ALGEBRAIC METHODS IN THE THEORY OF LOWER BOUNDS FOR BOOLEAN CIRCUIT COMPLEXITY

Roman Smolensky
Department of Mathematics
University of California, Berkeley

Abstract

We use algebraic methods to get lower bounds for complexity of different functions based on constant depth unbounded fan-in circuits with the given set of basic operations. In particular, we prove that depth k circuits with gates NOT, OR and MOD_p where p is a prime require $Exp(0(n^{\frac{1}{2k}}))$ gates to calculate MOD_r functions for any $r \neq p^m$. This statement contains as special cases Yao's PARITY result [Ya 85] and Razborov's new MAJORITY result [Ra 86] (MOD_m gate is an oracle which outputs zero, if the number of ones is divisible by m).

Introduction

Constant depth polynomial size circuits with unbounded fan-in were studied first for their connection with constructing oracles separating PSPACE from the polynomial hierarchy. Furst, Saxe and Sipser [FSS 81] and independently Ajtai [Aj 83] proved that AC^0 circuits (constant depth polynomial size) could not calculate the parity function.

The result was improved by Yao [Ya 85] who showed an exponential bound on the size of such circuits. This result allows the construction of the separating oracle. An almost optimal bound on the size was given by Hastad [Ha 86]. Cai [Ca 86] proved that small circuits not only fail to compute parity but give eventually 50% of error. This implies a separation by a random oracle. An independent proof of this is due to Babai.

Proving lower bounds for constant depth circuits is important not only for applications to oracles but because it may give us an idea of what kind of techniques we can use in proving lower bounds for more powerful models of computation.

A natural way to extend the notion of AC^0 circuits with AND and OR gates is to increase the number of basic operations (e.g. we allow PARITY gates in the circuit). This leads to the notion of AC^0 reducibility. It was conjectured in [FSS 81] that MAJORITY was not AC^0 reducible to PARITY.

Barrington [Ba 86] 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 $ACC \neq NC^1$.

On the other hand many of the symmetric functions are AC^0-reducible to each other as it was shown by Fagin et al. [FKPS 83].

Finally, Razborov [Ra 86] proved the conjecture of [FSS 81] by showing an exponential lower bound for calculating majority function using a constant depth circuit with AND and PARITY gates. The first part of his proof is similar to our proof and he has Lemma 1 for $F = Z_2$.

In full generality Lemma 1 was proved by David Barrington [Ba 2], who was working independently on proving lower bounds for circuits with MOD_p gates.

The main idea of the present algebraic approach is to map the boolean functions, on which the given boolean circuit operates, to some algebra A. In the previous works (except for Razborov's results) people were doing different surgeries on the boolean circuit going from gate to gate. On the contrary, in our proofs the circuit always stays the same, but going from gate to gate we make changes in the algebra A. While in the first part of our proof we are practically talking about Razborov's approximations, our algebraic setting and the notion of U_F^n- completeness give us more direct and powerful methods in the second part of the proof.

Basic Notation and Definitions

We consider the following types of operations.

1) AND - outputs one iff all of the inputs are ones.

2) OR - outputs one iff at least one input is one.

3) NOT - takes one input and computes the negation.

4) $MOD_{(s,p)}$ - outputs one iff the number of ones in the input is congruent to s mod p. $MOD_p = NOT(MOD_{(0,p)})$.

5) MAJORITY - outputs one iff at least half of the inputs are ones.

6) $EXACT_K$ - outputs one iff exactly k inputs are ones.

Let B be a collection of types of operations.

Definition: A boolean circuit C^n with the set B of basic operations is a transitively closed set together with an assignment of an operation from B to each nonminimal (under ϵ relation) element. The only minimal elements of C^n should be $X_1, X_2, ... X_n$.

The minimal elements of C^n are the inputs. The maximal elements are the outputs and nonminimal elements are the gates of the circuit.

The size of a circuit is the number of gates, the depth is the length of the longest chain of the gates linearly ordered by inclusion. In a natural way a circuit computes a boolean function.

Remark: We will be considering a collection of circuits C^n (one circuit for each length of the input) so the superscript n will appear almost on all objects of our discussion. Do not let it to confuse you. Formally, it means that we are talking about a sequence of objects instead of one object. That gives us the ability to use small and large 0 in functions of n. Informally, you can think that n is a very large fixed number and totally ignore the superscripts.

Definition: A boolean function f^n (or a set of functions $\{f_1^n, f_2^n, ..., f_s^n\}$) is AC^0 reducible to another function g^n (or a set of functions $\{g_1^n, g_2^n, ..., g_t^n\}$) if there exists a constant depth polynomial size circuit C^n with basic operations AND, OR, NOT, g (or AND,OR,NOT, $g_1, g_2 ... g_k$) and output f^n (or $f_1^n, f_2^n, ..., f_s^n$).

Clearly AC^0 reducibility is a transitive relation between sets of functions.

We give a list of AC^0 reductions which are not very hard to check.

1) The set of $MOD_{(s,p)}$ functions for s from zero to $p-1$ is AC^0-reducible to MOD_p.

2) The set of $EXACT_k$ functions for k from zero to n is AC^0-reducible to MAJORITY.

3) MOD_p is AC^0-reducible to the set of $EXACT_k$ functions and to MAJORITY.

4) MOD_a is AC^0 reducible to MOD_b when a divides b.

5) MOD_{p^m} is AC^0 reducible to MOD_p.

The Mappings from the set of Boolean functions to F-algebras

Let $X_1, X_2 \cdots X_n$ be boolean variables. By D^n we denote the set of the truth assignments on these variables. For any field F we denote by U_F^n the algebra of functions from D^n to F with pointwise addition and multiplication. We identify 'False' with 0_F and 'Truth' with 1_F. Then U_F^n contains as a subset the set of boolean functions in X_i's (the subset is proper when $F \neq Z_2$). In particular U_F^n contains X_i's (as a boolean function X_i is defined by $X_i(d) = d(X_i)$ for any $d \epsilon D^n$).

Proposition 1: U_F^n is generated as F-algebra by X_i's with the relations $X_i^2 = X_i$.

Proof: Fix $d_0 \epsilon D^n$. Then $\prod_{X_i(d_0)=1} X_i \cdot \prod_{X_j(d_0)=0} (1 - X_j)$ is a function in U_F^n that takes value 1 on d_0 and 0 elsewhere. Every function f in U_F^n is a linear combination of such functions and hence f can be written as a polynomial in X_i's.

The polynomial for f is unique, if we require that none of the X_i's appears with degree greater than 1. The uniqueness follows from the fact that the number of monomials of the form $\prod_{i \epsilon \omega} X_i$ (where ω is a subset of {1,2 ...n}) is 2^n, which is equal to the dimension of U_F^n.

Let E be a subset of D^n. The functions which are zero outside of E form an ideal I (it can be easily shown that all ideals of U_F^n can be obtained in this way.) We can think of the quotient algebra $A = \frac{U_F^n}{I}$ as if we ignore the assignments in E and identify the functions which coincide outside of E. A polynomial f will represent an element of A but such a representation is no longer unique. By the degree of f in A we will mean the minimum of the degrees of the polynomials which coincide with f in A. We denote this by $deg_A(f)$. We denote by Ω_F^n the set of all quotient algebras of the form $\frac{U_F^n}{I}$ for some ideal I.

F-easy and Nearly F-easy Operations

In this chapter we use U_F^n with its natural grading (by the degree of polynomials) to give an algebraic measure of how hard a boolean function is.

Definition: A boolean m-ary function $f^n(g_1, g_2, \ldots, g_m)$ is F-easy if it can be represented in g_i's as a polynomial of a constant degree λ.

For any field F, NOT (g) is (1 - g) in U_F^n. So the operation NOT is always F-easy. MOD_p is F-easy when $F = Z_p$, since we can write $MOD_p(g_1, g_2 \ldots g_m)$ as $(\sum_{i=1}^{m} g_i)^{p-1}$ in $U_{Z_p}^n$. This is also true for any field F of characteristic p since such a field contains Z_p as a subfield. Obviously, an arbitrary size constant depth circuit with F-easy basic operations computes an F-easy function.

The situation is more complicated if we want to use AND and OR gates in our circuits. An m-ary AND operation is $\prod_{i=1}^{m} g_i$ in U_F^n and it is not F-easy for any F. It happens that OR and AND can be represented by low degree polynomials in some algebras of Ω_F^n whose dimension is just slightly less than 2^n. This fact motivates the following definition.

Definition: A boolean m-ary function $f^n(x_1, x_2, \ldots, x_m)$ is nearly F-easy if for any choice of m n-ary boolean functions $g_1, g_2 \ldots g_m$ and any l there exists an F-algebra $A^n \epsilon \Omega_F^n$ of dimension at least $2^n - 2^{n-l}$ such that $f^n(g_1, g_2 \ldots g_n)$ can be written in A^n as a polynomial in g's of degree at most λl, where λ is a constant.

Lemma 1: OR is a nearly F-easy operation for any field F of characteristic $p \neq 0$

Proof: Suppose $f^n = \overset{m}{\underset{i=1}{OR}} g_i$. We will find a polynomial $\tilde{f}^n$ in g_i's of degree at most $(p-1) \cdot l$ such that $\tilde{f}^n$ and f^n differ on at most 2^{n-l} assignments. Take $A^n = \frac{U_F^n}{I^n}$ where I^n is the ideal generated by $f^n - \tilde{f}^n$. Then f^n coincides with $\tilde{f}^n$ in A^n and $dim(I^n) \leq 2^{n-l}$.

It is sufficient to work over Z_p since F contains Z_p as a subfield. Let S be the collection of all expressions of the form $\overset{l}{\underset{j=1}{OR}} (\sum_{i=1}^{m} C_{ij} g_i)^p - 1$ where $C_{i,j}$'s are arbitrary elements of Z_p. Taking the p-1 power makes any function of U_{Z_p} boolean. So every expression in S is a well defined boolean function and it is written as a polynomial of degree at most $(l \cdot p - 1)$. Let $d \epsilon D^n$ be a truth assignment. If f(d)=0, then for any i, $g_i(d) = 0$, so for every $s \epsilon S, s(d) = 0$. If f(d)=1, then for some i_0, $g_{i_0}(d) = 1$. In this case for any choice of $C_{i,j}$'s with $i \neq i_0$ there is only one choice of l elements $C_{i_0 1}, C_{i_0 2} \ldots C_{i_0 l}$ such that the whole expression is zero on d. In any case, if $d \epsilon D^n$ then for a random element $s \epsilon S$ the probability that $f(d) \neq s(d)$ is at most p^{-l}. By a counting argument there will be an element $\tilde{f} \epsilon S$ such that $\tilde{f}(d) \neq f(d)$ on at most $\frac{1}{p^l}$ of d's from D^n which is at most $2^n - l$ assignments. Q.E.D.

Remark: The same lemma holds for AND since we can write AND using OR and NOT.

If the size of a constant depth circuit C^n is not too big, and C^n uses only nearly F-easy operations then the output of C^n can be approximated by a low degree polynomial if we ignore just a small fraction of assignments. Lemma 2 states this precisely.

Lemma 2: Let C^n be a depth K circuit that has an arbitrary number of F-easy gates and 2^r nearly F-easy gates, where r is $o(n^{\frac{1}{2k}})$. Then there is an algebra $A^n \epsilon \Omega_F^n$ of dimension $2^n - o(2^n)$ such that all outputs of C^n have degree $o(\sqrt{n})$ in A^n.

Proof. Take $l = 2r$ and for each nearly F-easy gate find an ideal I of dimension $2^n - l$ such that in $A = \frac{U_F^n}{I}$ the operation performed by this gate can be expressed in terms of the children of the gate by a polynomial of degree λl. Let I_0 be the sum of all this ideals. The dimension of I_0^n is at most $2^r \cdot 2^n - l$ which is $o(2^n)$. In $A^n = \frac{U_F^n}{I_0^n}$, each gate computes the function that can be expressed in terms of its children as a polynomial of degree $\lambda l = 2\lambda o(n^{\frac{1}{2k}})$ which is still $o(n^{\frac{1}{2k}})$. Since we start with X_i 's and the depth of C^n is k, all outputs have a degree $o(\sqrt{n})$ in A.

U_F^n-complete elements and sets.

Many elements of U_F^n have a low degree only in F-algebras of dimension much smaller than 2^n. Lemma 4 shows this for a certain class of elements which we call U_F^n-complete.

Definition: An element $v^n \epsilon U_F^n$ (or a set of elements $v_1^n, v_2^n \ldots, v_s^n \epsilon U_F^n$) is U_F^n-complete if for any F-algebra $A \epsilon \Omega_F^n$ and any polynomial $u \epsilon U_F^n$, $deg_A(u) \leq \frac{n}{2} + deg_A(v^n)$ (or $deg_A(u) \leq \frac{n}{2} + \max(deg_A(v_i^n))$ where i=1,2...,s).

The following lemma gives an important example of an U_F^n-complete element.

Lemma 3: Let $h \epsilon F$, $h \neq 0$ and $h \neq 1$. Take $Y_i = (h-1)x_i + 1$ then $\prod_{i=1}^{n} Y_i$ *is* U_F^n-complete.

Proof: Y_i is the function on D^n that takes the value h when X_i is one and one when X_i is zero. It is easy to see that $X_i = (h-1)^{-1}(Y_i - 1)$ and $Y_i^{-1} = (h^{-1} - 1)X_i + 1$ (h^{-1} and $(h-1)^{-1}$ exist since h is not zero on one). If u is a polynomial in X_i's we can rewrite it as a polynomial in Y_i's using the substitution $(h-1)^{-1}(Y_i - 1)$ for X_i. So it is enough to show that for any monomial of the form $\prod_{i \epsilon \omega} Y_i$ (where ω is a subset of {1, 2 ... n}) $deg_A(\prod_{i \epsilon \omega} Y_i) \leq \frac{1}{2}n + deg_A(\prod_{i=1}^{n} Y_i)$ in any A. When $card(\omega) \leq \frac{n}{2}$ this is clear, since Y_i's are linear. When $card(\omega) > \frac{n}{2}$ we write $\prod_{i \epsilon \omega} Y_i$ as $\prod_{i=1}^{n} Y_i \cdot \prod_{i \epsilon \bar{\omega}} Y_i^{-1}$ (where $\bar{\omega}$ denotes the complement of ω in {1, 2 ... n}). Using that card $(\bar{\omega}) < \frac{n}{2}$ and Y_i^{-1}'s are linear we get that $deg_A(\prod_{i \epsilon \omega} Y_i)$ is still less than $\frac{N}{2} + deg_A(\prod_{i=1}^{n} Y_i)$. Q.E.D.

Definition: An element $a \epsilon F$ is a q-th root of unity if $a \neq 1$ and $a^q = 1$.

Corollary: If F contains a q-th root of unity then the set $\{MOD_{0,q}(X_1 \cdots X_n), \cdots MOD_{q-1,q}(X_1 \cdots X_n)\}$ is U_F^n-complete.

Proof: Take $h \epsilon F$ to be a q-th root of unity and $Y_i = (h-1)X_i + 1$. Let $d \epsilon D_n$ be an assignment that contains K ones. Let K be congruent to S mod q. Then $\prod_{i=1}^{n} Y_i(d) = h^k = h^s$. So $\prod_{i=1}^{n} Y_i$ can be written as $\sum_{s=0}^{q-1}(h^s \cdot MOD_{s,q}(X_1, X_2 \cdots X_n))$. So in any algebra the degree $\prod_{i=1}^{n} Y_i$ is the maximal degree of $MOD_{s,q}$ functions, and the statement follows from lemma 3. Q.E.D.

Lemma 4: If an element v^n (or a set $v_1^n \cdots v_s^n$) is U_F^n-complete, and in some algebra $A^n \epsilon \Omega_F^n$ its degree is $o(\sqrt{n})$ then the dimension of A^n is at most $2^{n-1} + o(2^n)$.

Proof: Every element in A^n can be written as a polynomial of degree at most $\frac{n}{2} + o(\sqrt{n})$. So A^n is equal to the linear span of all monomials of the degree at most $\frac{n}{2} + o(\sqrt{n})$. The number of such monomials is $\sum_{i=0}^{\frac{n}{2}+o(\sqrt{n})} \binom{n}{i}$ which can be estimated as $2^{n-1} + o(2^n)$. Q.E.D.

The Main Results

Now we are ready to describe a nice relation between U_F^n-complete elements (or sets) and nearly F-easy operations.

Theorem 1: Suppose depth k circuit C^n uses $exp(o(n^{\frac{1}{2k}}))$ nearly F-easy gates and an arbitrary number of F-easy gates. Then the output g (or outputs $g_1 g_2 \cdots g_s$) of C^n will differ from any U_F^n-complete element f (or set $f_1 f_2 \cdots f_s$) on $2^{n-1} - o(2^n)$ assignments.

Proof: By lemma 2 there is an algebra $A^n \epsilon \Omega_F^n$ such that g (or all g_i's) have degree $o(\sqrt{n})$ in A^n and the dimension of A^n is $2^n - o(2^n)$. If we ignore the assignments where g differs from f (or for some i, g_i differs from f_i) we will get a smaller algebra $\tilde{A}^n \epsilon \Omega_F^n$. In $\tilde{A}^n$, g_i's coincide with f_i's and hence have degree $o(\sqrt{n})$. So by lemma 4 dimension of $\tilde{A}^n$ is $2^{n-1} + o(2^n)$ and we had to ignore $2^{n-1} - o(2^n)$ assignments. Q.E.D.

Corollary: The output of any depth k size $exp(o(n^{\frac{1}{2k}}))$ circuit with basic operations AND, OR and NOT differs from MOD_2 function on $2^{n-1} - o(2^n)$ assignments.

Proof: Take $F = Z_3$. By corollary to lemma 3 $\{MOD_\alpha, NOT(MOD_\alpha)\}$ is $U_{Z_3}^n$-complete. AND and OR are nearly F-easy so theorem 1 applies. Q.E.D.

That gives the Yao's bound for parity [Ya 85] and implies Cai's separation result [Ca 86]. We want to find a field F such that MOD_p is F-easy but $MOD_{s,q}$ functions are U_F^n-complete.

Lemma 5: If p and q are two distinct primes then there is a field of characteristic p which contains q-th root of unity.

Proof: $F_{p^{q-1}}$ will work, for q divides $card(F_{p^{q-1}}^*)$. Q.E.D.

Theorem 2: Let p be a prime number and r is not a power of p then computing MOD_r by depth k circuit with basic operations AND, OR, NOT and MOD_p requires $exp(O(n^{\frac{1}{2k}}))$ AND and OR gates.

Proof: Let q be a prime divisor of r not equal to p. By lemma 5 choose a field F of characteristic p which contains q-th root of unity. Then MOD_p is F-easy, when the set $\{MOD_{0,q}, MOD_{1,q} \cdots MOD_{q-1,q}\}$ is U_F^n-complete and requires a large circuit. But this set is AC^0 reducible to MOD_r. Hence MOD_r also requires a large circuit. Q.E.D.

***Corollary:** If p is a prime then computing MAJORITY by depth K circuit with basic operations AND, OR, NOT and MOD_p requires $exp(O(n^{\frac{1}{2k}}))$ AND and OR gates.

Proof: Take any prime $q \neq p$. Then MOD_q is AC^0 reducible to MAJORITY. So apply theorem 2. Q.E.D.

When P = 2 this gives Razborov's new result.

Open Problems

It is not clear if Lemma 1 or some similar statement holds for a field of characteristic 0. If it does then some nice analytic methods can be used since the space of functions from D to R or C has a natural L_2 metric which coincides with the notion of distance for boolean functions.

Is the MOD_5 function AC^0 reducible to the MOD_6 function ? (It is consistent with our theorems.)

We also do not know if everything in NC^1 is AC^0-reducible to MAJORITY.

Acknowledgement

I am very grateful to Michael Sipser for introducing me to the subject.

References

[Aj 83] M. Ajtai, "E' formulae on finite structures", *Annals of Pure and Applied Logic.*

[Ba 86] D.A. Barrington, "Bounded-width polynomial-size branching programs recognize exactly those languages in NC", *Proc. 18th ACM STOC,* 1986.

[Ba 2] D.A. Barrington, "A note on the theorem of Razborov". (unpublished)

*The corollary was independently proved by David Barrington using modified Razborov's methods.

[Ca 86] Jin-yi Cai, "With probability one a random oracle separates PSPACE from the polynomial hierarchy". *Proc. 18th ACM STOC*, 1986.

[FKPS 83] A. 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.

[FSS 81] M. Furst, J.B. Saxe, and M. Sipser, "Parity, circuits and the polynomial time hierarchy", *Proc. 22nd IEEE FOCS*, 1981, 260-270.

[Ha 86] J. Hastad, "Almost optimal lower bounds for small depth circuits", *Proc. 18th ACM STOC*, 1986, 6-20.

[Ra 86] A.A. Razborov, "Lower bounds for the size of circuits of bounded depth with basis AND, XOR", preprint (in Russian). To appear in "Matem. zam."

[Ya 85] A.C.C. Yao, "Separating the polynomial-time hierarchy by oracles", *Proc. 26th IEEE FOCS*, 1985, 1-10.