Information Processing Letters 116 (2016) 537–540

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Correlation lower bounds from correlation upper bounds

Shiteng Chen [a], Periklis A. Papakonstantinou [b,*]

[a] IIIS, Tsinghua University, China

[b] MSIS, Rutgers Business School, Rutgers University, United States

ARTICLE INFO

Article history:
Received 29 July 2015
Accepted 27 March 2016
Available online 7 April 2016
Communicated by R. Uehara

Keywords:
Computational complexity
Circuit complexity
Correlation
Composite modulus

ABSTRACT

We prove a $2^{-O\left(\frac{n}{d(n)}\right)}$ lower bound on the correlation of $\mathrm{MOD}_m \circ \mathrm{AND}_{d(n)}$ and MOD_r, where m, r are positive integers. This is the first non-trivial lower bound on the correlation of such functions for arbitrary m, r. Our motivation is the question posed by Green et al., to which the $2^{-O\left(\frac{n}{d(n)}\right)}$ bound is a partial negative answer. We first show a $2^{-\Omega(n)}$ correlation upper bound that implies a $2^{\Omega(n)}$ circuit size lower bound. Then, through a reduction we obtain a $2^{-O(\frac{n}{d(n)})}$ correlation lower bound. In fact, the $2^{\Omega(n)}$ size lower bound is for $\mathrm{MAJ} \circ \mathrm{ANY}_{o(n)} \circ \mathrm{AND} \circ \mathrm{MOD}_r \circ \mathrm{AND}_{O(1)}$ circuits, which is of independent interest.

1. Introduction

Understanding the power of small-depth circuits that have MOD_m gates, in addition to the usual boolean gates, is one of the most fascinating areas of computational complexity. MOD_m is the boolean function that outputs 1 if and only if the number of 1s in its input is a multiple of m. The computational limitations of MOD_m gates for prime $m = p$ is well-understood since 1980s through the seminal works of Razborov [14] and Smolensky [15]. They proved that no constant depth polynomial size circuit with $\{\mathrm{MOD}_p, \mathrm{AND}, \mathrm{OR}, \mathrm{NOT}\}$ gates can compute the MOD_q function, for primes $p \neq q$. Smolensky further conjectured that the same holds true for composite moduli, which remains an important open question.

A main tool in the study of small-depth circuit lower bounds is via correlation upper bounds [2,3,9,11,13,8,7]. The notion of *correlation* quantifies the distance of two functions and was introduced by Hajnal et al. [13]; see p. 538 for definitions. The smaller the correlation between the circuit and a function the larger the circuit size to compute this function.

In this note we show a limitation of the correlation method, aiming to answer the question of Green et al. [11]. They asked whether it is possible to prove correlation upper bounds that yield size lower bounds for circuits of the form $\mathrm{MOD}_m \circ \mathrm{AND}_{\omega(\log n)}$, which correspond to functions $\mathrm{MOD}_m(P(x))$, for a polynomial P of degree $\omega(\log n)$. We show a correlation lower bound between MOD_r and $\mathrm{MOD}_m(P(x))$ where $m \in \mathbb{Z}$ is anything and P is of any degree. Previously, Green [10] and Viola [17] discussed correlation lower bounds that differ from ours. Viola's argument is for the correlation between symmetric functions and polynomials of degree $\sqrt{n}$ (i.e. high degree) over GF(2) (in fact, GF(p) for prime p), whereas Green's argument is only about MOD_2 and MOD_3.

Our goal is to lower bound the correlation between MOD_r and any circuit $\mathcal{C}_{\text{simple}}$ with a single layer of MOD_m. We prove this in two steps. In the first step we obtain a correlation *upper bound* but for more complicated circuits $\mathcal{C}_{\text{multi-layer}}$, which in particular includes circuits with two MOD layers. This correlation upper bound implies a circuit size *lower bound* for $\mathcal{C}_{\text{multi-layer}}$. In the second step we do a reduction to obtain the *lower bound* on the correlation of a specific $\mathcal{C}_{\text{simple}}$ and MOD_r.

* Corresponding author.
E-mail addresses: shitengchen@gmail.com (S. Chen), periklis.research@gmail.com (P.A. Papakonstantinou).

http://dx.doi.org/10.1016/j.ipl.2016.03.012
0020-0190/

There is considerable success in using correlation upper bounds in obtaining circuit lower bounds. In our argument we need to lower bound the size of circuits of the form $\mathrm{MAJ} \circ \mathrm{ANY}_{o(n)} \circ \mathrm{AND} \circ \mathrm{MOD}_r \circ \mathrm{AND}_{d(n)}$, for which no previous lower bounds were known.

Hajnal et al. [13] showed the discriminator lemma, according to which upper bounded correlation of f, g implies a lower bound for circuits of the form $\mathrm{MAJ} \circ f$ that compute g. MAJ outputs 1 if and only if the majority of input bits is 1. Cai et al. [3] studied depth 3 circuits of the form $\mathrm{MAJ} \circ \mathrm{MOD}_m \circ \mathrm{AND}$ and introduced the analytic study of *exponential sums*, which is important for our work as well. Their results were for symmetric MOD functions, later generalized by Green [9], whereas Bourgain [2] (for odd moduli) and Green et al. [11] and Chattopadhyay [5] finally showed an exponential size lower bound for $\mathrm{MAJ} \circ \mathrm{MOD}_m \circ \mathrm{AND}_{O(1)}$ computing MOD_q, when m, q are co-prime, i.e. $(m, q) = 1$.

For two layers of MOD gates, Grolmusz et al. [12] and Caussinus [4] studied $\mathrm{MOD}_m \circ \mathrm{MOD}_r$ circuits computing the AND function and proved, for any m, r, exponential circuit size lower bounds. Barrington and Straubing [1] considered $\mathrm{MOD}_p \circ \mathrm{MOD}_m$ circuits and proved an exponential size lower bound for such circuits computing MOD_q, where p is a prime and $(p, q) = (m, q) = 1$. Straubing [16] introduced a finite field representation of MOD gates and simplified the previous proofs [1,12]. Chattopadhyay et al. [6] studied $\mathrm{MOD}_r \circ \mathrm{MOD}_m$ to compute MOD_q, where $(r, q) = (m, q) = 1$, for composite r. The authors proved that the fan-in of the output MOD_r gate, or any ANY gate, must be $\Omega(n)$.

2. Notations and prerequisites

All operations in this note are over $\mathbb{C}$, e.g. in evaluating a polynomial function $P : \{0, 1\}^n \to \mathbb{Z}$ with integer coefficients the operations treat the inputs 0, 1 as integers. We write $||x||_1 := \sum_{i=1}^n x_i$ for $x \in \{0, 1\}^n$ and denote by MOD_m the boolean function (gate), where $\mathrm{MOD}_m(||x||_1) = 1$ if $m \big| ||x||_1$ and 0 otherwise; not to be confused with the modulus over $\mathbb{Z}$, i.e. $||x||_1 (\mod m)$. Thus, polynomial functions take inputs $\{0, 1\}^n$ and MOD functions take inputs from $\mathbb{Z}$. For $X \in \mathbb{Z}$ we write $e_m(X) := e^{X\frac{2\pi i}{m}}$, where $e^{\frac{2\pi i}{m}}$ is the m-th primitive root of 1. Then, $\mathrm{MOD}_m(X) = \frac{1}{m}\sum_{0\le k<m} e_m(kX)$. The correlation of the boolean functions $f, g : \{0, 1\}^n \to \{0, 1\}$ is defined as $\mathrm{Corr}(f, g) = |\Pr_x(f(x) = 1 \mid g(x) = 1) - \Pr_x(f(x) = 1 \mid g(x) = 0)| = |\frac{\mathbb{E}_x(f(x)\cdot g(x))}{\Pr_x(g(x)=1)} - \frac{\mathbb{E}_x(f(x)\cdot(1-g(x)))}{\Pr_x(g(x)=0)}|$. We extend the definition for $f : \{0, 1\}^n \to \mathbb{C}$ and $g : \{0, 1\}^n \to \{0, 1\}$ so that $\mathrm{Corr}(f, g) = |\frac{\mathbb{E}_x[f(x)\cdot g(x)]}{\Pr_x[g(x)=1]} - \frac{\mathbb{E}_x[f(x)\cdot(1-g(x))]}{\Pr_x[g(x)=0]}|$.

Now, let us state an observation we made, which is repeatedly used later on.

Observation 1 *(Sub-additivity). Let functions $f_1, f_2 : \{0, 1\}^n \to \mathbb{C}$ and boolean function g. Then, $\mathrm{Corr}(f_1 + f_2, g) \le \mathrm{Corr}(f_1, g) + \mathrm{Corr}(f_2, g)$ and $\mathrm{Corr}(c \cdot f, g) = |c| \cdot \mathrm{Corr}(f, g)$, for every constant $c \in \mathbb{C}$.*

The main tool for proving $\mathrm{MAJ} \circ \mathrm{ANY}$ circuit lower bounds is the following lemma [13]. In fact, this lemma applies not only to MAJ but to any threshold gate.

Lemma 2 *(Discriminator lemma [13]). Let T be a circuit consisting of a majority gate over sub-circuits $C_1, C_2, \ldots, C_s$ each taking n-bit inputs. Let f be the function computed by this circuit. If $\mathrm{Corr}(C_i(x), f(x)) \le \epsilon$ for each $i = 1, \ldots, s$, then $s \ge 1/\epsilon$.*

We use the above lemma together with elementary analytic techniques. The analytic machinery is explicit in the statement of the following Lemma 3.

Lemma 3. *(See [11].) For any $m, q, k \in \mathbb{Z}^+$, $(m, q) = 1$, a polynomial function P with integer coefficients, $\deg(P) = O(1)$, and $x \in \{0, 1\}^n$, then $\mathrm{Corr}(e_m(P(x)), \mathrm{MOD}_q(||x||_1)) \le 2^{-\Omega(n)}$.*

We represent functions $f : \{0, 1\}^n \to \{0, 1\}$ as $f(x) = \sum_{S\subseteq\{1,2,\ldots,n\}} \alpha_S \prod_{x_i\in S} x_i$, where $\alpha_S \in \mathbb{Z}$. This representation is unique, the α_S's are unique, since the functions $\{\prod_{i\in S} x_i | S \subseteq \{1, 2, \ldots, n\}\}$ form a function basis[1] for $\{0, 1\}^n \to \mathbb{C}$. These basis functions are not to be confused with the Fourier basis, which consists of the characters written multiplicatively ($\{-1, 1\}^n \to \{-1, 1\}$). We also introduce the definition of $\mathrm{norm}(f) := \sum_S |\alpha_S|$, which is particularly useful for our purposes.

3. Our results: statements and proofs

Our main results are Theorem 4, which states the circuit lower bound, and Theorem 5, which states the correlation lower bound. Note that Theorem 4 is used to show Theorem 5.

To simplify expression we represent a family of functions $\{g_m\}_m$ by one $g \in \{g_m\}_m$.

Theorem 4. *Let n be the input length to circuits and $\deg_g = o(n)$. Fix arbitrary $g : \{0, 1\}^{\deg_g} \to \{0, 1\}$ and $m, q \in \mathbb{Z}^+$, where $(m, q) = 1$. If a $\mathrm{MAJ} \circ g \circ \mathrm{AND} \circ \mathrm{MOD}_m \circ \mathrm{AND}_{O(1)}$ circuit computes MOD_q, then the fan-in of the MAJ gate on the top is $2^{\Omega(n)}$.*

Theorem 5. *For every $d \in \mathbb{Z}^+$ and every $m, q \in \mathbb{Z}^+$, $(m, q) = 1$ there exists a degree d polynomial P such that $\mathrm{Corr}(\mathrm{MOD}_m(P(x)), \mathrm{MOD}_q(||x||_1)) \ge 2^{-O(\frac{n}{d})}$.*

3.1. Proof of Theorem 4: via a correlation upper bound

First, the sub-additive properties of correlation (Observation 1) yield the following lemma.

Lemma 6 *(Bounded correlation amplifier). For every $d, m, q \in \mathbb{Z}^+$, $(m, q) = 1$ and every $g : \{0, 1\}^{\deg_g} \to \{0, 1\}$ and polynomial functions $P_i(x)$, $x \in \{0, 1\}^n$, whose degrees are $\deg(P_i(x)) \le d$ we have*

$$\mathrm{Corr}(g(\mathrm{MOD}_m(P_1(x)), \mathrm{MOD}_m(P_2(x)), \ldots, \mathrm{MOD}_m(P_{\deg_g}(x))), \mathrm{MOD}_q(||x||_1)) \le \mathrm{norm}(g) \cdot \max_{P(x)\in\mathbb{Z}[x], \deg(P)\le d} (\mathrm{Corr}(e_m(P(x)), \mathrm{MOD}_q(||x||_1)))$$

[1] Since $\prod_{i\in S} x_i \prod_{i\notin S}(1 - x_i)$ are easily shown to be orthogonal and the dimension of the function space is 2^n.