Information Processing Letters 116 (2016) 331–336

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

The simplified weighted sum function and its average sensitivity [☆]

Jiyou Li [a,*], Chu Luo [b]

[a] Department of Mathematics, Shanghai Jiao Tong University, Shanghai, PR China
[b] Department of Computer Science and Engineering, University of Oulu, Oulu, Finland

ARTICLE INFO

Article history:
Received 17 December 2014
Received in revised form 1 October 2015
Accepted 5 January 2016
Available online 7 January 2016
Communicated by R. Uehara

Keywords:
Boolean function
Weighted sum function
Average sensitivity
Computational complexity
Subset counting

ABSTRACT

In this paper we simplify the definition of the weighted sum Boolean function which used to be inconvenient to compute and use. We show that the new function has essentially the same properties as the previous one. In particular, the bound on the average sensitivity of the weighted sum Boolean function remains unchanged after the simplification.

1. Introduction

In previous study, the weighted sum function had a simple but not very clean structure. With a residue ring modulo a prime, the explicit definition of this function can be given using the weighted sum as follows [21]. Let $m \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ and prime number $p \geq m$ where no other prime numbers are between p and m. For vector $X = (x_1, x_2, \dots, x_m) \in \mathbb{Z}_2^m$, where $\mathbb{Z}_2 = \{0, 1\}$, let $u(X)$ be the least positive integer which satisfies

$$u(X) = \sum_{k=1}^{m} kx_k (\bmod p), 1 \leq u(X) \leq p.$$

Then the weighted sum function $g(X)$ is defined as

$$g(X) = \begin{cases} x_{u(X)}, & 1 \leq u(X) \leq m; \\ x_1, & \text{otherwise.} \end{cases} \tag{1.1}$$

This function was used to study read-once branching programs by P. Savický and S. Žák [21]. It was also used to demonstrate the exponential improvement from conventional read-once branching programs to quantum ones by M. Sauerhoff in [18], see also [19].

To simplify the definition of the previous weighted sum function, we define a new function $f(X)$ as follows. For $X = (x_0, x_1, \dots, x_{m-1}) \in \mathbb{Z}_2^m$, denote

$$s(X) = \sum_{k=0}^{m-1} kx_k (\bmod m),$$

and define the new weighted sum function

$$f(X) = x_{s(X)}.$$

It is worth noting that this new function $f(X)$ is more convenient to compute and use than $g(X)$. One particular reason for the prime modulus in the previous function $g(X)$ is that there are nice results and structures in prime fields. In this paper we call such $f(X)$ the simplified weighted sum function. Note that when m is prime then the two definitions are the same.

[☆] This work is supported by the National Science Foundation of China (11001170) and the Natural Science Foundation of Shanghai Municipal (13ZR1422500).

[*] Corresponding author.
E-mail addresses: lijiyou@sjtu.edu.cn (J. Li), chu.luo@ee.oulu.fi (C. Luo).

http://dx.doi.org/10.1016/j.ipl.2016.01.002
0020-0190/© 2016 Elsevier B.V. All rights reserved.

We believe that in many cases this new simplified function $f(X)$ has similar properties as the previous one $g(X)$. We give two examples to support this claim. As the first example, $g(X)$ was used in [21] to establish a lower bound of read-once branching programs. We show that a similar lower bound holds for $f(X)$.

A Boolean function is called k-mixed if for any two distinct partial assignments of any given k variables, the two subfunctions on the remaining $m-k$ variables are distinct. This notion was first introduced by Jukna [13]. For more applications on more functions, see [2,3,11,20,26].

One of the key ingredients in [21] is the following theorem, first proved by Simon and Szegedy [25].

Theorem 1.1. *If $h(X)$ is a k-mixed Boolean function, then every 1-branching program for $h(X)$ has size at least 2^k-1.*

The authors then showed that the weighted sum function $g(X)$ of m variables is $(m-o(m))$-mixed, by applying the following result in additive combinatorics and established the desired lower bound.

Theorem 1.2. *(See Dias da Silva and Hamidoune, [9].) Let $\epsilon > 0$ be a fixed constant. Then, for every large enough p and $A \subseteq \mathbb{Z}_p$ with $|A| \ge (2+\epsilon)\sqrt{p}$, and for every $b \in \mathbb{Z}_p$, there is a subset $B \subseteq A$ such that the sum of the elements of B is equal to b.*

The work of Freeze, Gao and Geroldinger in 2009 generalized this result to the general cyclic group case.

Theorem 1.3. *(See Freeze, Gao and Geroldinger, [10].) Let d be the smallest prime divisor of m. Then, for every $A \subseteq \mathbb{Z}_m$ with $|A| \ge \frac{m}{d}+d-2$, and for every $b \in \mathbb{Z}_m$, there is a subset $B \subseteq A$ such that the sum of the elements of B is equal to b.*

Similarly one can use this result to prove that the simplified weighted sum function $f(X)$ is $(m(1-\frac{1}{d})-d)$-mixed and thus establish the similar lower bound for $f(X)$ as well. This bound is pretty good especially when m's smallest prime divisor d is large compared to m. For instance, if we take m to be a product of two primes which are close enough, then the bound is as good as the prime case.

Interestingly, this argument can be applied to some other topics. As the second example, the k-mixed property was used to give a lower bound for Boolean circuits. For details we refer to [3].

We then determine the average sensitivity of this newly defined function $f(X)$ and show that it also satisfies the Shparlinski's conjecture [24] which says that the average sensitivity of $f(X)$ is asymptotically $m/2$. We introduce the main concepts of this conjecture in the following.

For an input $X=(x_0,x_1,\ldots,x_{m-1})$, the sensitivity $\sigma_{s,X}(f)$ on X denotes the number of variables such that flipping one of these variables will shift the value of f. Explicitly,

$$\sigma_{s,X}(f) = \sum_{i=0}^{m-1} \left| f(X) - f(X^{(i)}) \right|,$$

where $X^{(i)} = (x_0,\ldots,x_{i-1},1-x_i,x_{i+1}\ldots,x_{m-1})$ is the vector assignment after flipping the i-th coordinate in X. The sensitivity $\sigma_s(f)$ of $f(X)$ denotes the maximum of $\sigma_{s,X}(f)$ on vector X in $\mathbb{Z}_2^m$ and the average sensitivity $\sigma_{av}(f)$ is the mean value of sensitivity on every possible input, i.e.,

$$\sigma_{av}(f) = 2^{-m} \sum_{X\in\mathbb{Z}_2^m} \sum_{i=0}^{m-1} \left| f(X) - f(X^{(i)}) \right|.$$

Sensitivity, together with a more general concept called block sensitivity, is a useful measure to predict the complexity of Boolean functions. It has recently drawn extensive attention, for instance [1,4–8,14,17,22–24]. For a good survey on the main unsolved problems on sensitivity, please refer to [12].

In [24] Shparlinski addressed the average sensitivity problem of the previous weighted sum function $g(X)$ and obtained a lower bound from a nontrivial bound on its Fourier coefficients using exponential sums methods. He also developed several conjectures on the average sensitivity of the weighted sum function and the bounds of the Fourier coefficients. Explicitly, one conjecture was that the average sensitivity of $g(X)$ on m variables is not less than $(\frac{1}{2}+o(1))m$. In the same paper he gave a proof that the average sensitivity is greater than γm, where constant γ satisfies $\gamma \approx 0.0575$.

By applying a new sieving technique, in [14] the first author gave an asymptotic counting formulas of the subset sums over prime fields and thus confirmed the Shparlinski's conjecture on the average sensitivity of the weighted sum function.

In this paper we extend this result for the simplified weighted sum function $f(X)$. That is, for $f(X)$ with m variables, the average sensitivity of $f(X)$ is exactly $(1/2+o(1))m$.

In addition, we also compute the weight of $f(X)$. We prove that the weight of $f(X)$ on m variables is exactly $2^{m-1}(1+o(1))$. Thus, $f(X)$ is an asymptotically balanced function.

This paper is organized as follows. In Section 2 we present a sieve formula. By applying this formula, we give a series of formulas for counting subsets sums over cyclic groups in Section 3. The proof of the main results is given in Section 4. We also list several further questions in Section 5.

Notation For $x \in \mathbb{R}$, let $(x)_0 = 1$ and $(x)_k = x(x-1)\cdots(x-k+1)$ for $k \in \mathbb{Z}^+ = \{1,2,3,\ldots\}$. For $k \in \mathbb{N} = \{0,1,2,\ldots\}$ define the binomial coefficient $\binom{x}{k} = \frac{(x)_k}{k!}$.

2. A distinct coordinate sieving formula

For the purpose of our proof, we briefly introduce a sieving formula discovered by Li–Wan [15], which significantly improves the classical inclusion-exclusion sieving. We cite it here without any proof. For details and related applications, we refer to [15,16].

Let S_k be the symmetric group on k elements. It is well known that every permutation $\tau \in S_k$ factorizes uniquely as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. For $\tau \in S_k$, define