A NOTE ON A THEOREM OF RAZBOROV

David A. Barrington

COINS Technical Report 87-93

July, 1986

A Note on a Theorem of Razborov

David A. Barrington[1]
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139[2]

July 1986 ***DRAFT***

1. Abstract

Razborov [Ra86] has recently proved that a constant depth unbounded fan-in circuit with AND and PARITY gates requires exponential size to compute the majority function, affirming a five year old conjecture [FSS81]. Here we extend his technique to show the same result for circuits with AND gates and MOD-p gates for prime p, where a MOD-p gate outputs one if the sum mod p of its (boolean) inputs is nonzero and zero otherwise.

2. Introduction

The first major results in the study of constant depth unbounded fan-in circuits were obtained by Furst, Saxe, and Sipser [FSS81]. They proved that such a circuit of ANDs and ORs of polynomial size (an "AC^0" circuit) could not calculate the parity function. (This result was also obtained independently by Ajtai [Aj83].) They then defined the notion of AC^0 reductions among functions (calling it "cp-reducibility") to prove that the majority and binary multiplication functions were also not in AC^0. (A function f is AC^0 reducible to g if it can be calculated by a

[1]This work is supported by NSF grant MCS-8304769 and US Air Force grant AFOSR-82-0326.
[2]Address after 1 Sept 1986: Dept. of Computer and Information Sciences, Univ. of Massachusetts, Amherst MA 01003

constant depth polynomial size unbounded fan-in circuit of AND gates, OR gates, and oracle gates for g.) They conjectured that majority was not reducible to parity and suggested further study of the structure of the reducibility.

Further progress in this effort was made by Fagin et al. [FKPS83] who found many reducibilities between symmetric functions. With the demonstration of exponential lower bounds for constant depth parity circuits of ANDs and ORs [Ya85, Hå86] their results completely classify the symmetric functions in AC^0.

Barrington [Ba86] defined the class ACC (the closure under AC^0 reductions of the class of mod q functions) and showed that the word problem for any fixed group is either inside ACC (if the group is solvable) or complete under such reductions for the class NC^1. He conjectured that $ACC \neq NC^1$, strengthening the conjecture of [FSS81]. Barrington and Thérien [BT86] showed that the word problem for any solvable monoid is in ACC, and gave an algebraic characterization of the classes AC^0 and ACC.

Finally, Razborov [Ra86] proved the conjecture of [FSS81] by showing an exponential lower bound for a constant depth circuit of AND and PARITY gates calculating the majority function. His proof essentially appears below (with several simplifications due to Ravi Boppana) as the case $p = 2$ of our main result. We show here that circuits of AND and MOD-p gates also require exponential size to do the majority function, and conclude with some comments on the possibility of extending these results.

3. Approximating Circuits by Polynomials

Throughout what follows q will be an arbitrary integer greater than one and p will be an arbitrary prime. Define $R_{n,q}$ as the ring of polynomials over $\mathbf{Z}_q$ in indeterminates $x_1, \ldots, x_n$ satisfying $x_i^2 = x_i$. An element of $R_{n,q}$ defines a function from $\{0,1\}^n$ to $\mathbf{Z}_q$ by plugging in boolean values for the variables and evaluating in $\mathbf{Z}_q$.

Lemma 1: Such functions are in 1-1 correspondence with the polynomials.

Proof: The mapping from polynomials to functions is a linear transformation over $\mathbf{Z}_q$ and is easily seen to be an isomorphism.

A circuit of depth zero is defined to be an input variable or a constant zero or one. A circuit of depth d is a nonempty collection of circuits of depth $d-1$ connected by an AND gate or a MOD-q gate. The output of an AND gate is one if all its inputs are one and zero otherwise. The output of a MOD-q gate is one if

the sum mod q of its inputs is nonzero and zero otherwise. The size of a circuit is its number of gates. Note that OR gates and NOT gates can be simulated by these gates at small cost, so that they could be included without changing the class of functions calculated in constant depth and polynomial size.

Theorem 2: Let p be a prime and ℓ a positive integer. A depth k circuit of ANDs and MOD-ps of size s can be approximated by a polynomial f of degree at most $(p-1)^k \ell^k$, such that f gives the same value as the output of the circuit except on at most $s2^n(\frac{p-1}{p})^\ell$ inputs. Furthermore, the value of f is zero or one on all inputs.

Proof: We can obtain the result of one of our MOD-p gates on a set of polynomials by adding them together over $\mathbf{Z}_p$ and taking the $(p-1)$st power of the sum. Thus the MOD-p of an arbitrary number of polynomials of degree d is a polynomial of degree $d(p-1)$.

The AND of an arbitrary number of 0-1 valued polynomials can be approximated as follows. We will make ℓ different approximations randomly and independently. For a single approximation, we throw a p-sided coin for each polynomial to be ANDed and include that polynomial $0, 1, \ldots,$ or $p-1$ times accordingly in a grand sum. We also add in a constant so that if each of the polynomials to be ANDed has value 1, the grand sum will have value 1.

For a given input setting, the value of each grand sum is 1 if all the polynomials to be ANDed are 1, and a uniform random variable over $\mathbf{Z}_p$ otherwise. Thus, if the AND should be zero, a given grand sum is zero with probability $\frac{1}{p}$. The $(p-1)$st power of the product of the ℓ different grand sums is a 0-1 polynomial which gives the desired AND with probability $1-(\frac{p-1}{p})^\ell$. Since this probability represents an average error over all possible choices of the p-sided coin flips, there must be some choice which does at least this well. If the polynomials to be ANDed had degree d, the approximation to the AND has degree $(p-1)\ell d$.

The result follows by induction on k. Each gate causes an error on at most $2^n(\frac{p-1}{p})^\ell$ inputs, so all s gates cause at most s times this many errors. The degree of a polynomial exactly representing a degree 0 circuit is 1, so the degree of the apporoximation to a depth k circuit is at most $(p-1)^k \ell^k$.

4. A Hard Symmetric Function

We show that for each q, a certain symmetric function from $\{0,1\}$ to $\mathbf{Z}_q$ cannot be closely approximated by a low-degree polynomial — this will prove that it cannot

be computed by a small constant depth circuit. From this we will show below that the majority function is also hard. This part of the proof does not require q to be a prime.

For any d and d' less than n, we define a linear mapping $\Phi_{d,d'}$ (denoted Φ when the value of the subscripts is clear) on the set of functions from $\{0,1\}^n$ to $\mathbf{Z}_q$ into the set of $\binom{n}{d} \times (natopd')$ matrices as follows. The rows and columns of a matrix will be indexed by subsets of $\{1,\ldots,n\}$ of size d and d' respectively. Then for f from $\{0,1\}^n$ to $\mathbf{Z}_q$, $\Phi(f)_{IJ}$ is the sum mod q over all $\epsilon \in C(I \cup J)$ of $(-1)^{|\epsilon|} f(\epsilon)$, where $C(K)$ is the set of all $\epsilon \in \{0,1\}^n$ such that $\epsilon(i) = 0$ for all $i \in K$ and $|\epsilon|$ is the number of ones in ϵ.

This construction has two key properties:

Lemma 3: If $d+d'+d'' < n$, any polynomial f of degree at most d'' has $\Phi_{d,d'}(f)$ a matrix of all zeroes.

Proof: By linearity it suffices to prove this for a monomial of degree at most d''. Fix any I of size d and J of size d'. Let K be the subset of $\{1,\ldots,n\}$ corresponding to the variables in the monomial. There must be some element i of the complement of $I \cup J \cup K$. Note that the sum defining $\Phi(f)_{IJ}$ divides into terms for ϵ with $\epsilon(i) = 1$ and $\epsilon(i) = 0$, and that these terms cancel in pairs.

Lemma 4: If f_0 is defined by $f_0(\epsilon) = 1$ for $\epsilon = \epsilon_0$ and $f_0(\epsilon) = 0$ otherwise, then the rank of the matrix $\Phi(f_0)$ is at most one.

Proof: $\Phi(f_0)_{IJ} = (-1)^{|\epsilon_0|}$ if $\epsilon_0 \in C(I \cup J)$ and zero otherwise.

Now, by the subadditivity of the rank function, we get:

Proposition 5: If $d + d' + d'' < n$ and f is approximated by a polynomial of degree at most d'' with r errors, the rank of $\Phi_{d,d'}(f)$ is at most r.

We will now exhibit a specific matrix of large rank and show that it is the image under Φ of a symmetric function. Define a matrix $P_{d,d'}$ of zeroes and ones by $(P_{d,d'})_{IJ} = 1$ iff $I \cap J = \emptyset$. Define P_d to be the $\binom{n}{d} \times \binom{n}{\leq d}$ matrix obtained by concatenating all $P_{d,d'}$ for $d' \leq d$.

Lemma 6: P_d has full rank $\binom{n}{d}$ over $\mathbf{Z}_q$, and thus there exists a d' such that $P_{d,d'}$ has rank at least $\frac{1}{n}\binom{n}{d}$.

Proof: Define a $\binom{n}{\leq d} \times \binom{n}{d}$ matrix Q_d by $(Q_d)_{JI} = (-1)^{|J|}$ for $J \subseteq I$ and $(Q_d)_{JI} = 0$ otherwise. Note that $P_d Q_d$ is the identity matrix of size $\binom{n}{d}$.

Proposition 7: Let $d' \leq d < n/2$. If f is the sum mod q of all monomials of degree $n-d-d'$, then $\Phi_{d,d'}(f) = \pm P_{d,d'}$.

Proof: Consider any I of size d and J of size d'. If $I \cap J \neq \emptyset$, for any set K of size $n-d-d'$ there is an element i not in $I \cup J \cup K$ and the monomial in f corresponding to K maps to zero as in Lemma 3 above. By linearity $\Phi(f)_{IJ} = 0$.

On the other hand, if $I \cap J = \emptyset$, each monomial is mapped to zero except for that corresponding to the complement of $I \cup J$. This monomial, however, is mapped to $(-1)^{n-d-d'}$.

5. The Main Result

Setting $d = \frac{n}{2} - \sqrt{n}$ and $\ell = d^{1/k}/(p-1)$ will give us an exponential lower bound. Slight improvements are possible. The normal approximation to the binomial gives $\binom{n}{\frac{n}{2}-\sqrt{n}} = \Theta(2^n/\sqrt{n})$. Now the symmetric function of Proposition 7 maps to a matrix of rank $\Omega(2^n/n^{3/2})$. By Theorem 2, any circuit of depth k computing this function must have size $\Omega(2^{O(n^{1/2k})}/n^{3/2})$.

The result for majority comes from the well-known completeness of majority for symmetric functions with respect to AC^0 reductions (e.g., [FKPS83]). A depth k, size $s(n)$ family of majority circuits leads to a depth $k+1$, size $ns(2n)$ family for any symmetric function. Thus we can conclude:

Theorem 8: Any depth k family of circuits of AND and MOD-p gates computing the majority function has size $2^{\Omega(1/2k)}$.

6. Open Problems and Prospects

Can you show that AND and MOD-p gates cannot do the MOD-p' function?

Is there any hope of extending this to the MOD-q case for composite q? Unfortunately Theorem 2 may not be true. A polynomial over $\mathbf{Z}_6$, say, is simply a polynomial over $\mathbf{Z}_2$ and another over $\mathbf{Z}_3$ which are totally independent. There seems no reason to think that in a circuit of MOD-2 and MOD-3 gates the mod-2 and mod-3 behavior cannot interact.

Razborov [Ra86] mentions the possibility of extending his result (which can be viewed as about arithmetic circuits for the field $\mathbf{Z}_2$) to arithmetic circuits for $\mathbf{Z}_3$

or $\mathbf{Z}_p$. Because multiplication in $\mathbf{Z}_p$ requires counting modulo $p-1$, this would amount to our problem for $q = p(p-1)$. Razborov remarks that his Lemma 1 (our Theorem 2) does not appear to extend to the case $p = 3$.

7. Acknowledgements

Most of this proof (the $p = 2$ case) is due to Razborov [Ra86] with simplifications by Boppana. I would like to thank Ravi Boppana and Phil Klein for helpful discussions.

8. References

[Aj83] M. Ajtai, 'Σ_1^1 formulae on finite structures', Annals of Pure and Applied Logic 24 (1983), 1-48.

[Ba86] D. A. Barrington, 'Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1', Proc. 18th ACM STOC, 1986, 1-5.

[BT86] D. A. Barrington and D. Thérien, 'Finite monoids and the fine structure of NC^1', to appear.

[Co85] S. A. Cook, 'The taxonomy of problems with fast parallel algorithms', Information and Control 64 (Jan. 1985), 2-22.

[FKPS83] R. Fagin, M. M. Klawe, N. J. Pippenger, and L. Stockmeyer, 'Bounded depth, polynomial-size circuits for symmetric functions', IBM Report RJ 4040 (October 1983), IBM Research Laboratory, San Jose.

[FSS81] M. Furst, J. B. Saxe, and M. Sipser, 'Parity, circuits, and the polynomial-time hcirarchy', Proc. 22nd IEEE FOCS, 1981, 260-270.

[Hå86] J. Håstad, 'Almost Optimal Lower Bounds for Small Depth Circuits', Proc. 18th ACM STOC, 1986, 6-20.

[Ra86] A. A. Razborov, 'Lower bounds for the size of circuits of bounded depth with basis $\{\&, \oplus\}$, preprint (in Russian). To appear in 'Matem. zam.' Preliminary English translation available from Paul E. Dunne, Dept. of Computer Science, Univ. of Liverpool, L69 3BX, Great Britain.

[Ya85] A. C. C. Yao, 'Separating the polynomial-time heirarchy by oracles', Proc. 26th IEEE FOCS, 1985, 1-10.