Some Problems Involving Razborov-Smolensky Polynomials

David A. Mix Barrington *

Abstract

Several recent results in circuit complexity theory have used a representation of Boolean functions by polynomials over finite fields. Our current inability to extend these results to superficially similar situations may be related to properties of these polynomials which do not extend to polynomials over general finite rings or finite abelian groups. Here we pose a number of conjectures on the behavior of such polynomials over rings and groups, and present some partial results toward proving them.

1. Introduction

1.1. Polynomials and Circuit Complexity

The representation of Boolean functions as polynomials over the finite field $Z_2 = \{0,1\}$ dates back to early work in switching theory [**?**]. A formal language L can be identified with the family of functions $f_i : Z_2^i \to Z_2$, where $f_i(x_1, \ldots, x_i) = 1$ iff $x_1 \ldots x_i \in L$. Each of these functions can be written as a polynomial in the variables $x_1, \ldots, x_n$. We can consider algebraic formulas or circuits with inputs $\{x_1, \ldots, x_n\}$ and the usual complexity measures of size and depth, and get a complexity theory with an algebraic character. Since the binary AND and XOR functions can be simulated in constant size and depth by the binary AND and OR functions and vice versa, this is essentially the usual complexity theory of Boolean circuits and formulas.

Similar notions have been considered for some time. Skyum and Valiant [**?**] introduced a complexity theory along these lines, but used the two-element

*Department of Computer Science, University of Massachusetts, Amherst MA 01003 U.S.A. The author was partially supported by NSF Computer and Computation Theory grant CCR-8714714.

Boolean algebra, rather than Z_2, as the base of their polynomials. Along with the conventional complexity measure of circuit size, they considered the "degree" of a circuit, based on the depth of AND gates in it. For example, their class *pdC* of polynomials with circuit size and degree each polynomial in n, is the class now known as (non-uniform) $LOGCFL$. This work emphasized non-uniform complexity classes and very simple reductions between languages.

In this paper we will use a different and more purely algebraic notion of "degree", which depends only on the polynomial and not on the circuit used to calculate it. Since the input variables are each idempotent, we will define the degree of a monomial to be the number of variables occurring in it. As usual, the degree of a polynomial will be the maximum degree of any monomial occurring in it with a nonzero coefficient.

Razborov [**?**] used this algebraic view to develop a new lower bound technology for Boolean circuits. He noted that the functions in the class $AC^0[2]$ (those functions computable by constant-depth, poly-size, unbounded fan-in circuits of AND, OR, and XOR gates) share a certain algebraic property. Each such function can be approximated by a polynomial of relatively low degree (the function and the polynomial agree except on a small fraction of the inputs). He showed that the MAJORITY function cannot be so approximated, and thus confirmed the general belief that MAJORITY cannot be computed with such circuits.

Smolensky [**?**] extended Razborov's method in two ways. First (along with Barrington [**?**]) he developed an algebraic setting in which MOD-p, for a particular prime p, was a primitive operation instead of MOD-2. Given a field F of characteristic p, he defined the algebra of polynomials over F in variables $\{x_1, \ldots, x_n\}$ satisfying the identities $x_i^2 = x_i$. We will call this the Razborov-Smolensky ring of order n over F, $RS_n(F)$. (Later we will speak of the ring $RS_n(R)$ similarly defined with respect to any finite ring R, and even of the group $RS_n(G)$ defined with respect to any finite abelian group G.) A function from Z_2^n to F is represented by a unique polynomial in $RS_n(F)$, and (following Razborov) functions computable by constant-depth, poly-size, unbounded fan-in circuits of AND, OR, and MOD-p gates (the class $AC^0[p]$) can be approximated by low-degree polynomials in $RS_n(F)$ whenever F is of characteristic p. Razborov's method can then be extended [**?**] to show that MAJORITY is not in $AC^0[p]$.

Smolensky's second and more important contribution was to show that the iterated multiplication function of F cannot be so approximated. This not only provides a simpler proof that MAJORITY is not in $AC^0[p]$, but shows that none of the functions MOD-q (with q prime to p) are in that class.

(In retrospect, Smolensky's methods also provide a reasonably simple way to an earlier seminal result. This is the theorem of Furst-Saxe-Sipser [?] and Ajtai [?] that the functions MOD-q cannot be computed with constant-depth polynomial-size circuits of AND and OR gates (are not in the class AC^0)).

It is intriguing that these methods provide no way to place bounds on the computing power of such circuits with AND, OR, and MOD-q gates unless q is a prime or prime power. Indeed no non-trivial bounds on this class $AC^0[q]$ are known (it might be equal to NP) although no surprising functions are known to be in it. The union of $AC^0[q]$ for all integers q is called ACC^0 [?] (also earlier called ACC [?]). It is conjectured [?] that MAJORITY is not in ACC^0 and thus that ACC^0 is a strict subset of NC^1 (circuits of depth $O(\log n)$ and fan-in two). Yao [?] (see also [?], [?]) has recently shown that functions in ACC^0 can be computed by threshold circuits of depth 3 and quasipolynomial ($2^{(\log n)^{O(1)}}$) size, showing that either ACC^0 is small or such threshold circuits are very powerful.

1.2. The Programs-Over-Monoid Model

The same methods were subsequently used to obtain further lower bounds in circuit complexity, which are most easily stated using the language of programs over finite monoids [?]. A monoid is a set with an associative binary operation and an identity. In classical algebraic automata theory, the computation of a finite-state machine is viewed as an iterated multiplication in a particular finite monoid (the transformations of states of the machine, under the operation of composition). Every finite-state computable language has a particular minimal monoid (called the syntactic monoid) which must be contained within any finite-state machine which recognizes the language. A complexity theory of the regular languages has been developed, where one language is viewed as harder than another if its syntactic monoid contains that of the first. ("Contains" has a well-defined meaning — a monoid A contains B (or B *divides* A) if there is a monoid homomorphism from a submonoid of A onto B.)

Furthermore, there is a structure theory of finite monoids due originally to Krohn and Rhodes [?]. Just as every integer is a product of primes, and every finite group (by the Jordan-Hölder Theorem) can be built up from simple groups in a certain way, every finite monoid can be constructed from particular building blocks using particular operations. The building blocks are the simple groups (Z_p for prime p and various non-abelian groups) and one other monoid which is not a group. The operations are division and the *wreath product* — for details see [?] and [?].

To get natural subsets of the set of finite monoids (and hence natural subclasses of the regular languages), we can restrict which building blocks may be used in the wreath product operation. In this way we can get the classes of solvable groups (only groups of the form Z_p), all groups (only simple groups), aperiodic monoids (only the non-group component), solvable monoids (the non-group component and Z_p's), or all monoids (all components). For each such set of monoids we can look at the class of regular languages whose syntactic monoids lie within that set.

What does all this have to do with circuit complexity? It turns out that the structure of these classes of monoids and regular languages bears a close relationship to that of various circuit complexity classes [**?**]. Given a monoid M and a set $\{x_1, \ldots, x_n\}$ of Boolean inputs, define an *instruction* as the name of an input and a map from Z_2 to M (i.e., two elements of M). The *yield* of an instruction (i, a, b), say, is a if $x_i = 0$ and b if $x_i = 1$. A *program* over M is a sequence of instructions, and its yield is the ordered product of the elements of M yielded by each instruction. A program thus defines a map from Z_2^n into M, or a Boolean function on n variables if we divide the elements of M into "accepting" and "rejecting".

Barrington [**?**] showed that poly-length programs over the non-abelian simple group A_5 (which correspond to poly-length width-5 branching programs obeying certain restrictions) can be constructed to recognize any language in the circuit complexity class NC^1. NC^1 is easily seen to be powerful enough to simulate polynomial-length programs over any finite monoid, so it is equal to the class of languages recognized by such programs. The circuit complexity classes AC^0, $AC^0[p]$, and ACC^0 discussed above (each of which is a subclass of NC^1), are exactly the classes of languages recognized by poly-length programs over aperiodic monoids, p-monoids, and solvable monoids respectively [**?**]. (A p-monoid is one built up from the non-group component and Z_p in the Krohn-Rhodes framework, where p is prime.)

The connection between circuits and monoids is somewhat understood — the operations of modular and threshold counting occur in the same places in both settings, and the placing of one operation above another in a circuit corresponds to the wreath product operations. The classes of regular languages can also be thought of as very uniform versions of the corresponding circuit complexity classes, especially when both are considered as expressibility classes in the sense of Immerman [**?**]. Other complexity classes defined by programs have also been shown to be of interest. Szegedy [**?**] has shown that the languages recognized by programs over abelian monoids are exactly the languages of constant symmetric communication complexity. Bedard, Lemieux, and McKenzie [**?**] have defined an extension of the model to programs over finite *groupoids* (binary algebras, not necessarily associative) and

shown that poly-length programs over groupoids recognize exactly the class $LOGCFL$.

1.3. Polynomials and Programs over Groups

Barrington, Straubing and Thérien [?] have begun the study of the computational power of programs over finite groups. It is known that poly-length programs over any non-solvable group compute exactly NC^1, and that poly-length programs over any solvable group compute only languages in ACC^0. Since we believe that $ACC^0 \neq NC^1$, we believe that programs over solvable monoids are relatively limited in power. The power of solvable monoids can be studied in two stages: the power of solvable groups and the possible interactions between the group and non-group components of a monoid.

In particular, it is conjectured [?] that no poly-length program over a solvable group can compute the AND of all n variables. Given our polynomial language, this is fairly easily seen to be true for p-groups. A program over a p-group, of whatever length, can be simulated by a polynomial of constant degree over Z_p. If, for some f of constant degree, $f = a$ iff $x_1 x_2 \ldots x_n = 1$, then the polynomial $1 - (f - a)^{p-1}$ is also of constant degree and must be exactly $x_1 x_2 \ldots x_n$, which is impossible unless n is a constant.

Even moving to nilpotent groups (direct products of p_i-groups, in general involving more than one p_i), things are not so easy. In the case of programs over Z_6, for example, we can convert such a program into one polynomial over Z_2 and one over Z_3, each of constant degree. We know about the sets defined by each of these two polynomials, but how do we rule out the possibility that two of these sets intersect in the singleton $(1, 1, \ldots, 1)$? A Ramsey argument [?] shows that this is impossible for "sufficiently large", but still constant, n.

Over groups which are solvable but not nilpotent, it is possible for a program of exponential length to compute the AND of all the variables. For some of these groups, methods have been devised to show that exponential length is necessary, but in general this remains open. The known subcases are groups which divide the wreath product of a p-group and an abelian group [?], and dihedral groups [?]. A plausible but unproven conjecture about the ring $RS_n(Z_p)$ would extend the exponential lower bound to groups dividing the wreath product of a p-group and a nilpotent group [?].

These constructions, like Smolensky's, use the ring $RS_n(F)$ for a field F of characteristic p having elements of the desired multiplicative order. Rather than degree, the complexity measure used on polynomials is the number of terms needed to form them by addition, in two different bases of $RS_n(F)$.

The Razborov-Smolensky ring of polynomials can be defined over an arbitrary ring as well as over a field. The set of such polynomials over an arbitrary abelian group still forms a group under polynomial addition, though it no longer has a ring structure. Many properties, such as the unique representation of any function from Z_2^n to R by a polynomial, still hold, but some do not. One which does not is the one we used above to convert from one way to represent a set by a polynomial to another:

Definition 1.1 *A polynomial f in $RS_n(R)$* weakly represents *a set $A \subseteq Z_2^n$ if for some $a \in R$, $f(\mathbf{x}) = a$ iff $\mathbf{x} \in A$. A polynomial f* strongly represents *a set A if $f(\mathbf{x}) = 1$ for $\mathbf{x} \in A$ and $f(\mathbf{x}) = 0$ otherwise.*

Fact 1.2 *If f weakly represents A with value a over a finite field F, then $1 - (f - a)^{|F|-1}$ strongly represents A and has degree at most a constant multiple of that of f.* □

We know that this exact property can fail for polynomials over a ring which is not a field. Consider $R = Z_6$, and let $f = x_1 + x_2 + \ldots + x_n$. This linear polynomial weakly represents the set $A = \{\mathbf{x} : x_1 + x_2 + \ldots x_n = 0 \bmod 6\}$. But the unique polynomial strongly representing A over Z_6 can be calculated (using methods in [?] or [?]) — it is congruent mod 3 to the MOD-2 function and congruent mod 2 to the MOD-3 function. It has degree n, the maximal possible degree.

The inability to do this conversion occurs as a roadblock constantly in the algebraic approach to circuit lower bounds. In this paper we would like to raise the possibility that some relationship between weak and strong representation might hold for other reasons, and that this might allow these algebraic methods to be extended.

2. The Small Image-Set Conjecture

Let us first consider attempting to represent a small set with a polynomial of as small a degree as possible. (We will define the *size* of a subset $A \subseteq Z_2^n$ to be the fraction of the entire set it contains, i.e., $|A|/2^n$.) For strong representation degree n is needed because the unique polynomial representing that function has degree n (and an exponential number of terms). With degree d we can strongly represent a set of size 2^{-d}, but not one any smaller (we'll prove this later). We can do somewhat better if we are willing to settle for weak representation. For example, in Z_m we can have $m-1$ terms of degree $\lceil n/(m-1) \rceil$, each giving one if its variables are all one and zero otherwise. The sum of these terms gives $m-1$ iff all n variables are one. A reasonable first conjecture says that this construction is the best possible.

Conjecture 2.1 *(Small Image-Set Conjecture, Weak Form) Any nonempty set weakly represented by a polynomial of degree d over R has size at least* $2^{-d(|R|-1)}$.

Furthermore, something stronger seems to be true. If we consider the number of values taken on by the polynomial, we have a continuum between two (strong representation) and $|R|$ (weak representation). Using examples similar to those above and conjecturing that they are best possible, we are led to:

Conjecture 2.2 *(Small Image-Set Conjecture) Any nonempty set weakly represented by a polynomial of degree d which takes on r values has size at least* $2^{-d(r-1)}$.

Note that neither of these conjectures makes any reference to the multiplicative structure of $RS_n(R)$ — in fact they are conjectures about the group $RS_n(G)$, where G is the additive group of R. (The use of the letter R below will not necessarily imply the existence of a ring structure.)

Unfortunately, both these conjectures fail in the case $d = 3$ and $R = Z_6$. If we let s_i denote the sum of all terms of degree i in 27 variables over Z_6, the polynomial $s_3 + 5s_2 + 3s_1$ weakly represents the singleton set containing the all-zero element of Z_2^{27} (this example was discovered by David Applegate, Jim Aspnes, and Steven Rudich). This set has size 2^{-27}, smaller than the 2^{-15} predicted by Conjecture **??**.

Barrington, Beigel, and Rudich [**?**] have shown that this is an example of a general phenomenon for *symmetric* polynomials over an abelian group (where the monomials of a given degree must all have the same coefficient, with an absent monomial considered to have zero coefficient). Furthermore, this behavior is the best that symmetric polynomials can do, so that they satisfy a variant of Conjecture **??**. To state their result, let $\rho(g)$ be the number of distinct primes dividing the order of an abelian group G, so that $\rho(Z_6) = 2$.

Fact 2.3 *[?] The minimum size of a set weakly represented by a symmetric polynomial of degree d over G is* $2^{-\Theta(d^{\rho(G)})}$. □

Conjecture 2.4 *The minimum size of a set weakly represented by* any *polynomial of degree d over G is* $2^{-\Theta(d^{\rho(G)})}$.

This question remains open. Here we will continue with the progress made on the original conjectures before this work, commenting on the later results as necessary.

Observation 2.5 *The SIS Conjecture is trivially true if* $r = 1$, $d = 0$, *or if* $n \leq d(r-1)$. □

To prove the SIS conjecture in some more interesting special cases, let us consider the following construction. Let f be a polynomial of degree at most d on n variables, taking on at most r values. Write f as $g + hx_n$ so that g and h are independent of x_n, and let $g' = g + h$. Note that h is of degree at most $d-1$. The values taken on by f are exactly that of g (if $x_n = 0$) or of g' (if $x_n = 1$), so each of these functions is at most r-valued. If both take on the same r values, and the SIS Conjecture holds for smaller values of n, then it continues to hold for this n. This is because a set weakly represented by f in this case is the union of two subsets of Z_2^{n-1}, each weakly represented by a polynomial which is degree d and r-valued. But it is entirely possible for g, say, to take on only $r-1$ values, so that some value is taken on only with $x_n = 1$. In this case the size of the subset of Z_2^n on which f takes that value would be half of that of the subset of Z_2^{n-1} where g' takes it on. In two special cases, however, we can see how to carry out an inductive proof of the Conjecture.

Fact 2.6 *The SIS Conjecture holds in the case* $r = 2$.

Proof : Let f, g, h, g' be as above. The argument above suffices if g and g' each take on both the values taken on by f. But because $r = 2$, if either g or g' fails to do so, it must be a constant. But then the other differs from a constant by h and is thus of degree at most $d-1$. If we also induct on d, we can assume that a nonempty subset of Z_2^{n-1} weakly represented by g or g' has size at least $2^{-(d-1)}$, so that the same set viewed as a subset of 2^n has size at least 2^{-d}. □

Fact 2.7 *The SIS Conjecture holds in the case* $d = 1$.

Proof : Again we use the terminology above. If $d = 1$, then h must be a constant. This means that g and g' take on the same number of values. If this number is r, then each takes on all the values of f and the argument above suffices. Otherwise each is at most $(r-1)$-valued, and weakly represents sets of size only at least $2^{-(r-2)}$ in Z_2^{n-1}, which are of size $2^{-(r-1)}$ in Z_2^n. □

Fact 2.8 *The SIS Conjecture holds when* R *is a field.*

Proof : Here we can show that a set weakly represented by an r-valued f of degree d is also weakly represented by a two-valued polynomial of degree $d(r-1)$. (Over a field, this is the same as being strongly represented by a polynomial of that degree, because we can divide by any constant.) The desired result will then follow from Fact **??** above.

Suppose $f = a$ on the set in question, and on other points takes on some value in $\{b_1, \ldots, b_{r-1}\}$. Consider the product over all i of $f - b_i$. It equals zero off the set in question, and equals a particular nonzero constant on it — the product over all i of $a - b_i$. □

Fact 2.9 *Conjecture* **??** *(the weaker form of the SIS Conjecture) holds when* $R = Z_{p^k}$ *for some prime* p.

Proof : A trick of Chandra, Stockmeyer, and Vishkin [**?**], relating the MOD-p^k operation to the MOD-p operation, can be adapted to this setting. The sum modulo p^k of a set of Boolean terms is zero iff the modulo p sum of the terms is zero and the modulo p^{k-1} sum of all the products of p-tuples of the terms is also zero. Using this fact, we can take a degree d polynomial f over $R = Z_{p^k}$ and create a two-valued degree $d(p^k - 1)$ polynomial f' over Z_p such that $f = 0$ iff $f' = 0$. □

This means that the full SIS conjecture holds for the case $r = p^k$, but it is not known to hold for general r. In the case $r = 3$, if the range of f is $\{0, a, b\}$, the degree $2d$ polynomial $(f-a)(f-b)$ is two-valued and tests $f = 0$, unless $ab = 0$. The latter is possible only if p divides both a and b. But in that case f can be divided by p (a polynomial takes on all its values in a subgroup iff every term of it does), without changing its degree. In fact, for $r \leq 3$ and $r = p^k$, an r-valued polynomial of degree d over Z_{p^k} can be simulated by a two-valued degree $d(r-1)$ polynomial over Z_p. It is not know whether this holds for all r (it is interesting that so far whether it does appears to be independent of k). Note also that the cases shown here suffice to prove the full SIS conjecture for $R = Z_4$.

This makes $R = Z_6$ the smallest ring for which the mimimum size of a weakly representable set is unknown. We don't know whether a quadratic polynomial over Z_6 can weakly represent a singleton set with $n = 11$ (it can for $n = 10$). We don't even know whether a three-valued quadratic polynomial can weakly represent a singleton with $n = 5$ ($x_1x_2 + x_3x_4$ suffices for $n = 4$). In the special case of quadratic polynomials, no symmetric polynomial can weakly represent a singleton with $n > 9$, so the new results of [**?**] do not affect this case. But as described above, they do make a difference at $d = 3$, where a singleton can be weakly represented with $n = 27$, as opposed to the conjectured $n = 15$.

No symmetric polynomial can do better, but whether an asymmetric one can is unknown.

The quadratic case has an alternate representation as a graph problem. Label both the vertices and edges of an undirected graph with elements of R, and consider the sums of the vertex and edge labels in a clique. What is the largest graph for which every nonempty clique has a nonzero sum? Heath and Pemmaraju [personal communication] have looked at such graphs (for cyclic R) and defined "tight" graphs to be those where (1) every nonempty clique sum is nonzero and (2) the number of distinct clique sums is minimal over all graphs of that size satisfying (1). They conjecture that tight graphs with r distinct nonzero clique sums have $2r$ vertices. They speculate that tight graphs might necessarily posess some structure which would allow an inductive proof on r. Their conjecture is independent of the modulus, suggesting that it may have a combinatorial rather than an algebraic proof. A proof of the SIS conjecture in this quadratic case might still lead to progress on the general question, though the original SIS conjecture does not hold.

3. The Intersection Conjecture

One way to examine the sets of input values which can be defined by specific types of polynomials is to see how they intersect. For example, suppose that we have k equations $f_i = 0$, each of degree d. The SIS conjecture would give us limits on how small the locus of each equations could be, but would place no limits on the size of the intersection. Over a field, as we shall see below, we can use the multiplication to construct a single equation $f^\star = 0$ which is true iff $f_i = 0$ for all i. (One way to do this, which is not the most efficient, would be to raise each f_i to the $|F|-1$'th power to get an f_i' which is always zero or one, and then let F be the product over all i of $1 - f_i'$.) To what extent is this a general phenomenon for rings or abelian groups?

We know that if R is not a field, then two sets which are each strongly represented by a polynomial of low degree can intersect in a set whose strong representation has high degree. Let $R = Z_6$ and consider two sets of inputs: those summing to zero mod 2 and those summing to zero mod 3. The strong representations of these sets over Z_6 are linear and quadratic, respectively, but that of their intersection is degree n. In this case the intersection has a weak representation of low degree. Does this always happen?

Conjecture 3.1 *(Intersection Conjecture, Strong Form) If $\{f_i\}$ is a set of k polynomials of degree at most d over a finite group G, then there is a polynomial $f^\star$ of degree at most kd such that $f^\star = 0$ iff $f_i = 0$ for all i.*

Even if this is false, the following weaker statement might still be true:

Conjecture 3.2 *(Intersection Conjecture, Weak Form) Let $\{f_i\}$ be as above, and let S be the set of inputs $\mathbf{x}$ such that $f_i(\mathbf{x}) = 0$ for all i. If S is nonempty, then there is a polynomial $f^\star$ of degree at most kd such that the set $\{\mathbf{x} : f^\star(\mathbf{x}) = 0\}$ is also nonempty but is no bigger than S.*

Proposition 3.3 *Conjecture* **??** *holds when G is a finite field F.*

Proof : We will show that there is a polynomial g_k of degree k over F, in k variables which range over F (not just Z_2), such that $g_k(y_1, \ldots, y_k) = 0$ iff $y_i = 0$ for all i. Then we can let $f^\star$ be $g_k(f_1, \ldots, f_k)$, a polynomial of degree kd in the input variables with the desired property.

For any F and k there is another finite field E which is a vector space of dimension k over F. Fix a basis $\{w_1, \ldots, w_k\}$ of E, so that each $a \in E$ can be written as $a = y_1 w_1 + \ldots + y_k w_k$ and thus identified with the k-tuple $\{y_1, \ldots, y_k\}$ of elements of F. The operation of multiplication by a is a linear transformation of this vector space represented by a matrix M_a. The determinant of M_a is an element of F, which is zero iff a is the zero element of E. M_a is given in terms of the y_i as $y_1 M_{w_1} + \ldots + y_k M_{w_k}$, so that M_a is a matrix each of whose entries is a linear polynomial in $\{y_1, \ldots, y_k\}$ over F. The determinant of this matrix is a polynomial of degree k over F and is zero iff all its inputs are zero. □

Note that although we used the multiplicative structure of F in the course of this proof, the statement of Conjecture **??** makes no reference to this structure. Thus we know that the conjecture holds for any abelian group which can be given a field structure, i.e., any product Z_p^e for p prime.

Observation 3.4 *If Conjecture* **??** *holds for two abelian groups G and H, it holds for their direct product.*

Proof : Write each f_i as $\langle g_i, h_i \rangle$, with g_i over G and h_i over h. Each g_i has degree at most k, so there is a polynomial $g^\star$ over G of degree kd such that $g^\star = 0$ iff $g_i = 0$ for all i. Similarly there is an $h^\star$ over H of degree kd with $h^\star = 0$ iff $h_i = 0$ for all i. If $f^\star = \langle g^\star, h^\star \rangle$, then $f^\star = 0$ iff $g_i = 0$ and $h_i = 0$ for all i, which is true iff $f_i = 0$ for all i. □

Corollary 3.5 *Conjecture* **??** *is true for any abelian group which is a direct product of cyclic groups of prime order, or equivalently any group whose exponent (least common multiple of the orders of the elements) is square-free.* □

Proposition 3.6 *Conjecture* **??** *is true for groups of the form* Z_{p^e}.

Proof : By the proof of Fact **??** in the previous section, a set weakly representable in degree d over Z_{p^e} is weakly representable in degree $d(p^e-1)$ over Z_p. By Proposition **??** above, the intersection of k such sets is also weakly representable in degree $kd(p^e-1)$ over Z_p. If this intersection is nonempty, by Fact **??**, its size is at most $2^{-kd(p^e-1)}$. But over Z_{p^e} it is easy to construct a polynomial of degree kd which weakly represents a set of this size — take the sum of p^e-1 independent monomials of degree kd. (If there are not enough variables available to do this, it is still possible to weakly represent a singleton set, which has the minimum possible size of any nonempty set.) □

We do not know that the groups which satisfy Conjecture **??** are closed under direct product, so we still do not know whether it holds for Z_{12}, for example. The argument used for Observation **??** does not work.

The intuition here is that a polynomial of a certain degree has only so much power to isolate a small fraction of the input space. Our conjectures say in effect that the polynomial can do no better at isolating a small fraction of a subset of that space defined by another polynomial.

4. Making Change in an Abelian Group

A family of k equations over a finite abelian group G can equally well be thought of as a single equation over the direct product G^k. If the original equations are all of degree d, then so is the composite equation. This opens the possibility of applying the SIS Conjecture to the study of systems of equations. For example, we know that for $d=1$ and for any G, a family of k linear equations over G gives a single equation over G^k. A set weakly represented by this equation must be of size at most $2^{-(|G|^k-1)}$, because the SIS Conjecture holds with $d=1$. But if our Intersection Conjectures are correct, we can do better. The set of inputs satisfying each component has size at least $2^{-(|G|-1)}$, so the intersection of these sets would be size $2^{-k(|G|-1)}$. Perhaps a stronger form of the SIS Conjecture holds for many-fold direct products? The following problem is an attempt to investigate this. We restrict ourselves to the special case of linear polynomials, and as before we ignore any multiplicative structure which G might have and consider it as an abelian group.

Definition 4.1 *The* Boolean span *of a multiset of elements of* G *is the set of all sums of submultisets of it. The* proper span *of a multiset of nonzero elements is the set of all sums of nonempty submultisets.*

Problem 4.2 *What conditions on a multiset from G force its Boolean span to be all of G?*

We call this problem "change-making" because it is a variation of a familiar problem: How many coins of a specific type are needed to guarantee having change available for any amount? Rather than have the exact number of pence available for our purchase, we might be satisfied to have the correct number modulo 100, so we would be able to transfer an integral number of pounds. Thus we might want the Boolean span of our coins in Z_{100} to be all of Z_{100}.

A similar problem has been studied in the number theory literature – how large must a multiset from G be before its proper span includes 0? This number is at most one greater than the answer to our problem. Olson [**?**, **?**] answered this question for p-groups and for the direct product of two cyclic groups where the order of one divides the order of the other. Baker and Schmidt [**?**] gave an upper bound on this number for general groups which is within a logarithmic factor of the known lower bound in many important cases. We will present our independent treatment of the question here and discuss the consequences of their results as necessary and in our conclusion.

Lemma 4.3 *Any multiset of $p-1$ nonzero elements from Z_p has Boolean span Z_p.*

Proof : By induction on k, we show that any set of k coins spans a set of size at least $k+1$ in Z_p, if $k < p$. The $k = 0$ case is trivial. Given k coins spanning a set S and a new coin a, we can make all of S and also the set $S + a = \{s + a : s \in S\}$. $S + a$ has the same size as S and must be different from S (S could be invariant under translation by a nonzero a only if it were a subgroup). So the new Boolean span is strictly larger than S, and has size at least $k+2$ if S has size at least $k+1$. □

Corollary 4.4 *Any multiset of size at least $p-1$ of nonzero elements of Z_p has a submultiset of size $p-1$ whose Boolean span is Z_p.* □

We can apply this Corollary to get a lower bound on the size of a nonempty set weakly represented by a linear polynomial. If the linear polynomial is given by $\sum_{i=1}^{n} c_i x_i$, choose a subset of the c_i's spanning Z_p. The terms with these coefficients (with the other variables zero) give all possible values and take on each value on a set of size at least $2^{-(p-1)}$. Adding in the other variables one by one cannot give rise to a smaller set. Of course this is just

the $d = 1$ case of the SIS conjecture. But we will see that improved solutions to the change-making problem will give better bounds in the case of more general groups.

Applying this same argument to other cyclic groups, we get a more complicated result, because these groups might have nontrivial subgroups:

Lemma 4.5 *Any multiset of $m-1$ elements of Z_m has a nonempty submultiset whose Boolean span is a subgroup of Z_m.*

Proof : A zero element spans the trivial subgroup. The process from the Lemma above must terminate with S a proper subgroup or continue until the span is all of Z_m. □

This means that having $m-1$ "coins" no longer guarantees having change for all amounts, but any larger set must contain redundant coins.

Corollary 4.6 *Any multiset M of size at least $m-1$ elements of Z_m has a submultiset of size at most $m-1$ with the same Boolean span as M.*

Proof : Assume by induction that the Corollary is true for all Z_k with $k < m$. Using the Lemma, choose a submultiset N of M spanning a subgroup H, such that no proper submultiset of N spans a subgroup. Discard from M any other elements of H. If $H = Z_m$ then N must have only $m-1$ elements as otherwise we could apply the Lemma again to a proper submultiset of it. Otherwise H is isomorphic to Z_k for some $k < m$ and has at most $k-1$ elements. Now discard from M all but one element in each coset of H. of the subgroup. This has no effect on the span as the difference can be made up by the elements generating the subgroup. We are left with at most $(k-1) + (m/k - 1) < m - 1$ elements in M. □

As above, we can use the Corollary to show that any nonempty set weakly represented by a linear polynomial over Z_m has size at least $2^{-(m-1)}$. This is also a known special case of the SIS Conjecture. But for groups which are not cyclic, a stronger change-making result appears to hold, which could be used to get better lower bounds on the size. The key parameter of the group is not the order but, roughly, the sum of the orders of the ring's components.

Definition 4.7 *Let R be a finite abelian group. Let e be the maximum order of any element of R. The reader may verify that R can be written as a direct product $Z_e \times R'$. Define a function on abelian groups recursively $f(Z_1) = 0$ and $f(R) = (e-1) + f(R')$. We will call this function the* capacity *of the group.*

Fact 4.8 *For any R, there is a multiset of $f(R)$ elements such that (1) its Boolean span is R, (2) its proper span is $R \setminus \{0\}$.*

Proof : To get (1) and (2), write R as $Z_e \times R'$ and let the multiset be $e-1$ copies of $(1, 0_{R'})$ together with $(0, x)$ for each x in the set for R'. □

This means that a linear polynomial over R can weakly represent a set of size $2^{-f(R)}$. We believe that no polynomial can do better.

Conjecture 4.9 *No multiset of more than $f(R)$ elements from R satisfies conditions (1) and (2) in the Fact above. That is, no linear polynomial over R can weakly represent the function strongly represented by $ax_1x_2 \ldots x_{f(R)}$ (where $a \in G$).*

Olson proves that if G is a p-group [**?**] or the direct product of two cyclic groups the order of one of which divides the order of the other [**?**], then any multiset of size $f(G)+1$ has 0 in its proper span. Thus Conjecture **??** is true for these groups.

A natural way to try to prove Conjecture **??** in general would be to use induction on subgroups. We could duplicate the argument for cyclic groups above if we knew that every multiset of $f(R)$ elements has a subset spanning a subgroup H. Unfortunately, this is not true: Consider the multiset from $Z_2 \times Z_4$, listed as $\{(0,1),(0,1),(1,1),(1,1)\}$. No subset spans a subgroup (the sum $(1,0)$ cannot be formed). Similar examples exist in many other rings. A related property, however, is true in so far as we have been able to check and suffices for our purposes:

Conjecture 4.10 *(The Change Conjecture) Any multiset of $f(R)+1$ elements from R has a submultiset of size at most $f(R)$ whose Boolean span is a subgroup.*

Corollary 4.11 *(assuming Conjecture **??**) Any multiset M of more than $f(R)$ elements from R has a submultiset of size at most $f(R)$ whose Boolean span is the same as that of M.*

Proof : Assume by induction that the Corollary is true for all groups smaller than R. Apply the Conjecture to M to get a submultiset N of size at most $f(R)$ whose span is a subgroup H. If $H = R$ we are done. Otherwise replace N by a submultiset of size at most $f(H)$ which still spans H, by the inductive hypothesis. Discard any other elements of H in M. Now consider

the remaining elements of M as elements of R/H (as their effect on the span of M depends only on which coset they are in because any element of H can be formed). Using the inductive hypothesis again, find a submultiset of these of size at most $f(R/H)$ with the same span and discard the others. We are left with at most $f(H) + f(R/H) \leq f(R)$ elements. □

¿From this Corollary we get an improved bound for weak representation just as before:

Corollary 4.12 *(assuming Conjecture ??) Any nonempty set weakly represented by a linear polynomial over R has size at least $2^{-f(R)}$.* □

These last conjectures imply the weaker form of the Intersection Conjecture with $d = 1$, because k equations over R are equivalent to one equation over R^k, and $f(R^k) = kf(R) \leq k(|R| - 1)$.

5. Consequences

Our primary goal in this study is to extend our understanding of the computational power of Razborov-Smolensky polynomials over general finite rings and groups. We believe that resolving the conjectures here will require techniques which should be of general utility in the study of lower bounds for the related computational models of programs over groups and Boolean circuits. But there are some direct consequences which would ensue if certain of our conjectures were to be proven.

Though the original SIS conjecture is false, we have a revised version that includes the number of distinct primes dividing the order of the group, essentially saying that the symmetric functions of [?] are the best possible. A proof of this would show that programs over nilpotent groups cannot calculate functions whose polynomials have more than constant degree. In particular they cannot compute the AND function on more than a constant number of variables. Both of these facts are currently known, but the proof of them [?] involves a Ramsey argument. Because of this, the "constant" bound on the number of variables for a given nilpotent group is very large. The new proof would reduce this bound to a polynomial in the order of the group (whose degree is the number of primes dividing the order).

It is possible that similar techniques would allow the extension of the exponential lower bound for program length to groups which are the wreath products of nilpotent groups with abelian groups. This is because any such group divides a direct product of groups of the kind we can currently handle. But since other parameters than degree are used in the existing lower bound proofs, the new results would have to deal with them.

Our conjectures, even to the extent that they are already proven, have minor consequences in circuit complexity. Consider a circuit of MOD-6 gates computing the AND function (a MOD-6 gate, which has unbounded fan-in, outputs one iff the MOD-6 sum of its inputs is nonzero, and otherwise outputs zero). It is conjectured that such a circuit would require an exponential number of gates (this is implied by the conjecture that programs over solvable groups require exponential length to compute AND). Can we prove any kind of lower bound on the number of gates?

Prior to this work, the best known result along these lines was that of Smolensky [?], who showed that $\Omega(\log n)$ gates are required. We can duplicate this result, and also show that $\Omega(\log n)$ gates must occur on the level nearest the inputs, as follows.

If k is the number of gates on this level, then the level as a whole computes a function from Z_2^n to Z_6^k (before converting the output of this function to an element of Z_2^k). This function can be represented by a linear polynomial in the n Boolean input variables over the ring Z_6^k. By the $d = 1$ case of the SIS Conjecture, which we have proven, a nonempty set weakly represented by this linear function has size at least $2^{-(6^k-1)}$. For the circuit to compute the AND function, the first row must behave differently on the input $(1, 1, \ldots, 1)$, so that the polynomial for the first row must weakly represent a singleton set and thus k must be $\Omega(\log n)$.

The possibility of a better bound originally motivated much of the work here. Since the Intersection Conjecture holds for Z_6, we know that a linear polynomial over Z_6^k is equivalent to a polynomial of degree k over Z_6. Thus, the (false) SIS conjecture for $R = Z_6$ would tell us that $k = \Omega(n)$, and the (unproven) revised one would give $k = \Omega(\sqrt{n})$.

The (unproven) Change Conjecture for $R = Z_6^k$ would also give a linear lower bound, by the argument presented at the end of the last section. But although we do not know that a multiset of $f(Z_6^k) = 5k$ elements of Z_6^k must satisfy the conclusion of the Change Conjecture, it is not hard to show that a set of size $\Omega(k^2)$ must do so. Again by the argument in the last section, this yields an $\Omega(\sqrt{n})$ lower bound on the number of gates in a MOD-6 circuit for AND. Baker and Schmidt [?] improve this parameter to $\Omega(k \log k)$, yielding an $\Omega(n \log n)$ bound on the circuit size.

The best current result, however, uses other methods. Thérien [?] has recently proved an $\Omega(n)$ lower bound on the number of gates required to compute the AND function with a depth-2 circuit of MOD-q gates, for any q not a prime power. His short proof relies on the machinery developed in [?].

6. Acknowledgements

Much of this paper represents joint work with Denis Thérien, who suggested a number of these problems. I would like to thank him, the other participants in the 1989 and 1990 McGill Invitational Workshops, the participants in the 1990 Durham Symposium (especially Imre Leader), my colleagues in the COINS Theory Group, David Applegate, Jim Aspnes, Richard Beigel, Johan Håstad, Lenny Heath, Sriram Pemmaraju, and Steven Rudich for various helpful discussions. The two anonymous referees made a number of helpful suggestions and corrections which have improved the presentation. In addition, one of them provided the proofs of Proposition **??** and Observation **??**, improving the results from the earlier version.

References

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

[Al89] Allender E., *A note on the power of threshold circuits. Proceedings of the 30th IEEE FOCS Symposium (1989), 580-585.*

[BBR91] Barrington D.A.M., Beigel R., Rudich S., *Representing Boolean functions as polynomials modulo composite numbers. Submitted to 1992 FOCS, also COINS Technical Report 91-82 (Nov. 1991), University of Massachusetts.*

[BS80] Baker R.C., Schmidt W.M., *Diophantine problems in variables restricted to the values 0 and 1. J. of Number Theory 12 (1980), 460-486.*

[Ba86] Barrington D.A., *A note on a theorem of Razborov. COINS Technical Report 87-93 (July 1986), University of Massachusetts.*

[Ba89] Barrington D.A., *Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. J. Comp. Syst. Sci. 38:1 (Feb. 1989), 150-164.*

[BIS90] Barrington D.A.M., Immermman N., Straubing H., *On uniformity within NC^1. J. Comp. Syst. Sci. 41:3 (Dec. 1990), 274-306.*

[BST90] Barrington D.A.M., Straubing H., Thérien D., *Non-uniform automata over groups. Information and Computation 89:2 (Dec. 1990), 109-132.*

[BT88] Barrington D.A.M., Thérien D., *Finite monoids and the fine structure of NC^1. J. ACM (Oct. 1988), 941-952.*

[BLM90] Bédard F., Lemieux F., McKenzie P., *Extensions to Barrington's M-program model. Structure in Complexity Theory: Fifth Annual Conference (1990), 200-209.*

[BT91] Beigel R., Tarui J., *On ACC. Proceedings of the 32nd IEEE FOCS Symposium (1991), 783-792.*

[CSV84] Chandra A.K., Stockmeyer L.J., Vishkin U., *Constant depth reducibility. SIAM J. Comp. 13:2 (1984), 423-439.*

[FSS84] Furst M., Saxe J.B., Sipser M., *Parity, circuits, and the polynomial-time hierarchy. Math. Syst. Theory 17 (1984), 13-27.*

[KRT68] Krohn K.B., Rhodes J., Tilson B., in Arbib M.A., ed., *The Algebraic Theory of Machines, Languages, and Semigroups. Academic Press, 1968.*

[MT89] McKenzie P., Thérien D., *Automata theory meets circuit complexity. Proceedings of the 16th ICALP, Springer Lecture Notes in Computer Science 372 (1989), 589-602.*

[Ol69] Olsen J.E., *A combinatorial problem on finite Abelian groups, I. J. of Number Theory 1 (1969), 8-10.*

[Ol69a] Olsen J.E., *A combinatorial problem on finite Abelian groups, II. J. of Number Theory 1 (1969), 195-199.*

[Ra87] Razborov A.A., *Lower bounds for the size of circuits of bounded depth with basis* $\{\&, \oplus\}$. *Mathematicheskie Zametki 41:4 (April 1987), 598-607 (in Russian). English translation Math. Notes Acad. Sci. USSR 41:4 (Sept. 1987), 333-338.*

[Sh38] Shannon C.E., *A symbolic analysis of relay and switching circuits. Trans. AIEE 57 (1938), 713-723.*

[SV81] Skyum S., Valiant L.G., *A complexity theory based on Boolean algebra. Proceedings of the 22nd IEEE FOCS Symposium (1981), 244-253.*

[Sm87] Smolensky R., *Algebraic methods in the theory of lower bounds for Boolean circuit complexity. Proceedings of the 19th ACM STOC (1987), 77-82.*

[Sm90] Smolensky R., *On interpolation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates. Proceedings of the 31st IEEE FOCS Symposium (1990), 628-631.*

[St91] Straubing H., *Constant-depth periodic circuits. International Journal of Algebra and Computation 1:1 (1991), 1-39.*

[Sz90] Szegedy M., *Functions with bounded symmetric communication complexity and circuits with mod m gates. Proceedings of the 22nd ACM STOC (1990), 278-286.*

[Th91] Thérien D., *Linear lower bound on the size of $CC_2^0(q)$-circuits computing the AND function. Manuscript (May 1991), McGill University.*

[Ya90] Yao A.C.C., *On ACC and threshold circuits. Proceedings of the 31st IEEE FOCS Symposium (1990), 619-627.*