Degree Complexity of Boolean Functions
and Its Applications to Relativized Separations

Jun Tarui
Department of Computer Science
University of Rochester
Rochester, NY 14627 (tarui@cs.rochester.edu)

Abstract
We show that a simple function in $\mathsf{AC}^0$, OR of $\sqrt{n}$ disjoint ANDs, cannot be computed by decision trees of depth $\log^2 n$ where each node asks whether or not $p(x_1, \ldots, x_n) = 0$ for some polynomial $p$ of degree $\log^2 n$. This is in contrast to the recent results [12, 13] that every function in $\mathsf{AC}^0$ can be computed probabilistically by just one such query and can be deterministically computed by such decision trees if each node asks whether or not $p(x_1, \ldots, x_n) > 0$.

In terms of counting classes, this means that there is an oracle $A$ such that $(\Sigma_2^p)^A \not\subseteq \mathsf{PC}^{=P^A}$ in contrast to the recent (relativizable) results that the entire polynomial hierarchy is contained in $\mathsf{ZPP}^{\Sigma_2^p} \subseteq \mathsf{P}^\text{PP}$ and in $\mathsf{P}^\text{PP}$.

The proofs will be based on simple algebraic arguments that also provide alternative proofs for some known results.

1 Introduction

1.1 background
Recently, Toda [13] and Tarui [12] have shown that the polynomial hierarchy (PH) is contained in $\mathsf{P}^\#P$, thus in $\mathsf{PP}$ [13], and in $\mathsf{ZPP}^{\mathsf{C}^m\mathsf{P}}$ [12]. (Also see [14, 3]. The class $\mathsf{C}^m\mathsf{P}$ is explained in Section 1.4.)

There are corresponding results in terms of constant-depth circuits [12, 3], which are essentially results about representability of Boolean functions by low-degree (degree-$\log^2 n$) polynomials in $x_1, \ldots, x_n$: if $f = (f_n)_{n=1}^\infty$ is in $\mathsf{AC}^0$, then there is a sequence $p = (p_n)_{n=1}^\infty$ of low-degree polynomials such that $f_n(x)$ can be determined from $p_n(x)$, and there is a sequence $q = (q_n(x))_{n=0}^\infty$ of low-degree probabilistic polynomials such that $f_n(x) = q_n(x)$ with high probability and with one-sided error [12]. By converting low-degree polynomials into depth-two circuits with small fan-in we conclude that if $f = (f_n)_{n=1}^\infty$ is in $\mathsf{AC}^0$, then there is a sequence of depth-two size-$n^{\log^2 n}$ circuits with a symmetric gate at the output that computes $f$, and there is a sequence of depth-two size-$n^{\log^2 n}$ probabilistic circuits with a threshold gate at the output that computes $f$ with one-sided error.

Now that we know $\mathsf{PH} \subseteq \mathsf{P}^\text{PP}$ and $\mathsf{PH} \subseteq \mathsf{ZPP}^{\mathsf{C}^m\mathsf{P}}$ several people have asked [16, 7] whether or not $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{C}^m\mathsf{P}}$ holds. In this paper we exhibit a relativized world $A$ in which this containment does not hold: in particular $(\Sigma_2^p)^A \not\subseteq \mathsf{PC}^{=P^A}$. Although recently some important nonrelativizable results such as $\mathsf{IP} = \mathsf{PSPACE}$ [8] have been obtained, all the recent results about counting classes mentioned above are proved by the techniques that do relativize, thus our result suggests some limitations of techniques along these lines.
1.2 degree lower bounds and relativized separations

One of the standard techniques in relativized separations is to consider an oracle-dependent language

\[ L^A = \{0^n : f_n(z_1, \ldots, z_{2^n}) = 1\}, \]

where \( z_i = 1 \) iff the \( i \)-th string in \( \{0,1\}^n \) is in \( A \) and \( f = (f_n)_{n=1}^\infty \) is some sequence of Boolean functions. For example,

\[ L^A = \{0^n : |\{0,1\}^n \cap A| \neq 0\} = \{0^n : \text{OR}(z_1, \ldots, z_{2^n}) = 1\} \]

is clearly in \( NPA \). By ensuring that \( L^A \not\in \text{C}=P^A \), we obtain an oracle \( A \) such that \( \text{NPA} \not\subseteq \text{C}=\text{PA} \). To show that we can in fact ensure that \( L^A \not\in \text{C}=\text{PA} \), it suffices to show that \( \text{OR} \) can not be computed in a certain way that reflects the acceptance mechanism of \( \text{C}=\text{P} \), and thus we can diagonalize out of each machine for \( \text{C}=\text{P} \). In general, such diagonalizations can be intertwined so that we obtain a simultaneous separation.

In particular, machines for classes such as \( \text{NP} \), \( \text{C}=\text{P} \), and \( \text{MOD}_k \text{P} \) (The class \( \text{MOD}_k \text{P} \) is explained in Section 1.4.) have the property that each computational path can access only polynomially many \( z_i \)'s. In this case, since arbitrary Boolean function that depends on polynomially many \( z_i \)'s can be expressed by a multilinear polynomial in \( z_i \)'s of degree only polynomially big, it suffices to show that a certain Boolean function can not be expressed as a low-degree polynomial over an algebraic structure that corresponds to the acceptance mechanism being considered. Note that a polynomial in \( 2^n = N \) variable of degree \( n^{O(1)} \) corresponds to degree-\( n^{O(1)} \) \( N \) polynomial in \( N \) variables.

Throughout the paper we thus concentrate on \textit{degree lower bounds}, mostly omitting the translations of degree lower bounds to oracle constructions; It is a simple matter of using \( L^A \) above with the Boolean function being considered. Since low-degree polynomials correspond to depth-two small \textit{fan-in} (\( \text{fan-in} \log^{O(1)} n \)) circuits with an output gate that corresponds to an algebraic structure being considered, a degree lower bound also translates into a result that says that a certain type of circuits can not compute a particular Boolean function. We also omit these consequences in terms of circuits; Again it is a simple matter of translation.

Using a degree lower bound we also exhibit a simple algebraic proof that there exists an oracle \( A \) such that \( \text{NP}^A \not\subseteq \text{MOD}_k \text{P}^A \) for all \( k \geq 2 \) and \( \text{NP}^A \not\subseteq \text{C}=\text{P} \). These separations were first obtained by Torán [15], and alternative proofs were given by Beigel [2].

1.3 small-depth decision trees

As explained in Section 1.2, machines for classes such as \( \text{NP} \) and \( \text{C}=\text{P} \) correspond to certain depth-two circuits or low-degree polynomials. Although the following correspondence has not been used as much, it is equally easy to observe that machines for a class of the form \( \text{P}^C \) correspond to \textit{small-depth} (depth-\( \log^{O(1)} n \)) \textit{decision trees} where each node can ask a question corresponding to the class \( C \).

In particular, the results and questions mentioned in Section 1.1 will take the following forms.

Let \( f = (f_n)_{n=1}^\infty \) be in \( \text{AC}^0 \).

Then, there is a sequence \( p = (p_n)_{n=1}^\infty \) of low-degree polynomials over the integers such that the absolute values of \( p_n \)'s coefficients are in \( n^{\log^{O(1)} n} \) and \( f_n(x_1, \ldots, x_n) \) can be determined from \( p_n(x_1, \ldots, x_n) \). Thus by a binary search on the value of \( p_n(x_1, \ldots, x_n) \), \( f_n \) can be computed by small-depth decision trees where each node asks whether or not \( q(x_1, \ldots, x_n) > 0 \) for some low-degree polynomial \( q \) over the integers.

Also, probabilistically only one query of the form \( q(x_1, \ldots, x_n) \) is sufficient to give the correct answer with high probability (\( \geq 1 - 2^{-\log^* n} \)) and with one-sided error, and thus there is a sequence of probabilistic decision trees such that it always gives the correct answer, its expected
cost is constant, and its node asks whether or not $q(x_1, \ldots, x_n) = 0$ where a low-degree polynomial $q$ is chosen according to a certain probability distribution.

Decision trees that correspond to $PC^{P}_2$ are small-depth decision trees where each node asks whether or not $q(x_1, \ldots, x_n) = 0$ for some low-degree polynomial $q$ over the integers. Can every function in $AC_0$ be computed by such decision trees? We show that a simple function in $AC_0$, OR of $\bigwedge$ of disjoint ANDs of size $6$ each, cannot be computed by such algebraic decision trees. From this it follows that there is a relativized world $A$ in which $PC^{P} \subseteq \Sigma^P_2$.

1.4 definitions of $C_{\oplus}P$ and $MOD_kP$

Let $k$ be a fixed positive integer greater than $1$. The classes $MOD_kP$ and $C_{\oplus}P$ are defined as follows. For a nondeterministic polynomial-time Turing machine $M$ and an input $x$, let $\#\text{acc}(M, x)$ denote the number of accepting paths of $M$ on $x$. $MOD_kP$ is the class of languages $L$ for which there exists a nondeterministic polynomial-time Turing machine $M$ such that for every $x \in \{0, 1\}^*$,

$$x \in L \iff \#\text{acc}(M, x) \equiv 0 \pmod{k}.$$  

$C_{\oplus}P$ is the class of languages $L$ for which there exist a nondeterministic polynomial-time Turing machine $M$ and a polynomial-time computable function $f$ from $\{0, 1\}^*$ to the nonnegative integers such that for every $x \in \{0, 1\}^*$,

$$x \in L \iff \#\text{acc}(M, x) = f(x).$$

2 Main Results

In Section 2.1 we explain a general framework which is useful in putting our results in a perspective, but is not really necessary: A simple notion of reflection and Proposition 1, whose proof is simple and direct, are essentially all that are needed to understand the rest of the paper.

2.1 general algebraic framework

It is widely known that it is sometimes useful to consider a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ as a point in a $2^n$-dimensional vector space over a field $F$, i.e., $g : \{0, 1\}^n \rightarrow F$. Particularly, the cases where a field $F$ is a finite field, the field of rationals or reals, or the field of complexes (where we can use the Fourier transform in terms of characters) appear often in complexity theory. In this section, we explain some facts that hold over an arbitrary ring $R$. We can apply them in the cases where $R = Z$, the ring of integers, or $R = Z/kZ$, the ring of integers mod $k$.

Let $R$ be a ring. We consider the space of functions from a Boolean cube to $R$, $F_n(R) = \{g : \{0, 1\}^n \rightarrow R\}$, as an $R$-module with the natural $R$-module structure given by pointwise addition and multiplication over $R$. Roughly speaking, a module is like a vector space except that coefficients form a ring in general and may not be a field. But as we will see in a minute, $F_n(R)$ is more similar to a vector space than a general module is. (For more details about the language used and the facts stated in this section, see any standard textbook on algebra such as Jacobson’s [4].)

A set $S$ of points in an $R$-module $M$ is a basis for $M$ if $S$ generates $M$ and points in $S$ are $R$-linear independent, or equivalently, if each point in $M$ can be expressed as a unique $R$-linear combination of the points in $S$. A module $M$ is free if it admits a basis. If $R$ is commutative, the following holds in addition. Assume that $M$ is a free module over a commutative ring and $S \subseteq M$ with $|S| = n$ is a basis for $M$. If $T$ is another basis for $M$, then $|T| = n$. If $T$ with $|T| = n$ generates $M$, then $T$ is a basis for $M$. (i.e., The points in $T$ are $R$-linear independent.) Thus, the dimension of a free module over a commutative ring is well-defined, and arguments concerning dimension have proved useful in complexity theory. (For example, see Smolensky’s work [9].)

Now consider $F_n(R)$. For each subset $S = \{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$ ($i_1 < \cdots < i_m$), iden-
tify $S$ with a point $x \in \{0,1\}^n$ such that $\{i : x_i = 1\} = S$ and define the following.
Define $\chi_S : \{0,1\}^n \to R$ by $\chi_S(x) = 1$ if $x = S$, and 0 otherwise.
Define $p_S$ to be a monomial $x_i \cdots x_m$ with the convention that $p_S = 1$ if $S$ is empty.
Viewed as a polynomial over $R$, each $p_S$ naturally defines a function from $\{0,1\}^n$ to $R$, which we also denote by $p_S$.

The collection of $2^n$ points $A = \{x_S : \emptyset \subseteq S \subseteq \{1,\ldots,n\}\}$ is clearly a basis for $F_n(R)$, thus $F_n(R)$ is a free $R$-module. Since each point in $F_n(R)$ can be expressed as a multilinear polynomial over $R$, the collection of $2^n$ monomials $\Pi = \{p_S : \emptyset \subseteq S \subseteq \{1,\ldots,n\}\}$ generates $F_n(R)$. If $R$ is commutative, by the general principle above, $\Pi$ is also a basis for $F_n(R)$ (i.e., its points are $R$-linear independent.) since it has only $2^n$ points in it. Even when $R$ is noncommutative, $\Pi$ is a basis for $F_n(R)$. One way to see this is to apply the following proposition since, in particular, it says that over an arbitrary ring $R$, a nonzero multilinear polynomial over $R$ cannot vanish everywhere on $\{0,1\}^n$.

For a point $x \in \{0,1\}^n$, let $|x| = x_1 + \cdots + x_n$.

**Proposition 1.** Let $R$ be a ring and let $p(x_1,\ldots,x_n)$ be a multilinear polynomial over $R$ of degree $d$. Assume that $p(x) = 0$ for each $x \in \{0,1\}^n$ satisfying $0 \leq |x|_1 \leq d$. Then, $p \equiv 0$.

**Proof.** Let $p$ and $d$ be as above. To get a contradiction assume that $p$ is nonzero and let $\alpha \cdot p_S$ be a nonzero monomial in $p$ with the minimum degree. Then, $|S| \geq d+1$ must hold since $\alpha \cdot p_S(S) = \alpha \neq 0$, and this contradicts that the degree of $p$ is at most $d$.

(In other words, the constant term must be 0 since $p(0,\ldots,0) = 0$. Then, all the linear terms must be 0 since $p(0,\ldots,0,1,0,\ldots,0) = 0$. Similarly for quadratic terms and up to terms of degree $d$.)

For a point $x = (x_1,\ldots,x_n) \in \{0,1\}^n$, define the reflection of $x$, $\tilde{x}$, to be the point $\tilde{x} = (\tilde{x}_1,\ldots,\tilde{x}_n) = (1-x_1,\ldots,1-x_n)$, and for $f \in F_n(R)$, define the reflection of $f$, $\tilde{f}$, by $\tilde{f}(x) = f(\tilde{x})$. For a multilinear polynomial $p$, the reflection of $p$, $\tilde{p}$, is the multilinear polynomial that we obtain after substituting, for all $i$, $1-x_i$ for $x_i$ in $p$, which clearly coincides with the reflection of $p$ as a point (i.e., as a function) in $F_n(R)$. The reflection is a module automorphism of $F_n(R)$ with itself as its inverse, and in particular the reflection preserves the degree.

### 2.2 Results

**Proposition 2.** Let $R$ be a ring. Let $p(x_1,\ldots,x_n)$ be a multilinear polynomial over $R$ such that, for some nonzero $\alpha$ in $R$, the following holds for each $x \in \{0,1\}^n$.

\[
p(x_1,\ldots,x_n) = \begin{cases} 0 & \text{if } OR(x_1,\ldots,x_n) = 1, \\ \alpha & \text{if } OR(x_1,\ldots,x_n) = 0. \end{cases} \tag{1}
\]

Then, $p(x_1,\ldots,x_n)$ is uniquely determined as follows.

\[
p(x_1,\ldots,x_n) = \alpha(1-x_1)\cdots(1-x_n) \tag{2}
\]

In particular, $p(x_1,\ldots,x_n)$ has degree $n$.

As a corollary, as explained in Section 1.2, we obtain the following relativized separations, which were first proved by Torán [15]. We note that recent results by Toda [13] and Tarui [12] show that the containment does hold with a random oracle as stated below.

**Corollary 1.** There exists an oracle $A$ such that

\[
NP^A \not\subseteq C=P^A
\]

and for all $k \geq 2$

\[
NP^A \not\subseteq MOD_k P^A.
\]
Fact 1. With respect to a random oracle $R$, with probability 1,

$$PH^R \subseteq C=P^R$$

and for all $k \geq 2$

$$PH^R \subseteq MOD_k P^R.$$

First Proof of Proposition 2. Since $2^n$ multilinear monomials form a basis for $F_n(R)$, a point in $F_n(R)$ specified by equation (1) has the unique $R$-linear combination of such monomials, which must coincide with the right hand side of equation (2).

Second Proof of Proposition 2. Let $\bar{p}$ be the reflection of $p$, i.e., $\bar{p}(x_1, \ldots, x_n) = p(1 - x_1, \ldots, 1 - x_n)$. Then, $\bar{p}$ satisfies the following for each $x \in \{0, 1\}^n$.

$$\bar{p}(x_1, \ldots, x_n) = \begin{cases} 0 & \text{if } \text{AND}(x_1, \ldots, x_n) = 0, \\ \alpha & \text{if } \text{AND}(x_1, \ldots, x_n) = 1. \end{cases}$$

By applying the arguments in the proof of Proposition 1, we can show that $\bar{p}(x_1, \ldots, x_n) = \alpha x_1 x_2 \cdots x_n$. Since $p = \bar{p}$, we obtain the proposition.

The following generalizes Proposition 1.

Theorem 1. Let $R$ be a ring. Let $p(x_1, \ldots, x_n)$ be a multilinear polynomial over $R$ of degree at most $d$ and let $i$ be a nonnegative integer such that $0 \leq i \leq i + d \leq n$ and $p(x) = 0$ for each $x \in \{0, 1\}^n$ satisfying $i \leq |x| \leq i + d$. Then, $p \equiv 0$.

Proof. Let $p(x_1, \ldots, x_n)$, $d$ and $i$ be as above. To get a contradiction, suppose that $p$ does not vanish at some $x^0 \in \{0, 1\}^n$. Assume that $i + d < |x^0|_1 \leq n$. If $0 \leq |x^0|_1 < i$, consider the reflections $\bar{p}$ and $\bar{x}^0$ and apply the same argument. Let $j_1, \ldots, j_i$ be (arbitrary but for definiteness) the first $i$ coordinates of $x^0$ such that $x^0_{j_k} = 1$ ($1 \leq k \leq i$). Substitute $x^{j_k}_k = 1$ ($1 \leq k \leq i$) in $p$, and obtain $\bar{p}$. The degree of $\bar{p}$ does not exceed the degree of $p$.

$\bar{p} \neq 0$ since $p(x^0) \neq 0$, and since $i$'s are already set, $\bar{p}(y) = 0$ for each $y$ with $0 \leq |y|_1 \leq \alpha d$. But then, by Proposition 1, $\bar{p}$ must vanish everywhere, which is a contradiction.

A ring $R$ is a domain if $x \neq 0$, $y \neq 0 \implies xy \neq 0$ holds in $R$. We don't assume commutativity for a domain.

Theorem 2. Let $f = (f_n)_{n=1}^{\infty}$ be a sequence of Boolean functions on $n$ variables, let $c < 1$ be a positive constant, and let $(i_n)_{n=1}^{\infty}$ and $(j_n)_{n=1}^{\infty}$ be sequences of nonnegative integers such that, for each $n$, $i_n + n^c \leq n$, $j_n + n^c \leq n$, and

$$i_n \leq |x|_1 \leq i_n + n^c \implies f_n(x) = 0$$

$$j_n \leq |x|_1 \leq j_n + n^c \implies f_n(x) = 1.$$ 

Let $R$ be a domain and let $T = (T_n)_{n=1}^{\infty}$ be a sequence of decision trees of depth $\log^O(1,n)$ where each node asks, and branches according to, whether or not $q(x_1, \ldots, x_n) = 0$ for some polynomial $q$ over $R$ of degree $\log^O(1,n)$. Then, for all $n$ sufficiently large, $T_n$ does not compute $f_n$.

Let $g = (g_n)_{n=1}^{\infty}$ be a sequence of OR of $\sqrt{n}$ disjoint ANDs of size $\sqrt{n}$ each. Then since $g$ satisfies the condition of Theorem 2 with $c = 1/2$, $i_n = 0$, and $j_n = n - n^c$, we obtain the following corollary.

Corollary 2. Small-depth decision trees that ask, and branch according to, whether or not low-degree polynomials over a domain vanishes on an input can not agree with OR of $\sqrt{n}$ disjoint ANDs on the subset $x \in \{0, 1\}^n, |x|_1 \leq \sqrt{n}$ or $|x|_1 \geq n - \sqrt{n}$ of the Boolean $n$-cube for all $n$ sufficiently large.

Note that if the degree is low, allowing a query whether or not a polynomial over, say, the complexes vanishes on an input does not enable small-depth decision trees to compute $g$. By taking a ring $R$ to be $Z$, the ring of integers, we obtain the following relativized separation.
Corollary 3. There exists an oracle $A$ such that
\[(\Sigma^p_2)^A \not\subseteq P^{C=P^A}.\]

**Proof of Theorem 2.** Let $f_n$, $c$, $i_n$, $j_n$, and $T_n$ be as in the theorem. Let $n$ be sufficiently large as will become clear below and to get a contradiction assume that $T_n$ computes $f_n$. By pruning a redundant path, if necessary, assume that $T_n$ is non-redundant, i.e., every leaf is reached by some input.

Starting at the root of $T_n$, follow the path along the answer “no”, i.e., follow branching according to $p(x_1, \ldots, x_n) \neq 0$ to the leaf $L$, and let $P(x_1, \ldots, x_n)$ be the product of $\log^O(1)n$ polynomials of degree $\log^O(1)n$ that we encounter along the path.

Assume the answer at $L$ is 1. The other case is similar. This means that $P(x_1, \ldots, x_n) = 0$ for each $x$ satisfying $i_n \leq |x|_1 \leq i_n + n^c$, thus $P$ vanishes on each such $x$. But, for sufficiently large $n$, $n^c$ exceeds $\log^O(1)n$, the degree of $P$, thus by Theorem 1 $P$ must vanish everywhere, which contradicts our assumption that the leaf $L$ is reached by some input $y$ since $P(y) \neq 0$ must hold for this $y$ because we are working over an integral domain.

Now we wish to show a relativized separation that is somewhat stronger than Corollary 3. First we note that the following relation holds in the “real world” and with respect to every oracle. Lautemann’s proof [5] that $BPP \subseteq \Sigma^p_2$ essentially contains the proof that $BPP \subseteq R^{NP}$, thus we have the first part of the relation, $BPP \subseteq ZPP^{NP}$.

**Fact 2.**

\[
\begin{align*}
BPP &\subseteq ZPP^{NP} \subseteq (\Sigma^p_2 \cap \Pi^p_2) \\
&\subseteq \Pi^p_2 \subseteq (ZPP^{C=P} \cap B^{PP}).
\end{align*}
\]

Corollary 4 and its proof can also be thought of as an extension of, and an alternative proof of, Stockmeyer’s result [10] that there exists an oracle $A$ such that $BPP^A \not\subseteq (\Delta^p_2)^A$ since clearly $\Delta^p_2 \subseteq P^{C=P}$ holds with respect to every oracle.

A standard technique to construct an oracle $A$ with respect to which classes such as $BPP^A$, $R^A$, and $ZPP^A$ are *not* contained in a class $C$ is to consider a certain Boolean function $f$ on some restricted domain. We restrict the domain so that $f$ is easy for $BPP$, $R$, or $ZPP$, but that $f$ is still hard for the class $C$, and use $f$ as explained in Section 1.2.

**Proof Sketch of Corollary 4.** Consider the following oracle-dependent language.

\[
L^A = \{0^n : |\{0,1\}^n \cap A| > 2^n - 2^{n/2}\}.
\]

If we ensure, by our construction, that for each $n$ either

\[
|\{0,1\}^n \cap A| < 2^{n/2} \quad \text{or} \quad |\{0,1\}^n \cap A| > 2^n - 2^{n/2},
\]

then $L^A$ is clearly in $BPP^A$. Note that if we put $N = 2^n$, $N^{1/2} = 2^{n/2}$. By Corollary 2, we can diagonalize out of each machine for $P^{C=P}$ while maintaining the condition above that we have promised to ensure.

By a similar consideration, one can show, for example, that there is an oracle $A$ such that $ZPP^A \not\subseteq \text{MOD}_q P$ for all prime $q$.

### 2.3 alternative proof of Theorem 2 over the complexes

In this section we explain another method to prove Theorem 2 in the case that coefficients are complexes. This subsumes the case that coefficients are integers, which is of our main concern. Our
The main goal will be to prove the following weaker version of Theorem 1 over the complexes. One can easily check that the weaker bound is good enough to give Theorem 2 over the complexes.

Theorem 1.0. Let \( p(x_1, \ldots, x_n) \) be a multilinear polynomial over the complexes of degree at most \( d/2 \) and let \( i \) be a nonnegative integer such that 0 \( \leq i \leq i+d \leq n \) and \( p(x) = 0 \) for each \( x \in \{0,1\}^n \) satisfying \( i \leq |x| \leq i+d \). Then, \( p \equiv 0 \).

We use the technique, which at least dates back to the work of Minsky and Papert [6] in the late 60s, of symmetrizing a polynomial and converting it to an equivalent single-variate polynomial.

For a multivariate polynomial \( p(x_1, \ldots, x_n) \), define the symmetrization of \( p, \hat{p} \), by

\[
\hat{p}(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),
\]

where \( S_n \) denotes the set of permutations of \( \{1, \ldots, n\} \). Note that \( \hat{p} \) is a symmetric polynomial and its degree does not exceed that of \( p \). (The degree can decrease. Consider \( (x_1 - x_2) \).

Lemma (Minsky and Papert? [6]). Let \( F \) be a field with characteristic \( 0 \) and let \( p(x_1, \ldots, x_n) \) be a multilinear symmetric polynomial over \( F \). Then, there is a polynomial \( P(X) \) in one variable whose degree equals that of \( p(x_1, \ldots, x_n) \) and such that for every \( (x_1, \ldots, x_n) \in \{0,1\}^n \), if we put \( X = x_1 + \cdots + x_n \), \( p(x_1, \ldots, x_n) = P(X) \).

Note that it is necessary that we are working over a field with characteristic \( 0 \). For example, \( x_1x_2 \) can not be expressed in terms of \( X = x_1 + x_2 \) over \( \mathbb{Z}/2\mathbb{Z} \).

Proof of Theorem 1.0. Let \( p(x_1, \ldots, x_n) \), \( d \), and \( i \) as in Theorem 1.0.

Put \( q = \overline{p} \), where \( \overline{p} \) is the complex conjugate of \( p \), let \( \hat{q} \) be the symmetrization of \( q \), and let \( Q(X) \) be the single-variate polynomial that is equivalent to \( \hat{q} \) as given in the lemma above. Since \( q \) is nonnegative real everywhere, \( \hat{q} \) vanishes everywhere \( \iff \) \( q \) vanishes everywhere \( \iff \) \( p \) vanishes everywhere. If there is a point \( y \) on which \( q \) does not vanish, then \( \hat{q} \) does not vanish on the orbit that includes \( y \).

By our construction the single-variate polynomial \( Q(X) \) has degree at most \( d \). By the condition of theorem, \( Q(X) \) vanishes at \( X = i, i+1, \ldots, i+d, \) and hence must vanish everywhere since a nonzero single-variate polynomial of degree at most \( d \) over a field has at most \( d \) zeroes. Hence \( p \) must vanish everywhere.

3 Approximating MAJORITY

Let \( \text{sgn} \) be a function from the reals to \( \{0,1\} \) such that \( \text{sgn}(x) = 1 \) if \( x \geq 0 \), and 0 otherwise.

Recently, Aspnes, Beigel, Furst, and Rudich [1] have shown that for a sequence of low-degree (\( \text{deg} \log^O(1) \)) polynomials \( p = \{p_n\}_{n=1}^{\infty} \) over the reals, \( \text{sgn}(p_n(x_1, \ldots, x_n)) \) can not agree with \( \text{PARITY} \) on more than, say, 90% of inputs, and consequently, with respect to a random oracle, \( \text{\#PR \nsubseteq \text{PPR}} \) with probability 1. Their key observation is that over the reals, given arbitrary 10% of points in \( \{0,1\}^n \), there is a nonzero polynomial of degree \( n/2 - \Omega(\sqrt{n}) \) that vanishes on all those points.

For a predicate \( P \), let \( [P] \) denote the Boolean function that is 1 if \( P \) is true. Can \( \text{MAJORITY} \) be approximated as \( [p_n(x_1, \ldots, x_n) = 0] \) for some low-degree polynomials \( p_n \)'s? Szegedy [11] has shown that over a field or a finite ring such approximation of \( \text{MAJORITY} \) is impossible. From his result it follows that, with respect to a random oracle \( R \), \( \text{P}^{\text{PR}} \nsubseteq \text{P}^{\text{FPH}^R} \) and \( \text{P}^{\text{PR}} \nsubseteq \text{P}^{\text{MOR}^R} \) for all prime \( q \) with probability 1. The oracle construction goes as explained in Section 1.2, and from the nonapproximability we obtain probability one separation.

Szegedy’s proof uses a dimension argument similar to the one used in Smolensky’s work [9]. In this section, we note that there is an alternative way to prove Szegedy’s theorem.
Theorem (Szegedy). Let $F$ be an arbitrary field and let $p = (p_n)_{n=1}^\infty$ be a sequence of polynomials over $F$ of degree $\log^2(1)n$. Then, for all $n$ sufficiently large, $[p_n(x_1, \ldots, x_n) = 0]$ differs from $\text{MAJORITY}(x_1, \ldots, x_n)$ on at least 10% of inputs of length $n$.

Proof. Let $p = (p_n)_{n=1}^\infty$ be a sequence of low-degree polynomials over a field $F$. Let $n$ be sufficiently large as will become clear below, and to get a contradiction assume that $[p_n(x_1, \ldots, x_n) = 0]$ agrees with $\text{MAJORITY}$ on at least 90% of inputs, or equivalently, for at least 90% of inputs of length $n$, $\text{MAJORITY}(x_1, \ldots, x_n) = 1 \iff p_n(x_1, \ldots, x_n) = 0$.

Then, by the observation by Aspnes, Beigel, Furst, and Rudich, there is a nonzero polynomial $q_n$ over $F$ of degree $n/2 - \Omega(\sqrt{n})$ such that $q_n$ vanishes on all the points where $[p_n(x_1, \ldots, x_n) = 0]$ does not agree with $\text{MAJORITY}$.

Partition $\{0, 1\}^n$ into $A_0 = \text{MAJORITY}^{-1}(0)$ and $A_1 = \text{MAJORITY}^{-1}(1)$. For every point $x$ in $A_0$, $p_n(x) = 0 \implies q_n(x) = 0$ since $q_n(x)$ has been constructed to vanish on all the points on which $p_n$ makes a mistake, hence $q_n(x) \neq 0 \implies p_n(x) \neq 0$. But by Theorem 1, $q_n$ does not vanish everywhere on $A_0$, thus there is a point $x_0 \in A_0$ on which neither $p_n$ nor $q_n$ vanishes. Hence $p_n q_n$ is not identically zero. But by construction $p_n q_n$, whose degree is $n/2 - \Omega(\sqrt{n})$, vanishes everywhere on $A_1$, which is a contradiction since Theorem 1 says that a nonzero polynomial must have degree at least $n/2$ to behave in such a way. \[\square\]

Acknowledgment. The author would like to thank his advisor, Joel Seiferas for his encouragement and patience. He would also like to thank Joel, Richard Beigel, and Sanjay Jain for their helpful comments; Richard pointed out to the author that we need $\text{char}(F) = 0$ for Lemma 2 (Minsky and Papert).

References


Degree Complexity of Boolean Functions and Its Applications to Relativized Separations

J. Tarui

(Paper received late. Please refer to page 382)