DEGREE BOUNDS ON POLYNOMIALS AND RELATIVIZATION THEORY*

Holger Spakowski†
Institut für Informatik
Heinrich-Heine-Universität Düsseldorf
40225 Düsseldorf, Germany
spakowsk@cs.uni-duesseldorf.de

Rahul Tripathi‡
Department of Computer Science
University of Rochester
Rochester, NY 14627, USA
rahult@cs.rochester.edu

Abstract We demonstrate the applicability of the polynomial degree bound technique to notions such as the nonexistence of Turing-hard sets in some relativized world, (non)uniform gap-definability, and relativized separations. This way, we settle certain open questions of Hemaspaandra, Ramachandran & Zimand [HRZ95] and Fenner, Fortnow & Kurtz [FFK94], extend results of Hemaspaandra, Jain & Vereshchagin [HJV93] and construct oracles achieving desired results.

Keywords: Polynomial degree bounds, complexity classes, Turing hardness, gap-definability, relativization theory

1. Introduction

1.1 Background

In this paper, we are concerned with degree bounds of polynomials representing (not necessarily boolean) functions and their applications in constructing oracles. Polynomials were used in obtaining lower bounds for constant depth

*Due to page limitations, we do not include the proofs in this paper. A detailed version with all the proofs is available at http://www.cs.rochester.edu/trs/theory-trs.html as TR820 [ST03].

†Research supported in part by a grant from the DAAD and by DFG project RO 1202/9-1. Work done in part while visiting the University of Rochester.
‡Research supported in part by grant NSF-INT-9815095/DAAD-315-PPP-gü-ab.

circuits [Smo87, AB00], proving upper bounds on the power of complexity classes [Tod91, TO92], proving closure properties of counting classes [BRS95], proving bounds on the number of queries to compute a boolean function in the quantum black-box computing model [BBC$^+$01], and in the construction of oracles in complexity theory [Tar91, dGV02, FFKL03]. See Beigel [Bei93] and Regan [Reg97] for nice surveys on the application of polynomials in circuit complexity and computational complexity theory.

In relativization theory, the technique of using degree bounds of polynomials has been extensively used in constructing oracles that separate complexity classes (see, for instance [Tar91, Bei94, dGV02]). Beigel, Buhrman and Fortnow [BBF98] and Fenner et al. [FFKL03] showed that degree bounds of polynomials can be used to obtain relativized collapses as well. In particular, [BBF98] used polynomials to construct an oracle $\mathcal{A}$ such that $\mathrm{P}^{\mathcal{A}} = \oplus\mathrm{P}^{\mathcal{A}}$ and $\mathrm{NP}^{\mathcal{A}} = \mathrm{EXP}^{\mathcal{A}}$, and [FFKL03] showed that relative to an $\mathcal{SP}$-generic oracle, AWPP (a class defined in Section 2) equals P. We demonstrate the applicability of the polynomial degree bound technique to notions such as the nonexistence of Turing-hard sets in some relativized world, (non)uniform gap-definability, and relativized separations. Before stating our contributions, we give an overview of gap-definable counting classes which will be of interest to us in the paper.

1.2 Gap-definable Counting Classes

In this paper, we will study the relativized complexity of gap-definable counting classes using lower and upper bounds on the degree of polynomials representing certain functions. Informally speaking, a gap-definable counting class is a collection of all sets such that, for any set in the class, the membership of a string in the set depends (in a way particular to the class) on the gap (difference) between the number of accepting and rejecting paths produced by some nondeterministic polynomial-time Turing machine associated with the set. (See Section 2 for the definition of classes and Figure 1 for the inclusion relationship between classes mentioned here.) Gap-definable classes like LWPP and AWPP are, for instance, interesting because of their relevance to quantum computing: LWPP is the best known classical upper bound for EQP (a quantum analog of P) and AWPP is the best known classical upper bound for BQP (a quantum analog of BPP) [FR99]. Thus the investigation of gap-definable classes may shed light on the structure of the quantum classes EQP and BQP. The gap-definable class SPP is low for several counting classes including PP, $\mathrm{C}_{=}\mathrm{P}$ and $\mathrm{Mod}_k\mathrm{P}$, and is known to contain an important natural problem—the graph isomorphism problem [AK02].

1.3 Our Contributions

The existence of complete sets in a class is a topic of interest in complexity theory. Though classes like NP, $\mathrm{C_{=}P}$ and PP possess polynomial-time many-one complete sets, for several other natural classes like UP, BPP, etc., no complete set (under any weak enough to be interesting notion of reducibility) is known. This motivates the investigation of completeness for these promise classes in relativized worlds. That line of research was pursued in several papers [Sip82, HH88, HJV93]. In particular, Hemaspaandra, Jain and Vereshchagin [HJV93] showed that there is an oracle relative to which $\mathrm{UP} \cap \mathrm{coUP}$, UP, FewP and Few have no polynomial-time Turing complete sets. The existence of a relativized world where promise classes like SPP, LWPP, WPP and AWPP do not have complete sets has been unresolved for a long time [HRZ95]. We use the method of symmetrization, introduced by Minsky and Papert [MP88], combined with a result from approximation theory [EZ64, RC66] to construct a relativized world in which AWPP has no polynomial-time Turing hard set for $\mathrm{UP} \cap \mathrm{coUP}$. As a corollary we obtain that none of the classes SPP, LWPP, WPP and AWPP have Turing complete sets in some relativized world. This settles an open question in [HRZ95] and extends one of the main results in [HJV93]. Using a similar, though somewhat indirect, technique we construct another relativized world where AWPP has no polynomial-time Turing hard set for ZPP. The crux in both the proofs involves proving a *lower bound* on the degree of a univariate polynomial. We note that similar techniques have been used in proving a lower bound on the degree of univariate polynomials in [Bei94, NS94, BBC$^+$01].

Fenner, Fortnow and Kurtz [FFK94] showed that SPP is low for every uniformly gap-definable class (see Section 4 for the definition of uniform and nonuniform gap-definability). Thus SPP is low for each of PP, $\mathrm{C_{=}P}$, $\mathrm{Mod}_k\mathrm{P}$, and itself. Both LWPP and WPP are known to be nonuniformly gap-definable and, prior to this paper, it was an open question whether or not these classes are uniformly gap-definable. Thus [FFK94] asked whether SPP is also low for LWPP or WPP. We give a relativized answer to their question by exhibiting an oracle relative to which $\mathrm{UP} \cap \mathrm{coUP}$ is not low for LWPP as well as for WPP. We further relate showing the existence of a relativized world where SPP is not low for a relativized class $\mathcal{C}$ to proving that $\mathcal{C}$ is not uniformly gap-definable. As a consequence, we settle an open question of [FFK94] that both LWPP and WPP are not uniformly gap-definable.

Certain classes are known to be weak in some relativized worlds while their composition with themselves lead to powerful classes in every relativized world. $\mathrm{C_{=}P}$ is a class that is immune to RP in a relativized world [STT03], but its composition with itself, i.e. $\mathrm{C_{=}P}^{\mathrm{C_{=}P}}$, contains the polynomial-time hierarchy in every relativized world. (In fact, $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}[1]} \subseteq \mathrm{UP}^{\mathrm{C_{=}P}} \subseteq \mathrm{C_{=}P}^{\mathrm{C_{=}P}}$.)

Since ZPP $\not\subseteq$ WPP in some relativized world [STT03] and relative to an oracle WPP is not self-low (present paper), it is interesting to ask whether WPP, a class similar to $\mathrm{C_{=}P}$, behaves in the same way as $\mathrm{C_{=}P}$ when composed with itself. We use properties of low degree multilinear polynomials to construct an oracle world in which ZPP is not contained in $\mathrm{WPP}^{\mathrm{WPP}}$; thus we falsify this intuition. We also use an upper bound on the approximate degree of a boolean function to construct an oracle relative to which NP $\cap$ coNP $\not\subseteq$ AWPP.

The proof technique that we use is quite general and is applicable also to classes that are not known to be gap-definable. For instance, we use the degree lower bound of polynomials in constructing a relativized world where MIP $\cap$ coMIP has no polynomial-time Turing hard set for ZPP. This result can be viewed as an extension of a result from [HJV93], that states that relative to an oracle, IP $\cap$ coIP has no polynomial-time Turing hard set for ZPP.

2. Preliminaries

Let $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{Z}$ denote the set of positive integers, real numbers and integers, respectively. Our alphabet is $\Sigma = \{0,1\}$. For any set X of variables, and for any polynomial $p \in \mathbb{R}[X]$, $\deg(p)$ denotes the total degree of p. If $f : \{0,1\}^N \to \{0,1\}$ is a boolean function and $p \in \mathbb{R}[y_1, y_2, \ldots, y_N]$ is a multilinear polynomial such that, for every $y_1, y_2, \ldots, y_N \in \{0,1\}$, $f(y_1, y_2, \ldots, y_N) = p(y_1, y_2, \ldots, y_N)$, then p is said to be a polynomial representing f. If p is a smallest degree multilinear polynomial representing a boolean function f, then we use $\deg(f)$ to denote $\deg(p)$, the total degree of p.

We assume throughout the paper that the computation paths of an oracle Turing machine include the answers from the oracle. Given a nondeterministic Turing machine N, computation path ρ and $x \in \Sigma^*$, let $\mathrm{sign}(N, x, \rho) = +1$ if ρ is an accepting path of $N(x)$, and let $\mathrm{sign}(N, x, \rho) = -1$ if $N(x)$ rejects along ρ. Let $\#\mathrm{acc}_{N^A}(x)$ $(\#rej_{N^A}(x))$ denote the number of accepting (rejecting) paths of $N^A(x)$. For any oracle NPTM N and $A \subseteq \Sigma^*$, $gap_{N^A} : \Sigma^* \to \mathbb{Z}$ is defined as follows: for all $x \in \Sigma^*$, $gap_{N^A}(x) = \#\mathrm{acc}_{N^A}(x) - \#rej_{N^A}(x)$. We define the following complexity classes relevant to this paper.

DEFINITION 1
1 *[Gup91, FFK94]* $\mathrm{GapP} = \{g \mid (\exists \mathrm{NPTM}\, N)[g = gap_N]\}$.
2 *[OH93, FFK94]* $\mathrm{SPP} = \{L \mid (\exists g \in \mathrm{GapP})(\forall x \in \Sigma^*)[g(x) \in \{0,1\} \wedge (x \in L \iff g(x) = 1)]$.
3 *[FFK94]* $\mathrm{LWPP} = \{L \mid (\exists g \in \mathrm{GapP})(\exists h \in \mathrm{FP} : 0 \notin \mathrm{range}(h))(\forall x \in \Sigma^*)[g(x) \in \{0, h(0^{|x|})\} \wedge x \in L \iff g(x) = h(0^{|x|})]\}$.
4 *[FFK94]* $\mathrm{WPP} = \{L \mid (\exists g \in \mathrm{GapP})(\exists h \in \mathrm{FP} : 0 \notin \mathrm{range}(h))(\forall x \in \Sigma^*)[g(x) \in \{0, h(x)\} \wedge x \in L \iff g(x) = h(x)]\}$.

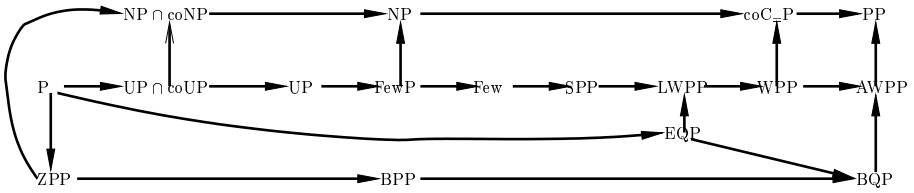

Figure 1. Complexity graph G where a node represents a complexity class and a directed edge (U, V) in G represents the fact that "class U is known to be robustly included in class V."

DEFINITION 2 ([FFKL03, FEN03]) *A language L is in* AWPP *if there exist a $g \in$ GapP, a polynomial p and $\epsilon > 0$ such that, for all $x \in \Sigma^*$,*

$$x \in L \implies \frac{(1+\epsilon)}{2} \leq \frac{g(x)}{2^{p(|x|)}} \leq 1, \text{ and}$$
$$x \notin L \implies 0 \leq \frac{g(x)}{2^{p(|x|)}} \leq \frac{(1-\epsilon)}{2}.$$

The inclusion relationship between classes considered in this paper is summarized in Figure 1. In our proofs, we use an encoding of finite sets (where the sets can be viewed as a source of a possible oracle extension at some stage of the oracle construction) defined in terms of multilinear polynomials with integer coefficients over variables representing the strings in the set. The formal description of our polynomial encoding is given below.

DEFINITION 3 *Let N be a nondeterministic polynomial-time oracle Turing machine with running time $t(.)$. Let $\mathcal{O}, \mathcal{T} \subseteq \Sigma^*$ be such that $\mathcal{O} \cap \mathcal{T} = \emptyset$, and let $x_1, x_2, \ldots, x_m$, where $m = ||\mathcal{T}||$, be the lexicographic enumeration of strings in $\mathcal{T}$. For any $x \in \Sigma^*$, a polynomial encoding of $\mathcal{T}$ w.r.t. $N^{\mathcal{O}}(x)$ is a multilinear polynomial $p \in \mathbb{Z}[y_1, y_2, \ldots, y_m]$ defined as follows: call a computation path ρ of $N^{(.)}(x)$ allowable if along ρ, all queries $q \in \mathcal{O}$ have a "yes" answer, all queries $q \notin \mathcal{O} \cup \mathcal{T}$ have a "no" answer and no query $q \in \mathcal{T}$ is answered in a conflicting way. Let $x_{i_1}, x_{i_2}, \ldots, x_{i_\ell}$ be the distinct queries to strings in $\mathcal{T}$ along an allowable ρ. Create a monomial* $\mathrm{mono}(\rho)$ *that is the product of terms z_{i_k}, $k \in [\ell]$, where $z_{i_k} = y_{i_k}$ if x_{i_k} is answered "yes" and $z_{i_k} = (1 - y_{i_k})$ if x_{i_k} is answered "no" along ρ. Define*

$$p(y_1, y_2, \ldots, y_m) = \sum_{\rho:\rho \text{ is allowable}} \mathrm{sign}(N, x, \rho) \cdot \mathrm{mono}(\rho).$$

The polynomial $p(y_1, y_2, \ldots, y_m)$ has the following properties:

1 for all $\mathcal{B} \subseteq \mathcal{T}$, $p(\chi_{\mathcal{B}}(x_1), \chi_{\mathcal{B}}(x_2), \ldots, \chi_{\mathcal{B}}(x_m)) = gap_{N^{\mathcal{O} \cup \mathcal{B}}}(x)$, and
2 $\deg(p) \leq t(|x|)$.

3. Robust Hardness under Turing Reducibility

Minsky and Papert [MP88] first introduced the technique of symmetrizing a multivariate polynomial $p \in \mathbb{R}[y_1, y_2, \ldots, y_N]$ representing a function $f : \{0,1\}^N \to \mathbb{R}$. A point worth noticing is that symmetrization leads to a symmetric polynomial $p_{sym} \in \mathbb{R}[y_1, y_2, \ldots, y_N]$ with $\deg(p_{sym})$ no more than $\deg(p)$.[1] Thus p_{sym} can be used to exploit the symmetry of f within a subdomain, and thereby to get a lower bound on $\deg(p)$.

DEFINITION 4 *Let $p \in \mathbb{R}[y_1, y_2, \ldots, y_N]$ be a multilinear polynomial. The symmetrization of p is defined by*

$$p_{sym}(y_1, y_2, \ldots, y_N) = \frac{\sum_{\pi \in S_N} p(y_{\pi(1)}, y_{\pi(2)}, \ldots, y_{\pi(N)})}{N!}.$$

LEMMA 5 ([MP88]) *If $p \in \mathbb{R}[y_1, y_2, \ldots, y_N]$ is a multilinear polynomial, then there exists a univariate polynomial $\tilde{p} \in \mathbb{R}[y]$, of degree at most the total degree of p, such that for all $y_1, y_2, \ldots, y_N \in \{0,1\}$, we have*

$$p_{sym}(y_1, y_2, \ldots, y_N) = \tilde{p}(y_1 + y_2 + \cdots + y_N).$$

We use a theorem from [EZ64, RC66] to lower bound the degree of univariate polynomials that satisfy certain constraints. (See also [Bei94, NS94, BBC+01], where the same technique has been used to get a lower bound on the degree of univariate polynomials.)

LEMMA 6 ([EZ64, RC66]) *Let $p \in \mathbb{R}[y]$ be a univariate polynomial with the following properties:*

1 *for any integer $0 \le \ell \le N$, $b_1 \le p(\ell) \le b_2$, and*
2 *for some real $0 \le z \le N$, the derivative of p satisfies $|p'(z)| \ge c$.*

Then $\deg(p) \ge \sqrt{cN/(c + b_2 - b_1)}$.

The proof of Theorem 7 uses Lemma 5 and Lemma 6. We mention that [HJV93] proved, using a different combinatorial technique, that relative to an oracle, FewP contains no polynomial-time Turing hard set for $\mathrm{UP} \cap \mathrm{coUP}$. Theorem 7 extends this result of [HJV93] and implies that there is a relativized world where SPP has no complete sets. That answers a question raised in [HRZ95] positively.

THEOREM 7 *There exists an oracle $\mathcal{A}$ such that $\mathrm{AWPP}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-hard set for $\mathrm{UP}^{\mathcal{A}} \cap \mathrm{coUP}^{\mathcal{A}}$.*

[1] It is well known that symmetrization may lead to a polynomial of total degree strictly smaller than that of the original polynomial. Example: Consider $p(y_1, y_2) = y_1 - y_2$.

COROLLARY 8 *There is an oracle $\mathcal{A}$ such that*

1. *for every complexity class $\mathcal{C} \in \{\mathrm{UP} \cap \mathrm{coUP}, \mathrm{UP}, \mathrm{FewP}, \mathrm{Few}\}$, $\mathcal{C}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-complete set [HJV93], and*
2. *for every complexity class $\mathcal{C} \in \{\mathrm{SPP}, \mathrm{LWPP}, \mathrm{WPP}, \mathrm{AWPP}\}$, $\mathcal{C}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-complete set.*

Through a similar, though somewhat involved, technique we show that there is a relativized world where AWPP has no polynomial-time Turing hard set for ZPP. We also have a more direct proof, that involves proving an *upper bound* on the degree of a certain multilinear polynomial, for a weaker version of Theorem 9—"existence of an oracle relative to which AWPP has no polynomial-time many-one hard set for ZPP."

THEOREM 9 $(\exists \mathcal{A})[\mathrm{AWPP}^{\mathcal{A}}$ *has no* $\leq_T^{p,\mathcal{A}}$*-hard set for* $\mathrm{ZPP}^{\mathcal{A}}]$.

COROLLARY 10 *There is an oracle $\mathcal{A}$ such that*

1. *for every class $\mathcal{C} \in \{\mathrm{ZPP}, \mathrm{RP}, \mathrm{coRP}\}$, $\mathcal{C}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-complete set [HJV93],*
2. *$\mathrm{BPP}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-complete set ([HH88] + [Amb86]), and*
3. *$\mathrm{BQP}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-complete set [FR99].*

Note: We obtained an alternative proof of Theorem 7 and Theorem 9 using a lemma by Vereshchagin [Ver94, Ver99] on proving whether a complexity class has a Turing-hard set for another complexity class. Fortnow and Rogers [FR99] used this lemma to prove that BQP has no polynomial-time Turing hard set for BPP in some relativized world. Since this alternative proof is also of independent interest, we sketch the proof of Theorem 9 in [ST03]. (An alternative proof of Theorem 7 can be obtained in a similar way.)

4. Lowness and Gap-Definability

The low hierarchy within NP was introduced by Schöning [Sch83] to study the inner structure of NP. Since the introduction of the low hierarchy, the concept of lowness has been generalized to arbitrary relativizable function and language classes. We now give a definition of lowness for arbitrary relativizable classes.

DEFINITION 11 (FOLKLORE) *A set $L \subseteq \Sigma^*$ is said to be low for a relativizable class $\mathcal{C}$ if $\mathcal{C}^L \subseteq \mathcal{C}$. A class $\mathcal{C}_2$ is said to be low for a relativizable class $\mathcal{C}_1$, denoted by $\mathcal{C}_1^{\mathcal{C}_2} \subseteq \mathcal{C}_1$ if every set $L \in \mathcal{C}_2$ is low for $\mathcal{C}_1$. If $\mathcal{C}_2$ is also a relativizable class then, for any $\mathcal{O} \subseteq \Sigma^*$, we say that $\mathcal{C}_2$ is low for $\mathcal{C}_1$ relative to the oracle $\mathcal{O}$, denoted by $\mathcal{C}_1^{\mathcal{C}_2^{\mathcal{O}} \oplus \mathcal{O}} \subseteq \mathcal{C}_1^{\mathcal{O}}$, if for every set $L \in \mathcal{C}_2^{\mathcal{O}}$, $\mathcal{C}_1^{L \oplus \mathcal{O}} \subseteq \mathcal{C}_1^{\mathcal{O}}$.*

Fenner, Fortnow and Kurtz [FFK94] introduced the notion of gap-definability to study the counting classes that can be defined using GapP functions alone. Since most of the well-known counting classes, like PP, $\mathrm{coC_{=}P}$, $\mathrm{Mod}_k\mathrm{P}$, etc., are gap-definable, any characterization for gap-definable classes carries over to these counting classes. For instance, it is known that SPP is low for every member of a particular collection of gap-definable classes, namely the collection of uniformly gap-definable classes. Thus, it follows that SPP is low for the counting classes PP, $\mathrm{coC_{=}P}$ and $\mathrm{Mod}_k\mathrm{P}$. The formal definition of gap-definability is given below.

DEFINITION 12 ([FFK94]) *A class $\mathcal{C}$ is gap-definable if there exist disjoint sets $A, R \subseteq \Sigma^* \times \mathbb{Z}$ such that, for any $L \subseteq \Sigma^*$, $L \in \mathcal{C}$ if and only if there exists an* NPTM *N such that for all $x \in \Sigma^*$,*

$$x \in L \Longrightarrow (x, gap_N(x)) \in A, \text{ and } x \notin L \Longrightarrow (x, gap_N(x)) \in R.$$

The class $\mathcal{C}$ is also denoted by Gap(A, R).

For a relativizable class, Fenner, Fortnow and Kurtz [FFK94] introduced two ways of defining gap-definability: uniform and nonuniform. A relativizable class $\mathcal{C}$ is said to be uniformly gap-definable if it is gap-definable w.r.t. any oracle with a fixed (independent of the oracle) choice of A and R. A relativizable class $\mathcal{C}$ is said to be nonuniformly gap-definable if it gap-definable w.r.t. an oracle where the choice of A and R is dependent on the oracle. Thus, the choice of A and R may vary with different oracles in case of nonuniform gap-definability. We now give a definition that expresses the oracle (in)dependence of the pair (A, R) in the notion of gap-definability. In what follows, (A, R) is called an accepting pair if $A, R \subseteq \Sigma^* \times \mathbb{Z}$ and $A \cap R = \emptyset$.

DEFINITION 13 ([FFK94])

1 *We say that a relativizable class $\mathcal{C}$ is gap-definable relative to an oracle $\mathcal{O}$ with accepting pair (A, R) if for any $L \subseteq \Sigma^*$, $L \in \mathcal{C}^{\mathcal{O}}$ if and only if there exists an oracle* NPTM *N such that for all $x \in \Sigma^*$,*

$$x \in L \Longrightarrow (x, gap_{N^{\mathcal{O}}}(x)) \in A, \text{ and } x \notin L \Longrightarrow (x, gap_{N^{\mathcal{O}}}(x)) \in R.$$

2 *We say that a relativizable class $\mathcal{C}$ is uniformly gap-definable with accepting pair (A, R) if for any oracle $\mathcal{O} \subseteq \Sigma^*$, it holds that $\mathcal{C}$ is gap-definable relative to $\mathcal{O}$ with accepting pair (A, R).*

We observe that there is a stronger characterization of uniformly gap-definable classes than the one stated in [FFK94].

OBSERVATION 14 *If $\mathcal{C}$ is a uniformly gap-definable class, then for any $\mathcal{O} \subseteq \Sigma^*$, it holds that $\mathcal{C}^{\mathrm{SPP}^{\mathcal{O}}} = \mathcal{C}^{\mathcal{O}}$.*

In Theorem 17, we construct a relativized world in which $\mathrm{UP} \cap \mathrm{coUP}$ is not low for LWPP as well as for WPP. Since $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{SPP}$ in every relativized world, this also shows that relative to the same oracle, SPP is not low for either of LWPP or WPP. Fenner, Fortnow and Kurtz [FFK94] proved that both LWPP and WPP are nonuniformly gap-definable. However, they leave open the question whether LWPP and WPP are uniformly gap-definable. From Observation 14 and Theorem 17, we conclude that LWPP and WPP are not uniformly gap-definable. Note that the definition of uniform and non-uniform gap-definability involves relativizing a class. Therefore, they are not properties of sets in the class, but rather are the properties of machines characterizing the class. So, proving that WPP and LWPP are not uniformly gap-definable does not imply in any obvious way that these classes separate from any uniformly gap-definable class in the real world.

We use a variant of the prime number theorem, stated in Lemma 15, in the proof of Theorem 17 to estimate the number of primes between two integers.

LEMMA 15 ([RS62]) *For every $n \geq 17$, the number of primes less than or equal to n, $\pi(n)$, satisfies $n/\ln n < \pi(n) < 1.25506\, n/\ln n$.*

The following lemma, Lemma 17, was used in [STT03] to construct a relativized world in which WPP is not closed under polynomial-time Turing reductions. We found the same lemma to be useful in proving Theorem 17.

LEMMA 16 ([STT03]) *Let $N, p \in \mathbb{N}$ be such that p is a prime and $p \leq N/2$. Let $s \in \mathbb{Z}[y_1, y_2, \ldots, y_N]$ be a multilinear polynomial with $\deg(s) < p$. If for some $val \in \mathbb{Z}$, it holds that*

1. *$s(0, 0, \ldots, 0) = 0$, and*
2. *for all $y_1, y_2, \ldots, y_N \in \{0, 1\}$ with $\sum_{i=1}^{N} y_i = p$, $s(y_1, y_2, \ldots, y_N) = val$*

then $p \mid val$.

THEOREM 17 $(\exists \mathcal{A})[\mathrm{LWPP}^{\mathrm{UP}^{\mathcal{A}} \cap \mathrm{coUP}^{\mathcal{A}}} \not\subseteq \mathrm{WPP}^{\mathcal{A}}]$.

COROLLARY 18 LWPP *and* WPP *are not uniformly gap-definable.*

COROLLARY 19 *There is a relativized world $\mathcal{A}$ such that (1) for any class $\mathcal{C} \in \{\mathrm{UP} \cap \mathrm{coUP}, \mathrm{UP}, \mathrm{FewP}, \mathrm{Few}, \mathrm{SPP}, \mathrm{LWPP}\}$, $\mathcal{C}^{\mathcal{A}}$ is not low for $\mathrm{LWPP}^{\mathcal{A}}$, and (2) for any class $\mathcal{C} \in \{\mathrm{UP} \cap \mathrm{coUP}, \mathrm{UP}, \mathrm{FewP}, \mathrm{Few}, \mathrm{SPP}, \mathrm{LWPP}, \mathrm{WPP}\}$, $\mathcal{C}^{\mathcal{A}}$ is not low for $\mathrm{WPP}^{\mathcal{A}}$.*

5. Relativized Noninclusion

Beigel [Bei94] constructed an oracle relative to which $\mathrm{P}^{\mathrm{NP}} \not\subseteq \mathrm{PP}$. As a consequence, there is a relativized world in which NP is not low for PP. However,

in contrast to NP, it is not clear whether NP $\cap$ coNP is not low for PP in some relativized world. In [STT03], it was shown that there is an oracle relative to which ZPP is not contained in WPP, a class known to be low for PP. Thus, it follows that relative to the same oracle, NP $\cap$ coNP $\not\subseteq$ WPP. In Theorem 23, we extend this result and show that there is a relativized world where NP $\cap$ coNP $\not\subseteq$ AWPP, where AWPP is a class known to be low for PP. This supports our belief that NP $\cap$ coNP might not be low for PP in a suitable relativized world. The proof of Theorem 23 uses a property of low-degree multilinear polynomials over rings given by Tarui (Lemma 20), and the notion of approximate degree of boolean functions. The use of approximate degree of a boolean function in Theorem 23 is inspired by the proof of Theorem 6.13 (AWPP has polynomial certificate complexity) in [FFKL03]. Fenner et. al. [FFKL03] used this theorem to show that relative to an $\mathcal{SP}$-generic G, $\mathrm{P}^G = \mathrm{NP}^G \cap \mathrm{coNP}^G = \mathrm{AWPP}^G$.

LEMMA 20 ([TAR91]) *Let $\mathcal{R}$ be a ring. Let s be a multilinear polynomial in $\mathcal{R}[y_1, y_2, \ldots, y_N]$ of total degree at most d and let i be a nonnegative integer such that $0 \leq i \leq i + d \leq N$ and $s(y_1, y_2, \ldots, y_N) = 0$ for each $y_1, y_2, \ldots, y_N \in \{0, 1\}$ satisfying $i \leq \sum_{j=1}^{N} y_j \leq i + d$. Then, $s \equiv 0$.*

DEFINITION 21 ([NS94]) *Given a boolean function $f : \{0,1\}^N \to \{0,1\}$ and a polynomial $p \in \mathbb{R}[y_1, \ldots, y_N]$, we say that p approximates f if there exists $0 \leq \epsilon < 1/2$ such that, for every $y_1, \ldots, y_N \in \{0,1\}$, $|f(y_1, \ldots, y_N) - p(y_1, \ldots, y_N)| \leq \epsilon$. The approximate degree of f, denoted by $\widetilde{\deg}(f)$, is the minimum integer d such that there is a polynomial of degree d that approximates f.*

Nisan and Szegedy [NS94] showed that both the degree and the decision tree complexity of a boolean function is polynomially related to its approximate degree. We use Lemma 22 to obtain an upper bound on the degree of boolean functions in the proof of Theorem 23.

LEMMA 22 ([NS94, BBC+01]) *There is a constant c such that, for any boolean function f, $\widetilde{\deg}(f) \leq \deg(f) \leq D(f) \leq c \cdot \widetilde{\deg}(f)^6$.*

THEOREM 23 $(\exists \mathcal{A})[\mathrm{NP}^{\mathcal{A}} \cap \mathrm{coNP}^{\mathcal{A}} \not\subseteq \mathrm{AWPP}^{\mathcal{A}}]$.

Certain classes are not very powerful in some relativized worlds, however their composition with themselves are found to be more powerful classes in every relativized world. For instance, [STT03] showed the existence of a relativized world in which RP is immune to $\mathrm{C_{=}P}$. But $\mathrm{C_{=}P}^{\mathrm{C_{=}P}}$ is known to contain the polynomial-time hierarchy in every relativized world. In fact in every relativized world, $\mathrm{UP}^{\mathrm{C_{=}P}}$ and $\mathrm{ZPP}^{\mathrm{C_{=}P}}$, which are subclasses of $\mathrm{C_{=}P}^{\mathrm{C_{=}P}}$,

contain the polynomial-time hierarchy. Using Torán's [Tor91] combinatorial technique, [STT03] constructed an oracle relative to which $\mathrm{ZPP} \not\subseteq \mathrm{WPP}$. Corollary 19 shows that there is a relativized world where WPP is not self-low, and so we cannot conclude directly from [STT03] that ZPP is not contained in $\mathrm{WPP}^{\mathrm{WPP}}$ relative to an oracle. Therefore, it is interesting to ask whether or not WPP exhibits a similar behavior as its superclass $\mathrm{C}_{=}\mathrm{P}$. That is, whether $\mathrm{WPP}^{\mathrm{WPP}}$ is as big a class as to contain the polynomial-time hierarchy in every relativized world. We show in Theorem 24 that this is not the case by constructing a relativized world in which ZPP is not contained in $\mathrm{WPP}^{\mathrm{WPP}}$. The proof of Theorem 24 uses Lemma 20.

THEOREM 24 $(\exists \mathcal{A})[\mathrm{ZPP}^{\mathcal{A}} \not\subseteq \mathrm{WPP}^{\mathrm{WPP}^{\mathcal{A}}}]$.

For any $k \in \mathbb{N}$, let WPP^k denote the k^{th} level of WPP hierarchy formed by composing WPP with itself up to k levels. The proof of Theorem 24 can be easily extended to show the following general result: $(\forall k \in \mathbb{N})(\exists \mathcal{A})[\mathrm{ZPP}^{\mathcal{A}} \not\subseteq \mathrm{WPP}^{k,\mathcal{A}}]$.

6. Extensions to Other Classes

In this section, we demonstrate the technique of using degree lower bound of polynomials in constructing relativized worlds for classes defined by probabilistic oracle Turing machines. Hemaspaandra, Jain and Vereshchagin [HJV93] showed that relative to an oracle, IP ∩ coIP has no polynomial-time Turing hard set for ZPP. We extend their result in Theorem 27 by constructing an oracle world where MIP ∩ coMIP has no polynomial-time Turing hard set for ZPP. In the proof, we use the characterization of MIP in terms of oracle proof systems as given by Fortnow, Rompel and Sipser [FRS94]. Note that in the real world (i.e., relative to $\emptyset$ as an oracle) $\mathrm{MIP}^{\emptyset} \cap \mathrm{coMIP}^{\emptyset} = \mathrm{NEXP} \cap \mathrm{coNEXP}$ and so, $\mathrm{MIP}^{\emptyset} \cap \mathrm{coMIP}^{\emptyset}$ contains polynomial-time Turing hard set for $\mathrm{ZPP}^{\emptyset} = \mathrm{ZPP}$. It follows that Theorem 27 does not hold in the real world.

DEFINITION 25 ([FRS94]) *We say that a set L has an oracle proof system if there exists a probabilistic polynomial-time oracle Turing machine N such that for all $x \in \Sigma^*$,*

$$x \in L \implies (\exists \mathcal{Q} \subseteq \Sigma^*) \left[\mathrm{Prob}[N^{\mathcal{Q}}(x) \textit{ accepts }] \geq 1 - 2^{|x|}\right] \textit{ and}$$

$$x \notin L \implies (\forall \mathcal{Q} \subseteq \Sigma^*) \left[\mathrm{Prob}[N^{\mathcal{Q}}(x) \textit{ accepts }] \leq 2^{-|x|}\right],$$

where the probability is over the random coin tosses done by N.

The next Theorem says that the class of sets accepted by multiprover interactive protocols (MIP) is the same as the one which contains sets that are accepted by oracle proof systems.

THEOREM 26 ([FRS94]) *A set L is accepted by an oracle proof system if and only if L is accepted by a multiprover interactive protocol.*

Since the proof of Theorem 26 relativizes, it suffices to construct a relativized world where no oracle proof system accepts a set that is Turing hard for ZPP. We construct such a relativized world in the next theorem.

THEOREM 27 *There exists an oracle $\mathcal{A}$ such that $\mathrm{MIP}^{\mathcal{A}} \cap \mathrm{coMIP}^{\mathcal{A}}$ has no $\leq_T^{p,\mathcal{A}}$-hard set for $\mathrm{ZPP}^{\mathcal{A}}$.*

COROLLARY 28 *There is an oracle relative to which*

1. ZPP, RP, coRP, $\mathrm{IP} \cap \mathrm{coIP}$ *have no polynomial-time Turing complete sets [HJV93],*
2. $\mathrm{BPP}^{\mathcal{A}}$ *has no $\leq_T^{p,\mathcal{A}}$-complete set ([HH88] + [Amb86]), and*
3. $\mathrm{MIP} \cap \mathrm{coMIP}$ *has no polynomial-time Turing complete sets.*

7. Conclusions

In this paper, we apply certain complexity measures (degree, approximate degree) of functions in the context of relativization theory. Likewise, Fenner et al. [FFKL03] and Vereshchagin [Ver94, Ver99] have used (related measures) certificate complexity and decision tree complexity, respectively, in constructing relativized worlds. It would be interesting to explore more connections between complexity measures of a function and relativization theory.

Acknowledgments

We are grateful to Lane Hemaspaandra for his encouragement, advice and guidance throughout the project. We thank Mayur Thakur for stimulating discussions.

References

[AB00] N. Alon and R. Beigel. Lower bounds for approximations by low degree polynomials over $\mathbb{Z}_m$. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity*, pages 184–187, Los Alamitos, CA, June 18–21 2000. IEEE Computer Society.

[AK02] V. Arvind and P. Kurur. Graph isomorphism is in SPP. In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science*, pages 743–750, Los Alamitos, November 16–19 2002. IEEE Computer Society.

[Amb86] K. Ambos-Spies. A note on complete problems for complexity classes. *Information Processing Letters*, 23(5):227–230, 1986.

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48, 2001.

[BBF98] R. Beigel, H. Buhrman, and L. Fortnow. NP might not be as easy as detecting unique solutions. In *Proceedings of the 30th ACM Symposium on Theory of Computing*, pages 203–208. ACM Press, May 1998.

[Bei93] R. Beigel. The polynomial method in circuit complexity. In *Proceedings of the 8th Structure in Complexity Theory Conference*, pages 82–95, San Diego, CA, USA, May 1993. IEEE Computer Society Press.

[Bei94] R. Beigel. Perceptrons, PP, and the polynomial hierarchy. *Computational Complexity*, 4(4):339–349, 1994.

[BRS95] R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. *Journal of Computer and System Sciences*, 50(2):191–202, 1995.

[dGV02] M. de Graaf and P. Valiant. Comparing EQP and $\mathrm{MOD}_{p^k}\mathrm{P}$ using polynomial degree lower bounds. Technical Report quant-ph/0211179, Quantum Physics, 2002.

[EZ64] H. Ehlich and K. Zeller. Schwankung von Polynomen zwischen Gitterpunkten. *Mathematische Zeitschrift*, 86:41–44, 1964.

[Fen03] S. Fenner. PP-lowness and a simple definition of AWPP. *Theory of Computing Systems*, 36(2):199–212, 2003.

[FFK94] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.

[FFKL03] S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder's toolkit. *Information and Computation*, 182(2):95–136, 2003.

[FR99] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[FRS94] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134:545–557, 1994.

[Gup91] S. Gupta. The power of witness reduction. In *Proceedings of the 6th Structure in Complexity Theory Conference*, pages 43–59. IEEE Computer Society Press, June/July 1991.

[HH88] J. Hartmanis and L. Hemachandra. Complexity classes without machines: On complete languages for UP. *Theoretical Computer Science*, 58:129–142, 1988.

[HJV93] L. Hemaspaandra, S. Jain, and N. Vereshchagin. Banishing robust Turing completeness. *International Journal of Foundations of Computer Science*, 4(3):245–265, 1993.

[HRZ95] L. Hemaspaandra, A. Ramachandran, and M. Zimand. Worlds to die for. *SIGACT News*, 26(4):5–15, 1995.

[MP88] M. Minsky and S. Papert. *Perceptrons: An Introduction to Computational Geometry*. MIT Press, Cambridge, Massachusetts, expanded edition, 1988. First edition appeared in 1968.

[NS94] N. Nisan and M. Szegedy. On the degree of boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, 1994.

[OH93] M. Ogiwara and L. Hemachandra. A complexity theory for feasible closure properties. *Journal of Computer and System Sciences*, 46(3):295–325, 1993.

[RC66] T. J. Rivlin and E. W. Cheney. A comparison of uniform approximations on an interval and a finite subset thereof. *SIAM Journal on Numerical Analysis*, 3(2):311–320, June 1966.

[Reg97] K. Regan. Polynomials and combinatorial definitions of languages. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 261–293. Springer-Verlag, 1997.

[RS62] J. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.

[Sch83] U. Schöning. A low and a high hierarchy within NP. *Journal of Computer and System Sciences*, 27:14–28, 1983.

[Sip82] M. Sipser. On relativization and the existence of complete sets. In *Proceedings of the 9th International Colloquium on Automata, Languages, and Programming*, pages 523–531. Springer-Verlag *Lecture Notes in Computer Science #140*, 1982.

[Smo87] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on Theory of Computing*, pages 77–82. ACM Press, May 1987.

[ST03] H. Spakowski and R. Tripathi. Degree bounds on polynomials and relativization theory. Technical Report TR820, Department of Computer Science, University of Rochester, November 2003.

[STT03] H. Spakowski, M. Thakur, and R. Tripathi. Quantum and classical complexity classes: Separations, collapses, and closure properties. In *Proceedings of the 23rd Conference on FSTTCS*, pages 375–386. Springer-Verlag *Lecture Notes in Computer Science #2914*, December 2003.

[Tar91] J. Tarui. Degree complexity of boolean functions and its applications to relativized separations. In *Proceedings of the 6th Annual Conference on Structure in Complexity Theory (SCTC '91)*, pages 285–285, Chicago, IL, USA, June 1991. IEEE Computer Society Press.

[TO92] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 21(2):316–328, 1992.

[Tod91] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[Tor91] J. Torán. Complexity classes defined by counting quantifiers. *Journal of the ACM*, 38(3):753–774, 1991.

[Ver94] N. Vereshchagin. Relativizable and nonrelativizable theorems in the polynomial theory of algorithms. *Russian Academy of Sciences–Izvestiya–Mathematics*, 42(2):261–298, 1994.

[Ver99] Nikolai K. Vereshchagin. Relativizability in complexity theory. In *L.D. Beklemishev, M. Pentus, and N. Vereshchagin, Provability, Complexity, Grammars*, volume 192 of *2*, pages 87–172. AMS Translations, 1999.