Representing Boolean Functions as Polynomials Modulo Composite Numbers

David A. Mix Barrington,
Richard Beigel and Steven Rudich

Computer and Information Science Department
University of Massachusetts

COINS Technical Report 91-82

Representing Boolean Functions as Polynomials Modulo Composite Numbers
(Extended Abstract)

David A. Mix Barrington[*] Richard Beigel[†] Steven Rudich[‡]

November 4, 1991

Abstract

Define the MOD_m-degree of a boolean function F to be the degree of the smallest degree polynomial P, over the ring of integers modulo m, such that for all 0-1 assignments $\vec{x}$, $F(\vec{x}) = 0$ iff $P(\vec{x}) = 0$. We obtain the unexpected result that the MOD_m-degree of the OR of N variables is $O(\sqrt[r]{N})$, where r is the number of distinct prime factors of m. This is optimal in the case of representation by purely symmetric polynomials. The MOD_n function is 0 if the number of input ones is a multiple of n and is 1 otherwise. We show that the MOD_m-degree of both the MOD_n and $\neg MOD_n$ functions is $N^{\Omega(1)}$ exactly when there is a prime dividing n but not m. The MOD_m-degree of the MOD_m function is 1; we show that the MOD_m-degree of $\neg MOD_m$ is $N^{\Omega(1)}$ if m is not a power of a prime, $O(1)$ otherwise. A corollary is that there exists an oracle relative to which the MOD_mP classes (such as $\oplus$P) have the following structure: MOD_mP is closed under complement and union iff m is a prime power, and MOD_nP is a subset of MOD_mP iff all primes dividing n also divide m.

1 Introduction

Lower bounds in circuit complexity are currently hindered by what at first glance appears to be a small technical point. It is known that $\mathbf{AC}^0$ circuits which also allow mod-p gates for some fixed prime, p, can't compute the mod-q function for any q which is not a power of p [18, 19]. In contrast, it is not known if $\mathbf{AC}^0$ circuits which also allow mod-6 gates can compute every function in NP. It is conjectured that (as with the case of mod-p) $\mathbf{AC}^0$ with mod-m gates for any integer m can't compute the mod-n function when there is a prime dividing n but not m [19]. Indeed, it might be that some slight extension of the Razborov-Smolensky techniques will prove the conjecture. But there is also the very interesting possibility that mod-6 gates really are more powerful than mod-p gates! If this were true, it would pinpoint why mod-6 lower bounds are not forthcoming.

How could mod-6 be computationally different from mod-p? In this paper, we study this question in the polynomial model of computation. We say that a polynomial P over Z_m

[*]Computer Science Department, University of Massachusetts, Amherst MA 01003. Email: barring@fiji.cs.umass.edu. Supported by NSF Computer and Computation Theory grant CCR-8714714

[†]Dept. of Computer Science, 51 Prospect Street, P.O. Box 2158, Yale Station, New Haven, CT 06520-2158. Email: beigel-richard@cs.yale.edu. Supported in part by NSF grants CCR-8808949 and CCR-8958528.

[‡]School of Computer Science, Carnegie Mellon University, 5000 Forbes Ave, Pittsburgh PA 15213. Email: rudich@cs.cmu.edu.

represents a boolean function F if for all 0-1 valued assignments $\vec{x}$, $F(\vec{x}) = 0$ iff $P(\vec{x}) = 0$. In other words, we interpret the output of P to be the boolean value 1 if $P(\vec{x}) \neq 0 \bmod m$, and 0 otherwise. This is very similar to the standard definition of a mod-m gate which outputs 1 iff the number of input 1s is non-zero modulo m [18, 19, 3]. The MOD_m-degree of F, denoted $\delta(F, m)$, is the degree of the lowest degree polynomial which represents it. This model of boolean function complexity has been well explored in the case where m is a prime power [19, 8, 11, 10]. It is known that for the OR of N variables $\delta(OR, p) = \lceil v/(p-1) \rceil$ [19]. It is also known that $\delta(\text{mod-}n, p) = \Omega(N)$ when n is not a power of p [19].

In the case of composite moduli, there have been no results in this model. The obvious reason for this technical gap is that the techniques in the case of a prime modulus, p, have heavily relied on the fact that Z_p is a field. We prove results, modulo a composite m, which shed light on the essential similarities and differences between working mod-p and working mod-m.

A natural conjecture is that $\delta(OR, m) = \lceil v/(m-1) \rceil$, just as in the prime case [8]. We prove that $\delta(OR, m) = O(\sqrt[r]{v})$ where r is the number of distinct prime factors of m. We find this surprising. It gives a natural computational setting where mod-6 really is more powerful than mod-p. Furthermore, our construction uses only symmetric polynomials. Our upper bound is the best possible if only symmetric polynomials are allowed. We leave open the tantalizing possibility that for non-symmetric polynomials the degree of OR might be as low as an almost constant function (such as inverse Ackerman) [6]. We show that a low degree or sparse sub-linear degree polynomial for OR would have as a consequence the existence of small, low-depth mod-m circuits for the AND function.

Define the N-variable boolean function MOD_n to be 0 only when the number of input ones is a multiple of n, and 1 otherwise. We extend what is known to a composite modulus: for any integer m, $\delta(MOD_n, m) = N^{\Omega(1)}$ and $\delta(\neg MOD_n, m) = N^{\Omega(1)}$ when n has a prime divisor that is not a divisor of m. In the case of a square free m, we have $\delta(\neg MOD_n, m) = \Omega(N)$. For all m it is obvious that $\delta(MOD_m, m) = 1$. If m is a prime power then it is known that $\delta(\neg MOD_m, m) = O(1)$. In contrast, if m is not a prime power, we show that $\delta(\neg MOD_m, m) = N^{\Omega(1)}$ ($\Omega(N)$ is m is square free).

MOD_mP is defined to generalize the definition of $\oplus$P. A language L belongs to MOD_mP if there exists a nondeterministic polynomial-time machine M such that $x \in L \iff$ the number of accepting paths of M(x) is non-zero modulo m [1, 23, 21] Using our lower bounds we construct an oracle such that: MOD_nP is closed under complement and union iff n is a prime power, and $MOD_n\text{P} \not\subset MOD_m\text{P}$ iff n has a prime divisor that is not a divisor of m This oracle is consistent with the known structure of these classes.

A MOD_m polynomial of degree d has an associated MOD_m circuit consisting of an unbounded fan-in MOD_m gate at the root where each wire leading into it is a function of no more than d of the input variables. Such circuits could be thought of as the MOD_m versions of perceptrons [17]. Our upper bound for the OR function shows that such circuits can be more powerful than expected. Our lower bound proves that, when m is not a prime power, natural complexity classes based on these circuits are not closed under complement. Thus, definitions which were robust for prime powers fail to be for other numbers. We suggest a more robust definition: $\Delta(F, m) \equiv$ the degree of the lowest degree polynomial P over Z_m such that $F(\vec{x}) = 0$ and $F(\vec{y}) = 1$ implies $P(\vec{x}) \neq P(\vec{y})$. In the section on open problems, we propose the Δ measure as the correct next step.

2 Computing OR modulo a composite m

2.1 Background

It is natural to expect that it is difficult to compute the AND or OR function with components which can only sum their inputs modulo a constant. In the setting of constant-depth unbounded fan-in circuits, this intuition leads to the conjecture that exponential size is needed [16], in particular that AND is not in the polynomial size class called variously CC^0 [16] or "pure ACC" [24, 11]. Progress towards proving this conjecture has been very limited, as we shall see.

The same intuition also says that the MOD_m-degree of the OR function should be large, because simply summing modulo m should not be able to convert any number of small AND or OR operations into a large one. It is not hard to construct a polynomial of degree $\lceil \frac{N}{m-1} \rceil$ representing the N-variable OR function, or to prove that this degree is optimal in the case where m is a prime or prime power. But for general non-prime-power m, the best lower bound known on the m-degree of OR is a nonconstant but very slowly-growing function arising from a Ramsey argument [6]!

This and related questions came up in the study of permutation branching programs, or non-uniform automata over groups (see, e.g., [4, 7, 6] for background). This model of computation is closely related both to polynomials over finite rings and to circuits of MOD_m gates [5, 8]. It was here, in the study of width three permutation branching programs [2], that an important distinction was noticed. With MOD_m calculations, it is difficult or impossible to force a computation to always give one of two output values (e.g., compute the characteristic function of a set) rather than any of m values (e.g., "representing" a set in our current terminology). Later the nonconstant bound on the MOD_m-degree of OR showed that OR cannot be computed in any size by non-uniform automata over nilpotent groups, which correspond to a restricted case of MOD_m circuits [6].

Thérien posed the question of the MOD_m degree of OR, and the related question of how large a collection of linear polynomials modulo m is needed for the collection to represent OR, in the sense that the inputs are all zero iff all the polynomials are zero. Any lower bound in the latter case gives a corresponding lower bound on the size of MOD_m circuits for AND or OR, of any depth. Smolensky [20] had previously shown an $\Omega(\log n)$ lower bound on this size by a different argument. Then Barrington [8] showed an $\Omega(n/\log n)$ lower bound in the course of a general investigation of both these questions, and finally Thérien gave an $\Omega(n)$ lower bound [22] by the methods of [6]. This result would be implied by a linear lower bound on the MOD_m degree of OR, but not vice versa. (Krause and Waack [15] have exponential size lower bounds for a different but somewhat related model.)

2.2 A Surprising Upper Bound

In fact the MOD_m degree of OR for non-prime-power m is less than linear, and there is even a symmetric function that witnesses that fact. To see this, we need some notation dealing with symmetric functions. For simplicity, let $m = p_1 \ldots p_r$ with $r > 1$ be a square-free composite number. Define the n^{th} elementary symmetric function $s_n(\vec{x})$ to be the sum of all monomials of degree n in the N input variables. If j of the input variables are on, the value of $s_n(\vec{x})$ is $\binom{j}{n}$ mod-m, independently of N — we will write this as $s_n(j)$. We may think of the s_n as being single polynomals over infinitely many variables, noting that their value is well-defined whenever only finitely many of the inputs are 1. A symmetric polynomial of degree d is simply a linear combination of $s_0, s_1, \ldots, s_d$.

It is not hard to show that for prime p, the function $s_n(j)$ mod-p = $\binom{j}{n}$ mod-p is periodic, with period the least power of p such that $n \leq p$. Furthermore, the polynomials $s_0, \ldots, s_{p^e-1}$ are linearly independent modulo p, so that they are a basis of the vector space of symmetric functions with period p^e. If $N < p^e$, the OR of N variables is represented mod p by the function $f(j)$ with $f(j) = 0$ for $j = 0$ mod-p^e and $f(j) = 1$ otherwise. This function has degree at most $p^e - 1$.

But now consider an arbitrary degree d and let q_i be the greatest power of p_i such that $q_i - 1 \leq d$. By the above, there is a degree-d symmetric polynomial f_i such that $f_i(j) = 0$ mod-p_i iff $j = 0$ mod-q_i. Using the Chinese Remainder Theorem, let f be the unique polynomial mod m such that $f = f_i$ mod-p_i for all i. Clearly $f(j) = 0$ mod-m iff $f_i(j) = 0$ mod-p_i for all i iff $j = 0$ mod-q, where q is the product of the q_i. This f thus represents the OR of up to $q - 1$ variables. Since each q_i is $\Theta(d)$, $q = \Theta(d^r)$ and so we have that for square-free composite m, the MOD_m degree of the OR of m variables is $O(n^{1/r})$.

In the case where m is not sqare-free but still not a prime power, the same result can be proved similarly. First, consider the periodicity of the function $s_i(j)$ mod-p^e for a single prime p. One can show by induction that if $i < p^z$, then $s_i(j + p^{e+z-1}) = s_i(j)$ mod-p^e. Furthermore, although the functions s_i for $i < p^z$ do not generate all functions of this period, they do generate a function g satisfying $g(j) = 0$ mod-p^e iff $j = 0$ mod-p^z. This means that the MOD_{p^e} degree of the OR of N variables is $O(N)$, making the MOD_m degree $O(N^{1/r})$ if $m = p_1^{e_1} \ldots p_r^{e_r}$. Summarizing, then, we have:

Theorem 1 *The MOD_m degree of the OR of N variables is $O(N^{1/r})$, where r is the number of distinct primes dividing m.*

□

2.3 A Matching Lower Bound for Symmetric Polynomials

While we cannot rule out the possibility that some other polynomials of very slowly growing degree represent OR, we can say that any *symmetric* polynomials do essentially no better than our upper bound above:

Theorem 2 *If a symmetric polynomial modulo m represents the OR of N variables, then it has degree $\Omega(n^{1/r})$, where r is the number of distinct primes dividing m.*

Proof: We observed above that for any prime power p^e, any symmetric function of degree d satisfies $f(j) = f(j + p^{e+z-1})$ mod-p^e, where z is such that $p^z = \Theta(d)$. This means that any symmetric function modulo m is also periodic, with period $\Theta(d^r)$. Thus unless $N = O(d^r)$ (i.e., $d = \Omega(n^{1/r})$), the symmetric function has $f(j) = f(0)$ for some $0 < j \leq n$ and cannot represent the OR function. □

2.4 Consequences

It is natural to see how this surprising upper bound might help us build mod-m circuits for AND or OR. Suppose the MOD_m degree of OR is $d(N)$. With a single MOD_m gate we can reduce the N-way AND to at most $\binom{N}{d}$ d-way ANDs. We then have two choices

— implement the d-way ANDs by depth-2 mod-m circuits each of size $O(2^d)$, or apply the construction recursively to the d-way ANDs. If we use our $d = \Theta(N^{1/r})$ construction without recursion, we get a depth-3 mod-m circuit of size $2^{O(N^{1/r}\log N)}$. The recursion increases the depth without much reduction in the size. It is easy to construct depth-k, size $2^{O(N^{1/(k-1)})}$ mod-m circuits for AND whenever m is not a prime power, so these circuits are not too surprising.

If it were possible to reduce the degree further, however, there would be important consequences. Getting a MOD_m degree below polynomial ($d = N^{o(1)}$), would yield subexponential circuits of depth 3, and degree poly-log would yield quasi-polynomial size circuits. This may be interpreted either to say that such small MOD_m circuits for AND and OR are conceivable or that improving the degree bound is unlikely.

Even with degree $N^{\Omega(1)}$, there would be interesting mod-m circuits if we could get a polynomial with many fewer than $\binom{N}{d}$ nonzero terms. By the recursive construction, a representation of OR with degree $d = n^\alpha$ ($\alpha < 1$) and s terms would give a mod-m circuit of depth $O(\log\log n)$ and size $s^{\log\log n}$. Of course, our symmetric polynomials have every possible nonzero term of their degree.

3 Lower bounds for MOD$_p$ and the complement of MOD$_m$

.

In this section we present an $N^{\Omega(1)}$ lower bound (N denotes the number of Boolean inputs) on the MOD$_m$-degree of the MOD$_n$ function whenever there is a prime divisor of n that is not a divisor of m. For composite m, this is the first progress on Smolensky's question [19] whether poly-size circuits of AND, OR, and mod-m gates can compute the mod-p function for some prime p that is not a divisor of m.

We also present an $N^{\Omega(1)}$ lower bound on the MOD$_m$-degree of the $\neg$MOD$_m$ function for composite m. Our bounds contrast sharply with prior related results [14, 10, 11, 8, 19]. If the set of prime divisors of n is contained in the set of prime divisors of m then the MOD$_m$-degrees of $\neg$MOD$_n$ and of MOD$_n$ are also $O(1)$. If m is prime then the MOD$_m$-degree of the function $\neg$MOD$_m$ is $O(1)$.

Lemma 3 *Let q be a polynomial in binary variables $x_1, \ldots, x_N$. Let m be a square-free number whose largest prime divisor is $p_{\max}$. Suppose that q satisfies:*

$$q(x_1, \ldots, x_N) \not\equiv 0 \pmod{m} \quad \textit{if } x_1 = \cdots = x_N = 0$$
$$q(x_1, \ldots, x_N) \equiv 0 \pmod{m} \quad \textit{if } \textstyle\sum_{1 \le i \le N} x_i \textit{ is a power of a prime divisor of } m.$$

Then the degree of q is at least $N/(2p_{\max})$.

Proof: The proof is by contradiction. Suppose that q satisfies our hypothesis and that the degree of q is less than $N/(2p_{\max})$. Then the degree of q is less than $N/(2p)$ for every prime p that divides m.

Let p be any prime that divides m. Find the largest k such that $2p^k - 1 \le N$. Let $n = 2p^k - 1$. Let

$$r(x_1, \ldots, x_n) = q(x_1, \ldots, x_n, 0, \ldots, 0)$$

be obtained by setting $x_{N-n+1}, \ldots, x_N$ to 0 in q. Note that the degree of r is less than or equal to the degree of q and that $r(0, \ldots, 0) = q(0, \cdots, 0)$. Furthermore, r satisfies

$$\begin{array}{lll} r(x_1, \ldots, x_n) \not\equiv 0 & \pmod{m} & \text{if } x_1 = \cdots = x_n = 0 \\ r(x_1, \ldots, x_n) \equiv 0 & \pmod{m} & \text{if } \sum_{1 \le i \le n} x_i \text{ is a power of a prime divisor of } m. \end{array}$$

Let S denote a subset of $\{x_1, \ldots, x_n\}$. Let

$$\begin{aligned} \pi_S &= \left(\prod_{x \in S} x\right) \cdot \left(\prod_{x \notin S} (1 - x)\right), \\ \pi'_S &= \prod_{x \in S} x. \end{aligned}$$

We can write r in two ways:

$$r(x_1, \ldots, x_n) = \sum_S c_S \pi_S, \tag{1}$$

$$r(x_1, \ldots, x_n) = \sum_S c'_S \pi'_S, \tag{2}$$

where c_S and c'_S satisfy

$$\begin{array}{lll} c_\emptyset \not\equiv 0 & \pmod{m}, & \\ c_S \equiv 0 & \pmod{m} & \text{if } |S| \text{ is a power of a prime divisor of } m, \\ c'_S = 0 & & \text{if } |S| \ge N/(2p). \end{array}$$

Let

$$\begin{aligned} \sigma_i &= \sum_{|S|=i} c_S, \\ \sigma'_i &= \sum_{|S|=i} c'_S. \end{aligned}$$

Then

$$\begin{array}{lll} \sigma_0 = c_\emptyset, & & \\ \sigma_i \equiv 0 & \pmod{m} & \text{if } i \text{ is a power of a prime divisor of } m. \\ \sigma'_i = 0 & & \text{if } i \ge N/(2p). \end{array}$$

We note that

$$c'_S = \sum_{T \subseteq S} (-1)^{|S|-|T|} c_T.$$

Therefore,

$$\begin{aligned} \sigma'_i &= \sum_{|S|=i} \sum_{T \subseteq S} (-1)^{|S|-|T|} c_T \\ &= \sum_T \sum_{|S|=i, S \supseteq T} (-1)^{|S|-|T|} c_T \\ &= \sum_j \sum_{|T|=j} \sum_{|S|=i, S \supseteq T} (-1)^{|S|-|T|} c_T \end{aligned}$$

$$
\begin{aligned}
&= \sum_j \sum_{|T|=j} \binom{n-j}{i-j} (-1)^{i-j} c_T \\
&= (-1)^i \sum_j \binom{n-j}{i-j} (-1)^j \sum_{|T|=j} c_T \\
&= (-1)^i \sum_j \binom{n-j}{i-j} (-1)^j \sigma_j \\
&= (-1)^i \sum_j \binom{n-j}{n-i} (-1)^j \sigma_j .
\end{aligned}
$$

Recall that $n = 2p^k - 1$. Let $i = p^k$, so that $n - i = p^k - 1$. By Kummer's theorem,

$$
\begin{aligned}
\binom{n}{n-i} &\not\equiv 0 \pmod p, \\
\binom{n-j}{n-i} &\equiv 0 \pmod p \qquad \text{if } 0 < j < i.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
\sigma_i' &\equiv (-1)^i \left(\binom{n-i}{n-i} (-1)^i \sigma_i + \binom{n-0}{n-i} (-1)^0 \sigma_0 \right) \pmod p \\
&\equiv (-1)^i \left((-1)^i \sigma_i + \binom{n}{n-i} c_\emptyset \right) \pmod p \qquad \text{because } \sigma_0 = c_\emptyset .
\end{aligned}
$$

But $\sigma_i \equiv 0 \pmod m$ because $i = p^k$. Therefore

$$\sigma_i' \equiv (-1)^i \binom{n}{n-i} c_\emptyset \pmod p.$$

Because k was chosen so that $2p^{k+1} - 1 > N$, it follows that $i = p^k \geq N/(2p)$, so $\sigma_i' = 0$. Since $\binom{n}{n-i} \not\equiv 0 \pmod p$, it is necessary that $c_\emptyset \equiv 0 \pmod p$. Therefore

$$q(0, \ldots, 0) = r(0, \ldots, 0) = c_\emptyset \equiv 0 \pmod p.$$

Since $q(0, \ldots, 0)$ is divisible by every prime p that divides m, and m is square-free, $q(0, \ldots, 0) \equiv 0 \pmod m$, a contradiction. □

It follows that the MOD$_m$-degree of the complement of the MOD$_m$ predicate is $\Omega(N)$ if m is a square-free composite number.

Theorem 4 *Let q be a polynomial in binary variables $x_1, \ldots, x_N$. Let m be a square-free composite number whose largest prime divisor is $p_{\max}$. Suppose that q satisfies:*

$$q(x_1, \ldots, x_N) \equiv 0 \pmod m \iff \sum_{1 \leq i \leq N} x_i \not\equiv 0 \pmod m.$$

Then the degree of q is at least $N/(2p_{\max})$.

Proof: q satisfies the hypotheses of Lemma 3. □

Assume that m is a square-free number and p is not a divisor of m. We can show that the MOD_m-degree of the complement of the MOD_p predicate is $\Omega(N)$, and the MOD_m-degree of the MOD_p predicate is $\Omega(N^{1/(p-1)})$.

Theorem 5 *Let q be a polynomial in binary variables $x_1, \ldots, x_N$. Let m be a square-free number whose largest prime divisor is $p_{\max}$. Let p be any prime that is not a divisor of m.*

1. *Suppose that q satisfies:*

$$q(x_1, \ldots, x_N) \equiv 0 \pmod{m} \iff \sum_{1 \le i \le N} x_i \not\equiv 0 \pmod{p}.$$

Then the degree of q is at least $N/(2p_{\max})$.

2. *Suppose that q satisfies:*

$$q(x_1, \ldots, x_N) \equiv 0 \pmod{m} \iff \sum_{1 \le i \le N} x_i \equiv 0 \pmod{p}.$$

Then the degree of q is at least $\lfloor((N-1)/(p-1))^{1/(p-1)}\rfloor/(2p_{\max}(p-1))$.

Proof:

1. q satisfies the hypotheses of Lemma 3.

2. Let $n = \lfloor((N-1)/(p-1))^{1/(p-1)}\rfloor$. Let $\ell = (p-1)n^{p-1}$ Write $(p-1)(x_1 + \cdots + x_n)^{p-1}$ as the sum of ℓ monomials, $y_1 + \cdots + y_\ell$, each with coefficient 1. Let $r(x_1, \ldots, x_n) = q(y_1, \ldots, y_\ell, 1, 0, \ldots, 0)$. Then

$$\begin{aligned} r(x_1, \ldots, x_n) \equiv 0 \pmod{m} &\iff (p-1)(\sum_{1 \le i \le n} x_i)^{p-1} + 1 \equiv 0 \pmod{p} \\ &\iff (\sum_{1 \le i \le n} x_i)^{p-1} \equiv 1 \pmod{p} \\ &\iff \sum_{1 \le i \le n} x_i \not\equiv 0 \pmod{p}, \end{aligned}$$

by Fermat's little theorem. By Theorem 4 above, the degree of r is at least $\lfloor((N-1)/(p-1))^{1/(p-1)}\rfloor/(2p_{\max})$. Therefore, the degree of q is at least equal to $\lfloor((N-1)/(p-1))^{1/(p-1)}\rfloor/(2p_{\max}(p-1))$.

□

These results can be extended to general m via standard techniques (cf. [14, 10, 11]).

Theorem 6 *Let m be any number and let p be a prime that is not a divisor of m. Then the MOD_m-degrees of the functions MOD_p, $\neg\text{MOD}_p$, and $\neg\text{MOD}_m$ are all $N^{\Omega(1)}$.* □

This is very different from the behavior for prime moduli. If m is prime then the MOD_m-degree of the $\neg\text{MOD}_m$ function is a constant, $m-1$ by a folklore theorem [10, 14, 11, 8, 19].

Corollary 7 *Let m and n be any two numbers such that the set of prime divisors of n is not contained in the set of prime divisors of m. Then the MOD_m-degree of the functions MOD_n and $\neg\text{MOD}_n$ are both $N^{\Omega(1)}$.*

Proof: Let p be a prime divisor of n, but not of m. Observe that

$$\sum_{1\leq i\leq \lfloor N/p\rfloor} x_i \equiv 0 \pmod p \iff \sum_{1\leq j\leq p}\sum_{1\leq i\leq \lfloor N/p\rfloor} x_i \equiv 0 \pmod n,$$

so the MOD_m-degree of the function $\mathrm{MOD}_n(x_1,\ldots,x_N)$ is at least the MOD_m-degree of the function $\mathrm{MOD}_p(x_1,\ldots,x_{\lfloor N'\rfloor})$. where $N' = \lfloor N/p\rfloor$. □

On the other hand if n and m have the same set of prime divisors then the MOD_m-degree of the function MOD_n is $O(1)$ by a folklore theorem [14, 10, 11, 8, 19].

4 An oracle for the conjectured relations among $\mathrm{MOD}_m\mathrm{P}$ classes

The class $\mathrm{MOD}_m\mathrm{P}$ is a generalization of Papadimitrou and Zachos's counting class $\oplus$P. First developed by Cai and Hemachandra [12], these classes have since been studied by many others [9, 10, 14, 1, 23, 21]. It is known that $\mathrm{MOD}_m\mathrm{P} = \mathrm{MOD}_{m'}\mathrm{P}$ where m' is the product of all distinct prime divisors of m [14]; that $\mathrm{MOD}_n\mathrm{P} \subseteq \mathrm{MOD}_m\mathrm{P}$ if every prime divisor of n is a divisor of m [14]; that $\mathrm{MOD}_m\mathrm{P}$ is closed under polynomial-time Turing reductions if m is a power of a prime [10]; that $\mathrm{MOD}_m\mathrm{P}$ is closed under intersection for all m [14]; and that $\mathrm{MOD}_m\mathrm{P}$ is closed under union if and only if $\mathrm{MOD}_m\mathrm{P}$ is closed under complementation [14].

By standard techniques [13] it is possible to take circuit lower bounds and construct oracles that separate complexity classes. From our circuit lower bounds we can construct an oracle relative to which no containment relations hold among $\mathrm{MOD}_m\mathrm{P}$ classes, except for the relations listed in the preceding paragraph.

Theorem 8 *There exists an oracle relative to which:*

- $\mathrm{MOD}_n\mathrm{P} \subseteq \mathrm{MOD}_m\mathrm{P}$ *if and only if every prime divisor of n is a prime divisor of m.*
- $\mathrm{MOD}_m\mathrm{P}$ *is closed under complementation if and only if m is a prime power.*
- $\mathrm{MOD}_m\mathrm{P}$ *is closed under union if and only if m is a prime power.*

□

5 Open Problems and Conclusions

Relative to the δ measure, AND has a different complexity from OR, and MOD_m has a different complexity from $\neg MOD_m$. This says that δ does not provide a robust, well-behaved measure for the purposes of boolean function complexity. This deficiency is alleviated by proposing a measure which is robust in both these senses.

Definition 9 $\Delta(F,m) \equiv$ *the degree of the lowest degree polynomial P over Z_m such that $F(\vec{x}) = 0$ and $F(\vec{y}) = 1$ implies $P(\vec{x}) \neq P(\vec{y})$.*

Our results concerning OR are robust in the sense that $\Delta(OR, m) = \delta(OR, m)$ for all m. We ask if there is a degree N^{ϵ} mod m polynomial for the OR which has only a quasi-polynomial number of non-zero terms. If this is possible, we have shown that there would exist a small depth, small sized circuit for the AND (using only MOD_m gates).

As far as we know $\Delta(MOD_n, m)$ could be $\Omega(\delta(MOD_n, m))$. We consider our lower bounds for δ to be a first step in getting good bounds for the Δ measure.

6 Acknowlegements

Much thanks to David Applegate who wrote the program which found the first examples of lower than expected degree polynomials for the OR. Jim Aspnes also wrote some useful search programs and helped by simplifying the proof and the exposition of the symmetric OR polynomial construction. We have had several useful discussions with David Applegate, Jim Aspnes, Russell Impagliazzo, Roman Smolensky, Jiri Sgall, and Denis Thèrien.

References

[1] L. Babai and L. Fortnow. A characterization of #P by arithmetic straight-line programs. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 26–34, 1990.

[2] D. A. Barrington. Width 3 permutation branching programs. Technical Report TM-291, MIT Laboratory for Computer Science, Cambridge, Mass., dec 1985.

[3] D. A. Barrington. A note on a theorem of Razborov. Technical Report COINS TR 87-93, COINS Dept., U. of Massachusetts, Amherst, Mass., jul 1986.

[4] D. A. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *J. Comput. Syst. Sci.*, 38(1):150–164, Feb. 1989.

[5] D. A. M. Barrington. The current state of circuit lower bounds. Technical Report COINS TR 90-61, COINS Dept., U. of Massachusetts, Amherst, Mass., jul 1990.

[6] D. A. M. Barrington, H. Straubing, and D. Thèrien. Non-uniform automata over groups. *Information and Computation*, 89(2):109–132, Dec. 1990.

[7] D. A. M. Barrington and D. Thèrien. Finite monoids and the fine structure of NC^1. *J. ACM*, 35(4):941–952, Oct. 1988.

[8] D. M. Barrington. Some problems involving Razborov-Smolensky polynomials. Technical Report 90-59, UMass COINS, 1990. A revised version will appear in a special volume of the Proceedings of the London Mathematical Society devoted to the 1990 Durham Symposium.

[9] R. Beigel. Relativized counting classes: Relations among thresholds, parity, and mods. *J. Comput. Syst. Sci.*, 42(1):76–96, Feb. 1991.

[10] R. Beigel, J. Gill, and U. Hertrampf. Counting classes: Thresholds, parity, mods, and fewness. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*, pages 49–57. Springer-Verlag, Feb. 1990. Vol. 415 of *LNCS*.

[11] R. Beigel and J. Tarui. On ACC. In *Proceedings of the 32nd IEEE Symposium on Foundations of Computer Science*, pages 783–792, 1991.

[12] J. Cai and L. Hemachandra. On the power of parity polynomial time. *Mathematical Systems Theory*, 23:95–106, 1990.

[13] M. Furst, J. B. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, April 1984.

[14] U. Hertrampf. Relations among MOD-classes. *Theoretical Comput. Sci.*, 74(3):325–328, Aug. 1990.

[15] M. Krause and S. Waack. Variation ranks of communication matrices and lower bounds for depth two circuits having symmetric gates with unbounded fan-in. In *Proceedings of the 32nd IEEE Symposium on the Foundations of Computer Science*, pages 777-782, 1991.

[16] P. McKenzie and D. Thèrien. Automata theory meets circuit complexity. In *Proceedings of the 16th ICALP*, pages 589–602. Springer-Verlag, 1989. Lecture Notes in Computer Science 372.

[17] M. L. Minsky and S. A. Papert. *Perceptrons.* MIT Press, Cambridge, MA, 1988. Expanded Edition. The first edition appeared in 1968.

[18] A. A. Razborov. Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. *Math. notes of the Academy of Science of the USSR*, 41(4):333–338, Sept. 1987.

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

[20] R. Smolensky. On interpretation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 628–631, 1990.

[21] J. Tarui. Randomized polynomials, threshold circuits, and the polynomial hierarchy. In *Proceedings of the 8th Annual Symposium on Theoretical Aspects of Computer Science.* Springer-Verlag, 1991.

[22] D. Thèrien. Linear lower bound on the size of $CC_2^0(q)$-circuits computing the and function. Manuscript, McGill University, 1991.

[23] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. In *Proceedings of the 6th Annual Conference on Structure in Complexity Theory.* IEEE Computer Society Press, 1991. To appear.

[24] A. C.-C. Yao. On ACC and threshold circuits. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 619–627, 1990.