Chicago Journal of Theoretical Computer Science

MIT Press

Volume 1995, Article 2

21 July, 1995

ISSN 1073–0486. MIT Press Journals, 55 Hayward St., Cambridge, MA 02142; (617)253-2889; *journals-orders@mit.edu, journals-info@mit.edu*. Published one article at a time in LaTeX source form on the Internet. Pagination varies from copy to copy. For more information and other articles see:

- *http://www-mitpress.mit.edu/jrnls-catalog/chicago.html/*
- *http://www.cs.uchicago.edu/publications/cjtcs/*
- *gopher.mit.edu*
- *gopher.cs.uchicago.edu*
- anonymous *ftp* at *mitpress.mit.edu*
- anonymous *ftp* at *cs.uchicago.edu*

The *Chicago Journal of Theoretical Computer Science* is a peer-reviewed scholarly journal in theoretical computer science. The journal is committed to providing a forum for significant results on theoretical aspects of all topics in Computer Science.

On the Weak mod m Representation of Boolean Functions

Vince Grolmusz

21 July, 1995

Abstract

Abstract-1 Let P be a polynomial over the ring of mod m integers. P *weakly represents* Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ if there is a subset $S \subseteq \{0,1,\ldots,m-1\}$ such that $f(x)=0$ if and only if $P(x) \in S$. The smallest degree of polynomials P weakly representing f is called the *weak* mod m *degree of* f. We give here an $\Omega(\log n)$ lower bound for the weak degree of the generalized inner product function (GIP) of Babai, Nisan, and Szegedy [BNS92]. This is the first lower-bound result for the weak degree of a Boolean function that does not deteriorate if the number of prime divisors of m increases.

Abstract-2 In the second part of the paper, we give superpolynomial lower bounds for the number of monomials with nonzero coefficients in polynomials weakly representing the OR and the GIP$\circ$PARITY functions.

1 Introduction

1-1 One of the central problems of theoretical computer science is the estimation of the computational complexity of Boolean functions. One well studied measure of the complexity of Boolean function f is the *degree* of a polynomial P, which best *approximates* or *represents* f in some sense (see [Raz87], [Smo87], [NS94], [ABFR91], or [Bei93] for a survey). According to this approach, a Boolean function is considered "hard" if the polynomial that represents or best approximates it has a high degree.

1-2 Barrington, Beigel, and Rudich [BBR94] defined the $\bmod m$ degree of Boolean function f to be the smallest degree of any polynomial P over the ring of $\bmod m$ integers such that, for all 0–1 assignments of x, $f(x) = 0$ if and only if $P(x) = 0$. They obtained the following surprising result: The $\bmod m$ degree of the n-variable OR function is $O(n^{1/r})$, where r is the number of distinct prime factors of m.

1-3 Since some computationally very similar functions, including OR and AND, as well as $\bmod m$ and $\neg \bmod m$, have different $\bmod m$ degrees, the *weak* $\bmod m$ *degree*, a more robust measure, is defined in [BBR94]:

Definition 1 *Let $f\colon \{0,1\}^n \to \{0,1\}$ be a Boolean function, and let P be defined as a polynomial of n variables over $\mathbb{Z}_m$ (the integers $\bmod m$),*

$$P(x_1, x_2, \ldots, x_n) = \sum_{H \in \mathcal{H}} a_H \prod_{i \in H} x_i$$

where $\mathcal{H} \subseteq 2^{\{1,2,\ldots,n\}}$ and $0 \neq a_H \in \mathbb{Z}_m$. We say that P weakly represents *f if there is a set $S \subseteq \{0,1,\ldots,m-1\}$ such that, for every $x \in \{0,1\}^n$,*

$$f(x) = 0 \Longleftrightarrow P(x) \in S$$

Let $\Delta(f,m)$ be the minimum degree of polynomials $\bmod m$ that weakly represent f. The size *of polynomial P is defined to be $|\mathcal{H}|$. Let $\Sigma(f,m)$ denote the minimum size of polynomials $\bmod m$ that weakly represent f.*

Note that the $\bmod m$ degree and the weak $\bmod m$ degree of the OR function are the same.

1-4 Tardos and Barrington [TB95] proved an $\Omega(\log n)$ lower bound for the weak $\bmod m$ degree of the OR function, if m has only two distinct prime divisors. More generally, if the number of distinct prime divisors of m is r, and the smallest prime divisor is q, then their lower bound is

$$\Delta(\mathrm{OR}, m) \geq \Big(1/(q-1) - o(1)\Big)(\log n)^{1/(r-1)} \tag{1}$$

1-5 The following function was first defined by Babai, Nisan, and Szegedy [BNS92]:

Definition 2 *Let $A \in \{0,1\}^{l \times k}$. Let $\mathrm{GIP}_{l,k}(A)$ denote the number of all-*1 *rows in matrix A,* $\bmod 2$.

This is the $\bmod 2$ generalized inner product of the columns of A.

1-6 Here we show an $\Omega(\log n)$ lower bound for $\Delta(\mathrm{GIP}_{l,k}, m)$, where m is an arbitrary integer (i.e., our lower bound does not deteriorate when the number of different prime divisors of m increases):

Theorem 1 *Let l and k be positive integers that satisfy $c \log l < k \le (1/3)\log l$ for some $0 < c < 1/3$, and let $n = kl$. Then for every integer m that satisfies $1 < m \le \exp(n^{1/4})$,*

$$\Delta(\mathrm{GIP}_{l,k}, m) \ge k = \Omega(\log n)$$

This is the tightest possible lower bound that holds for $m = 2$, since the definition of $\mathrm{GIP}_{l,k}$ is just a polynomial $\bmod 2$ of degree k: the sum $\bmod 2$ of the product of each row.

1-7 Unfortunately, our degree lower bound method does not apply to the theoretically interesting case when f is the OR function. However, we can prove that the *size* of the polynomials weakly representing OR must be large:

Theorem 2

1. *Let m be the product of two different primes. Then there exists a constant $c_m > 0$ such that*

$$\Sigma(\mathrm{OR}, m) \ge n^{c_m \log n}$$

2. *Suppose that m has r different prime divisors. Then there exists a constant $c_m > 0$ such that*

$$\Sigma(\mathrm{OR}, m) \ge n^{c_m (\log n)^{1/(r-1)}}$$

1-8 The proof of Theorem 2 is based on the method of Razborov and Wigderson [RW93] and the degree lower bound (1) of Tardos and Barrington [TB95]. Consequently, the bound depends on the number of prime divisors of m. Using the degree lower bound of our Theorem 1, we give a lower bound for the size, which does not deteriorate if the number of prime divisors of m increases.

1-9 Razborov and Wigderson [RW93] used the function

$$f_n(x) = \bigoplus_{i=1}^{h} \bigwedge_{j=1}^{\lfloor \frac{1}{3}\log h \rfloor} \bigoplus_{k=1}^{h} x_{ijk}$$

to prove an $\Omega(n^{\log n})$ lower bound on size for some depth-3 circuits, where $n = h^2 \lfloor (1/3)\log h \rfloor$. Observe that f_n is the composition of the GIP and the PARITY functions.

Theorem 3 *Let $m > 1$ be an arbitrary integer. Then*

$$\Sigma(f_n, m) = n^{\Omega(\log n)}$$

2 Communication Complexity

2-1 Our main tool in proving Theorem 1 is a *multiparty communication game*. In a multiparty communication game [CFL83], k players, $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_k$, intend to compute the value of $g(A_1, A_2, \ldots, A_k)$ cooperatively, where $g\colon \{0,1\}^{l\times k} \to \{0,1\}$ and $A_i \in \{0,1\}^l$, for $i = 1, 2, \ldots, k$. Player $\mathbf{p}_i$ knows the value of each variable, except A_i. The players have unlimited computational power, and they communicate with the help of a blackboard viewed by all players. Only one player may write on the blackboard at a time. The goal is to compute $g(A_1, A_2, \ldots, A_k)$ in such a way that at the end of the computation, all players know this value. The cost of the computation is the number of bits written on the blackboard for the given $A = (A_1, A_1, \ldots, A_k) \in \{0,1\}^{l\times k}$.

2-2 The cost of a multiparty protocol is the maximum number of bits communicated for any A in $\{0,1\}^{l\times k}$. The k-party communication complexity of a function g, $C^{(k)}(g)$, is the minimum of the costs of those k-party protocols that compute g. Babai, Nisan, and Szegedy examined the multiparty communication complexity of the GIP function in [BNS92], and they proved the following theorem.

Theorem 4 ([BNS92], Theorem 2)

$$C^{(k)}(\mathrm{GIP}_{l,k}) = \Omega(l/4^k)$$

3 Proving the Degree Bound

3-1 The proof is based on Theorem 4 and on an idea from [GH90].

Proof of Theorem 1-1 **Proof of Theorem 1** From Theorem 4, with $k < (1/2 - \nu)\log n$ players, for some $\nu > 0$,

$$C^{(k)}(\mathrm{GIP}_{l,k}) \geq cl/4^k = n^{\Omega(1)}$$

On the other hand, suppose that some $\mod m$ polynomial P of degree $k-1$ weakly represents $\mathrm{GIP}_{l,k}$. Then the following k-player protocol can evaluate P with a small number of communicated bits. P is the sum of several monomials of degree at most $k-1$. Since for each variable of a monomial there is at most one player who does not know it, for every monomial there exists a player who knows all of its variables. Before starting the communication game for P, the players agree on who computes each monomial. Then each player—without any communication—privately computes the $\mod m$ sum of their assigned monomials. Next, communicating $k\lceil\log(m+1)\rceil$ bits, each player announces this $\bmod m$ sum, and every player privately adds up the numbers seen. Now, if the result is in the set S, then $\mathrm{GIP}_{l,k}=0$; otherwise, it is 1.

Proof of Theorem 1-2 From the preceding paragraph and Theorem 4,

$$k\lceil\log(m+1)\rceil \geq C^{(k)}(\mathrm{GIP}_{l,k}) = n^{\Omega(1)}$$

which leads to a contradiction.

Proof of Theorem 1 □

4 Random Restrictions and the Size Bounds

Proof of Theorem 2-1 **Proof of Theorem 2** To prove part 1, let

$$P(x_1,x_2,\ldots,x_n)=\sum_{H\in\mathcal{H}} a_H \prod_{i\in H} x_i$$

be a $\bmod m$ polynomial, weakly representing the OR of n variables, where $\mathcal{H} \subseteq 2^{\{1,2,\ldots,n\}}$ and $0\neq a_H\in\mathbb{Z}_m$. We apply *random restrictions* independently to each variable x_i, for $i=1,2,\ldots,n$, in a similar fashion to Ajtai [Ajt83], Furst, Saxe, and Sipser [FSS84] and Razborov and Wigderson [RW93]. Let

$$\rho(x_i)=\begin{cases} 0 & \text{with probability } 1-p \\ * & \text{with probability } p \end{cases}$$

where $\rho(x_i)=*$ means that x_i remains unrestricted, and $p=(1/2)n^{-1/2}$.

Proof of Theorem 2-2 For every $c>0$ and $|H|\geq (c/2)\log n$,

$$\Pr\left(\prod_{i\in H}\rho(x_i)\neq 0\right) \leq p^{\frac{c}{2}\log n} \leq n^{-\frac{c}{4}\log n} \tag{2}$$

Suppose that $|\mathcal{H}|$, the size of P, satisfies $|\mathcal{H}|\leq n^{\varepsilon\log n}$, for a small enough $\varepsilon>0$. Then, because of (2), the degree of the polynomial after the restriction will be small with high probability:

$$\Pr\Big(\deg(P\circ\rho)<(c/2)\log n\Big)=1-o(1)$$

while $P \circ \rho$ still represents the OR of at least $\sqrt{n}$ variables with probability $1-o(1)$. So, from (1), setting $c = \big(1/(q-1) - o(1)\big)$, where q is the smallest prime divisor of m, we arrive at a contradiction.

Proof of Theorem 2-3 Part 2 can be proved in similar fashion, using inequality (1) with $r \geq 2$ instead of $r = 2$. The details are left to the reader.

Proof of Theorem 2 □

Proof of Theorem 3 Let

$$P(x_1, x_2, \ldots, x_n) = \sum_{H \in \mathcal{H}} a_H \prod_{i \in H} x_i$$

be a $\bmod m$ polynomial, weakly representing f_n. We apply random restrictions independently to each variable x_i, for $i = 1, 2, \ldots, n$, as in the proof of Theorem 2, or as in [Ajt83], [FSS84], or [RW93]. Let

$$\rho(x_i) = \begin{cases} 0 & \text{with probability } (1-p)/2 \\ 1 & \text{with probability } (1-p)/2 \\ * & \text{with probability } p \end{cases}$$

where $p = (2 \ln h)/h$. Then, as in the proof of Theorem 2, or as in the proof of Theorem 3 in [RW93], if

$$|\mathcal{H}| \leq n^{\varepsilon \log n}$$

for a sufficiently small $\varepsilon > 0$, then

$$\Pr\Big(\deg(P \circ \rho) < \lfloor (1/3) \log h \rfloor\Big) \geq 1 - o(1) \tag{3}$$

while

$$\Pr\left(\bigoplus_{k=1}^{h} \rho(x_{ijk}) \text{ is a constant}\right) = (1-p)^h \leq 1/h^2$$

So, from (3) we conclude that—after fixing some more variables—there exists a $\bmod m$ polynomial that weakly represents $\mathrm{GIP}_{l,k}$ with degree less than $\lfloor (1/3) \log h \rfloor$, and this contradicts our Theorem 1.

Proof of Theorem 3 □

5 Acknowledgments

5-1 The author is indebted to David Barrington and to Gábor Tardos for discussions on this subject, and to Alexander Razborov, who directed the author's attention to the random restriction techniques.

Acknowledgement of support: The author acknowledges the support of the grants OTKA 4271, OTKA F 014919, and of the Magyar Tudományért Foundation.

References for CJTCS Volume 1995, Article 2

References

[ABFR91] James Aspnes, Richard Beigel, Merrick L. Furst, and Steven Rudich. The expressive power of voting polynomials. In *Proceedings of the 23rd ACM Symposium on Theory of Computation*, pages 402–409. Association for Computing Machinery, 1991.

[Ajt83] Miklós Ajtai. $\sum_1^1$ formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.

[BBR94] David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4:367–382, 1994. Also appeared in *Proceedings of the 24th ACM Symposium on Theory of Computing*, 1992.

[Bei93] Richard Beigel. The polynomial method in circuit complexity. In *Proceedings of the 8th Annual Conference on Structure in Complexity Theory*, pages 82–95. Institute of Electrical and Electronics Engineers, IEEE Computer Society Press, 1993.

[BNS92] László Babai, Noam Nisan, and Márió Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space tradeoffs. *Journal of Computer and System Sciences*, 45:204–232, 1992.

[CFL83] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *Proceedings 15th ACM Symposium on Theory of Computing*, pages 94–99. Association for Computing Machinery, 1983.

[FSS84] Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits and the polynomial time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.

[GH90] Mikael Goldmann and Johann Håstad. On the power of the small-depth threshold circuits. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 610–618. Institute of Electrical and Electronics Engineers, 1990.

[NS94] Noam Nisan and Márió Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4:462–467, 1994. Also apeared in *Proceedings of the 24th ACM Symposium on Theory of Computing*, 1992.

[Raz87] Alexander Razborov. Lower bounds for the size of circuits of bounded depth with basis (AND, XOR). *Mathematical Notes of the Academy of Science of the USSR*, 41(4):333–338, 1987.

[RW93] Alexander Razborov and Avi Wigderson. $n^{\Omega(\log n)}$ lower bounds on the size of depth-3 threshold circuits with AND gates at the bottom. *Information Processing Letters*, 45(6):303–307, April 1993.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on Theory of Computing*, pages 77–82. Association for Computing Machinery, 1987.

[TB95] Gábor Tardos and David A. Mix Barrington. A lower bound on the MOD 6 degree of the OR function. In *Proceedings of the 3rd Israel Symosium on the Theory of Computing and Systems*, pages 52–56, 1995.