REPRESENTING BOOLEAN FUNCTIONS AS POLYNOMIALS MODULO COMPOSITE NUMBERS

David A. Mix Barrington,
Richard Beigel, and Steven Rudich

Abstract. Define the MOD_m-degree of a boolean function F to be the smallest degree of any 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 symmetric polynomials. The MOD_n function is 0 if the number of input ones is a multiple of n and is one otherwise. We show that the MOD_m-degree of both the MOD_n and $\neg\mathrm{MOD}_n$ 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 $\neg\mathrm{MOD}_m$ 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 $\mathrm{MOD}_m\mathrm{P}$ classes (such as $\oplus\mathrm{P}$) have this structure: $\mathrm{MOD}_m\mathrm{P}$ is closed under complementation and union iff m is a prime power, and $\mathrm{MOD}_n\mathrm{P}$ is a subset of $\mathrm{MOD}_m\mathrm{P}$ iff all primes dividing n also divide m.
Key words. Complexity of finite functions; circuit complexity; computation by polynomials; relativized complexity.
Subject classifications. 68Q15, 68Q40.

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 (Razborov 1987, Smolensky 1987). 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 (Smolensky 1987). 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 represents a boolean function F on N inputs if for all 0-1 valued assignments $\vec{x} \in \{0,1\}^N$, $F(\vec{x}) = 0$ 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 (Razborov 1987, Smolensky 1987, Barrington 1986). 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 (Smolensky 1987, Barrington 1992a, Beigel and Tarui 1991, Beigel and Gill 1992). It is known that $\delta(\mathrm{OR}, p) = \lceil N/(p-1) \rceil$ (Smolensky 1987). It is also known that $\delta(MOD_n, p) = \Omega(N)$ when n is not a power of p (Smolensky 1987).

In the case of composite moduli, there have been very few results in this model (see, e.g., Krause and Waack 1991, Szegedy 1989, which we review below). 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 $\delta(\mathrm{OR}, m) = \lceil N/(m-1) \rceil$, just as in the prime case (Barrington 1992a). In Section 2, we prove that $\delta(\mathrm{OR}, m) = O(\sqrt[r]{N})$, 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 MOD_m-degree of OR might be as low as $O(\log N)$, the lower bound proved after our work by Tardos and Barrington (1994)—previously the best bound was only $\omega(1)$ (Barrington *et al.* 1990). 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. In Section 3, we extend what is known to a composite modulus: for any integer m, $\delta(MOD_n, m) = N^{\Omega(1)}$ and

$\delta(\neg\mathrm{MOD}_n, m) = N^{\Omega(1)}$ when n has a prime divisor that is not a divisor of m. In the case of a square free m, we have $\delta(\neg\mathrm{MOD}_n, m) = \Omega(N)$. For all m, it is obvious that $\delta(\mathrm{MOD}_m, m) = 1$. If m is a prime power, then it is known that $\delta(\neg\mathrm{MOD}_m, m) = O(1)$. In contrast, if m is not a prime power, we show that $\delta(\neg\mathrm{MOD}_m, m) = N^{\Omega(1)}$ ($\Omega(N)$ if m is square free).

The complexity class $\mathrm{MOD}_m\mathrm{P}$ is defined to generalize the definition of $\oplus\mathrm{P}$. A language L belongs to $\mathrm{MOD}_m\mathrm{P}$ if there exists a nondeterministic polynomial-time machine M such that $x \in L$ iff the number of accepting paths of $\mathrm{M}(x)$ is non-zero modulo m (Babai and Fortnow 1990, Toda and Ogiwara 1992, Tarui 1993). In Section 4, we use our lower bounds to construct an oracle such that $\mathrm{MOD}_n\mathrm{P}$ is closed under complementation and union iff n is a prime power, and $\mathrm{MOD}_n\mathrm{P} \subseteq \mathrm{MOD}_m\mathrm{P}$ iff all prime divisors of n are divisors 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 can be thought of as the MOD_m versions of perceptrons (Minsky and Papert 1968). 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 complementation. Thus, definitions which were robust for prime powers fail to be for other numbers. We suggest a more robust definition: $\Delta(F, m)$ is the lowest degree of any 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 Section 5, 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 (McKenzie *et al.* 1991), in particular that AND is not in the polynomial size class called variously "CC^0" (McKenzie *et al.* 1991) or "pure ACC" (Yao 1990, Beigel and Tarui 1991). 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 $\lceil(N/(m-1)\rceil$ 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 until recently on the MOD_m-degree of OR was a nonconstant but very slowly-growing function arising from a Ramsey argument (Barrington *et al.* 1990). There is now a $(\log N)^{\Omega(1)}$ lower bound, which is $O(\log N)$ if m is divided by only two distinct primes, due to Tardos and Barrington (1994).

This and related questions came up in the study of permutation branching programs, or non-uniform automata over groups (Barrington 1989, Barrington and Thérien 1988, Barrington *et al.* 1990). This model of computation is closely related both to polynomials over finite rings and to circuits of MOD_m gates (Barrington 1990, 1992a). It was here, in the study of width three permutation branching programs (Barrington 1985), 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., to compute the characteristic function of a set) rather than any of m values (e.g., to "represent" 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 (Barrington *et al.* 1990).

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 N 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 (1990) had previously shown an $\Omega(\log N)$ lower bound on this size by a different argument. Then, Barrington (1992a) showed an $\Omega(N/\log N)$ lower bound in the course of a general investigation of both these questions, and finally Thérien (1992) gave an $\Omega(N)$ lower bound by the methods of Barrington *et al.* (1990). This result would be implied by a linear lower bound on the MOD_m-degree of OR, but not vice versa.

Independently of this effort, other researchers have also derived degree lower bounds for MOD_m polynomials. Krause and Waack (1991) use a form of communication complexity to investigate the complexity of the boolean function $EQ_N(x, y)$, which is one iff the N-bit strings x and y are identical. They show that any polynomial computing this function in our sense has exponentially many terms, and this implies that this function has linear MOD_m-degree (Krause, personal communication). In his Ph.D. thesis, Szegedy (1989) extends the methods of Smolensky (1987) to give an $\Omega(\sqrt{N})$ lower bound on the MOD_m-degree of the N-variable majority function. His bound also holds for functions which agree with the majority function on all but a constant fraction of the possible input assignments. Subsequent to our own work, Tsai (1993) has shown a lower bound of $N/2$ for the MOD_m-degree of the majority function and Grolmusz (1994) has shown an $O(\log N)$ lower bound on the degree of the generalized inner product function (even with the more robust definition of Section 5).

2.2. A Surprising Upper Bound. In fact, the MOD_m-degree of OR for a non-prime-power m is less than linear, and there is even a symmetric function which witnesses that fact. To see this, we need some notation dealing with symmetric functions. For simplicity, let $m = p_1 \dots p_r$, 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 $\binom{j}{n}$, independently of N—we will write this as $s_n(j)$. We may think of the s_n as being single polynomials 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 $s_0, s_1, \dots, s_d$.

It is not hard to show that for prime p, the function $s_n(j) \bmod p$, which is equal to $\binom{j}{n} \bmod p$, is periodic. The period is p^e, the least power of p such that $n < p^e$. Furthermore, the polynomials $s_0, \dots, s_{p^e-1}$ 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 modulo p by the function $f(j)$ with $f(j) = 0$ for $j \equiv 0 \pmod{p^e}$ 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 $f_i(j) \equiv 0 \pmod{p_i}$ iff $j \equiv 0 \pmod{q_i}$. Using the Chinese Remainder Theorem, let f be the unique polynomial modulo m such that $f \equiv f_i \pmod{p_i}$ for all i. Clearly, $f(j) \equiv 0 \pmod{m}$ iff $f_i(j) \equiv 0 \pmod{p_i}$ for all i iff $j \equiv 0 \pmod{q}$, 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 N variables is $O(N^{1/r})$.

In the case where m is not square-free but still not a prime power, the same result can be proved similarly. First, consider the periodicity of the function $s_i(j) \bmod p^e$ for a single prime p. One can show by induction that if $i < p^z$, then $s_i(j+p^{e+z-1}) \equiv s_i(j) \pmod{p^e}$. Furthermore, although the functions s_i for $i < p^z$ do not generate all functions of this period, they do generate a function g which correctly computes the OR of up to $p^z - 1$ variables, namely:

$$g = \sum_{i=1}^{p^z-1} (-1)^{i+1} s_i.$$

(This is because for any j such that $1 \leq j \leq p^z - 1$, $g(j) = 1$ over the integers and hence also in Z_{p^e}.) 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 the following theorem.

THEOREM 2.1. *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* polynomial does essentially no better than our upper bound above:

THEOREM 2.2. *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 polynomial of degree d satisfies $f(j) \equiv f(j+p^{e+z-1}) \pmod{p^e}$, where z is such that $p^z = \Theta(d)$. This means that any symmetric polynomial 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 $f(j) \equiv f(0) \pmod{m}$ for some $0 < j \leq N$ and cannot represent the OR function. □

2.4. Consequences. It is natural to ask whether this surprising upper bound might help us build MOD_m circuits for AND or OR. Suppose the MOD_m-degree of OR is $d(N)$. Using DeMorgan's Law, with a single MOD_m gate we can reduce the N-way AND to at most $(m-1)\binom{N}{d}$ d-way ANDs. We then have two choices: implement the d-way ANDs by brute force, using 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 $2^{O(N^{1/r}\log N)}$. Additional recursion increases the depth without much reduction in the size. (It is straighforward, extending the $k = 2$ version of Barrington (1985), to construct depth-k, size $2^{O(N^{1/(k-1)})}$ MOD_m circuits for AND whenever m is not a prime power. Therefore these circuits are not too surprising.)

If it were possible to reduce the MOD_m-degree of OR further, however, there would be important consequences. Getting the MOD_m-degree below polynomial ($d = N^{o(1)}$), would yield subexponential circuits of depth 3, and getting it poly-log would yield quasi-polynomial size circuits. The latter result would collapse the quasi-polynomial size circuit complexity classes qCC^0 and $qACC^0$, as defined in Barrington (1992b). This may be interpreted either to say that such small MOD_m circuits for AND and OR are conceivable or that improving the MOD_m-degree bound is unlikely.

Even with a MOD_m-degree of $N^{\Omega(1)}$, 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 $s^{\log\log N}$. Unfortunately, symmetric polynomials have every possible nonzero term of their degree.

3. Lower bounds for MOD_p and the negation of MOD_m

.

In this section, we present an $N^{\Omega(1)}$ lower bound 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 (1987) whether polynomial 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 $\neg\mathrm{MOD}_m$ function when m is not a prime power. This lower bound contrasts sharply with the corresponding lower bounds when m is a prime power (Hertrampf 1990, Beigel and Gill 1992, Beigel and Tarui 1991, Barrington 1992a, Smolensky 1987). If the set of prime divisors of n is contained in the set of prime divisors of m, then the MOD_m-degrees of $\neg\mathrm{MOD}_n$ and of MOD_n are also $O(1)$. If m is a prime power then the MOD_m-degree of the function $\neg\mathrm{MOD}_m$ is $O(1)$.

Our $N^{\Omega(1)}$ lower bounds become $\Omega(N)$ lower bounds in the special case where the modulus m is square-free. Subsequent to our work, Tsai (1993) has been able to remove this restriction and demonstrate that if m is not a prime power and n has a prime divisor that does not divide m, each of the functions $\neg\mathrm{MOD}_m$, MOD_n, and $\neg\mathrm{MOD}_n$ requires linear degree.

LEMMA 3.1. *Let q be a polynomial in binary variables $x_1, \dots, x_N$. Let m be a square-free number whose largest prime divisor is $p_{\max}$. Suppose that q satisfies:*

- $q(x_1, \dots, x_N) \not\equiv 0 \pmod{m}$ *if the sum of the inputs is zero, and*
- $q(x_1, \dots, x_N) \equiv 0 \pmod{m}$ *if this sum is a power of a prime divisor of m (an "m-power").*

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 $2p^k - 1 \leq N$. Let $n = 2p^k - 1$. Let

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

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

- $r(x_1, \dots, x_n) \not\equiv 0 \pmod{m}$ if $x_1 = \cdots = x_n = 0$, and
- $r(x_1, \dots, x_n) \equiv 0 \pmod{m}$ if $\sum_{1 \leq i \leq n} x_i$ is an m-power.

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

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

We can write r in two ways:

$$r(x_1, \dots, x_n) = \sum_S c_S \pi_S, \tag{3.1}$$

$$r(x_1, \dots, x_n) = \sum_S c'_S \pi'_S, \tag{3.2}$$

where c_S and c'_S satisfy the following equalities:

$$\begin{array}{ll} c_\emptyset \not\equiv 0 \pmod{m}, & \\ c_S \equiv 0 \pmod{m} & \text{if } |S| \text{ is an } m\text{-power}, \\ c'_S = 0 & \text{if } |S| \geq N/(2p). \end{array}$$

Let

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

Then we have the following equalities:

$$\begin{array}{ll}\sigma_0 = c_\emptyset, & \\ \sigma_i \equiv 0 \pmod{m} & \text{if } i \text{ is an } m\text{-power},\\ \sigma'_i = 0 & \text{if } i \geq N/(2p).\end{array}$$

We note that

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

Therefore,

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

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,

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

(because $\sigma_0 = c_\emptyset$). 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. $\square$

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

THEOREM 3.2. *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 $q(x_1, \ldots, x_N) \equiv 0 \pmod{m}$ iff the sum of the inputs is nonzero modulo m. Then the degree of q is at least $N/(2p_{\max})$.*

PROOF. q satisfies the hypotheses of Lemma 3.1. $\square$

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 negation 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 3.3. *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 $p_{\max}$. Let p be any prime that is not a divisor of m.*

1. *Suppose that $q(x_1, \ldots, x_N) \equiv 0 \pmod{m}$ iff the sum of the inputs is nonzero modulo p. Then the degree of q is at least $N/(2p_{\max})$.*

2. *Suppose that $q(x_1, \ldots, x_N) \equiv 0 \pmod{m}$ iff the sum of the inputs is zero modulo 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 3.1.

2. Let $n = \lfloor((N-1)/(p-1))^{1/(p-1)}\rfloor$. Let $\ell = (p-1)n^{p-1}$. We may 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, letting $s = \sum_{1\le i\le n} x_i$, we have that

$$\begin{array}{rcll} r(x_1,\ldots,x_n) & \equiv & 0 \pmod m & \iff \\ (p-1)s^{p-1}+1 & \equiv & 0 \pmod p & \iff \\ s^{p-1} & \equiv & 1 \pmod p & \iff \\ s & \not\equiv & 0 \pmod p, & \end{array}$$

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

$$\lfloor((N-1)/(p-1))^{1/(p-1)}\rfloor/(2p_{\max}(p-1)),$$

as required. □

These results can be extended to general m via standard techniques (Hertrampf 1990, Beigel and Gill 1992, Beigel and Tarui 1991).

THEOREM 3.4. *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, $\neg\mathrm{MOD}_p$, and $\neg\mathrm{MOD}_m$ 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 $\neg\mathrm{MOD}_m$ function is a constant, $m-1$, by a folklore theorem (Beigel and Gill 1992, Hertrampf 1990, Beigel and Tarui 1991, Barrington 1992a, Smolensky 1987).

COROLLARY 3.5. *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 $\neg\mathrm{MOD}_n$ are both $N^{\Omega(1)}$.*

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

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

so the MOD_m-degree of the MOD_n function of N variables is at least the MOD_m-degree of the MOD_p function of N' variables, 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 (Beigel and Gill 1992, Hertrampf 1990, Beigel and Tarui 1991, Barrington 1992a, Smolensky 1987).

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 the counting class $\oplus\mathrm{P}$ (Papadimitriou and Zachos 1983, Goldschlager and Parberry 1986). First developed by Cai and Hemachandra (1990), these classes have since been studied by many others (Beigel 1991, Beigel and Gill 1992, Hertrampf 1990, Babai and Fortnow 1990, Toda and Ogiwara 1992, Tarui 1993). 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 (Hertrampf, 1990); that $\mathrm{MOD}_n\mathrm{P} \subseteq \mathrm{MOD}_m\mathrm{P}$ if every prime divisor of n is a divisor of m (Hertrampf, 1990); that $\mathrm{MOD}_m\mathrm{P}$ is closed under polynomial-time Turing reductions if m is a power of a prime (Beigel and Gill, 1992); that $\mathrm{MOD}_m\mathrm{P}$ is closed under intersection for all m (Hertrampf, 1990); and that $\mathrm{MOD}_m\mathrm{P}$ is closed under union if and only if $\mathrm{MOD}_m\mathrm{P}$ is closed under complementation (Hertrampf, 1990).

By standard techniques (Furst *et al.* 1984) 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 4.1. *There exists an oracle relative to which the following properties hold:*

- $\mathrm{MOD}_n\mathrm{P} \subseteq \mathrm{MOD}_m\mathrm{P}$ *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, recent progress, and conclusions

Relative to the δ measure, AND has a different complexity from OR, and MOD_m has a different complexity from $\neg\mathrm{MOD}_m$. 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 5.1. *$\Delta(F, m)$ is defined to be the lowest degree of any polynomial P over Z_m such that $F(\vec{x}) = 0$ and $F(\vec{y}) = 1$ implies $P(\vec{x}) \neq P(\vec{y})$.*

Because the OR function is zero on only one input setting, it is easy to see that $\Delta(\mathrm{OR}, m) = \delta(\mathrm{OR}, m)$ for all m. Therefore, our results concerning OR are robust. In contrast, as far as we know, $\Delta(\mathrm{MOD}_n, m)$ could be much smaller than $\delta(\mathrm{MOD}_n, m)$. On the other hand, it is also possible that $\Delta(\mathrm{MOD}_n, m)$ could be $\Omega(\delta(\mathrm{MOD}_n, m))$. We consider our lower bounds for δ to be a first step in getting good bounds for the Δ measure.

Subsequent to our work, there have been two separate $\Omega(\log N)$ degree lower bounds proven for the Δ measure, which are now the best known for natural functions. Tardos and Barrington (1994) have proven such a bound for the OR function in the case when m has only two distinct prime divisors (if it has r prime divisors, the bound degrades to $\Omega((\log N)^{1/(r-1)})$). Grolmusz (1994) has observed that an $\Omega(\log N)$ degree lower bound for the generalized inner product function follows from the lower bound on the k-party communication complexity of that function due to Babai, Nisan, and Szegedy (1989).

We have mentioned Tsai's extensions of our work (Tsai, 1993) as appropriate in the main text. He proves linear lower bounds on the degree of the majority function, as in earlier work by Szegedy (1989), and on the degree of the functions $\neg\mathrm{MOD}_m$, MOD_n, and $\neg\mathrm{MOD}_n$, where m is not a prime power and n has a prime divisor which does not divide m. The latter results improve ours in the case when m is not square-free.

Another important question is whether or not there is a degree N^ϵ polynomial over Z_m that computes OR and has only a quasi-polynomial number of non-zero terms. If so, there exist small depth-3 circuits, consisting entirely of MOD_m gates, that compute the AND function.

Some of our results were inspired by computer examination of small cases of the general problem. For example, what is the largest N such that $\delta(\mathrm{OR}, 6) = 2$ on N variables? For symmetric polynomials the answer is $N = 8$, but it is easy to construct non-symmetric polynomials showing $N \geq 10$. Our conjecture is that $N = 10$, but we have been unable to confirm this. Recent work by one of us (Barrington) along these lines has made some progress, which we summarize here. Extensive but far from exhaustive computer searches have failed to find a counterexample to the $N = 10$ conjecture. However, actually confirming the conjecture directly by computer search seems so far to be infeasible. It has been shown analytically (Tardos and Barrington, 1994) that $\delta(\mathrm{OR}, 6) = \Omega(\log(N))$ in general, and $\delta(\mathrm{OR}, 6) > 2$ for $N > 18$, but this is not a satisfying answer.

Acknowledgements

Many 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, Dan Spielman, Gabor Tardos, Denis Thérien, and Shi-Chun Tsai. This paper is a revision of an earlier conference version (Barrington *et al.* , 1992). David A. Mix Barrington was supported by NSF grants CCR-8922098 and CCR-9207829. Richard Beigel was supported in part by NSF grants CCR-8808949 and CCR-8958528.

References

L. Babai and L. Fortnow, A characterization of #P by arithmetic straight-line programs. In *Proc. 31st Ann. IEEE Symp. Found. of Comput. Sci.*, 1990, 26–34.

L. Babai, N. Nisan, and M. Szegedy, Multiparty protocols and pseudorandom sequences. In *Proc. Twenty-first ACM Symp. Theor. Comput.*, 1989, 1-11.

D. A. Barrington, *Width 3 permutation branching programs.* Technical Report TM-291, MIT Laboratory for Computer Science, Cambridge, Mass., Dec. 1985.

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

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

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

D. A. M. Barrington, Some problems involving Razborov-Smolensky polynomials. In *Boolean Function Complexity*, ed. M. S. Patterson, London Mathematical Society Lecture Note Series 169, Cambridge University Press, 1992a, 109–128.

D. A. M. Barrington, Quasipolynomial size circuit complexity. In *Structure in Complexity Theory: Seventh Annual Conference*, 1992b, 86-93.

D. A. M. Barrington, R. Beigel, and S. Rudich, Representing Boolean functions as polynomials modulo composite numbers. In *Proc. Twenty-fourth ACM Symp. Theor. Comput.*, 1992, 455-461.

D. A. M. Barrington, H. Straubing, and D. Thérien, Non-uniform automata over groups. *Inform. and Comput.* **89** (1990), 109–132.

D. A. M. Barrington and D. Thérien, Finite monoids and the fine structure of NC^1. *J. Assoc. Comp. Mach.* **35** (1988), 941–952.

R. Beigel, Relativized counting classes: Relations among thresholds, parity, and mods. *J. Comput. System. Sci.* **42** (1991), 76–96.

R. Beigel and J. Gill, Counting classes: Thresholds, parity, mods, and fewness. *Theoret. Comput. Sci.* **103** (1992), 3–23.

R. Beigel and J. Tarui, On ACC. In *Proc. 32nd Ann. IEEE Symp. Found. Comput. Sci.*, 1991, 783–792. Revised version in this volume.

J. Cai and L. Hemachandra, On the power of parity polynomial time. *Math. Systems Theory* **23** (1990), 95–106.

M. Furst, J. B. Saxe, and M. Sipser, Parity, circuits, and the polynomial-time hierarchy. *Math. Systems Theory*, **17** (1984), 13–27.

L. Goldschlager and I. Parberry, On the construction of parallel computers from various bases of Boolean functions. *Theoret. Comput. Sci.* **43** (1986), 43–58.

V. Grolmusz, *On the Weak Mod-m Degree of the GIP Function.* Draft, Eötvös University, April 1994.

U. Hertrampf, Relations among MOD-classes. *Theoret. Comput. Sci.* **74** (1990), 325–328.

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 *Proc. 32nd Ann. IEEE Symp. Found. Comput. Sci.*, 1991, 777–782.

P. McKenzie, P. Péladeau and D. Thérien, NC^1: the automata-theoretic viewpoint. *Comput. Complexity* **1** (1991), 330–359.

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

C. Papadimitriou and S. Zachos, Two remarks on the power of counting. *Proc. Sixth GI Conf. Theoret. Comp. Sci., Lecture Notes in Computer Science* **145**, Springer-Verlag, Berlin, 1983, 269–276.

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** (1987), 333–338.

R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. Nineteenth Ann. ACM Symp. Theor. Comput.*, 1987, 77–82.

R. Smolensky, On interpretation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates. In *Proc. 31st Ann. IEEE Symp. Found. Comput. Sci.*, 1990, 628–631.

M. Szegedy, *Algebraic Methods in Lower Bounds for Computational Models with Limited Communication.* Ph.D. thesis, University of Chicago, Dec. 1989.

G. Tardos and D. A. M. Barrington, *A Lower Bound on the Mod 6 Degree of the OR Function.* Draft, U. of Massachusetts, April 1994.

J. Tarui, Probabilistic polynomials, AC^0 functions, and the polynomial-time hierarchy. *Theoret. Comput. Sci.* **113** (1993), 167–183.

D. Thérien, Circuits of MOD m gates cannot compute AND in sublinear size. In *Proc. LATIN '92 (First Latin American Symposium on Theoretical Computer Science)*, 1992. Revised version in this volume.

S. Toda and M. Ogiwara, Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM J. Comput.* **21** (1992), 316-328.

S.-C. Tsai, Lower bounds on representing Boolean functions as polynomials in Z_m. In *Proc. Structure in Complexity Theory: Eighth Ann. Conference*, 1993, 96–101.

A. C.-C. Yao, On ACC and threshold circuits. In *Proc. 31st Ann. IEEE Symp. Found. Comput. Sci.*, 1990, 619–627.

Manuscript received 7 May 1993

David A. Mix Barrington
Computer Science Department
P. O. Box 34610
University of Massachusetts
Amherst, MA 01003-4610, U.S.A.
barring@cs.umass.edu

Richard Beigel
Yale University
Department of Computer Science
P.O. Box 208285
New Haven, CT 06520-8285, U.S.A.
beigel-richard@cs.yale.edu

Steven Rudich
School of Computer Science
Carnegie Mellon University
5000 Forbes Ave
Pittsburgh, PA 15213, U.S.A.
rudich@cs.cmu.edu