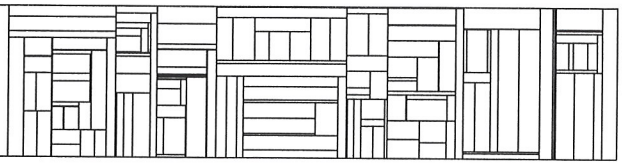
ISSN 0105-8517

Extended Smolensky's Method

Zhi-Li Zhang*

DAIMI PB – 315
July 1990

COMPUTER SCIENCE DEPARTMENT
AARHUS UNIVERSITY
Ny Munkegade, Building 540
DK-8000 Aarhus C, Denmark



* This work was done while the author was visiting School of Computer Science, Carnegie-Mellon University, USA

ISSN 0105-8517

PB – 315 Zhi-Li Zhang: Extended Smolensky's Method

Abstract

We give a simple extension of Smolensky's method by replacing Smolensky's concept of U_F^n-completeness by a new definition: F-hardness. An easy consequence of this definition is that F-hard functions do not have constant depth, polynomial size Boolean circuit with Mod_p, where p is the characteristic of F. By this extension, we can explicitly show many functions are hard, we establish a *Hardness Lemma* for a class of functions, and characterize when a function over a finite field is hard to compute by a small depth with Mod_p gates. Furthermore, we discuss the difficulties in extending Smolensky's theory over a general ring. While in general the nice relationship between the Boolean circuit model and the algebra of functions representing Boolean functions over a ring collapses, we can still extend the complexity theoretic notions introduced by this extended Smolensky's theory to a ring in order to classify functions over such a ring by their relative complexity. A result states that any representation of $Majority$ over any ring $R = Z/(r)$ for any fixed $r \in \mathbf{N}$ is hard. This provides a kind of evidence that $Majority$ is not AC^0 reducible to Mod_r.

1 Introduction

Since the seminal paper of Furst, Saxe and Sipser [FSS], in which they proved that AC^0 Boolean circuits (*i.e.* constant depth, polynomial size, in the sequel, we will call them small depth circuits) could not compute the *Parity* function (this result was also independently proved by Ajtai [Aj83]), small depth Boolean circuits have been under extensive investigation, which turned out to be very successfully: first by Yao [Ya 85] and later improved by Haståd [Ha 86], an exponential lower bound on the size of constant depth Boolean circuits computing *Parity* was obtained. Cai [Cai 86] (and independently Babai) proved that small depth circuits not only fail to compute *Parity* but also give eventually 50% of error. More recently, Linial, Mansour and Nisan [LMN 89] proved that AC^0 Boolean functions have essentially only non-vanishing coeffiecients in lower degree terms.

A natural extension of AC^0 circuits is to provide them with more powerful gates *e.g.* *Parity* (Mod_2) or Mod_p gates, where p is a fixed prime. This motivated the definition of AC^0 reduction: a function f is AC^0 reducible to a function g $(g_1, ..., g_n)$ if there exists a small depth Boolean circuit with g $(g_1, ..., g_n)$ as new gate(s) computing f. It was conjectured in [FSS] that Majority is not AC^0 reducible to Parity. This conjectured was proved by Razborov [Ra 87] who showed an expenential lower bound for computing *Majority* using constant depth Boolean circuits with *Parity*. Shortly afterwards, in his ingenious paper [Sm 87], Smolensky extended Razborov's result to any fixed finite field of characteristic p, by purely algebraic methods, showing that there are no small depth circuits with Mod_p that can approximate Mod_q well, where p, q are distinct primes. Hence, Mod_q is not AC^0 reducible to Mod_p. Apparently, his method could not be extended to a general ring, hence he conjectured that for a fixed composite number r, and for a fixed prime q, if q does not divide r, then Mod_q is not AC^0 reducible to Mod_r, in particular, Mod_5 is not AC^0 reducible to Mod_6.

In their studying of polynomial length nonuniform deterministic finite autamata (NUDFA) over monoids and groups, Barington and Thérien [Ba 86, BT 87, BT 88] defined the complexity class ACC which is the AC^0 closure of Mod_r gates for any fixed $r \in \mathbf{N}$ and conjectured that *Majority* is outside ACC. Although they have discovered and established many interesting and enlightening relationships between various classes inside

NC^1 and families of polynomial legth NUDFA over different types of monoids and groups, so far they still could not resolve their conjecture.

In [Sm 87], in order to show Mod_q is not AC^0 reducible to Mod_p, Smolensky introduced the concept of U_F^n-completeness, which enabled him to achieve his goal. However, this concept became a major obstacle when trying to apply his method to show some other functions are hard to compute by a small depth Boolean circuit with Mod_p. U_F^n-completeness is too restrictive a condition for many other functions. In section 2, we replace his concept of U_F^n-completeness by a new definition: F-hardness. This comes from a simple but keen observation: We say a function is $\mathcal{F}_p$-hard, if to force it to have low degree in some quotient algebra over $\mathcal{F}_p$, we always have to ignore a large fraction of inputs, thus the dimension of the quotient algebra is very small; on the other hand, we know small depth Boolean circuits with Mod_p yield polynomials which have low degrees over some quotient algebra of not too small dimension. Hence, the main theorem of Smolensky becomes an easy consequence of this definition of F-hardness – F-hard functions cannot be approximated well by small depth Boolean circuit with Mod_p gates. What left now is to show some classes of functions are F-hard. We establish a Hardness Lemma for a class of functions which we call *semi-threshold* functions, where $Majority$ and all $Threshold$ functions are important examples among them. The idea and the proof technique can be applied to other functions, too. It's not too hard to foresee that essentially all dense, high degree polynomials over a fixed finite field do not have small depth Boolean circuits with Mod_p where p is the characteristic of the field, this gives a sort of supplement to the result of Linial, et al [LMN 89].

In section 3, we discuss the difficulties in extending Smolensky's theory to a general ring. The problem lies in the insurmountable gap between the Boolean circuit model and any model we choose to represent Boolean functions by polynomials over a ring. The nice relationship between the small depth Boolean circuits with module gates and the algebra of functions representing Boolean functions which enables us to establish the theory over a field simply collapses over a general ring. However, we can still extend the complexity theoretic notations induced by this extended Smolensky's theory to a ring in order to classify functions over such a ring by their relative hardness. We prove that any representation of $Majority$ is hard over any such rings, this gives an evidence that $Majority$ cannot be aprroximated well by Mod_r. Then, a remaining open problem is how

well this classification reflects the complexity of the Boolean functions. We conjecture that any R-hard function over $R = Z/(r)$ cannot be approximated well by a small depth Boolean circuit with Mod_r gates, hence it is not AC^0 reducible to Mod_r.

2 Smolensky's Method and F-hardness

F-algebra $U^n_{F_p}$ and its quotient algebra

Recall some basic notations and definitions in [Sm 87].

Let $\mathcal{F}_p$ be a finite field of characteristic p, $\mathbf{B}$= {0,1}.

The $\mathcal{F}_p$-algebra $U^n_{F_p}$ is defined as the set of functions $f(\underline{x}) : \mathbf{B}^n \to \mathcal{F}_p$, or the set of polynomials over $\mathcal{F}_p$ with the degree in each variable being linear. Formally,

$$U^n_{F_p} = \frac{\mathcal{F}_p[\underline{x}]}{J}$$

where

$$J = (x_1^2 - x_1, ..., x_n^2 - x_n)$$

The superscript n in $U^n_{F_p}$ denotes the input size, throughout the paper, we assume n is very large.

$U^n_{F_p}$ is both an $\mathcal{F}_p$-algebra and a vector space over $\mathcal{F}_p$. Each function $f(\underline{x}) \in U^n_{F_p}$ are uniquely determinated by its set of nonvanishing points, as

Fact $\mathcal{B}_1 = \{\Pi_{i\in S} x_i \Pi_{i\in \bar{S}}(1 - x_i) |\ S \subseteq \{1, ..., n\}\}$ and $\mathcal{B}_2 = \{\Pi_{i\in S} x_i |\ S \subseteq \{1, ..., n\}\}$ are two bases for $U^n_{F_p}$. Moreover, $dim\, U^n_{F_p} = 2^n$.

Let $\underline{a} \in \mathbf{B}^n = \{0,1\}^n$, define $\underline{x}(\underline{a}) = \Pi_{a_i=1} x_i \Pi_{a_i=0}(1 - x_i)$, then $\mathcal{B}_1 = \{\underline{x}(\underline{a}) |\ \underline{a} \in \mathbf{B}^n\}$. Each function can be uniquely expressed in $\mathcal{B}_1$ (the interpolation) or in $\mathcal{B}_2$ (the usual polynomial representation).

Let $E \subseteq \mathbf{B}^n, V = \mathbf{B}^n \setminus E$, define $I = I(V) = \{ f(\underline{x}) \in U^n_{F_p} |\ f(\underline{x})$ is zero on $V\}$, an ideal of $U^n_{F_p}$. Obviously, $I = span\{\underline{x}(\underline{a}) |\ \underline{a} \in E\}$ as a linear subspace, $dim\, I = |E|$. And all ideals of $U^n_{F_p}$ are generated in this way.

The quotient algebra of $U^n_{F_p}$ is defined as $A^n_{F_p} = \frac{U^n_{F_p}}{I}$, obviously $dim\, A^n_{F_p}$ $= 2^n - dim\, I = 2^n - |E|$. We use $\Omega^n_{F_p}$ to denote the set of all quotient algebras of $U^n_{F_p}$. For any $\tilde{f} \in A^n_{F_p}, deg_A(\tilde{f}) = min\{deg(f)$ such that $f - \tilde{f} \in I\}$.

Complexity Theory on $U^n_{F_p}$

We follow the definitions of Smolensky.

First observe that a Boolean circuit with Mod_p induces naturally a polynomial over $\mathcal{F}_p$ as

$$Not(x) \to 1 - x, \quad \bigwedge_{i=1}^{n} x_i \to \prod_{i=1}^{n} x_i,$$

$$\bigvee_{i=1}^{n} x_i \to 1 + \prod_{i=1}^{n} (1 - x_i),$$

$$Mod_p(\underline{x}) \to (\sum_{i=1}^{n} x_i)^{p-1}$$

Clearly, when restricted to $\mathbf{B}^n$, the induced functions always have zero-one outputs.

Over $\mathcal{F}_p$, we will represent a Boolean function $g(\underline{x})$ by a function $f(\underline{x}) \in U_{F_p}^n$ such that $f(\underline{x})|_{\mathbf{B}^n} = g(\underline{x})$, where $f(\underline{x})|_{\mathbf{B}^n} : \mathbf{B}^n \to \mathbf{B}$. This representation is unique. Therefore, we can identify a Boolean function with its representation over $\mathcal{F}_p$.

We point out here that over a general ring, the above remark is not true (Refer to section 3).

Definition 1 *A function $f(x_1, ..., x_m) \in U_{F_p}^n$ is $\mathcal{F}_p$-easy if $f(\underline{x})$ can be represented as a polynomial of constant degree over $\mathcal{F}_p$.*

Examples of F-easy functions are Not over any finite field and Mod_p over any fixed finite field of characteristic p.

Definition 2 *A function $f \in U_{F_p}^n$ is nearly $\mathcal{F}_p$-easy if for any l, there exists a quotient algebra $A_{F_p}^n \in \Omega_{F_p}^n$ of dimension at least $2^n - 2^{n-l}$ such that $deg_A(f) \leq \lambda l$.*

Lemma 1 *Or and And are F-easy over any fixed finite field F.*

Now we introduce the concept of $\mathcal{F}_p$-hardness.

Definition 3 *A function $f \in U_{F_p}^n$ is $\mathcal{F}_p$-hard if for any $A_{F_p}^n \in \Omega_{F_p}^n$ such that $deg_A(f) = o(\sqrt{n})$, then $\dim A_{F_p}^n \ll 2^n - 2^{n - c \log n}$, for some constant c. Equally, suppose $A_{F_p}^n = \frac{U_{F_p}^n}{I}$, where $I = \{\underline{x}(\underline{a}) | \underline{a} \in E\}$, then $\dim I = |E| \gg 2^{n - c \log n}$, for any constant c.*

An easy consequence of this definition is that all $\mathcal{F}_p$-hard functions do not have good approximation by a small depth Boolean circuit with Mod_p. This can be seen as follows.

First we record a Lemma in [Sm 87] with a slight modification.

Lemma 2 *Let C^n be a depth k circuit with any number of $\mathcal{F}_p$-easy gates, 2^r nearly $\mathcal{F}_p$-easy gates where $r = o(n^{\frac{1}{2k}})$, then there exists a quotient algebra $A^n_{F_p} \in \Omega^n_{F_p}$ with $dim\, A^n_{F_p} > 2^n - 2^{n-c\log n}$ for any constant c such that the degrees of all outputs in $A^n_{F_p}$ are of order $o(\sqrt{n})$.*

Proof Just take, say, $l = r + \log^2 n$ in Smolensky's original proof instead of $l = 2r$.

Main Theorem

Let C^n be of depth k and use $exp(o(n^{\frac{1}{2k}}))$ nearly $\mathcal{F}_p$-easy gates and an arbitrary number of $\mathcal{F}_p$-easy gates. Then the output g of C^n will differ from any $\mathcal{F}_p$-hard function on at least $2^{n-c\log n} - o(2^{n-c\log n})$ assignments, where c is a constant. Therefore, $\mathcal{F}_p$-hard functions cannot be approximated well by a small depth circuits with $\mathcal{F}_p$-easy and nearly $\mathcal{F}_p$-easy gates.

Proof By Lemma 2, there exists a quotient algebra $A^n_{F_p} = \frac{U^n_{F_p}}{I}$ such that $deg_A(g) = o(\sqrt{n}), dim\, A^n_{F_p} > 2^n - 2^{n-c\log n}$ for any constant c.

Ignore all assignments $\underline{a}$ such that $f(\underline{a}) \neq g(\underline{a})$, we go into a smaller algebra $\tilde{A^n_{F_p}}$ where $g(\underline{x}) = f(\underline{x})$, so $deg_{\tilde{A^n_{F_p}}}(f) = o(\sqrt{n})$. As f is $\mathcal{F}_p$-hard, $dim\, \tilde{A^n_{F_p}} \ll 2^n - 2^{n-c\log n}$ for some constant c, so at least $2^{n-c\log n} - o(2^{n-c\log n})$ inputs have been ignored. □

$\mathcal{F}_p$-hard Functions

We will establish a general technique to show some classes of functions are $\mathcal{F}_p$-hard. For clarity, we first fix some terminology, then demonstrate the technique by proving a *Hardness Lemma* for a class of (symmetric) Boolean functions, which we call *semi-threshold function* $ST_t(\underline{x})$:

$f(\underline{x}) \in ST_t(\underline{x})$ if for $\underline{x} \in \mathbf{B}^n = \{0,1\}^n$

$$\begin{array}{lll} f(\underline{x}) = 0 & \text{if} & |\underline{x}| < t \\ f(\underline{x}) = 1 & \text{if} & |\underline{x}| = t \\ f(\underline{x}) = 0 \text{ or } 1 & \text{if} & |\underline{x}| => t \end{array}$$

where $|x| = \sum_{i=1}^n x_i$.

$Exact_t(\underline{x})$, $Threshold_t(\underline{x})$, $Majority$ $(t = \frac{n}{2})$, $Mod_t(\underline{x})$ and $Mod_{p^s}(\underline{x})$ $(t = p^s)$ are examples of semi-threshold functions.

Furthermore, we say a function $f(\underline{x}) \in U_{F_p}^n$ is an *Extended semi − threshold$_t$* function, denoted as $f(\underline{x}) \in EST_t(\underline{x})$ if

$$\begin{array}{lll} \text{for } \underline{x} \in \mathbf{B}^n & f(\underline{x}) = 0 & \text{if } |\underline{x}| < t \\ & f(\underline{x}) \neq 0 & \text{if } |\underline{x}| = t \\ & f(\underline{x}) = \text{ arbitrary value in } \mathcal{F}_p & \text{if } |\underline{x}| > t \end{array}$$

Clearly, the representation of any *semi-threshold* Boolean function over $\mathcal{F}_p$ is an *Extended semi-threshold function.*

We say t is *suitably large* if $t \gg \sqrt{n}$ (and $n - t \gg \sqrt{n}$) and $\binom{n}{t} \gg 2^{n - c\log n} = \frac{2^n}{n^c}$ for some constant c.

As $t \gg \sqrt{n}$, and n is very large, in general, we will assume $t - \sqrt{n}$ is still *suitably large.* For example, for a constant k, $t = \frac{n}{2} \pm k$ is suitably large, whereas $t = n - k$ is not, it is too large!

We say a function $f(\underline{x}) \in U_{F_p}^n$ is of low degree if $deg(f)$ is at most $\sqrt{n}$. Otherwise, we say it is of high degree.

Suppose f is a (symmetric) function of high degree in $U_{F_p}^n$, f induces a sequence of functions f_0, f_1, ..., f_l, where $f_j \in U_{F_p}^{n-j}$. The induced functions are defined recursively as follows:

$$f_0 = f$$

$$\text{for } 1 \leq j \leq l, \ f_{j-1} = x_i f_j + f_j' \quad \text{for some } i$$

where f_j, f_j' contains no x_i.

f_j is obtained from f_{j-1} by grouping terms containing x_i together, then extracting x_i out; f_j' is obtained from f_{j-1} by grouping terms without x_i together. If f is symmetric, then f_{j-1} is symmetric, the choice of i is immaterial. However, in general, by choosing different i at each stage, we will obtain different sequences of functions with different possible length l. For our purpose, we will assume we always choose some sequence of largest possible length l. As f is of high degree, $l \geq \sqrt{n}$. Without loss of generality, we assume $i = n - (j-1)$ at stage j. Note $f_{j-1} \in U_{F_p}^{n-(j-1)}$, a function of $n - (j-1)$ variables, all of linear degree, as f_j contains one less variable than f_{j-1}, hence $f_j \in U_{F_p}^{n-j}$.

Example Let $f(\underline{x}) \in U_{F_p}^n$ be a representation of a semi-threshold function in $ST_t(\underline{x})$, or $f(\underline{x}) \in EST_t(\underline{x})$, where t is suitably large. By considering interpolation at its nonvanishing points, it is easy to see f has only monomials of degree greater than or equal to t. Hence, $f(\underline{x})$ is of high degree,

f induces a sequence of functions f_0, f_1, ..., f_l. The induced functions are all Extended semi-threshold functions, as we

Claim For $0 \leq j \leq l$, $f_j(\underline{x})$ has the property that

$$\text{for } \underline{x} \in \{0,1\}^{n-j} \quad f_j(\underline{x}) = 0 \quad \text{if } |\underline{x}| < t - j$$

$$f_j(\underline{x}) \neq 0 \quad \text{if } |\underline{x}| = t - j$$

Proof by induction:

If $j = 0$, $f_0 = f$, the claim is trivial.

Assume the claime is true for f_{j-1}. We prove it is also true for f_j.

Note that $f_{j-1}(x_1, ..., x_{n-(j-1)}) = x_{n-(j-1)} f_j(x_1, ..., x_{n-j}) + f'_j(x_1, ..., x_{n-j})$.

Consider $\underline{a}' = \{a_1, ..., a_{n-j}\} \in \{0,1\}^{n-j}$, by induction hypothesis,

for $|\underline{a}'| \leq t - j$, we have

$f_{j-1}(\underline{a}', 0) = f'_j(\underline{a}') = 0$ and $f_{j-1}(\underline{a}', 1) = f_j(\underline{a}') + f'_j(\underline{a}') = f_j(\underline{a}')$.

Therefore,

for $|\underline{a}'| < t - j$, $f_{j-1}(\underline{a}', 1) = 0$, hence $f_j(\underline{a}') = 0$.

for $|\underline{a}'| = t - j$, $f_{j-1}(\underline{a}', 1) \neq 0$, hence $f_j(\underline{a}') \neq 0$. □

Remark

1. Suppose $f(\underline{x})$ is a semi-threshold function, then when $|\underline{a}| = t - j$, $f_j(\underline{a}) = k \neq 0$, $k^{-1} f_j(\underline{a}) = 1$. Without loss of generality, we can assume $f_j(\underline{a}) = 1$ when $|\underline{a}| = t - j$. Hence f_j can be regarded as a representation of some semi-threshold function $f' \in ST_{t-j}(x_1, ..., x_{n-j})$. Note as t is suitably large, if we cut the sequence at $j < \sqrt{n}$, then $t' = t - j$ is still suitably large.

2. If f is the representaion of a specific semi-threshold Boolean function, say, $Exact_t(\underline{x})$, then f_1, ..., f_l are not necessarily representations of the same function, say, $Exact_{t'}(\underline{x})$ for some t', but they are still representations of some semi-threshold functions.

Some more notations.

Denote $S_t = \{\underline{a} \in \mathbf{B}^n | |\underline{a}| = t\}$, $S_{t-1} = \{\underline{a} \in \mathbf{B}^n | |\underline{a}| = t - 1\}$, $S'_{t-1} = \{\underline{a}' \in \mathbf{B}^{n-1} | |\underline{a}'| = t - 1\}$. $\underline{x} = \{x_1, ..., x_n\}$, $\underline{x}' = \{x_1, ..., x_{n-1}\}$.

Suppose P is a predicate on $\underline{x} \in S \subseteq \mathbf{B}^n = \{0,1\}^n$. We say for *many* $\underline{x} \in S$ $P(\underline{x})$ holds if $|\{\underline{a} \in S \subseteq \mathbf{B}^n | P(\underline{a}) \text{ is } \mathbf{true}\}| \gg \frac{2^n}{n^c}$ for some constant c. We state the converse as for *almost all* $\underline{x} \in S$, $P(\underline{x})$ does not hold, *i.e.* $|\{\underline{a} \in S \subseteq \mathbf{B}^n | P(\underline{a}) \text{ is } \mathbf{false}\}| < \frac{2^n}{n^c}$ for any constant c.

Define $N_g = \{\underline{a} \in \mathbf{B}^n | g(\underline{a}) \neq 0\}$, the set of points where $g(\underline{x})$ do not vanish.

We are now ready to prove the Hardness Lemma for semi-threshold functions $ST_t(\underline{x})$ and Extended semi-threshold functions $EST_t(\underline{x})$, where t is suitably large.

Hardness Lemma For $ST_t(\underline{x})$ And $EST_t(\underline{x})$

Let $f(\underline{x}) \in U^n_{F_p}$ be a representation of a semi-threshold function in $ST_t(\underline{x})$ or $f(\underline{x}) \in EST_t(\underline{x})$ where t is suitably large. For any $A^n_{F_p} \in \Omega^n_{F_p}$, if $deg_A(f) = o(\sqrt{n})$, then $dim\, A^n_{F_p} \ll 2^n - 2^{n-c\log n}$ for some constant c. In other words, let $A^n_{F_p} = \frac{U^n_{F_p}}{I}$, $I = span\{\underline{x}(\underline{a}) | \underline{a} \in E \subseteq \mathbf{B}^n\}$, if there exists a $g(\underline{x}) \in I$ such that $h(\underline{x}) = f(\underline{x}) + g(\underline{x})$ has $deg(h) < \sqrt{n}$, then $dim\, I = |E| \gg 2^{n-c\log n}$ for some constant c.

Remark Since I is the ideal of functions which are zero outside E, and $g \in I$, g is zero outside E. Therefore if $g(\underline{a}) \neq 0$ then $\underline{a} \in E$. We have $dim\, I = |E| \geq |N_g|$. It suffices to show $|N_g| \gg 2^{n-c\log n} = \frac{2^n}{n^c}$ for some constant c (where c depends on the parameter t and the quantity of *'many-ness'* below).

Proof It suffices to prove the lemma for $EST_t(\underline{x})$, where t is suitably large. We prove, by induction on the degree of h, the following assertion:

> Let $f(\underline{x})$ be a function in $EST_t(\underline{x})$, where t is suitably large. If there exists a function $g(\underline{x}) \in U^n_{F_p}$ such that $h(\underline{x}) = f(\underline{x}) + g(\underline{x})$ has degree less than $\sqrt{n}$, then $|N_g| \gg \frac{2^n}{n^c}$ for some constant c.

Induction Basis

$deg(h) = 0$. Assume $h(\underline{x}) = k \in \mathcal{F}_p$. $k = f(\underline{x}) + g(\underline{x})$.

As t is suitably large, and the field is fixed and finite, there exists a $k_0 \in \mathcal{F}_p$, $k_0 \neq 0$ such that for *many* $\underline{a} \in S_t$, $f(\underline{a}) = k_0$.

1) If $k \neq k_0$, then for *many* $\underline{a} \in S_t$, $f(\underline{a}) = k_0$, $g(\underline{a}) = k - k_0 \neq 0$

Hence $|N_g| \geq |\{$ *many* $\underline{x} \in S_t\}| \gg \frac{2^n}{n^c}$ for some constant c, as t is suitably large and by the definition of '*many-ness*'.

2) If $k = k_0$, then for any $\underline{a} \in S_{t-1}$, $f(\underline{a}) = 0$, $g(\underline{a}) = k_0 \neq 0$

Hence $|N_g| \geq |S_{t-1}| = \binom{n}{t-1} \gg \frac{2^n}{n^c}$ for some constant c , as t is suitably large.

Induction Hypothesis

Suppose that for any $h(\underline{x}) \in U^n_{F_p}$ with $deg(h) < d < \sqrt{n}$, if $h(\underline{x}) = f(\underline{x}) + g(\underline{x})$ for some $g(\underline{x}) \in U^n_{F_p}$, then $|N_g| \gg \frac{2^n}{n^c}$ for some constant c.

Now consider any $h(\underline{x})$ with $deg(h) = d < \sqrt{n}$. Suppose there exists a $g(\underline{x}) \in U^n_{F_p}$ such that $h(\underline{x}) = f(\underline{x}) + g(\underline{x})$.

Write $h = x_n h_1 + h_2$, $f = x_n f_1 + f_2$ and $g = x_n g_1 + g_2$
where h_i, f_i, g_i, $i = 1, 2$, contain no x_n, that is, they are the induced functions on $\underline{x}' = \{x_1, ..., x_{n-1}\}$.
For any $\underline{x}' \in \mathbf{B}^{n-1}$, we have

$$h(\underline{x}', 0) = h_2(\underline{x}') = f_2(\underline{x}') + g_2(\underline{x}')$$

$$h(\underline{x}', 1) = h_1(\underline{x}') + h_2(\underline{x}') = f_1(\underline{x}') + f_2(\underline{x}') + g_1(\underline{x}') + g_2(\underline{x}')$$

Hence, $h_1(\underline{x}') = f_1(\underline{x}') + g_1(\underline{x}')$, where $deg(h_1) = d - 1$.
We know $f_1(\underline{x}')$ is an Extended semi-threshold function in $EST_{t-1}(\underline{x}')$, where $t - 1$ is still suitably large. (Note: as $d < \sqrt{n}$, the induction goes at most $d < \sqrt{n}$ steps. All f's in question are some Extended semi-threshold functions of suitably large t.)
By induction hypothesis, $|N_{g_1}| \gg \frac{2^{n-1}}{(n-1)^c}$ for some constant c
$\sim \frac{2^n}{n^c}$ as n is large.
Consider $\underline{x}' \in \mathbf{B}^{n-1}$, we have

$$g(\underline{x}', 1) = g_1(\underline{x}') + g_2(\underline{x}'), \quad g(\underline{x}', 0) = g_2(\underline{x}')$$

1) If for *many* $\underline{x}' \in \mathbf{B}^{n-1}$, $g_2(\underline{x}') \neq 0$, then $g(\underline{x}', 0) \neq 0$ for *many* $(\underline{x}', 0) \in \mathbf{B}^n$. Hence

$|N_g| \geq |\{(x', 0)| \, g(\underline{x}', 0) \neq 0, \underline{x}' \in \mathbf{B}^{n-1}\}|$
$\gg \frac{2^{n-1}}{(n-1)^c}$ for some constant c
$\sim \frac{2^n}{n^c}$ by the definition of "*many-ness*".

2) Otherwise, for *almost all* $\underline{x}' \in \mathbf{B}^{n-1}$, $g_2(\underline{x}') = 0$, that is, for any constant c, $|N_{g_2}| < \frac{2^n}{n^c}$.
But, remember $|N_{g_1}| \gg \frac{2^n}{n^c}$ for some constant c. Since $g(\underline{x}', 1) = g_1(\underline{x}') + g_2(\underline{x}')$, we have

$|N_g| \geq |N_{g_1}| - |N_{g_2}| \gg \frac{2^n}{n^c}$ for some constant c. □

Theorem 3 *For t suitably large, any Extended semi-threshold function in $EST_t(\underline{x})$ is $\mathcal{F}_p$-hard. Especially, any semi-threshold function in $ST_t(\underline{x})$ is $\mathcal{F}_p$-hard, therefore they do not have small depth Boolean circuits with Mod_p.*

Corollary 4 *For t suitably large, $Exact_t(\underline{x})$, $Threshold_t(\underline{x})$ are $\mathcal{F}_p$- hard. In particular, Majority is $\mathcal{F}_p$-hard. Therefore, they are not AC^0 reducible to Mod_p.*

Corollary 5 *For r suitably large (hence r must be a function of n), Mod_r is $\mathcal{F}_p$-hard. In paticular, if $r = p^m$ is suitably large, Mod_{p^m} is $\mathcal{F}_p$- hard. Therefore, they are not AC^0 reducible to Mod_p.*

Remark This corollary cannot be proved by Smolensky's original method, which is only applicable to a fixed prime.

Now we discuss for what kind of functions we can establish a Hardness Lemma.

Let $f(\underline{x}) \in U^n_{F_p}$, we say it satisfies the *Hardness* condition if its induced sequence of functions $f_0 = f$, f_1,..., f_l has length $l > \sqrt{n}$ and for each j, $0 \leq j \leq \sqrt{n} \leq l$, $f_j(\underline{x})$ has the following property:

(*) there exist *suitably large* t_j and t'_j, $t_j \neq t'_j$ such that
for *many* $\underline{x} \in S_{t_j}$ $f_j(\underline{x}) = 0$
and for *many* $\underline{x} \in S_{t'_j}$ $f_j(\underline{x}) \neq 0$

We see that the proof of Hardness Lemma for $EST_t(\underline{x})$ functions holds for functions satisfying *Hardness* condition with almost no modifications. Hence, the corresponding Boolean functions they represent are hard to compute by small depth Boolean circuits with Mod_p. We suspect that almost, all high degree, dense polynomials over $\mathcal{F}_p$ satisfy the *Hardness* condition, thus are hard to compute.

As for a low degree polynomial, its induced sequence of functions has length at most $d < \sqrt{n}$, where d is its degree. In other words, the sequence stops at d with $f_d(\underline{x})$ is identically a constant in $\mathcal{F}_p$. Obviously, low degree polynomials do not satisfy the *Hardness* condition. Similarly, the Hardness Lemma does not hold for those high degree polynomials whose all possible induced sequences of functions have length $l < \sqrt{n}$, or at some stage $j < \sqrt{n}$, the induced function does not satisfy the condition (*). $f(\underline{x}) = \Pi^n_{i=1}(1 - x_i)$ and $f(\underline{x}) = x_1 + x_1x_2 + \cdots + x_1x_2 \cdots x_n$ are such examples.

Lastly, we remark that Smolensky's result that for any fixed prime $q \neq p$, Mod_q is not AC^0 reducible to Mod_pcan also be proved by this general technique.

Let $f(\underline{x})$ be the representation of Mod_q over $\mathcal{F}_p$. It is well known that $f(\underline{x})$ has degree $O(n)$ (*e.g.* by *Chevalley-Warning's Theorem*, see, for example, Chapter 10 in [IR 84] or Chapter 6 in [LN 83]). So its induced sequence of functions has length $O(n)$. Now consider those induced func-

tions $f_j(\underline{x})$ with $0 \leq j \leq \sqrt{n}$. One can check that they satisfy $(*)$ *i.e.* $f(\underline{x})$ satisfies the *Hardness* condition. Therefore, we have

Theorem 6 *Mod_q is $\mathcal{F}_p$-hard over $\mathcal{F}_p$. In other words, Mod_q is not AC^0 reducible to Mod_p.*

3 Dilemma Over A Ring

It was natural to try to extend Smolensky's theory to a general ring. However, it turned out to be a failure. There is an insurmountable gap between the model of constant depth, polynomial circuits with module a fixed composite number gates and any model of representing Boolean functions by polynomials over the corresponding ring by some specific criteria: under any such representing model, either the nice relationship (as in the case of a field) between the complexity of the circuits and the *hardness* of the induced polynomials by the circuits collapses, or the circuits do not always induce a polynomial satisfying the criteria set for our model. Let's elaborate more on this.

As in the case of a field, we would naturally represent a Boolean function by a polynomial over a ring such that when restricted to $\{0,1\}^n$, the polynomial only takes 0 or 1. As we are only interested in zero-one inputs, we assume the degree in each variable is reduced to linear. It is not hard to see that such a polynomial is uniquely determined by its zero set (one set), *i.e.* the set of inputs where the polynomial takes value 0 (1).

Now consider the circuits with Mod_6. The corresponding ring is $R = \mathbf{Z}/(6) = \mathcal{F}_2 \times \mathcal{F}_3$. Let $f(\underline{x})$ be the representation of Mod_6 over such that when restricted to $\mathbf{B}^n$, it takes value 1 if $|\underline{x}| \bmod 6 = 0$, otherwise it takes value 0. Since $f(\underline{x})$ is determined by its nonvanishing points, hence $f(\underline{x})$ has the form

$$f(\underline{x}) = \sum_{\substack{\underline{a} \in \mathbf{B}^n \\ |\underline{a}| \equiv 0 \bmod 6}} \underline{x}(\underline{a})$$

Let $f_1(\underline{x})$ and $f_2(\underline{x})$ be its components in $U^n_{F_2}$ and $U^n_{F_3}$ respectively, then $f_1(\underline{x})$ ($f_2(\underline{x})$) is a representation of Mod_6 over $\mathcal{F}_2$ ($\mathcal{F}_3$) which is $\mathcal{F}_2$-hard ($\mathcal{F}_3$-hard), by Smolensky's theory over fields. It can be argued that if a

Notice that at some stage the induced function may not have a zero output, however, it always have at least two distinct output values, thus by adding a constant, we can adjust it into our model.

function is hard over one of the component field, then it is *hard* over R (*e.g.* by a direct translation of the definition of hardness from a field into a ring). Therefore, this model provides us only a *distorted* image of the Boolean circuit model.

Then, what about considering the model of representing Boolean functions as follows:

We say a function $f(\underline{x})$ over R is a representation of a Boolean function $g(\underline{x})$ if

$$\text{for } \forall \underline{x} \in \mathbf{B}^n \quad \begin{array}{ll} g(\underline{x}) = 0 & \text{then} \quad f(\underline{x}) = 0 \\ g(\underline{x}) = 1 & \text{then} \quad f(\underline{x}) \neq 0 \end{array}$$

Note that we assume that the degree of each variable in $f(\underline{x})$ is linear.

More generally, we can represent a Boolean function $g(\underline{x})$ in the follwing manner:

Let $\emptyset \neq S \subset \mathbf{B}^n$, we say $f(\underline{x})$ is a representation of $g(\underline{x})$ if

for any $\underline{x} \in \mathbf{B}^n$ $g(\underline{x}) = 0$ *iff* $f(\underline{x}) \in S$

The latter model is in general a stronger model, and contains the former as a subcase. For our purpose, it suffices to investigate the former model.

Without loss of generality, we assume $r = p_1 p_2 \cdots p_s$ with all p_i's distinct. Hence $R = Z/(r)$ is the direct product of $\mathcal{F}_{p_1}, \mathcal{F}_{p_2}, \ldots, \mathcal{F}_{p_s}$. Clearly, under the former model we defined, Mod_r can be represented by a polynomial $f(\underline{x}) = \sum_{i=1}^{n} x_i$ which is of linear degree. Note that $f(\underline{x})$ can take any value in R. Due to this fact, when making the naive bottle-up transformation from a circuit into a polynomial, we will soon find that we will get stuck somewhere producing polynomials which are no longer consistent with our representing model, for example, we cannot simply replace the *AND* of m Boolean functions by the multiplication of their corresponing representations, as the final representation can take value 0 where none of its multiplicand take value 0. Similarly for Mod_r. For *NOT* gate, we simply cannot find a representation which is consistent with our model, hence is the case for *OR*. This model turns out to be disaster to us: although we know any such circuit defines a Boolean function, hence inducing a class of functions over R which are representations of the Boolean function under our model, it merciless defies our attempt to inductively construct such a representation directly from the circuit.

Although we lose track of what the function computed by a Boolean circuit looks like under this model of representing Boolean functions, we

believe there is still some relationship between the Boolean function computed by a Boolean circuit with Mod_r gates and its representations over the corresponding ring $R = Z/(r)$ under this model, hence by investigating the relative hardness of these functions, we can gain some information or evidence about the relative complexity of the Boolean functions they represent. This is the main theme of the next section.

4 Classifications Of Functions Over A Ring

For our purpose, it suffices to consider rings which are direct product of fields. Hence, we assume

$$R = F_1 \times F_2 \times \cdots F_s$$

where F_i is a finite field, $1 \leq i \leq s$.

Analogous to the case of fields, we define R-algebra and quotient algebras as follows.

Let $J = J_1 = \cdots = J_s = (x_1^2 - x_1, \ldots, x_n^2 - x_n)$ over $R, F_1, \ldots, F_s$ respectively.

Define

$$U_R^n = \frac{R[\underline{x}]}{J} \simeq \frac{F_1}{J_1} \times \cdots \times \frac{F_s}{J_s} \simeq U_{F_1}^n \times \cdots \times U_{F_s}^n$$

the algebra of functions defined from $\mathbf{B}^n$ to R.

Let $I \simeq I_1 \times \cdots \times I_s$ where I is an ideal of U_R^n, and I_i is an ideal of $U_{F_i}^n$, $1 \leq i \leq s$.

Consider $f(\underline{x}) \in I$, $f(\underline{x}) \longleftrightarrow (f_1(\underline{x}), \ldots, f_s(\underline{x}))$, $f_i \in I_i$, $1 \leq i \leq s$. Clearly, for $\underline{a} \in \mathbf{B}^n$, $f(\underline{a}) = 0$ iff $\forall i$, $f_i(\underline{a}_i) = 0$, and $f(\underline{a}) \neq 0$ iff $\exists i$, $f_i(\underline{a}_i) = 0$, where $\underline{a} \leftrightarrow (\underline{a}_1, \ldots, \underline{a}_s)$, $\underline{a}_i \in \mathbf{B}^n$. Since $0 \leftrightarrow (0, \ldots, 0)$ and $1 \leftrightarrow (1, \ldots, 1)$, $\underline{a} = \underline{a}_i$, $1 \leq i \leq s$.

Let E_i be the set of points in $\mathbf{B}^n$ where not all functions in I_i vanish, *i.e.* $I_i = span\{\underline{x}(\underline{a}) | \underline{a} \in E_i\}$.

Define $E = \cup_{i=1}^s E_i$. It is easy to check that for $\underline{a} \in \mathbf{B}^n \backslash E$, $f(\underline{a}) = 0$ for all $f(\underline{x}) \in I$ and for $\underline{a} \in E$, $f(\underline{a}) \neq 0$ for some $f(\underline{x}) \in I$.

Hence I is the ideal of functions which are zero outside E. In other words, I is generated by $\{\underline{x}(\underline{a}) | \underline{a} \in E\}$ as in the case of a finite field. Since each f_i is uniquely determined by its nonvanishing points, so is f.

We measure the size of I by the cardinality of E, which we still call the *dimension* of I by abuse of terminology (*Rank* might be a better name). Hence, we have

$$dim\, I = |E| \geq max_i\, |E_i| = max_i\, dim\, I_i$$

In particular, $dim\, U_R^n = 2^n$.

The quotient algebra, as usual, has the form

$$A_R^n = \frac{U_R^n}{I} \simeq \frac{U_{F_1}^n}{I_1} \times \cdots \times \frac{U_{F_s}^n}{I_s} = A_{F_1}^n \times \cdots \times A_{F_s}^n$$

Clearly,

$dim\, A_R^n = dim\, U_R^n - dim\, I \leq dim\, U_R^n - min_i\, dim\, I_i$, as $dim\, I \geq dim\, I_i$, $1 \leq i \leq s$.

Finally, Ω_R^n denotes the set of all quotient algebras of U_R^n.

Due to the model we chose for the representation of Boolean functions, we introduce a new concept:

Definition 4 *Let $f(\underline{x})$ and $\tilde{f}(\underline{x})$ are functions in U_R^n, we say $f(\underline{x})$ and $\tilde{f}(\underline{x})$ are compatible over A_R^n, where $A_R^n = \frac{U_R^n}{I}$, $I = span\{\underline{x}(\underline{a}) | \underline{a} \in E \subseteq \mathbf{B}^n\}$ if $\{\underline{a} \mid f(\underline{a}) = 0$ but $\tilde{f}(\underline{a}) \neq 0$, or $f(\underline{a}) \neq 0$ but $\tilde{f}(\underline{a}) = 0\} \subseteq E$. In other words, $f(\underline{x}) = 0$ iff $\tilde{f}(\underline{x}) = 0$ over A_R^n.*

We denote it as $f(\underline{x}) \sim_A \tilde{f}(\underline{x})$

In particular, if $\tilde{f}(\underline{x}) \sim_{U_R^n} f(\underline{x})$ then $\tilde{f}(\underline{x}) = 0$ iff $f(\underline{x}) = 0$.

Lemma 7 *If $f(\underline{x}) \sim_A \tilde{f}(\underline{x})$, where $A_R^n = \frac{U_R^n}{I}$, then there exist an $f'(\underline{x}) \in U_R^n$ and a $g(\underline{x}) \in I$ such that $\tilde{f}(\underline{x}) = f'(\underline{x}) + g(\underline{x})$ and $f'(\underline{x}) \sim_{U_R^n} f(\underline{x})$.*

Proof Suppose $I = span\{\underline{x}(\underline{a}) | \underline{a} \in E \subseteq \mathbf{B}^n\}$, define $f'(\underline{x})$ and $g(\underline{x})$ as follows:

for all $\underline{x} \notin E$ define $f'(\underline{x}) = \tilde{f}(\underline{x})$ and $g(\underline{x}) = 0$
and for all $\underline{x} \in E$
if $f(\underline{x}) \neq 0$ and $\tilde{f}(\underline{x}) \neq 0$, then define $f'(\underline{x}) = \tilde{f}(\underline{x})$ and $g(\underline{x}) = 0$
if $f(\underline{x}) = 0$ but $\tilde{f}(\underline{x}) \neq 0$, then define $f'(\underline{x}) = 0$ and $g(\underline{x}) = \tilde{f}(\underline{x})$
if $f(\underline{x}) \neq 0$ but $\tilde{f}(\underline{x}) = 0$, then define $f'(\underline{x}) = f(\underline{x})$ and $g(\underline{x}) = -f(\underline{x})$
It is easy to see that $f'(x)$ and $g(\underline{x})$ are required functions. □

Now we define R-easiness, nearly R-easiness and R-hardness over R.

Definition 5 *R-easiness, nearly R-easiness and R-hardness*
1. A function $f(\underline{x}) \in U_R^n$ is R-easy if it has constant degree.
2. A function $f(\underline{x}) \in U_R^n$ is nearly R-easy if there exists a quotient algebra $A_R^n \in \Omega_R^n$ and a function $\tilde{f}(\underline{x}) \in U_R^n$ such that dim $A_R^n > 2^n - 2^{n-c\log n}$ for any constant c, deg($\tilde{f}(\underline{x})$) $= o(\sqrt{n})$ and $f(\underline{x}) \sim_A \tilde{f}(\underline{x})$.
3. A function $f(\underline{x}) \in U_R^n$ is R-hard if for any quotient algebra $A_R^n \in \Omega_R^n$ and any function $\tilde{f}(\underline{x})$ with deg($\tilde{f}(\underline{x})$) $= o(\sqrt{n})$ such that $f(\underline{x}) \sim_A \tilde{f}(\underline{x})$, then dim $A_R^n \ll 2^n - 2^{n-c\log n}$ for some constant c.

Notice the difference in the definition of nearly R-easiness over a ring R and that of nearly F-easiness over a field F. Informally, a function over R is nearly R-easy, if by ignoring a small fraction of inputs, we can force it to have low degree; while for R-hard functions, we have always to ignore a large fraction inputs.

We say a Boolean function $g(\underline{x})$ is R-easy or nearly R-easy if it has a representation which is R-easy or nearly R-easy. And a Boolean function is R-hard if all of its representations are R-hard.

Clearly, all R-easy function can be computed by a small depth Boolean circuits with Mod_r gates where $R = Z/(r)$. A lemma in [BT 87] states that any R-easy function can not represent the Boolean operation AND. But clearly, both AND and OR are nearly R-easy. And we conjecture that any Boolean function computed by a small depth Boolean circuit with Mod_r gates is R-easy or nearly R-easy. This is equivalent to say that the set of the input points which turn the Boolean function on have such a pattern that by ignoring some small fraction of the input points or adding some small fraction of input points and carefully choosing the value the function might take, we are able to construct a polynomial by interpolation such this polynomial is compatible with the Boolean function in the resulting quotient algebra.

Conjecture *Any Boolean function computed by a small depth Boolean circuit with Mod_r gates has an R-easy or a nearly R-easy representation over $R = Z/(r)$. In other words, any R-hard function cannot be computed by a small depth Boolean circuit with Mod_r gates.*

Now we show some classes of functions are R-hard.

As in section 2, we define the class of Extended semi-threshold functions as follows:

Let $f(\underline{x}) \in U_R^n$, we say $f(\underline{x})$ is an *Extended semi-threshold function*

$EST_t(\underline{x})$ if

$$\begin{array}{lll} \text{for any } \underline{x} \in \mathbf{B}^n, & f(\underline{x}) = 0 & \text{if } |\underline{x}| < t \\ & f(\underline{x}) \neq 0 & \text{if } |\underline{x}| = t \\ & f(\underline{x}) = \text{arbitrary value in } R & \text{if } |\underline{x}| > t \end{array}$$

Note that any function in $EST_t(\underline{x})$ is of degree at least t, as the coefficients of monomials of degree t do not vanish. For t suitably large, it can be checked that any sequence of functions induced by an $EST_t(\underline{x})$ functions are still Extended semi-threshold functions for some suitably large t'.

Observe that the proof of Hardness Lemma in section 2 actually does not rely on the fact that the underlying structure is a field, it works also for a ring. Hence, we have

Hardness Lemma For $EST_t(\underline{x})$ Over R

Let $f(\underline{x}) \in EST_t(\underline{x})$, where t suitably large. For any $A_R^n = \frac{U_R^n}{I}$, if there exists a $g(\underline{x}) \in I$ such that $h(\underline{x}) = f(\underline{x}) + g(\underline{x})$ has degree $o(\sqrt{n})$, then $dim\, I \gg 2^{n-c\log n}$ for some constant c, hence $dim\, A_R^n \ll 2^n - 2^{n-c\log n}$

Now we prove that for suitably large t, any function in $EST_t(\underline{x})$ is R-hard.

Theorem 8 *For t suitably large, any function in $EST_t(\underline{x})$ is R-hard. In particalur, any semi-threshold function in $ES_t(\underline{x})$ do not have small depth circuit with Mod_r.*

Proof Let $f(\underline{x}) \in EST_t(\underline{x})$. For any $\tilde{f}(\underline{x})$ and any $A_R^n \in \Omega_R^n$, suppose $f(\underline{x}) \sim_A \tilde{f}(\underline{x})$, then by Lemma 7, we know there exist an $f'(\underline{x}) \in U_R^n$ and a $g(\underline{x}) \in I$ with the property that $f(\underline{x}) \sim_{U_R^n} f'(\underline{x})$ and $\tilde{f}(\underline{x}) = f'(\underline{x}) + g(\underline{x})$. As $f'(\underline{x})$ is compatible with $f(\underline{x})$ over U_R^n, we have $f'(\underline{x}) \in EST_t(\underline{x})$. Applying the Hardness Lemma to $f'(\underline{x})$, it follows that $dim\, A_R^n \ll 2^n - 2^{n-c\log n}$ for some constant c. Therefore, $f(\underline{x})$ is R-hard.
Since any representation of a semi-threshold Boolean function in $ES_t(\underline{x})$, where t suitably large, is a function in $EST_t(\underline{x})$, hence any semi-threshold Boolean function in $ST_t(\underline{x})$ is R-hard functions over $R = Z/(r)$. □

In particular, we have

Corollary 9 *Majority is R-hard over $R = Z/(r)$ for any fixed $r \in \mathbf{N}$. For t large, $Exact_t(\underline{x})$, $Threshold_t(\underline{x})$, are R-hard functions over $R = Z/(r)$.*

Corollary 10 *For t suitably large, $Mod_t(\underline{x})$ is R-hard, and in particular, for r^m suitably large, $Mod_{r^m}(\underline{x})$ is R-hard functions over $R = Z/(r)$.*

As in section 2, we can extend the proof of Hardness Lemma to show that all high degree, dense polynomials which satisfy the *Hardness* condition are R-hard.

To show Mod_q is R-hard over $R = Z/(r)$, where q is a fixed prime and q does not divide r, we only have to show all possible representations of Mod_q over R have high degrees, then as in section 2, we can check that its induced sequence of functions satisfies the *Hardness* condition.

Therefore, if all possible representations of Mod_q are of high degree, then Mod_q is R-hard over $R = Z/(r)$. We can show this is true for r satisfying certain condition (see the following lemma); however, in the general case, we are still not able to produce a rigorous proof.

Lemma 11 *Let q be a fixed prime, $r = p_1 p_2 \cdots p_s$ be a fixed squarefree number, all p_i's and q being distinct. If there exists i such that $p_1 u_i \geq r$ where u_i is the inverse of p_i in $\mathcal{F}_q$, then any representation of Mod_q over $R = \mathbf{Z}/(r)$ under our model has degree $O(n)$.*

Sketch of the proof Let $f(\underline{x})$ be any represenation of Mod_q over $R = Z/(r)$. For any $\underline{a}$ such that $|\underline{a}| \bmod q = 0$, then $f(\underline{a}) \in R \backslash \{0\} = \{1, 2, \ldots, r-1\}$. Let $f'(\underline{x})$ be the function in U_R^n corresponding to the function $f(\underline{x})^{(q-1)\varphi(r)}$, where $\varphi(r)$ is the Euler function, *i.e.* $\varphi(r)$ equals the order of the multiplicative group of R. Then for any $\underline{a}$ such that $|\underline{a}| \bmod q = 0$, $f'(\underline{a}) \bmod q = 1$. Hence $f'(\underline{a}) \equiv 1 - (x_1 + x_2 + \cdots + x_n)^{q-1} (\mathrm{mod} q)$. By careful comparison of the coefficients from the lower degree monomials to the higher degree ones, we find out that for any $\underline{a}$ such that $|\underline{a}| \bmod q = 0$, $f'(\underline{a}) \equiv 1 (\mathrm{mod} r)$. Hence $f'(\underline{x})$ has degree of order $O(n)$, so is $f(\underline{x})$. □

Theorem 12 *For r and q satisfying the condition in the above lemma, Mod_q is R-hard over $R = Z/(r)$.*

It is easy to see that 5 and 6 satisfy the condition, hence

Corollary 13 *Mod_5 is R-hard over $R = Z/(6)$.*

5 Conclusion

We gave a simple extension of Smolensky's method by replacing $U^n_{F_p}$-completeness with a weaker definition $\mathcal{F}_p$-hardness, we were able to demonstrate explicitly and argue more directly that many more functions are hard to compute by small depth Boolean circuits with Mod_p. We established a *Hardness Lemma* for a class of functions and characterized when a function over $\mathcal{F}_p$ is hard to compute by a constant depth, polynomial size circuit with Mod_p gates.

Although we cannot extend Smolensky's method directly to a general, due to the insurmoutable gap between the Boolean circuits with gates module a composite number and any model of representing Boolean functions by functions over the corresponding ring, we introduced the analogous complexity theoretic notions into a ring, and gave a classification of functions accoring to their relative hardness. This classification provides some information about the relative complexity of the Boolean functions they represent. In particular, we proved that any representation of $Majority$ over a ring R is R-hard.

To finally resolve the open problems in [Sm 87] and in [BT 87], we have to find new algebraic models which have a strong connection with the Boolean model and allow new techniques to be applied. Algebraic decision tree model [SY 82] is one possible approach, where each query node is a bounded degree polynomial over a ring. However, we suspect this model is too weaker. Recently, Szegedy [Sz 90] suggested using communication complexity approach, which yieded some weak results. One of the very promising approach was the joint work of Barrington and Thérien [BT 87, BT 88]. They established a very interesting and nice relationship between non-uniform deterministic finite automata over monoids and groups and subclasses of NC^1 class. They proved that ACC corresponds exactly to the families of languages recognizable by NUDFA over solvable monoids, whereas NC^1 corresponds to families of lauguages recognizable by NUDFA over unsolvable groups. In spite of many efforts devoted to this area, so far, the aforementioned two open problems remain widely open.

Acknowlegdement

I am grateful to my advisor, Carl Sturtivant, for many inspiring and helpful discussions.

References

[Aj 83] M. Ajtai, "Σ_1^1 formulae on finite structures" *Annals of Pure and Appl. Logic*, Vol. 24, 1984

[Ba 86] D.A.M. Barrington, "Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1" *Proc. 18th ACM STOC*, 1986

[BT 87] D.A Barington, D. Thérien "Non-uniform automata over groups" *Proc. 14th International Colloqium Automata, Languages, and Programming* Lecture Notes in Computer Science, Vol. 267, Springer Verlag 1987, pp. 163-173

[BT 88] D.A.M. Barrington, D. Thérien "Finite Monoids and the Fine Structure of NC^1", *JACM* Vol. 35, No. 4 Oct. 1988 pp. 941-952

[Cai 86] J-Y. Cai, "With probability one a random oracle separates PSPACE from the polynomial hiearachy", *Proc. 18th ACM STOC*, 1986

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

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

[HM 87] A. Hajnal, W. Maass, Pavel Pudlák, M. Szegedy, and G. Turán "Threshold circuits of bounded depth", *Proc. 28th IEEE FOCS*, 1987, pp. 99-110

[IR 84] K. Ireland, M. Rosen *A Classical Introduction to Modern Number Theory* Springer-Verlag, 1984

[La 84] S. Lang *Algebra* Addison-Wesley, 1984

[LMN 89] N. Linial, Y. Mansour, N. Nisan "Constant depth circuits, Fourier Transform, and Learnability". *Proc. 30th IEEE FOCS*, 1989, pp. 574-579

[LN 83] R. Lidl, H. Niederreiter *Finite Fields* Encycl. of Math. and Its Appl., vol. 20, Addison-Wesley, 1983

[Ra 87] A.A. Razborov "Lower bounds on the size of bounded depth networks overa complete basis with logical addition", *Matem. Zamet.* 41:4 (in Russian). English translation *Mathematical Notes of the Academy of Sciences of the USSR* 41:4, 333-338

[Sm 87] R. Smolensky "Algebraic methods in the theory of lower bounds for Boolean circuit complexity", *Proc. 19th ACM STOC*, 1987, pp. 77-82

[Sz 90] M. Szegedy "Functions with bounded symmetric communication complexity and circuits with Mod_m gates" *Proc. 22th STOC*, 1990, pp. 278-286

[SF 87] C. Sturtivant, G. Frandsen *The Computational Efficacy of Finite Field Arithmetic* Technique Report Daimi PB 227, Comp. Sci. Dept. Aarhus Univ. Denmark, 1987
[St 88] C. Sturtivant *Lecture Notes on Algebraic Complexity* Comp. Sci. Dept. Aarhus Univ. Denmark, spring 1988 (unpublished)
[SY 82] J.M. Steele, A.C.C. Yao "Lower bounds for algebraic ddecision trees", *Journal of Algorithms*, Vol. 3, 1982, pp. 1-8 [Ya 85] A.C.C. Yao "Separating the polynomial hiearachy by oracles", *Proc. 26th IEEE FOCS*, 1985, pp. 1-10
[Ya 89] A.C.C. Yao "Circuits and local computation", *Proc. 21th ACM STOC*, 1989, pp. 186-196