A LOWER BOUND ON THE MOD 6 DEGREE OF THE OR FUNCTION

Gábor Tardos and David A. Mix Barrington

Abstract.

We examine the computational power of modular counting, where the modulus m is not a prime power, in the setting of polynomials in boolean variables over Z_m. In particular, we say that a polynomial P weakly represents a boolean function f (both have n variables) if for any inputs x and y in $\{0,1\}^n$ we have $P(x) \neq P(y)$ whenever $f(x) \neq f(y)$. Barrington, Beigel, and Rudich (1994) investigated the minimal degree of a polynomial representing the OR function in this way, proving an upper bound of $O(n^{1/r})$ (where r is the number of distinct primes dividing m) and a lower bound of $\omega(1)$. Here we show a lower bound of $\Omega(\log n)$ when m is a product of two primes and $\Omega((\log n)^{1/(r-1)})$ in general. While many lower bounds are known for a much stronger form of representation of a function by a polynomial (Barrington, Beigel and Rudich 1994, Tsai 1996), using this liberal (and, we argue, more natural) definition very little is known. While the degree is known to be $\Omega(\log n)$ for the generalized inner product because of its high communication complexity (Grolmusz 1995), our bound is the best known for any function of low communication complexity and any modulus not a prime power.

Key words. Circuit complexity, modular counting, boolean function complexity.

Subject classifications. 68Q15

1. Introduction

One measure of our ignorance of circuit complexity is that we still know very little about how simple operations (such as AND, OR, or modular counting)

can combine in parallel to compute boolean functions. In the model of circuits of constant depth and unbounded fan-in, we know that AND and OR alone need exponential size to compute any MOD-m function, that MOD-p alone for prime p cannot do AND or OR at all, and that AND, OR, and MOD-p need exponential size to do MOD-r unless r is a power of p. (See, e.g., Boppana and Sipser (1990) for a survey of these results.) But we have very few lower bounds on the computational power of MOD-m in this setting (m not a prime power, as prime powers are equivalent in power to their primes). A notorious statement of this is that we cannot yet rule out the implausible idea that MOD-6 gates alone might be able to compute NP-complete problems in constant depth and polynomial size, whereas we have no reason to believe that they can do AND or OR within these bounds.

The lower bounds on the power of MOD-p gates in *circuits* use the auxiliary model of *polynomials* in n boolean variables over Z_p, with *degree* as the complexity measure. Counting modulo p is clearly an easy operation in this model. AND and OR of unbounded fan-in are hard (hence the impossibility of doing them with MOD-p gates alone) but Razborov (1987) showed that AND or OR are approximated by polynomials of low degree. This means that small circuits of AND, OR, and MOD-p gates cannot perform operations like MAJORITY or MOD-r that can be shown to be not approximable in this way (Razborov 1987, Smolensky 1987).

Representing circuits by polynomials is a powerful general technique (for example, see the survey article of Beigel (1993), which is largely concerned with using polynomials over the integers or reals to bound the power of circuits with some MAJORITY gates). It is natural to try to use polynomials over Z_m to bound the power of MOD-m gates for general m, but the technique breaks down. A MOD-m gate adds its inputs modulo m, which is easy for a Z_m polynomial, but then must somehow convert the answer to boolean form, which is no longer an algebraically simple operation as it was in the prime modulus case. Circuits can simulate low-degree polynomials but not, so far as we know, vice versa. But even this apparently weaker model has us stumped for the most part, as we shall see. Following Barrington, Beigel, and Rudich (1994), we investigate the degree of polynomials over Z_m that represent the OR function and present a new lower bound on this degree.

To begin with, though, we must decide what it means for a polynomial P over Z_m to represent a boolean function f. In the definitions x and y denote arbitrary $0-1$ vectors. We present three successively more liberal candidate definitions:

- **Strong representation:** We insist that $f(x) = P(x)$ for all x, in particular that $P(x)$ is always zero or one.
- **One-sided representation:** We insist that $f(x) = 0$ iff $P(x) = 0$. If $f(x) = 1$, we let $P(x)$ take on any nonzero value in Z_m.
- **Weak representation:** We insist that for any x and y, $P(x) \neq P(y)$ whenever $f(x) \neq f(y)$. Equivalently, there is a subset S of Z_m such that $f(x) = 0$ iff $P(x) \in S$.

Each definition gives us a complexity measure on boolean functions – the minimal degree of a polynomial representing the function in each way, which we will call the *strong degree*, *one-sided degree*, and *weak degree*. In the case of a prime modulus p, converting a weak representation into a strong one requires only that we multiply the degree by $p - 1$, so we can see that the three degree measures then differ only by a multiplicative constant. We observe below that a similar relationship holds when the modulus is a prime power, but no such relationship holds if it is not. To take one example, the "one-sided MOD-m" function, whose one-sided representation is $\sum_{i=1}^{n} x_i$, has one-sided degree 1 but strong degree n.

The strong degree is generally easy to calculate because the polynomial strongly representing a given boolean function is essentially unique. But if we want to use polynomials to gain insight into computation by circuits, we will need to deal with the other two measures. A one-sided or weak representation of degree d is equivalent to a depth-two circuit consisting of a single MOD-m gate on the top and several AND gates of fan-in at most d below. The difference is how the MOD-m gate converts its Z_m sum to a boolean value — zero to zero and nonzero to one (as in the one-sided representation and in the most usual definition for MOD-m gates) or by an arbitrary function from Z_m to $\{0, 1\}$ (as in the weak representation).

Barrington, Beigel and Rudich (1994) and Tsai (1996) proved a number of strong lower bounds for the one-sided model, that allow the construction of oracles under which the conjectured containments hold among the complexity classes MOD_mP. However, these results also point out some problems with the model. Modulo m, the boolean function which is one iff the sum of the inputs is divisible by m (the negation of the one-sided MOD-m function above) has linear one-sided degree, while its negation has a one-sided degree of 1. The lower bound arguments themselves also rely on the fact that the target functions have a large number of zero values, which impose corresponding zero values on any polynomials that are one-sided representations. The bounds thus exploit

what appears to us to be an artifact of the definition rather than a fundamental property of modular counting.

In this paper we use the weak degree (denoted $\Delta(f, m)$) which we argue is the most interesting and natural of the three measures. Clearly lower bounds on it apply to both the other measures. Furthermore, if we want to bound the computational power of modular counting, it is only fair to allow an algorithm to extract all possible information out of the result of such counting, an element of Z_m.

Fortunately, as noted by Barrington, Beigel, and Rudich (1994), the distinction between one-sided and weak degree disappears in the case of the OR function, where there is only one zero value to worry about. Thus the results there on the one-sided degree of OR apply to the weak degree, and are in fact the first results on the weak degree of any function modulo a non-prime power. They proved that the weak degree of OR is $O(n^{1/r})$, where r is the number of distinct primes dividing m. In fact they achieve this bound by a symmetric polynomial, they show that no symmetric polynomial can do better, and they conjecture that this bound is actually optimal for all polynomials. Their only lower bound was $\omega(1)$, obtained by a Ramsey argument, though this can be improved to $\Omega(\log\log n/\log\log\log n)$ by an argument of Baker and Schmidt (1980).

In this paper we improve this lower bound significantly to $(\log n)^{\Omega(1)}$. Specifically, if r again is the number of distinct primes dividing m, the weak degree is $\Omega((\log n)^{1/(r-1)})$ (in particular, $\Omega(\log n)$ when m is the product of two primes or prime powers).

We do not believe that this lower bound is at all tight, and in fact such a small weak degree of OR would have some strange consequences. As described by Barrington, Beigel, and Rudich (1994), this would allow us to simulate an AND or OR gate by a constant depth quasipolynomial size circuit of MOD-m gates alone, collapsing the complexity classes qCC^0 and $qACC^0$ defined in Barrington (1992a).

Determining the weak degree of OR is an interesting problem in its own right as it deals with the ability of extremely natural problems to simulate each other in a natural setting. More importantly, it is a focal point for the examination of the computational power of modular counting. A better upper bound on the degree would provide a new computational technique that might have wider utility. Lower bounds on the degree, such as the one we provide here, are currently the best we can do toward proving limits on this computational power.

Subsequent to our work, Grolmusz (1995) has shown an $\Omega(\log n)$ lower

bound on the weak degree of the generalized inner product function (the parity of $8n/\log n$ AND's of size $(\log n)/8$ each). This is because Babai, Nisan, and Szegedy (1989) showed that this function has high k-party communication complexity for $k = (\log n)/8$, and a function weakly represented by a polynomial of degree $k-1$ has k-party communication complexity only $O(k \log m) = O(k)$. Of course, the OR function has constant communication complexity of any type, so such techniques will not work to bound its degree.

2. Lower bounds for the OR function

We begin by clarifying the relationship between strong and weak representation for prime power moduli, in a form that will be particularly useful later. This result is well-known but included for completeness — we adapt the presentation in Barrington (1992)

LEMMA 1. *Let $q = p^e$ be a prime power, and let P be a polynomial of degree d in n Boolean variables over Z_q. If P weakly represents a Boolean function f then there exists a polynomial P^* over Z_p, of degree at most $(q-1)d$ strongly representing f.*

PROOF. Suppose first that P one-sidedly represents f.

We use induction on the exponent e. If $e = 1$, $q = p$ is prime and we may take $P^* = P^{q-1}$. For the inductive case, we use the fact (Barrington 1992, Chandra, Sstockmeyer, and Vishkin 1984) that any polynomial Z is zero modulo p^{e+1} iff Z is zero modulo P and $\binom{Z}{p}$ is zero modulo p^e, where $\binom{Z}{p}$ denotes the sum of all possible products of p terms from Z (we avoid using coefficients in writing Z as sum of monomial terms, we repeat terms instead if necessary). Note that $\binom{Z}{p}$ has degree pd. Using the inductive hypothesis, we choose a polynomial R over Z_p, of degree at most $(p^e-1)(pd)$, which is zero when $\binom{P}{p}$ is zero modulo p^e and one otherwise. Then we may take $P^* = 1-(1-P^{p-1})(1-R)$. The degree of P^* is bounded above by $(p-1)d + (p^e-1)pd = (q-1)d$.

If P weakly represents f then the set of zeros of f is the disjoint union of the set of zeros of the function one-sidedly represented by some of the polynomials $P-c$, where $c \in Z_q$. Thus a polynomial strongly representing f over Z_p can be obtained by taking a suitable linear combination of the polynomials strongly representing those functions. □

COROLLARY 2. *If q is a prime power, and $d(q-1) < n$, no polynomial of degree d can weakly represent the OR function over Z_q.*

PROOF. By Lemma 1, if this happened we would have a polynomial over Z_p, of degree at most $d(q-1)$, strongly representing the OR function of n variables. But the polynomial that strongly represents OR is essentially unique and has degree n. □

We will abuse notation by denoting sets of input variables and their characteristic vectors the same way (so, for example, "$\mathbf{0}$" will represent the empty set of variables or the setting where all of them are false). Our main tool is the following lemma:

LEMMA 3. *Let P be an n-variable polynomial of degree d over the ring Z_q, where q is a prime power. If $k \geq 1$ satisfies $n \geq k + (q-1)\sum_{i=1}^{d}(d+1-i)\binom{k}{i}$, then we can find pairwise disjoint and nonempty sets of variables $S^1, \ldots, S^k$ such that for every $\epsilon \in \{0,1\}^k$ we have $P(\sum_{i=1}^{k} \epsilon_i S^i) = P(\mathbf{0})$.*

PROOF. We are going to find the sets S^i recursively with $|S^i| \leq s_i$, where s_i is a number to be defined later.

We begin by taking a set of variables S of size $|S| = s_1 = (q-1)d+1$. If we restrict the degree d polynomial P to S by setting all other variables to zero, by Corollary 2 this polynomial cannot weakly represent the OR function modulo q. Therefore there must be some subset S^1 of S with $P(S^1) = P(\mathbf{0})$. This is the base step of our argument. We now give the argument for the general recursive step, of which this base step is a special case.

Let $0 \leq j < k$. Without loss of generality we may suppose that $P(\mathbf{0}) = 0$, that the sets $S^1, \ldots, S^j$ of the appropriate size are already chosen, and that they satisfy $P(\sum_{i=1}^{j} \epsilon_i S^i) = 0$ for any $\epsilon \in \{0,1\}^j$. Let us choose a set S of s_{j+1} input variables disjoint from all of $S^1, \ldots, S^j$. We require $n \geq \sum_{j=1}^{k} s_j$ to ensure that this is possible.

For any $\epsilon \in \{0,1\}^j$, let P_ϵ denote the following restriction of P. We fix all the variables in S^i to ϵ_i for $i = 1, \ldots, j$, and fix all the variables that are outside both S and all the S^i's to 0. So P_ϵ is a polynomial over the variables in S.

By assumption each P_ϵ is zero at $\mathbf{0}$. Our goal is to find another common zero, say $P_\epsilon(S^*) = 0$ for all ϵ. Then the nonempty set S^* can be chosen as our next set S^{j+1}. But if such a set S^* did not exist, then using Lemma 1 we could construct a low degree polynomial that would strongly represent OR modulo p. We need only construct the mod p polynomial P^*_ϵ strongly representing

the Boolean function one-sidedly represented by P_ϵ for each ϵ using Lemma 1. Then mod p polynomial $R = 1 - \prod_{\epsilon\in\{0,1\}^j}(1 - P_\epsilon^*)$ takes only 0-1 values and $R(\mathbf{x}) = 0$ if and only if $P_\epsilon(\mathbf{x}) = 0$ for every $\epsilon \in \{0,1\}^j$, so unless there exists the required set S^*, R strongly represents OR modulo q. We get a contradiction by choosing $|S|$ or s_{j+1}, the number of variables of R, to be larger than the degree of R which is at most $2^j(q-1)d$.

We can save a little bit on this degree by taking inclusion-exclusion sums of the P_ϵ first. As the higher degree terms are the same in the different P_ϵ's, they cancel out.

For 0-1 vectors δ and ϵ, we say $\delta \le \epsilon$ if $\delta_i \le \epsilon_i$ for each coordinate i, and we define $|\delta|$ to be the number of ones in δ. Let $Q_\epsilon = \sum_{\delta\le\epsilon}(-1)^{|\delta|}P_\delta$. Take any monomial term of P and an S^i that contains no variables from the term. The contribution of this term to the value of P_δ and $P_{\delta'}$ is naturally the same if δ and δ' differ only in the ith coordinate. This makes the contribution of our monomial term to Q_ϵ vanish if $\epsilon_i = 1$. So the contribution to Q_ϵ of a monomial term of P is nonzero only if the term has variables from each set S^i where $\epsilon_i = 1$. Thus the monomial, being of degree at most d, has at most $d - |\epsilon|$ variables in S. This makes the degree of Q_ϵ at most $d - |\epsilon|$ and in case $|\epsilon| \ge d$ we have $Q_\epsilon = 0$.

As the common zeros of the P_ϵ are the same as the common zeros of the Q_ϵ we can use $R' = 1 - \prod_{\epsilon\in\{0,1\}^j}(1 - Q_\epsilon^*)$ in place of R. Here Q_ϵ^* is the mod p polynomial strongly representing the function one-sidedly represented by Q_ϵ guaranteed by Lemma 1. The degree of R' is at most $(q-1)\sum_{i=0}^{d-1}\binom{j}{i}(d-i)$, so choosing $|S|$ larger suffices. For this reason we define s_{j+1} to be $1 + (q-1)\sum_{i=0}^{d-1}\binom{j}{i}(d-i)$.

In order to have enough variables to choose $S^1, \ldots, S^k$ from we must have $n \ge \sum_{j=1}^{k} s_j$. This is exactly the bound on n in the lemma. □

Definition 4. *We call a Boolean function g a strict restriction of the Boolean function f if g is what we get by setting some variables of f to 0, while setting some sets of variables to be equal. The number of variables of g is therefore the number of equivalence classes of the nonzero variables of f. We call a polynomial Q a strict restriction of the polynomial P if we can obtain Q from P via this kind of restriction. Note that in this case the degree of Q is never more than the degree of P.*

Using this notion Lemma 3 says that every n-variable modulo q polynomial of degree d has a k-variable strict restriction that is constant on the 0-1 inputs if k and n satisfy the inequality in the lemma.

LEMMA 5. *Let $m = pq$ where p is a prime power and q is relatively prime to p. Let f be an n-variable Boolean function and let k be a number satisfying the inequality of Lemma 3. Then there exists a function g, a k-variable strict restriction of f, such that $\Delta(f,m) \geq \Delta(g,q)$.*

PROOF. Suppose P is a polynomial over Z_m weakly representing f. Let P_p be P modulo p and P_q be P modulo q. Using Lemma 3 P_p has a k-variable strict restriction that is constant on the 0-1 inputs. Now the same restriction of P_q has to weakly represent the corresponding restriction of f. This gives the lemma. □

Lemma 5 immediately gives a lower bound on the weak degree of the OR function modulo composite numbers. By a "maximal prime power divisor", we mean a prime power $p > 1$ such that $m = pq$ and p and q are relatively prime.

THEOREM 6. *Let m have $r \geq 2$ distinct prime divisors, and let p be the smallest maximal prime power divisor of m. Then for the n-variable OR function we have $\Delta(OR,m) \geq ((1/(p-1) - o(1)) \log n)^{1/(r-1)}$.*

PROOF. It is more convenient to consider the maximal number $n(m,d)$ of variables of an OR function weakly representable by a degree d polynomial modulo m. In this setting we need to prove $\log n(m,d) \leq (p-1+o(1))d^{r-1}$. For prime power modulus p we have $n(p,d) = (p-1)d$. For general moduli we use induction on r. Let $m = p_1 q$ where p_1 is a maximal prime power divisor of m different from p. Since any strict restriction of the OR function is again an OR function, by Lemma 5 we get $n(m,d) < k + (p_1 - 1)\sum_{i=1}^{d}(d+1-i)\binom{k}{i}$ where $k = n(d,q) + 1$.

If $r = 2$ then $q = p$ is a prime power and $k = (p-1)d+1$. Using $\sum_{i=1}^{d}\binom{k}{i} < \sum_{i=0}^{k}\binom{k}{i} = 2^k$ we have $n(m,d) \leq 2(p_1-1)d2^{(p-1)d}$. Thus $\log n(m,d) \leq (p-1+o(1))d$.

By induction we have $\log k \leq (p-1+o(1))d^{r-2}$ in the $r > 2$ case. We use a different method to estimate the sum: $n(m,d) \leq k+(p_1-1)\sum_{i=1}^{d}(d+1-i)\binom{k}{i} \leq (p_1-1)k^d$. Thus $\log n(m,d) \leq \log(p_1-1) + d\log k \leq (p-1+o(1))d^{r-1}$. □

We remark that more careful calculation can improve the $1/(p-1)$ constant in the result to $1/((p-1)H(1/(p-1)))$ with the binary entropy function H.

The best previous result for the weak degree of OR is implicit in Baker and Schmidt (1980) — it works equally well for any (constant) modulus but is

inferior to our result. (In this paper we have not considered moduli growing with n.)

THEOREM 7. *(Baker and Schmidt, 1980) For any fixed integer m and the n-variable OR function we have $\Delta(OR, m) = \Omega(\log\log n / \log\log\log n)$.*

3. Open problems

The upper and lower bounds for $\Delta(OR, m)$ are still far apart for any m not a prime power. If m is the product of two different primes the bounds are $O(\sqrt{n})$ and $\Omega(\log n)$. It would be interesting to improve on either bound. Also, for moduli with more than two distinct prime factors, there remains the technical problem of whether the combinatorial techniques here can be improved to get an $\Omega(\log n)$ degree bound.

While the power of linear polynomials to weakly represent OR is easily understood, the quadratic case already poses an amusing specific problem. What is the largest n such that the OR function of n variables can be weakly represented by a quadratic polynomial modulo 6, for example? The argument of Barrington, Beigel and Rudich (1994) shows that $n = 8$ is the exact answer for symmetric polynomials, but general polynomials for $n = 10$ are easy to construct. Is this best possible? Extensive (but not exhaustive) computer searches by the second author have failed to find a polynomial for $n = 11$, and we conjecture that none exists. The argument of this paper shows that $n = 21$ is impossible, as we construct sets of size at most $s_1 = 5$, $s_2 = 7$, and $s_3 = 9$. In fact an *ad hoc* argument shows that we can find a set S^1 of size three, so the best known upper bound is $n \leq 18$.

Currently, $\Omega(\log n)$ is the best lower bound on the weak degree of not only the OR function but of *any* explicit function modulo an m not a prime power. (Grolmusz (1995) proves such a bound for the generalized inner product function.) The most important open problem on this complexity measure is to prove high ($\Omega(n)$ or at least $n^{\Omega(1)}$) lower bounds on the weak degree of an explicit function.

Acknowledgements

The authors are greatly indebted to Noga Alon, Richard Beigel, Vince Grolmusz, Endre Szemerédi, and Shi-Chun Tsai for fruitful discussions on this subject. Gábor Tardos was supported by NSF grants CCR-95-03254 and DMS-9304580, a grant from Fuji Bank and the grant OTKA-F014919. David Mix Barrington was supported by NSF grant CCR-9207829.

References

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

R. Baker and W. Schmidt, Diophantine Problems in Variables Restricted to the Values 0 and 1. *Journal of Number Theory* **12** (1980), 460–486.

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

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

D. A. M. Barrington, R. Beigel, and S. Rudich, Representing Boolean functions as polynomials modulo composite numbers. *Computational Complexity* **4** (1994), 367-382.

R. Beigel, The polynomial method in circuit complexity. In *Structure in Complexity Theory: Eighth Annual Conference* (1993), 82–95.

R. B. Boppana and M. Sipser, The complexity of finite functions. In *Handbook of Theoretical Computer Science: Volume A, Algorithms and Complexity*, MIT Press/Elsevier (1990), 757–804.

A. K. Chandra, L. J. Stockmeyer, and U. Vishkin, Constant depth reducibility. *SIAM J. Comput.* **13:2** (1984), 423–439.

V. Grolmusz, On the weak mod-m representation of Boolean functions. *Chicago Journal of Theoretical Computer Science* **1995** (1995), No. 2.

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) (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.

S.-C. Tsai, Lower bounds on representing Boolean functions as polynomials in Z_m. *SIAM J. Disc. Math.* **9:1** (Feb. 1996), 55-62.

Manuscript received 29 September 1994

Gábor Tardos
Mathematical Institute of the
Hungarian Academy of Sciences
Pf 127
Budapest, HUNGARY H-1088
tardos@cs.elte.hu
Current address:
Institute for Advanced Study
Olden Lane
Princeton, NJ, USA 08540
gabor@ias.edu

David A. Mix Barrington
Computer Science Department
University of Massachusetts
Amherst, MA, USA, 01003-4610
barring@cs.umass.edu