POLYNOMIAL REPRESENTATIONS OF SYMMETRIC PARTIAL BOOLEAN FUNCTIONS

MART DE GRAAF[*] AND PAUL VALIANT[†]

Abstract. For Boolean polynomials in $\mathbb{Z}_p$ of sufficiently low degree we derive a relation expressing their values on one level set in terms of their values on another level set. We use this relation to derive linear upper and lower bounds, tight to within constant factor, on the degrees of various *approximate majority functions*, namely functions that take the value 0 on one level set, the value 1 on a different level set, and arbitrary 0-1 values on other Boolean inputs. We show sub-linear upper bounds in the case of moduli that are not prime powers.

Key words. Boolean function complexity, polynomial interpolation, lower bounds on degree, polynomial representation of Boolean functions, approximate majority function

AMS subject classifications. 68Q17, 68R05, 05E05, 94C10

1. Introduction.

Methods bounding the degree of polynomials that represent Boolean functions have been important tools in complexity theory. These techniques have been used to obtain several results that shed light on the complexity of Boolean functions. In particular, such polynomial degree lower bounds have consequences for the constant-depth circuit complexity of the associated Boolean functions.

We say that a polynomial represents a Boolean function if the polynomial is non-zero when the Boolean function is TRUE and zero when it is FALSE. The functions AND, OR, and Majority have been studied extensively in this framework and are examples of the more general class of threshold functions. Specifically, a threshold function is one which has value TRUE iff the number of non-zero inputs is at least a certain threshold. For AND, OR, and Majority, the respective thresholds are the number of inputs n, one, and $n/2$ respectively. Most of the work in this area concerns polynomials that either represent these functions exactly, or at a large fraction of the points. Our results instead bound the degree of a large class of Boolean functions with values fixed at only a small subset of the domain. In particular, we study the *approximate majority function*, which is defined for fixed A, B with $A < B$ as any function that is TRUE if exactly B of the inputs are TRUE, and FALSE if exactly A are TRUE. Using properties of the binomial coefficients, we provide a linear lower bound on the degree of polynomials representing such approximate majority functions. For example, if for some prime $p, n = 4p^k, A = n/4$, and $B = 3n/4$ we prove a lower bound linear in n/p on the degree of a polynomial representing this approximate majority function over $\mathbb{Z}_p$. Our general linear lower bounds, however, hold only modulo powers of primes. For composite moduli with multiple prime factors, we prove sublinear upper bounds.

Degree lower bounds for Boolean polynomials were first used by Razborov [Raz87] and Smolensky [Smo87] in the context of proving lower bounds on the size of constant-depth Boolean circuits. These results inspired much work on the degree of threshold

[*] Work done while at CWI, Amsterdam, The Netherlands. Email: mgdgraaf@cwi.nl. Partially supported by the EU fifth framework project QAIP, IST–1999–11234, and by grant 612.055.001 from the Netherlands Organization for Scientific Research (NWO).

[†] Stanford University. Research supported in part by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Army Research Office under grant DAAD19-00-1-0177. Current address: MIT Computer Science and Artificial Intelligence Laboratory, The Stata Center, Building 32, 32 Vassar Street, Cambridge, MA 02139. Email: pvaliant@mit.edu.

and other functions over various rings. Beigel [Bei93] gives an overview of much of the earlier work in this area. For example, Barrington, Straubing, and Thérien [BST90] proved linear upper bounds on the degree of a polynomial representing the OR function over $\mathbb{Z}_m$, and showed that they are tight for prime m. These upper bounds were improved by Barrington, Beigel, and Rudich [BBR92] to be sublinear for the case of composite m. In the case of majority, Tsai [Tsai96] proves a lower bound for all m of $n/2$ on the degree of the majority function over $\mathbb{Z}_m$. The approximate majority function with $A = n/4$ and $B = 3n/4$ arises naturally in the context of quantum complexity [GP01]. We show that the degree of this function is within a constant factor of that of the majority function for prime powers, but significantly lower otherwise.

2. Preliminaries.

2.1. Combinatorics.

For natural numbers n and k, we denote by $(n)_k$ the k-ary representation of n, i.e. the string $\ldots a_2a_1a_0$, with $0 \leq a_i < k$, such that $n = \sum_i a_ik^i$. Note that the first (from the right) nonzero digit of $(n)_k$ is given by the least i such that $k^{i+1} \nmid n$, an observation to which we shall frequently refer.

In 1878 Lucas [Luc78] gave a method for easily determining the value of $\binom{n}{k}$ mod p, for prime p. This result is now known as Lucas's Theorem. It is one of the main ingredients in the proofs of our results. By $x[i]$ we denote the symbol at the ith position from the right of string x.

Theorem 1 (Lucas). *Let p be a prime number, and n, k positive integers. Then*

$$\binom{n}{k} \equiv \prod_{i=0}^{m} \binom{(n)_p[i]}{(k)_p[i]} \pmod{p},$$

where m is the maximal index i such that $(n)_p[i] \neq 0$ or $(k)_p[i] \neq 0$, and where we use the convention that $\binom{a}{x} = 0$ whenever $x > a$.

2.2. Representation of Boolean Functions over $\mathbb{Z}_m$.

We now define what it means for a polynomial over $\mathbb{Z}_m$ to represent a Boolean function. We should note that there are several ways of representing a Boolean function by a polynomial over $\mathbb{Z}_m$, as discussed, for instance in Tardos and Barrington [TB95]. The definition we use here is what is sometimes called *one-sided representation.*

Definition 1. *Let $g : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and $P : \mathbb{Z}_m^n \to \mathbb{Z}_m$ a multilinear polynomial. We say that P represents g over $\mathbb{Z}_m$ iff for all $x \in \{0,1\}^n$, $P(x) \equiv 0 \Leftrightarrow g(x) = 0$. By the degree* $\deg(P)$ *of a polynomial $P : \mathbb{Z}_m^n \to \mathbb{Z}_m$, we mean the degree of its largest monomial. The degree of a Boolean function $g : \{0,1\}^n \to \{0,1\}$ over $\mathbb{Z}_m$ is then defined as* $\deg(g,m) = \min\{\deg(P) \mid P$ *represents* g *over* $\mathbb{Z}_m\}$.

Note that since for all $x \in \{0,1\}$ and $\ell > 0$, we have that $x^\ell = x$, the restriction to *multilinear* polynomials is without loss of generality.

We will sometimes restrict ourselves to polynomials with outputs in $\{0,1\}$, which thus *strictly* represent Boolean functions. When the modulus is a prime power p^k, the following lemmas relate the degrees of the *strict* and *one-sided* representations to be within a factor of $(p-1)(2p^{k-1}-1)$. Both are usually stated as being folklore results. See [Bei93] for an overview of these and other similar results. The proof of Lemma 3 is due to Richard Beigel (personal communication, October 2002) correcting a misstatement in [Bei93].

LEMMA 2. *Let p be a prime, and $g : \mathbb{Z}_p^n \to \mathbb{Z}_p$ be a polynomial of degree d; then there is a polynomial $h : \mathbb{Z}_p^n \to \mathbb{Z}_p$ of degree $(p-1)d$ such that for all $x \in \{0,1\}^n$, $h(x) \in \{0,1\}$, and $h(x) \equiv 0$ iff $g(x) \equiv 0$.*

Proof Take $h = g^{p-1}$. By Fermat's little theorem, $h(x) \equiv 1 \pmod{p}$ iff $g(x) \not\equiv 0$. □

LEMMA 3. *Let k be a positive integer, and p a prime. If $g : \mathbb{Z}_{p^k}^n \to \mathbb{Z}_{p^k}$ is a polynomial of degree d, then there exists a degree $d(2p^{k-1}-1)$ polynomial $h : \mathbb{Z}_p^n \to \mathbb{Z}_p$, such that for all $x \in \{0,1\}^n$, $h(x) \equiv 0$ iff $g(x) \equiv 0$.*

Proof By Theorem 1, we have that for every prime p, and positive integer m,

$$\binom{m}{p^i} \equiv \binom{(n)_p[i]}{1} \equiv (n)_p[i] \pmod{p}.$$

Thus we have that for every such p, m

$$m \equiv 0 \pmod{p^k} \Leftrightarrow \forall i < k \left[\binom{m}{p^i} \equiv 0 \pmod{p}\right]. \tag{2.1}$$

Define the ith elementary symmetric function of the n variables $y_1, \ldots, y_n$, $i \le n$, as

$$\sum_{1 \le \ell_1 < \cdots < \ell_i \le n} \prod_{j=1}^{i} y_{\ell_j}.$$

Note that if each $y_i \in \{0,1\}$, and exactly $|y|$ of them are 1, then the value of the above expression is $\binom{|y|}{i}$. Now write g as a sum of monomials of coefficient 1, i.e., replace for example $3x_1x_2$ by $x_1x_2 + x_1x_2 + x_1x_2$. Let $\binom{g(x)}{i}$ be the i-th elementary symmetric function of the monomials in g. Define $h(x)$ as

$$h(x) = \sum_{i=0}^{k-1} \binom{g(x)}{p^i} \prod_{j=0}^{i-1} \left(1 - \binom{g(x)}{p^j}^{p-1}\right).$$

We have that the degree of $\binom{g(x)}{p^i}$ is $dp^i \le dp^{k-1}$. Also, the degree of the product is at most $\sum_{j=0}^{k-2} d(p-1)p^j = d(p^{k-1}-1)$. Thus the degree of $h(x)$ is $d(2p^{k-1}-1)$. If $g(x) \equiv 0 \pmod{p^k}$, then by Equation 2.1, $\binom{g(x)}{p^i} \equiv 0 \pmod{p}$ for all $0 \le i < k$, hence $h(x) \equiv 0 \pmod{p}$. On the other hand, if $g(x) \not\equiv 0 \pmod{p^k}$, then using Equation 2.1, let r be the least value such that $\binom{g(x)}{p^r} \not\equiv 0 \pmod{p}$. Note that the rth term in $h(x)$ is nonzero modulo p, but all the others are zero modulo p, since all terms after the rth contain the factor $\left(1 - \binom{g(x)}{p^r}^{p-1}\right) \equiv 0$, and hence $h(x) \not\equiv 0 \pmod{p}$. □

3. Level Set Relations. In this section we restrict ourselves to the field $\mathbb{Z}_p$, where p is a prime. For a binary string x, let $|x|$ denote its Hamming weight, the number of 1s. Note that in the following, we often identify an input $x \in \{0,1\}^n$ with the set $S = \{x_i \mid x_i = 1\}$. By definition $|x| = |S|$.

The following theorem relates the value of a polynomial at a set U with the sum of its values on subsets of U of a fixed cardinality, provided the polynomial is of sufficiently low degree.

THEOREM 4. *Let p be prime, and let $g : \mathbb{Z}_p^n \to \mathbb{Z}_p$ be a polynomial of degree at most p^r. Let $a < b$ be integers satisfying $\binom{b-1}{a-1} \not\equiv 0 \pmod p$. Then for any assignment $U \subset [n]$ with $|U| = bp^r$,*

$$g(U) \equiv (1 - b/a)g(\emptyset) + \binom{b-1}{a-1}^{-1} \sum_{\substack{|S|=ap^r \\ S \subset U}} g(S) \pmod p$$

unless $a \equiv 0 \pmod p$ in which case b/a is replaced by $\binom{b}{a}\binom{b-1}{a-1}^{-1}$.

Proof Let $c_g(S)$ represent the coefficient in g of the term $\prod_{i \in S} x_i$. Then since g has degree at most p^r we can evaluate it at some point S with the following expression

$$g(S) = \sum_{l \le p^r} \sum_{\substack{|Z|=l \\ Z \subset S}} c_g(Z).$$

Thus we have

$$\begin{aligned} \sum_{\substack{|S|=ap^r \\ S \subset U}} g(S) &= \sum_{\substack{|S|=ap^r \\ S \subset U}} \sum_{l \le p^r} \sum_{\substack{|Z|=l \\ Z \subset S}} c_g(Z) \\ &= \sum_{l \le p^r} \sum_{\substack{|S|=ap^r \\ S \subset U}} \sum_{\substack{|Z|=l \\ Z \subset S}} c_g(Z) \\ &= \sum_{l \le p^r} \sum_{\substack{|Z|=l \\ Z \subset U}} \binom{bp^r - l}{ap^r - l} c_g(Z), \end{aligned}$$

where the last equality holds since there are $\binom{bp^r-l}{ap^r-l}$ ways to choose the remaining $ap^r - l$ elements to form a set S with $Z \subset S \subset U$ of size ap^r.

From Lucas's theorem we have that for $0 < l \le p^r$, $\binom{bp^r-l}{ap^r-l} \equiv \binom{b-1}{a-1}$ and for $l = 0$, $\binom{bp^r}{ap^r} \equiv \binom{b}{a}$. Thus we may simplify the above as follows:

$$\begin{aligned} \sum_{l \le p^r} \sum_{\substack{|Z|=l \\ Z \subset U}} \binom{bp^r - l}{ap^r - l} c_g(Z) &\equiv \binom{b}{a} c_g(\emptyset) + \binom{b-1}{a-1} \sum_{l \le p^r} \sum_{\substack{|Z|=l \\ Z \subset U}} c_g(Z) \\ &= \left[\binom{b}{a} - \binom{b-1}{a-1}\right] g(\emptyset) + \binom{b-1}{a-1} \sum_{\substack{|Z| \le p^r \\ Z \subset U}} c_g(Z) \\ &= \left[\binom{b}{a} - \binom{b-1}{a-1}\right] g(\emptyset) + \binom{b-1}{a-1} g(U). \end{aligned}$$

Rearranging terms gives us the desired result. □

We would expect this theorem to be useful in proving degree lower bounds on polynomials representing Boolean functions whose values are only specified on certain level sets. We provide a few examples.

4. Lower Bounds. As a first application, consider a Boolean function $g : \{0,1\}^n \to \{0,1\}$, that has $g(x) = 1$ if $|x| = n/4$ and $g(x) = 0$ if $|x| = 3n/4$, which can be thought of as the negation of an "approximate majority function." We start with the special case when $n = 4p^k$ and prove that $\deg(g, p) = \Omega(n)$.

THEOREM 5. *Let p be a prime, $n = 4p^r$, and $g : \{0,1\}^n \to \{0,1\}$ be such that $g(x) = 0$ if $|x| = n/4$, and $g(x) = 1$ if $|x| = 3n/4$. Then*

$$\deg(g, p) > \frac{n}{4(p-1)}.$$

Proof Consider any degree $d \leq \frac{n}{4(p-1)}$ multilinear polynomial P over $\mathbb{Z}_p$ that represents g. Using Lemma 2, transform P into a polynomial q that represents g over $\mathbb{Z}_p$, and that has $q(x) \in \{0,1\}$ for all $x \in \{0,1\}^n$. This will only increase the degree of q by a multiplicative factor $(p-1)$. We now prove a lower bound of $n/4$ on the degree of q.

Suppose for the sake of contradiction that we have such a polynomial of degree $n/4$. From Theorem 4 with $a = 1, b = 3, r = r$ we have

$$\begin{aligned} 1 \equiv g([3n/4]) &\equiv -2g(\emptyset) + \sum_{\substack{|S|=n/4 \\ S \subset [3n/4]}} g(S) \\ &= -2g(\emptyset) + 0. \end{aligned}$$

Thus for $g(\emptyset) \in \{0,1\}$ we have $2g(\emptyset) \equiv -1$, which implies that $p = 3$ and $g(\emptyset) = 1$. We now apply Theorem 4 again for $a = 1, b = 2, r = r$ to yield

$$\begin{aligned} g([2n/4]) &\equiv -1g(\emptyset) + \sum_{\substack{|S|=ap^r \\ S \subset [2n/4]}} g(S) \\ &= -1 + 0 \equiv 2, \end{aligned}$$

contradicting the fact that q is $0-1$ valued. Hence q must have degree greater than $n/4$. □

Using Lemma 3 we have the following corollary.

COROLLARY 6. *Let p be a prime, $n = 4p^r$, and $g : \{0,1\}^n \to \{0,1\}$ be such that $g(x) = 0$ if $|x| = n/4$, and $g(x) = 1$ if $|x| = 3n/4$. Then*

$$\deg(g, p^k) > \frac{n}{4(2p^{k-1} - 1)(p-1)}.$$

We note that in the above applications the number of variables n may be any integer $n \geq 3p^r$. We also note that the key to our proof is the fact that the degree of any polynomial *strictly* representing g is greater than $n/4$, which applies equally to the negation of g. Thus the preceding and following theorems apply equally to the approximate majority function as to its negation.

THEOREM 7. *Let p be a prime, $n \in \mathbb{Z}$, $A = ap^r, B = bp^r, A < B \leq n$ with neither b nor $\binom{b-1}{a-1}$ a multiple of p, and $g : \{0,1\}^n \to \{0,1\}$ be such that $g(x) = 0$ if $|x| = A$, and $g(x) = 1$ if $|x| = B$. Then the degree of any polynomial over $\mathbb{Z}_p$ that* strictly *represents g is greater than p^r, with the following bound for the one-sided representation:*

$$\deg(g, p^k) > \frac{p^r}{(2p^{k-1} - 1)(p-1)}.$$

Proof As above we prove the degree bound for the strict representation, and then apply Lemmas 2 and 3.

Suppose for the sake of contradiction there exists a polynomial P of degree $\leq p^r$ that strictly represents g over $\mathbb{Z}_p$. Note that the conditions of the theorem imply that $a \not\equiv 0$, for if $a \equiv 0$ and $b \not\equiv 0$, then Lucas's theorem would imply $\binom{b-1}{a-1} \equiv 0$, in violation of our assumptions. Thus from Theorem 4 we have that

$$1 \equiv (1 - b/a)g(\emptyset) + 0 \equiv (1 - b/a)g(\emptyset) \pmod{p}.$$

Since $g(\emptyset)$ is either 0 or 1, $g(\emptyset)$ must equal 1. Thus $b \equiv 0$, contradicting our assumption. Thus any *strictly* representing polynomial P must have degree greater than p^r, as desired. Note that the condition that $\binom{b-1}{a-1} \not\equiv 0 \pmod{p}$ is required by Theorem 4. □

5. Upper Bounds. We now use Lucas's theorem to produce symmetric polynomials to represent approximate majority functions. In many cases, these polynomials have degrees relatively close to the lower bounds proved above.

We now work over the ring $\mathbb{Z}_m$ where m is some integer greater than 1. Given an approximate majority function $g(x)$ defined to be 0 when $|x| = A$ and 1 when $|x| = B$ for some A, B, we again wish to find a one-sided representing polynomial P such that $P \equiv 0 \pmod{m}$ iff $g = 0$. The strategy will be to find some number k such that

$$\binom{A}{k} \not\equiv \binom{B}{k} \pmod{m},$$

and then represent g as

$$P = \binom{x}{k} - \binom{A}{k}.$$

This leads to the following theorem.

THEOREM 8. *Given an approximate majority function $g : \{0,1\}^n \to \{0,1\}$ such that $g(x) = 0$ if $|x| = A$ and $g(x) = 1$ if $|x| = B$ for some $A, B \leq n$ then for $m > 1$, $\deg(g, m) \leq p^{r-1}$ where p^{r-1} is the smallest power of a prime factor of m such that $A \not\equiv B \pmod{p^r}$. Further, if m is squarefree, p^{r-1} is the minimum degree of a* symmetric *representing polynomial.*

Proof Clearly if p^{r-1} is the smallest such power of a factor of m then m contains exactly $r - 1$ factors of p. Thus the rth digits (from the right) in the base p representations of A and B must differ while the first $r - 1$ digits must be identical. From Lucas's theorem, these rth digits of A and B must equal $\binom{A}{p^{r-1}}$ and $\binom{B}{p^{r-1}}$ respectively modulo p, which values must thus be different. Hence we may represent g as

$$P = \binom{x}{p^{r-1}} - \binom{A}{p^{r-1}},$$

where the notation $\binom{x}{p^{r-1}}$ is taken to mean the elementary symmetric polynomial on x of degree p^{r-1}. Clearly when $|x| = A$, $P(x) = 0$, and when $|x| = B$, $P(x) \not\equiv 0 \pmod{m}$ since $P(x) \not\equiv 0 \pmod{p}$.

Consider now the case where m is squarefree. Let k be the smallest degree of a symmetric function $\binom{x}{k}$ which differs on the levels A and B modulo m. Clearly any symmetric representing polynomial must have degree at least k, for otherwise it would have identical values on the levels A and B. We show $k \geq p^{r-1}$. Let q be some prime factor of m such that $\binom{A}{k} \not\equiv \binom{B}{k} \pmod{q}$. Then for some r' the r'th digits base q of A and B must differ. Consider the smallest such r'. Since $\binom{A}{k} \not\equiv \binom{B}{k} \pmod{q}$, Lucas's theorem implies $q^{r'-1} \leq k$. Since the r'th digits base q of A and B differ, we have $A \not\equiv B \pmod{q^{r'}}$. However, by hypothesis, p^{r-1} is the smallest power of a factor of m with this property, so $p^{r-1} \leq q^{r'-1}$. Thus $p^{r-1} \leq k$ as desired. □

We note that an alternate way of defining p^{r-1} is as follows. Factor $B - A$ as

$$B - A = p_1^{r_1} ... p_j^{r_j}.$$

Then p^{r-1} as defined in Theorem 8 equals

$$\min_{p_i | m} p_i^{r_i}. \tag{5.1}$$

This leads to the following corollary.

Corollary 9. *Given an approximate majority function $g : \{0,1\}^n \to \{0,1\}$ such that $g(x) = 0$ if $|x| = A$ and $g(x) = 1$ if $|x| = B$ for some $A, B \leq n$ then for $m > 1$, $\deg(g, m) \leq (B - A)^{1/q}$ where q is the number of distinct prime factors of m.*

Proof Factor $B - A$ as a product of powers of prime factors of m and some remaining factor. Clearly one of the q prime power factors must be at most $(B - A)^{1/q}$, implying the corollary by the above observation. □

We note that from equation 5.1, if a prime factor of m does not divide $B - A$ then the degree of the representing polynomial is 1!

Finally, we combine Theorems 7 and 8 to yield the following constant factor bound. (Note that if $p = 2$ the conditions of the theorem will never hold.)

Theorem 10. *Let p be a prime, $n \in \mathbb{Z}$, $A = ap^r, B = bp^r, A < B \leq n$ with neither $b - a$, b nor $\binom{b-1}{a-1}$ a multiple of p, and $g : \{0,1\}^n \to \{0,1\}$ such that $g(x) = 1$ if $|x| = A$, and $g(x) = 0$ if $|x| = B$. Then*

$$\frac{p^r}{(2p^{k-1} - 1)(p - 1)} < \deg(g, p^k) \leq p^r.$$

6. Discussion and Open Problems.

We presented a relation between values of a low degree polynomial on different level sets. We studied applications of this relation towards providing degree lower bounds for polynomials representing *approximate majority functions*. Further, many of these bounds lie suprisingly close to upper bounds given by symmetric functions. We note that an interesting consequence of the lower bound is a construction of an oracle separating EQP from $\mathsf{MOD_{p^k}P}$ [GP01] that is alternative to one implicit in [Bei91].

A number of open questions are left by this research. First of all, in $\mathbb{Z}_{p^k}$, Theorem 10 provides lower and upper bounds that differ by a factor of $(2p^{k-1} - 1)(p - 1)$. It would be interesting to see how this constant size gap can be closed. Theorem 10 relies on several conditions on the relation between A, B, and p, and we are curious to see which of these, if any, could be relaxed.

A possibly more fundamental open question raised by this paper is to find good lower bounds on the degree of approximate majority functions over $\mathbb{Z}_m$ for composite m. The techniques used in §4 seem to break down here, even for squarefree m.

Acknowledgments. The first author would like to thank Harry Buhrman and Frederic Green for initially suggesting this problem, and then, Leen Torenvliet, and Ronald de Wolf for some interesting and useful discussions on the subject. The second author would like to thank Madhu Sudan for bringing this problem to his attention.

REFERENCES

[BBR92] D. Mix Barrington, R. Beigel, and S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. In *Proceedings of the 24th ACM Symposium on Theory of Computing*, pages 455–461, 1992.

[Bei91] R. Beigel. Relativized counting classes: relations among thresholds, parity, and mods. In *Journal of Computer and System Sciences*, 42(1), 76-96, 1991.

[Bei93] R. Beigel. The polynomial method in circuit complexity. In *Proceedings of the 8th IEEE Structure in Complexity Theory Conference*, pages 82–95, 1993.

[BST90] D. Mix Barrington, H. Straubing, and D. Thérien. Non-uniform automata over groups. *Inf. & Comp.*, 89(2):109-132, 1990.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. Earlier version in STOC'93.

[GP01] F. Green and R. Pruim. Relativized separation of EQP from P(NP). *Information Processing Letters*, 80(5):257–260, 2001.

[Luc78] E. Lucas. Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques, suivant un module premier. *Bull. Soc. Math. France*, 6:49–54, 1878.

[Pap94] C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[Raz87] A. A. Razborov. Lower bounds for the size of circuits of bounded depth with basis AND, OR. In *Math. notes of the Academy of Science of the USSR*, 41(4):333-338, 1987.

[Smo87] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th STOC*, pp. 77-82, 1987.

[TB95] G. Tardos and D. Mix Barrington. A lower bound on the mod 6 degree of the OR function. In *Israel Symposium on Theory of Computing Systems*, pages 52–56, 1995.

[Tsai96] S.C. Tsai Lower bounds on representing boolean functions as polynomials in $\mathbb{Z}_m$. In *SIAM J. Discret Math.*, pp. 55-62 1996.