minterm-transitive functions, Theoret. Comput. Sci. 412 (41) (2011) 5796–5801]. Due to the matching lower bound by Drucker, it is shown that the minimum achievable block sensitivity for non-constant minterm-transitive function is $\Theta(n^{3/7})$.

1. Introduction and results

For a Boolean function $f:\{0,1\}^n \to \{0,1\}$, the *block sensitivity* of f on input $x = (x_1, \dots, x_n)$, denoted by $bs(f,x)$, is the maximum number b such that there are pairwise-disjoint subsets $B_1, \dots, B_b$ of $\{1,2,\dots,n\}$ for which $f(x) \neq f(x^{B_i})$; here x^{B_i} denotes the input obtained from x by flipping all the bits x_j such that $j \in B_i$.

For $b \in \{0,1\}$, define *b-block sensitivity*, of f, denoted by $bs_b(f)$, as $\max_{x \in f^{-1}(b)} bs(f,x)$. Define the *block sensitivity* of f, denoted by $bs(f)$, as $bs(f) = \max(bs_0(f), bs_1(f))$.

The *sensitivity* of a Boolean function f is defined identically to $bs(f)$, but with the further restriction that all blocks must be of size 1. The sensitivity was first introduced in [5], and the block sensitivity was introduced in [8]. Since then, these two measures as well as related measures on Boolean functions have been extensively studied over two decades. See e.g., [3,7] for a good survey and e.g., [1,2,10] for some recent results on this topic.

In this note, we focus on the block sensitivity of a special class of Boolean functions called *minterm-transitive* functions introduced by Chakraborty [4].

For convenience, in what follows, we index the coordinates of $x \in \{0,1\}^n$ by $\mathbb{Z}_n = \{0,1,\dots,n-1\}$. Define a *pattern* as a mapping $p:\mathbb{Z}_n \to \{0,1,*\}$. For a pattern p, the *domain* of p is defined as $\mathrm{dom}(p) = \{i \mid p(i) \in \{0,1\}\}$, and the *width* of p is defined as $i - j + 1$ where i and j are the largest and smallest integer in $\mathrm{dom}(p)$. A pattern p naturally represents a partial assignment that contains all the variables in its domain.

Given a pattern p and a permutation σ on $\mathbb{Z}_n$, we say that an input $x = (x_0, \dots, x_{n-1}) \in \{0,1\}^n$ *matches* p *under* σ if $x_{\sigma(i)} = p(i)$ whenever $i \in \mathrm{dom}(p)$. For $i \notin \mathrm{dom}(p)$, the value of $x_{\sigma(i)}$ is arbitrary. For a pattern p and a set Γ of permutations on $\mathbb{Z}_n$, define the function $f^{\Gamma,p}:\{0,1\}^n \to \{0,1\}$ as

$$f^{\Gamma,p}(x) = 1 \iff \exists \sigma \in \Gamma \text{ such that } x \text{ matches } p \text{ under } \sigma.$$

A permutation group Γ is *transitive* if for all $i, j \in \mathbb{Z}_n$, there exists $\sigma \in \Gamma$ such that $\sigma(i) = j$. A Boolean function

* Tel.: +81 277 30 1823, fax: +81 277 30 1802.
E-mail address: amano@cs.gunma-u.ac.jp.

0020-0190/$ – see front matter
doi:10.1016/j.ipl.2011.09.008

f is called *minterm-transitive* if $f = f^{\Gamma,p}$ for some transitive group Γ and pattern p.

A natural example of transitive group is a set of cyclic shifts of coordinates. Let $\mathcal{T}$ be the set of cyclic shifts on $\mathbb{Z}_n$, i.e.,

$$\mathcal{T} = \left\{\mathrm{sft}_j\colon \mathrm{sft}_j(i) = i + j \bmod n\right\}_{j\in\mathbb{Z}_n}.$$

A Boolean function f is called *minterm-cyclic* if $f = f^{\mathcal{T},p}$ for some pattern p. Obviously, every minterm-cyclic function is also minterm-transitive.

Sun [9] gave a construction of a minterm-transitive (in fact minterm-cyclic) function f on n variables with $bs(f) = O(n^{3/7}\ln n)$. Recently, Drucker [6] showed that this upper bound is almost tight by proving $\Omega(n^{3/7})$ lower bounds on the block sensitivity of every non-constant minterm-transitive function. In addition, he improved Sun's upper bound to $O(n^{3/7}\ln^{1/7} n)$, but left as an open problem whether we can remove the log-factor entirely.

In this note, we resolve this problem by giving an explicit construction of a minterm-cyclic function with block sensitivity $O(n^{3/7})$. Thus we show that the minimum achievable block sensitivity for non-constant minterm-transitive functions is $\Theta(n^{3/7})$.

2. Construction of functions with small $bs(f)$

In this section, we prove our main theorem:

Theorem 1. *There is a minterm-cyclic Boolean function f such that $bs(f) = O(n^{3/7})$.*

We follow the idea of Sun [9] and Drucker [6] to construct a function with small block sensitivity. However, unlike their constructions, we do not use a probabilistic argument.

We need some notations introduced in [6]. A set of four elements in $\mathbb{Z}_n$ is called 4-*set*. For a 4-set $A = \{a_1,\dots,a_4\}$ and a pattern p, we say that *p contains a balanced shifted copy of A* if (i) there exists a cyclic shift sft_j such that the domain of the shifted pattern $\mathrm{dom}(\mathrm{sft}_j(p))$ contains A, and (ii) $\mathrm{sft}_j(p)$ equals 0 on exactly two of four coordinates in A and equals 1 on the other two. If p and A satisfy the condition (i) but not necessarily (ii), we simply say that *p (or $\mathrm{dom}(p)$) contains a shifted copy of A*.

We use the following two lemmas shown by Sun [9] (see also [6]). These lemmas reduce the problem of finding a function with small block sensitivity to the problem of finding a pattern with small domain and some good covering property.

Lemma 1. *(See [9].) For any $f = f^{\mathcal{T},p}$, $bs_1(f) \leqslant |\mathrm{dom}(p)|$.*

Lemma 2. *(See [9].) Suppose that, for every set $S \subseteq \mathbb{Z}_n$ of size d, there is a 4-set $A \subseteq S$ for which p contains a balanced shifted copy of A. Then $bs_0(f) < d$ for $f = f^{\mathcal{T},p}$.*

The main contribution of this note is to give an explicit construction of a pattern satisfying the following lemma. We didn't make any effort to improve the constants (i.e., 2^{17} or 2^{19}) in the lemma.

Lemma 3. *For every sufficiently large k, there is a pattern p with $\mathrm{dom}(p) \subseteq \{0,1,\dots,2^{19}k^4-1\}$ such that*

(i) *p contains a shifted balanced copy of every 4-set in $\{0,1,\dots,k^4-1\}$, and*
(ii) $|\mathrm{dom}(p)| \leqslant 2^{17}k^3$.

Before proving Lemma 3, we give the proof of Theorem 1.

Proof of Theorem 1. Let $k = n^{1/7}$. Fix a pattern p as in Lemma 3. We show that the minterm-cyclic function $f^{\mathcal{T},p}$ has block sensitivity $O(n^{3/7})$.

By Lemma 1, we have $bs_1(f^{\mathcal{T},p}) = |\mathrm{dom}(p)| = O(n^{3/7})$.

Let $S \subseteq \mathbb{Z}_n$ be any set of size at least $4n^{3/7}$. Then there exists an interval $[a, a+n^{4/7}-1]$ (mod n) that contains at least four elements of S. Let A be these elements. Then, by Lemma 3, p contains a shifted balanced copy of A since all elements of A lies in an interval of length $n^{4/7} = k^4$. Therefore, by Lemma 2, we have $bs_0(f^{\mathcal{T},p}) = O(n^{3/7})$ and hence $bs(f^{\mathcal{T},p}) = O(n^{3/7})$. $\square$

Proof of Lemma 3. We will construct a pattern p satisfying (i) and (ii) in the lemma. Our pattern p is a "concatenation" of five subpatterns $p_1,\dots,p_5$. We design p_1 so that it contains a balanced shifted copy of *large fraction* of 4-sets in $\{0,\dots,k^4-1\}$, and then add p_2 to p_5 to cover the remaining sets. Since $|\mathrm{dom}(p)| = \sum_{i=1}^{5}|\mathrm{dom}(p_i)|$, it should satisfy $|\mathrm{dom}(p_i)| = O(k^3)$ for $i = 1,\dots,5$. Similarly, the width of each subpattern should be $O(k^4)$.

Construction of p_1. Following Sun [9], we represent numbers under base-k and use $[d_3,d_2,d_1,d_0]_k$ to denote the number $d_3k^3+d_2k^2+d_1k+d_0$. Let

$$\begin{aligned}
S_1 &= \left\{[0,s_2,s_1,s_0]_k \;\middle|\; s_2,s_1,s_0 = 0,1,\dots,k\right\},\\
S_2 &= \left\{[s_3,0/1,s_1,s_0]_k \;\middle|\; s_1,s_0 = 0,1,\dots,k-1,\right.\\
&\qquad \left. s_3 = 0,1,\dots,k+1\right\},\\
S_3 &= \left\{[s_3,s_2,0/1,s_0]_k \;\middle|\; s_2,s_0 = 0,1,\dots,k-1,\right.\\
&\qquad \left. s_3 = 0,1,\dots,k+1\right\},\\
S_4 &= \left\{[s_3,s_2,s_1,0]_k \;\middle|\; s_2,s_1 = 0,1,\dots,k-1,\right.\\
&\qquad \left. s_3 = 0,1,\dots,k+1\right\},
\end{aligned}$$

and $\tilde{S} = S_1 \cup S_2 \cup S_3 \cup S_4$. The second digit of S_2 and the third digit of S_3 are 0 or 1. The value 1 will be used to handle the carry in the addition. Note that, for a technical reason, s_2,s_1,s_0 can take the value k only in the definition of S_1. An equivalent definition is

$$\begin{aligned}
S_1 = {}&\left\{[0,s_2,s_1,s_0]_k \;\middle|\; s_2,s_1,s_0 = 0,1,\dots,k-1\right\}\\
&\cup \left\{[1,0,s_1,s_0]_k, [1,1,0,s_0]_k, [1,1,1,0]_k \;\middle|\right.\\
&\qquad \left. s_1,s_0 = 0,1,\dots,k-1\right\}.
\end{aligned}$$

Note also that the largest number in $\tilde{S}$ is $(k+2)k^3-1 < 2k^4$.

Fix any $A = \{a_1,a_2,a_3,a_4\} \subseteq \{0,1,\dots,k^4-1\}$ where $a_1 < a_2 < a_3 < a_4$. Set $\alpha = a_2 - a_1$, $\beta = a_3 - a_1$ and $\gamma =$