On Unique Satisfiability and the Threshold Behavior of Randomized Reductions

Richard Chang[†]
Cornell University

Jim Kadin[‡]
University of Maine

Pankaj Rohatgi[†]
Cornell University

Abstract

The research presented in this paper is motivated by the following new results on the complexity of the unique satisfiability problem, USAT.

- if USAT $\equiv^{\mathrm{P}}_{\mathrm{m}} \overline{\mathrm{USAT}}$, then $\mathrm{D^P} = \text{co-}\mathrm{D^P}$ and PH collapses.
- if USAT $\in$ co-$\mathrm{D^P}$, then PH collapses.
- if USAT has OR_ω, then PH collapses.

The proofs of these results use only the fact that USAT is complete for $\mathrm{D^P}$ under randomized reductions—even though the probability bound of these reductions may be low. Furthermore, these results show that the structural complexity of USAT and of $\mathrm{D^P}$ many-one complete sets are very similar, and so they lend support to the argument that even sets complete under "weak" randomized reductions can capture the properties of the many-one complete sets.

However, under these "weak" randomized reductions, USAT is complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$ as well, and in this case, USAT does not capture the properties of the sets many-one complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$. To explain this anomaly, the concept of the *threshold behavior* of randomized reductions is developed. Tight bounds on the thresholds are shown for NP, co-NP, $\mathrm{D^P}$and co-$\mathrm{D^P}$. Furthermore, these results can be generalized to give upper and lower bounds on the thresholds for the Boolean Hierarchy. These upper bounds are expressed in terms of Fibonacci numbers.

1 Introduction

Traditionally, researchers have defined randomized reductions without giving much consideration to the error probability that the reduction is required to achieve. Typically, the reduction is required to behave correctly for a constant fraction of the random trials, but sometimes the probability is as low as inverse polynomial.

In this paper, we examine randomized reductions under a new light. We find that in many situations there is a right definition — especially when one considers *completeness* under randomized reductions. Intuitively, when the probability of a correct reduction taking place is too low, even trivial sets can be complete under randomized reductions. Conversely, if the probability of correctness is required to be very high, then randomized reductions behave like many-one reductions. Hence, the complete languages under this kind of randomized reductions would have a complexity that is representative of the complexity of the entire class. (The meaning of trivial and representative will be made clear.) Presumably, at some exact point, the probability of correctness is just

[†] Department of Computer Science, Cornell University, Ithaca, NY 14853. Supported in part by NSF Research Grant CCR-88-23053.

[‡] Department of Computer Science, University of Maine, Orono, ME 04469.

high enough to make the definition right. We call this point the *threshold*. It turns out that this threshold is different for different complexity classes. In this paper, we give tight upper and lower bounds on the thresholds for NP, co-NP, $\mathrm{D^P}$ and co-$\mathrm{D^P}$. These results are consequences of some new theorems about the complexity of USAT, the Unique Satisfiability problem. We show that

- if USAT $\equiv_{\mathrm{m}}^{\mathrm{P}}$ $\overline{\mathrm{USAT}}$, then $\mathrm{D^P}$ = co-$\mathrm{D^P}$ and PH collapses.
- if USAT $\in$ co-$\mathrm{D^P}$, then PH collapses.
- if USAT has OR_ω, then PH collapses.

We also generalize these results to the levels of the Boolean Hierarchy and of the Query Hierarchy, where we give upper and lower bounds on the thresholds.

We begin this paper with an historical review of the role of randomized reductions in the complexity of the class $\mathrm{D^P}$ and the Unique Satisfiability problem. We show that the often quoted statement "USAT is complete for $\mathrm{D^P}$ under randomized reductions" can give misleading results about the complexity of optimization problems, because under the same type of randomized reductions, USAT is complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$ as well. Next, we show that thresholds are natural concepts for the classes NP and co-NP. The probability thresholds for NP and co-NP can be identified by some simple observations. Then, we go on to prove that the threshold probability is $1/\mathit{poly}$ for $\mathrm{D^P}$ and $1/2 + 1/\mathit{poly}$ for co-$\mathrm{D^P}$. Finally, we generalize these results to higher levels of the Boolean Hierarchy. We prove a lower bound on the threshold for BH_k of $1 - 2/k$ and an upper bound of $1 - 1/\mathcal{F}_k + 1/\mathit{poly}$, where $\mathcal{F}_k$ is the k^{th} Fibonacci number.

2 An Historical Account

From the beginning, the study of the complexity of unique satisfiability has been tied to the class $\mathrm{D^P}$ and to randomized reductions. Papadimitriou and Yannakakis [15] first defined $\mathrm{D^P}$ to study the complexity of the facets of polytopes and the complexity of optimization problems such as MAX-k-CLIQUE.

Definition: We define $\mathrm{D^P}$, co-$\mathrm{D^P}$and their $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages SAT$\wedge\overline{\mathrm{SAT}}$ and $\overline{\mathrm{SAT}}\vee$SAT.

$$\begin{aligned} \mathrm{D^P} &= \{\ L_1 \cap \overline{L_2} \mid L_1, L_2 \in \mathrm{NP}\ \} \\ \text{co-}\mathrm{D^P} &= \{\ \overline{L_1} \cup L_2 \mid L_1, L_2 \in \mathrm{NP}\ \} \end{aligned}$$

$$\begin{aligned} &\mathrm{SAT}\wedge\overline{\mathrm{SAT}} = \{\ (F_1, F_2) \mid F_1 \in \mathrm{SAT} \text{ and } F_2 \in \overline{\mathrm{SAT}}\ \} \\ &\overline{\mathrm{SAT}}\vee\mathrm{SAT} = \{\ (F_1, F_2) \mid F_1 \in \overline{\mathrm{SAT}} \text{ or } F_2 \in \mathrm{SAT}\ \}. \end{aligned}$$

The set of uniquely satisfiable Boolean formulas, USAT, is contained in $\mathrm{D^P}$. So, the natural question to ask is: Can USAT be complete for $\mathrm{D^P}$? Blass and Gurevich [5] answered this question partially. They noticed that

$$\begin{aligned} \text{USAT is } \leq_{\mathrm{m}}^{\mathrm{P}}\text{-complete for } \mathrm{D^P} &\iff \mathrm{SAT}\wedge\overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT} \\ &\iff \mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT}. \end{aligned}$$

So, the question of whether USAT can be $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for $\mathrm{D^P}$ hinges on whether there is a $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction from SAT to USAT. Then, they showed that there are oracle worlds where no such reduction can exist. This meant a non-relativizing proof technique would be needed to answer the question—a formidable obstacle, indeed.

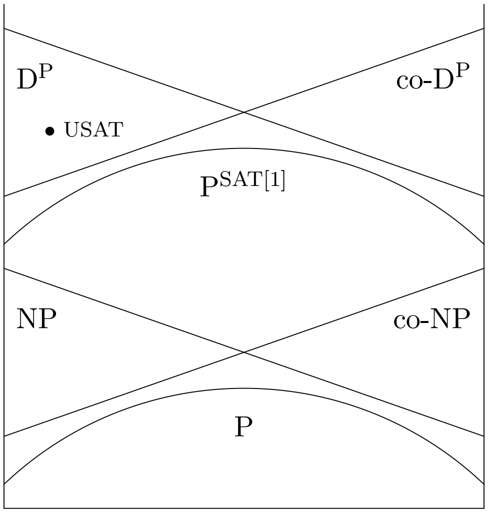

Figure 1: USAT and related complexity classes.

Valiant and Vazirani [20] did not surmount this obstacle, but they did manage to circumvent it. They were able to construct a *randomized reduction* from SAT to USAT. More precisely, they constructed a polynomial time function f such that

$$x \in \text{SAT} \Longrightarrow \text{Prob}_z[\ f(x,z) \in \text{USAT}\ ] \geq \frac{1}{4|x|}$$
$$x \notin \text{SAT} \Longrightarrow \text{Prob}_z[\ f(x,z) \notin \text{USAT}\ ] = 1.$$

Thus, USAT becomes complete for D^P under randomized reductions[1]. However, this variety of randomized reduction is not quite satisfying, because the probability of the reduction being correct can approach zero as the length of x increases. One would have expected a probability bound of 1/2 (in keeping with the Adleman-Manders [1] definition). The justification for the Valiant-Vazirani definition is that in many situations the probability bound can be amplified, in which case, the definitions would be equivalent. Before we continue, we need to introduce some notation and terminology to facilitate our discussion of randomized reductions with different probability bounds.

Definition: We say that A randomly reduces to B (written $A \leq_\text{m}^\text{rp} B$) with probability δ, if there exists a polynomial time function f and a polynomial bound q such that

$$x \in A \Longrightarrow \text{Prob}_z[\ f(x,z) \in B\ ] \geq \delta$$
$$x \notin A \Longrightarrow \text{Prob}_z[\ f(x,z) \notin B\ ] = 1,$$

where z is chosen uniformly over $\{0,1\}^{q(n)}$.

Using this terminology, Valiant and Vazirani showed that SAT randomly reduces to USAT with probability $1/(4n)$. As a special case, we will write $A \leq_\text{m}^\text{vv} B$ if $A \leq_\text{m}^\text{rp} B$ with probability $1/p(n)$ for some polynomial bound p. We will reserve the term "the Valiant-Vazirani reduction" to name the randomized reduction from SAT to USAT. Similarly, the Adleman and Manders definition of randomized reductions would be randomized reductions with probability 1/2. Also, in statements

[1] Valiant and Vazirani credit Alan Selman for this application of their randomized reduction.

where the exact probability bound is not important, we will use the terms $1/\mathit{poly}$ and $1/\mathit{exp}$ to indicate that the statement holds for any inverse polynomial and inverse exponential function. As we mentioned before, under certain conditions, $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions and randomized reductions with probability 1/2 are equivalent.

Definition: For any language B, we define the following classes.

$$\begin{aligned}\mathrm{OR}_2(B) &= \{\ \langle x, y\rangle \mid x \in B \text{ or } y \in B\ \}\\ \mathrm{OR}_\omega(B) &= \{\ \langle x_1, \ldots, x_n\rangle \mid \text{for some } i, 1 \leq i \leq n,\ x_i \in B\ \}\\ \mathrm{AND}_2(B) &= \{\ \langle x, y\rangle \mid x \in B \text{ and } y \in B\ \}\\ \mathrm{AND}_\omega(B) &= \{\ \langle x_1, \ldots, x_n\rangle \mid \text{for all } i, 1 \leq i \leq n,\ x_i \in B\ \}.\end{aligned}$$

If $\mathrm{OR}_2(B) \leq_{\mathrm{m}}^{\mathrm{P}} B$ via some polynomial time function, then we say that B has an OR_2 function, or simply that B has OR_2. We use the same terminology for OR_ω, AND_2 and AND_ω. If a language B has OR_ω, then it is possible to amplify the probability bound of a $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction to B. Thus, when B has OR_ω, $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions and $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions with high probability are equivalent.

Fact 1 If $A \leq_{\mathrm{m}}^{\mathrm{vv}} B$ and B has OR_ω, then $A \leq_{\mathrm{m}}^{\mathrm{rp}} B$ with probability $1 - 1/\mathit{exp}$.

Robust languages such as SAT and $\overline{\mathrm{SAT}}$ have both OR_ω and AND_ω. So, in cases where one randomly reduces to a robust language, it does not matter which definition of randomized reduction is used. However, there are some good reasons to believe that USAT does not have OR_ω (see Corollary 8). Thus, there is no obvious way to amplify the Valiant-Vazirani reduction from SAT to USAT. In the next section, we investigate some anomalies created by the non-robustness of USAT.

3 Anomalous Behavior

The first and most obvious problem with the statement "USAT is complete for $\mathrm{D^P}$ under randomized reductions" is that it fails to consider that USAT can be complete for larger classes as well. In fact, a simple observation will show that USAT is $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete for a much larger class, $\mathrm{P}^{\mathrm{SAT}[\log n]}$. $\mathrm{P}^{\mathrm{SAT}[\log n]}$ is the class of languages accepted by polynomial time Turing machines which ask at most $O(\log n)$ queries to the SAT oracle. Introduced by Papadimitriou and Zachos [16], $\mathrm{P}^{\mathrm{SAT}[\log n]}$ captures problems such as Sat-Mod-k, Clique-Mod-k, Unique Optimal Clause Satisfiability, Unique Optimal Clique and other problems related to optimal solution sizes of many NP optimization problems. [11, 13].

Lemma 1. USAT is $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$.

Proof: Using the fact that $\mathrm{OR}_\omega(\mathrm{SAT}\wedge\overline{\mathrm{SAT}})$ is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$, observe that there is a trivial $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction from $\mathrm{OR}_\omega(\mathrm{SAT}\wedge\overline{\mathrm{SAT}})$ to $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$. On input $\langle x_1, \ldots, x_n\rangle$, the reduction chooses $1 \leq i \leq n$ at random and prints out x_i. This randomized reduction will succeed with probability $1/n$. So, combined with the Valiant-Vazirani reduction, we get a $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction from $\mathrm{OR}_\omega(\mathrm{SAT}\wedge\overline{\mathrm{SAT}})$ to USAT with probability $1/(4n^2)$. □

There is compelling evidence that the classes $\mathrm{P}^{\mathrm{SAT}[\log n]}$ and $\mathrm{D^P}$ have very different structural properties. For example, $\mathrm{P}^{\mathrm{SAT}[\log n]}$ is closed under complementation, but $\mathrm{D^P}$ cannot equal co-$\mathrm{D^P}$ unless PH collapses [8, 10]. Also, all $\mathrm{P}^{\mathrm{SAT}[\log n]}$ $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages have OR_ω, but $\mathrm{D^P}$ $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages cannot have OR_2 unless PH collapses [9]. Since we expect complete sets to inherit structural properties of the classes they represent, USAT being $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete for both these classes raises doubts as to whether completeness under $\leq_{\mathrm{m}}^{\mathrm{vv}}$ reductions makes sense. Lemma 1 can also give misleading results about the complexity of certain optimization problems. For instance, it implies that all the Unique Optimization problems in $\mathrm{P}^{\mathrm{SAT}[\log n]}$ can be reduced to Unique Satisfiability. At first glance, this appears to highlight the power of randomization. After all, it shows that using randomization one can solve optimization problems without doing optimization. However, the probability of a correct reduction taking place is only $1/(4n^2)$. Moreover, there is no known way to improve this probability bound (see Corollary 8). In fact, this lemma really demonstrates the anomalies created by randomized reductions that allow very low probability bounds.

One might hope that these anomalies would disappear if we used only the Adleman-Manders definition of randomized reductions. However, in the next section, we will show that even if we restrict our attention to $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions with probability 1/2, anomalies can still happen. First, we must explain what *threshold behavior* means.

4 Threshold Behavior

Considering the anomalous behavior of randomized reductions described above, the reader may be tempted to dismiss completeness under randomized reductions as meaningless. However, the $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction from SAT to USAT proved to be useful in many areas of research. For example, Richard Beigel [4] used it to show that SAT is superterse unless RP = NP. Also, Toda [19] used a similar reduction in his proof that $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}[1]}$. This result, in turn, led to the Lund, Fortnow, Karloff and Nisan [14] result: $\mathrm{PH} \subseteq \mathrm{IP}$. So, there should be little doubt in the reader's mind regarding the usefulness of the Valiant-Vazirani reduction. The more pertinent questions are: What does this reduction mean? Does USAT being $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete for D^{P} mean that it is somehow representative of the whole class? How does the complexity of $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete sets compare with the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages? We answer these questions in terms of *thresholds* of probability bounds.

4.1 Examples of Threshold Behavior

To illustrate what we mean by threshold behavior, we turn to a more familiar setting—namely that of NP and co-NP. Let A be any $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete set for NP. Then, we know that A has the following properties [1, 23, 6, 18].

- $A \notin \mathrm{P}$, unless RP = NP and PH collapses.
- $A \notin \mathrm{RP}$, unless RP = NP and PH collapses.
- $A \notin \text{co-NP}$, unless NP/*poly* = co-NP/*poly* and PH collapses.

This compares favorably with the many-one complete set SAT, for which we know the following.

- SAT $\notin$ P, unless P = NP.
- SAT $\notin$ RP, unless RP = NP and PH collapses.
- SAT $\notin$ co-NP, unless NP = co-NP.

From this comparison, we can draw the conclusion that the $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete set, A, behaves like the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete set, SAT, and that the complexity of the set A is representative of the complexity of the entire class NP.

In contrast, the trivial singleton set $B = \{1\}$ is complete for NP under randomized reductions with probability 2^{-n}. Clearly, B is not representative of the complexity of NP. So, completeness under $\leq_{\rm m}^{\rm rp}$-reductions with probability 2^{-n} does not make sense for NP. However, they *do* make sense for co-NP. Let C be a set complete for co-NP under $\leq_{\rm m}^{\rm rp}$-reductions with probability 2^{-n}. Then, $C \notin$ NP, unless NP = co-NP.

These results show that completeness for randomized reductions make sense only if the randomized reductions have a probability bound above a certain threshold. Moreover, the threshold is different for different complexity classes. For NP, the threshold is $1/poly$; for co-NP, $1/exp$. Alternatively, we can look at these results in terms of randomized reductions from a set to its complement.

- SAT $\leq_{\rm m}^{\rm rp} \overline{\rm SAT}$ with probability 2^{-n}.
- SAT $\not\leq_{\rm m}^{\rm rp} \overline{\rm SAT}$ with probability $1/p(n)$, for any polynomial $p(n)$, unless NP/*poly* = co-NP/*poly* and PH collapses.

These two statements show that when we consider randomized functions which reduce SAT to $\overline{\rm SAT}$, a probability threshold occurs at $1/poly$. Similarly, for $\overline{\rm SAT}$, the probability threshold occurs at $1/exp$.

- There is no known $\leq_{\rm m}^{\rm rp}$-reduction from $\overline{\rm SAT}$ to SAT with probability greater than 0.
- $\overline{\rm SAT} \not\leq_{\rm m}^{\rm rp}$ SAT with probability $2^{-p(n)}$, for any polynomial $p(n)$, unless NP = co-NP.

4.2 Threshold Behavior in the classes $\mathbf{D^P}$ and co-$\mathbf{D^P}$

In this section, we show how probability thresholds can explain the anomaly presented in Section 3. Recall that SAT$\wedge\overline{\rm SAT}$ and $\overline{\rm SAT}\vee$SAT are the $\leq_{\rm m}^{\rm P}$-complete sets for $\rm D^P$ and co-$\rm D^P$, respectively. We will show that beyond a certain probability threshold, the $\leq_{\rm m}^{\rm rp}$-complete sets for $\rm D^P$ and for co-$\rm D^P$ have many of the properties of the $\leq_{\rm m}^{\rm P}$-complete sets. Some of these properties are [8, 9, 10]:

- SAT$\wedge\overline{\rm SAT} \not\equiv_{\rm m}^{\rm P} \overline{\rm SAT}\vee$SAT, unless $\rm D^P$ = co-$\rm D^P$ and PH collapses.
- SAT$\wedge\overline{\rm SAT} \notin$ co-$\rm D^P$ and $\overline{\rm SAT}\vee$SAT $\notin \rm D^P$, unless $\rm D^P$ = co-$\rm D^P$ and PH collapses.
- SAT$\wedge\overline{\rm SAT}$ does not have $\rm OR_2$, unless $\rm D^P$ = co-$\rm D^P$ and PH collapses.
- $\overline{\rm SAT}\vee$SAT does not have $\rm AND_2$, unless $\rm D^P$ = co-$\rm D^P$ and PH collapses.

We will use these properties as a benchmark to test if a particular concept of completeness for $\rm D^P$ and co-$\rm D^P$ makes sense. First, we show that for completeness under $\leq_{\rm m}^{\rm rp}$-reductions, the probability threshold for $\rm D^P$ is bounded below by 2^{-n}.

Lemma 2. $\overline{\rm SAT}$ is complete for $\rm D^P$ under $\leq_{\rm m}^{\rm rp}$-reductions with probability 2^{-n}.

Proof: To reduce $(F_1, F_2) \in$ SAT$\wedge\overline{\rm SAT}$ to $\overline{\rm SAT}$, the reduction guesses a satisfying assignment for F_1. If F_1 is satisfiable, the guess is correct with probability at least 2^{-n}. If a satisfying assignment is found, the reduction simply prints out F_2. Otherwise, it prints out a fixed satisfiable formula. □

Corollary 3. SAT$\wedge\overline{\rm SAT} \leq_{\rm m}^{\rm rp} \overline{\rm SAT}\vee$SAT with probability 2^{-n}.

Since $\overline{\rm SAT} \in$ co-$\rm D^P$ and since $\overline{\rm SAT}$ has $\rm OR_\omega$ and $\rm AND_\omega$, we can safely say that completeness under $\leq_{\rm m}^{\rm rp}$-reductions with probability $1/exp$ does not make sense for $\rm D^P$. The following theorems, show that completeness under $\leq_{\rm m}^{\rm rp}$-reductions starts making sense when the probability bound is $1/poly$. Hence, the probability threshold for $\rm D^P$ is bounded above by $1/poly$.

Theorem 4. $\mathrm{SAT}\wedge\overline{\mathrm{SAT}} \not\leq_{\mathrm{m}}^{\mathrm{vv}} \overline{\mathrm{SAT}}\vee\mathrm{SAT}$, unless $\mathrm{PH} \subseteq \Delta_3^{\mathrm{P}}$.

Proof: Before we go on, we need to define some probabilistic and nonuniform classes.

Definition: For any class $\mathcal{C}$, $A \in \mathrm{BP}\cdot\mathcal{C}$ if there exists $B \in \mathcal{C}$ and a constant $\epsilon > 0$ such that

$$\forall x,\ \mathrm{Prob}_y[\ x \in A \iff (x,y) \in B\ ] > 1/2 + \epsilon.$$

Definition: Let $\mathcal{C}$ be any class of languages and let f be a polynomially bounded function (i.e., there exists k such that $|f(y)| \leq |y|^k + k$). $A \in \mathcal{C}/f$ if there exists $B \in \mathcal{C}$ such that

$$\forall x,\ x \in A \iff (x, f(1^{|x|})) \in B.$$

f is called the advice function and $f(1^{|x|})$ the advice string. Note that the advice string depends only on the length of x. Also, we write $\mathcal{C}/\mathit{poly}$ for the union of $\mathcal{C}/f$ over all possible polynomially bounded advice functions.

The "hard/easy formulas" proof, which showed that $\mathrm{D^P} = \text{co-}\mathrm{D^P}$ implies PH collapses, used the following line of reasoning. Suppose $\mathrm{D^P} = \text{co-}\mathrm{D^P}$, then there is a many-one reduction from $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ to $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$. With the help of an advice function f, this reduction can be converted into a reduction from $\overline{\mathrm{SAT}}$ to SAT. Thus, $\overline{\mathrm{SAT}} \in \mathrm{NP}/f$. Then, by a theorem due to Yap [21], PH collapses to Σ_3^{P}. In the next theorem, we will show that the $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction from $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ to $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ can be converted into an $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction from $\overline{\mathrm{SAT}}$ to SAT (with help from an advice function). It follows that $\overline{\mathrm{SAT}}$ is contained in the rather awkward class $\mathrm{BP}\cdot(\mathrm{NP}/f)$.

Now, suppose there exists a $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction from $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ to $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$. Since $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ has OR_ω, the probability bound of this $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reduction can be amplified by Fact 1.[2] That is, using the disjunctive reduction to combine the results of polynomially many $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions, we can construct a polynomial time function h and a polynomial q such that

$$(F_1,F_2) \in \mathrm{SAT}\wedge\overline{\mathrm{SAT}} \implies \mathrm{Prob}_z[\ h(F_1,F_2,z) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT}\ ] \geq 1 - 2^{-n}$$

$$(F_1,F_2) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT} \implies \mathrm{Prob}_z[\ h(F_1,F_2,z) \in \mathrm{SAT}\wedge\overline{\mathrm{SAT}}\ ] = 1$$

where $n = |(F_1,F_2)|$ and z is chosen uniformly over $\{0,1\}^{q(n)}$.

To prove the theorem, we will construct an advice function f computable in Δ_3^{P} such that $\overline{\mathrm{SAT}} \in \mathrm{BP}\cdot(\mathrm{NP}/f)$. Then, using the techniques in Schöning's proof [18] that $\mathrm{BP}\cdot(\mathrm{NP}/f) \subseteq \mathrm{NP}/\mathit{poly}$ and the fact that f is computable in Δ_3^{P}, $\mathrm{PH} \subseteq \Delta_3^{\mathrm{P}}$.

Now, we construct the advice function f. We call F *easy* if $F \in \overline{\mathrm{SAT}}$ and

$$\exists x, y \text{ such that } |x| = |F|,\ y \in \{0,1\}^{q(n)},\ \pi_2(h(x,F,y)) \in \mathrm{SAT},$$

where π_i is the i^{th} projection function (that is, $\pi_i(x_1,\ldots,x_m) = x_i$). F is called easy in this case because there is "existential evidence" that F is unsatisfiable. If $F \in \overline{\mathrm{SAT}}$ and F is not easy, then we call F a *hard* string. On input 1^n, the advice function simply outputs the lexically smallest hard string of length n if it exists. Otherwise, it outputs the empty string, ε. From the definition of easy, it is clear that checking whether a string is hard is a co-NP question. So, using binary search and an $\mathrm{NP^{NP}}$ oracle, the advice function f can be computed in Δ_3^{P}.

Now, consider the following NP program, N. On input (F,H,z), N treats F as a Boolean formula of length n, takes H as an advice string of length 0 or n, and parses z into a $q(n)$ bit long guess string. (If the input does not conform to this syntax, N rejects outright.) Then, N does the following.

[2] We can prove this theorem without using amplification, but this simplifies the presentation. In the general case, one cannot rely on amplification.

1. If the advice string H is the empty string, then accept if and only if there exists x, $|x| = n$ and $y \in \{0,1\}^{q(n)}$ such that $\pi_2(h(x, F, y)) \in \mathrm{SAT}$.
2. If $|H| = n$, then accept if and only if $\pi_1(h(F, H, z)) \in \mathrm{SAT}$.

<u>CLAIM:</u> The NP program above shows that $\overline{\mathrm{SAT}} \in \mathrm{BP}\cdot(\mathrm{NP}/f)$. That is,

$$\mathrm{Prob}_z[\ F \in \overline{\mathrm{SAT}} \iff N(F, f(1^n), z) \text{ accepts }] \geq 1 - 2^{-n}.$$

Note that whether there is a hard string of length n does not depend on the guess string z. So, we can analyze the program in two cases.

<u>CASE 1:</u> Consider the case where all the strings in $\overline{\mathrm{SAT}}$ of length n are easy—i.e., $f(1^n) = \varepsilon$. If the input $F \in \overline{\mathrm{SAT}}$, then F must also be easy which means the appropriate x and y would be found in step 1. So,

$$F \in \overline{\mathrm{SAT}} \Longrightarrow \mathrm{Prob}_z[\ N(F, \varepsilon, z) \text{ accepts }] = 1.$$

If $F \in \mathrm{SAT}$, then for all x, $(x, F) \in \overline{\mathrm{SAT}} \vee \mathrm{SAT}$. So, by the description of the reduction h,

$$\mathrm{Prob}_z[\ h(x, F, z) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}\ ] = 1.$$

However, $h(x, F, z) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ implies that $\pi_2(h(x, F, z)) \in \overline{\mathrm{SAT}}$. So, N must reject in step 1. Thus, in the easy case

$$\mathrm{Prob}_z[\ F \in \overline{\mathrm{SAT}} \iff N(F, \varepsilon, z) \text{ accepts }] = 1.$$

<u>CASE 2:</u> Suppose the advice string H is a hard string of length n. If $F \in \overline{\mathrm{SAT}}$, then $(F, H) \in \overline{\mathrm{SAT}} \vee \mathrm{SAT}$. By the description of the reduction h,

$$\mathrm{Prob}_z[\ h(F, H, z) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}\ ] = 1.$$

So, for all z, $\pi_1(h(F, H, z)) \in \mathrm{SAT}$. Therefore, for all z, N will accept in step 2 and

$$F \in \overline{\mathrm{SAT}} \Longrightarrow \mathrm{Prob}_z[\ N(F, H, z) \text{ accepts }] = 1.$$

If $F \in \mathrm{SAT}$, then $(F, H) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ because H is hard implies that $H \in \overline{\mathrm{SAT}}$. Also, since H is hard,

$$\forall x, |x| = n,\ \forall z, z \in \{0,1\}^{q(n)},\ \pi_2(h(x, H, z)) \in \overline{\mathrm{SAT}}.$$

Therefore, for all choices of z, we know that

$$h(F, H, z) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}} \iff \pi_1(h(F, H, z)) \in \mathrm{SAT}.$$

Moreover, by the description of h and the fact that $(F, H) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$,

$$\mathrm{Prob}_z[\ h(F, H, z) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}\ ] \leq 2^{-n}.$$

So, $\mathrm{Prob}_z[\ \pi_1(h(F, H, z)) \in \mathrm{SAT}\ ] \leq 2^{-n}$. Thus,

$$F \in \mathrm{SAT} \Longrightarrow \mathrm{Prob}_z[\ N(F, H, z) \text{ accepts }] < 2^{-n}. \qquad \square$$

An immediate corollary of Theorem 4 is that completeness under $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions *does* make sense for $\mathrm{D^P}$. Moreover, we can show that languages complete for $\mathrm{D^P}$ under $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions have properties very similar to the properties of the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language $\mathrm{SAT} \wedge \overline{\mathrm{SAT}}$.

Theorem 5. Let A be complete for $\mathrm{D^P}$ under $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions. Then,

1. $A \not\equiv_{\mathrm{m}}^{\mathrm{P}} \overline{A}$, unless $\mathrm{PH} \subseteq \Delta_3^{\mathrm{P}}$.
2. $A \notin \text{co-}\mathrm{D^P}$, unless $\mathrm{PH} \subseteq \Delta_3^{\mathrm{P}}$.
3. A does not have OR_ω, unless $\mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$.

Proof (Sketch): Parts 1 and 2 follow from Theorem 4. The proof of part 3 is similar to the proof of Theorem 4. Simply note that if A has OR_ω, then there is an $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction from $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ to $\mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ with very high probability. This condition is sufficient to mimic the proof that $\overline{\mathrm{SAT}}\vee\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{SAT}\wedge\overline{\mathrm{SAT}} \Longrightarrow$ PH collapses. See Theorem 11. □

As a special case of a language $\leq_{\mathrm{m}}^{\mathrm{vv}}$-complete for $\mathrm{D^P}$, USAT has all the properties listed above. However, since $\overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{P}}$ USAT the results can be made stronger. We list these properties separately, because these results give a new understanding about the complexity of USAT.

Theorem 6. $\mathrm{USAT} \not\equiv_{\mathrm{m}}^{\mathrm{P}} \overline{\mathrm{USAT}}$, unless $\mathrm{D^P} = \text{co-}\mathrm{D^P}$ and $\mathrm{PH} \subseteq \Delta_3^{\mathrm{P}}$.

Proof: Since $\overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{P}} \mathrm{USAT}$, $\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{P}} \overline{\mathrm{USAT}}$. However, we assumed that $\mathrm{USAT} \equiv_{\mathrm{m}}^{\mathrm{P}} \overline{\mathrm{USAT}}$, so SAT $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduces to USAT as well. Thus, USAT becomes $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for $\mathrm{D^P}$, so $\mathrm{D^P} = \text{co-}\mathrm{D^P}$ and the Polynomial Hierarchy collapses to Δ_3^{P} by Kadin [10]. □

Corollary 7. $\mathrm{USAT} \notin \text{co-}\mathrm{D^P}$, unless $\mathrm{PH} \subseteq \Delta_3^{\mathrm{P}}$.

Corollary 8. USAT does not have OR_ω, unless $\mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$.

So, we can conclude that Valiant and Vazirani made right decision when they used $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions to talk about completeness for $\mathrm{D^P}$ under randomized reductions. However, completeness under $\leq_{\mathrm{m}}^{\mathrm{vv}}$-reductions may not make sense for other complexity classes. In fact, the following theorems show that the threshold for co-$\mathrm{D^P}$ is $1/2 + 1/poly$.

Lemma 9. $\mathrm{SAT}\oplus\overline{\mathrm{SAT}}$ is complete for co-$\mathrm{D^P}$ under $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions with probability $1/2 + 2^{-n^2}$.

Proof (Sketch): Recall that $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$ is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for co-$\mathrm{D^P}$and that

$$\mathrm{SAT}\oplus\overline{\mathrm{SAT}} = \{\ 0F \mid F \in \mathrm{SAT}\ \} \cup \{\ 1F \mid F \in \overline{\mathrm{SAT}}\ \}.$$

It is simple to construct a randomized reduction with probability greater than or equal to 1/2, because

$$(F_1, F_2) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT} \iff F_1 \in \overline{\mathrm{SAT}} \text{ or } F_2 \in \mathrm{SAT}.$$

Thus, a randomized function can choose F_1 or F_2 with equal probability, then output $1F_1$ or $0F_2$. If (F_1, F_2) is indeed an element of $\overline{\mathrm{SAT}}\vee\mathrm{SAT}$, then $\mathrm{Prob}_{i\in\{0,1\}}[\ iF_{2-i} \in \mathrm{SAT}\oplus\overline{\mathrm{SAT}}\ ] \geq 1/2$. On the other hand, if $(F_1, F_2) \notin \overline{\mathrm{SAT}}\vee\mathrm{SAT}$, then $\mathrm{Prob}_{i\in\{0,1\}}[\ iF_{2-i} \in \mathrm{SAT}\oplus\overline{\mathrm{SAT}}\ ] = 0$. To improve the probability beyond 1/2, simply observe that if $F_2 \in \mathrm{SAT}$, then there is a small probability of finding a satisfying assignment through random guessing. This fact can be used to improve the probability to $1/2 + 2^{-n^2}$. □

Corollary 10. $\overline{\mathrm{SAT}}\vee\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ with probability $1/2 + 2^{-n^2}$.

Since $\mathrm{SAT}\oplus\overline{\mathrm{SAT}} \in \mathrm{D^P}$, we again conclude that this set does not meet our criteria for a sensible complete language. However, if we require the reduction to have a probability bound above $1/2 + 1/\mathit{poly}$, then completeness makes sense.

Theorem 11. $\overline{\mathrm{SAT}}\vee\mathrm{SAT} \not\leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ with probability $1/2 + 1/p(n)$, for any polynomial $p(n)$, unless $\mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$.

Proof: We are given a polynomial time function h and a polynomial bound q such that

$$(F_1, F_2) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT} \implies \mathrm{Prob}_z[\ h(F_1, F_2, z) \in \mathrm{SAT}\wedge\overline{\mathrm{SAT}}\ ] \geq \frac{1}{2} + \frac{1}{p(n)}$$
$$(F_1, F_2) \in \mathrm{SAT}\wedge\overline{\mathrm{SAT}} \implies \mathrm{Prob}_z[\ h(F_1, F_2, z) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT}\ ] = 1,$$

where $n = |(F_1, F_2)|$ and z is chosen uniformly over $\{0,1\}^{q(n)}$.

Again, we use a variation of the hard/easy proof technique [10] to prove this lemma. We call a string F *easy* if $F \in \overline{\mathrm{SAT}}$ and

$$\exists x,\ |x| = |F|,\ \mathrm{Prob}_z[\ \pi_2(h(x, F, z)) \in \mathrm{SAT}\ ] \geq \frac{1}{2},$$

where π_i is the i^{th} projection function. We call F a *hard* string if $F \in \overline{\mathrm{SAT}}$ and F is not *easy.* We construct an advice function f which on input 1^n outputs the lexically smallest hard string of length n, if it exists. Thus, on input F our advice string can either be the empty string ε (which means that there is no hard string of length $|F|$) or some string H of length $|F|$.

Now, we construct an NP machine N. On input (F, ε, x, z), N accepts iff $\pi_2(h(x, F, z)) \in \mathrm{SAT}$. Otherwise, if the input is of the form (F, H, x, z), where $H \neq \varepsilon$, then N accepts iff $\pi_1(h(F, H, z) \in \mathrm{SAT}$. Note that in the second case, the output of the machine N is independent of x.

Analysis: Given F there are two cases, depending on the advice string.

Case 1: In this case, the advice string is empty. Since $H = f(1^{|F|}) = \varepsilon$, we know that all strings of size $|F|$ which are in $\overline{\mathrm{SAT}}$ are *easy.* Thus, if $F \in \overline{\mathrm{SAT}}$ then F is easy. Therefore,

$$\exists x,\ |x| = |F|,\ \mathrm{Prob}_z[\ \pi_2(h(x, F, z)) \in \mathrm{SAT}\ ] \geq \frac{1}{2},$$

which implies $\exists x$, $|x| = |F|$, such that $\mathrm{Prob}_z[\ N(F, \varepsilon, x, z)$ accepts $] \geq 1/2$.

If, on the other hand, $F \in \mathrm{SAT}$, then $\forall x, (x, F) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT}$. Thus, by the random reduction, $h(x, F, z) \in \mathrm{SAT}\wedge\overline{\mathrm{SAT}}$ with probability $1/2 + 1/p(n)$. So,

$$\forall x,\ |x| = |F|, \mathrm{Prob}_z[\ \pi_2(h(x, F, z)) \in \overline{\mathrm{SAT}}\ ] \geq \frac{1}{2} + \frac{1}{p(n)}.$$

That is, $\forall x$, $|x| = |F|$, $\mathrm{Prob}_z[\ N(F, \varepsilon, x, z)$ accepts $] < 1/2 - 1/p(n)$.

Case 2: In the second case, the advice is not empty. By construction, H is a *hard* string of size n, which implies $H \in \overline{\mathrm{SAT}}$. If $F \in \overline{\mathrm{SAT}}$ then $(F, H) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT}$ and by the definition of the random reduction h,

$$\mathrm{Prob}_z[\ \pi_1(h(F, H, z)) \in \mathrm{SAT}\ ] \geq \frac{1}{2} + \frac{1}{p(n)}.$$

For the sake of uniformity, we use a dummy quantifier and state that

$$\exists x,\ |x| = |F|,\ \mathrm{Prob}_z[\ \pi_1(h(F,H,z)) \in \mathrm{SAT}\ ] \geq \frac{1}{2} + \frac{1}{p(n)},$$

(since $\pi_1(h(F,H,z)) \in \mathrm{SAT}$ is independent of x). This allows us to say

$$\exists x,\ |x| = |F|,\ \mathrm{Prob}_z[\ N(F,H,x,z) \text{ accepts }\ ] \geq \frac{1}{2} + \frac{1}{p(n)}.$$

Conversely, if $F \in \mathrm{SAT}$ then $(F,H) \in \mathrm{SAT}\wedge\overline{\mathrm{SAT}}$, and by the definition of h we know that

$$\mathrm{Prob}_z[\ h(F,H,z) \in \overline{\mathrm{SAT}}\vee\mathrm{SAT}\ ] = 1.$$

However, H is a hard string. Thus, $\forall x,\ |x| = |H|,\ \mathrm{Prob}_z[\ \pi_2(h(x,H,z)) \in \mathrm{SAT}\ ] < 1/2$. In particular, $\mathrm{Prob}_z[\ \pi_2(h(F,H,z)) \in \mathrm{SAT}\ ] < 1/2$. Therefore, $\mathrm{Prob}_z[\ \pi_1(h(F,H,z)) \in \overline{\mathrm{SAT}}\ ] \geq 1/2$, which implies $\mathrm{Prob}_z[\ \pi_1(h(F,H,z)) \in \mathrm{SAT}\ ] < 1/2$. Again, by adding an additional dummy quantifier, we obtain

$$\forall x,\ |x| = |F|,\ \mathrm{Prob}_z[\ N(F,H,x,z) \text{ accepts }\ ] < \frac{1}{2}.$$

To summarize, we have shown that N behaves in the following manner. If $f(1^{|F|}) = H = \varepsilon$, then

$$F \in \overline{\mathrm{SAT}} \Longrightarrow \exists x,\ \mathrm{Prob}_z[\ N(F,H,x,z) \text{ accepts }\ ] \geq \frac{1}{2}$$

$$F \in \mathrm{SAT} \Longrightarrow \forall x,\ \mathrm{Prob}_z[\ N(F,H,x,z) \text{ accepts }\ ] \leq \frac{1}{2} - \frac{1}{p(n)}.$$

If $f(1^{|F|}) = H \neq \varepsilon$, then

$$F \in \overline{\mathrm{SAT}} \Longrightarrow \exists x,\ \mathrm{Prob}_z[\ N(F,H,x,z) \text{ accepts }\ ] \geq \frac{1}{2} + \frac{1}{p(n)}$$

$$F \in \mathrm{SAT} \Longrightarrow \forall x,\ \mathrm{Prob}_z[\ N(F,H,x,z) \text{ accepts }\ ] < \frac{1}{2},$$

where $x \in \{0,1\}^{|F|}$, $z \in \{0,1\}^{q(n)}$ and $n = |(F,F)|$. These conditions show that there is a *nonuniform* Merlin-Arthur-Merlin game [2] for $\overline{\mathrm{SAT}}$. As we will see in Appendix B, they are also sufficient to show that co-NP $\subseteq$ BP$\cdot$(NP/*poly*). Finally, since BP$\cdot$(NP/*poly*) $\subseteq$ NP/*poly*, co-NP $\subseteq$ NP/*poly*. Then, by Yap's theorem [21], the Polynomial Hierarchy collapses to Σ_3^{P}. □

Now we can show that the languages complete for co-D$^{\mathrm{P}}$ under $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions with probability beyond the threshold of $1/2 + 1/$*poly* have many properties enjoyed by the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages for co-D$^{\mathrm{P}}$.

Theorem 12. Let A be complete for co-D$^{\mathrm{P}}$ under $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions with probability $1/2 + 1/p(n)$, for some polynomial p. Then,

1. $A \not\equiv_{\mathrm{m}}^{\mathrm{P}} \overline{A}$, unless PH $\subseteq \Delta_3^{\mathrm{P}}$.
2. $A \notin \mathrm{D}^{\mathrm{P}}$, unless PH $\subseteq \Sigma_3^{\mathrm{P}}$.
3. A does not have AND$_2$, unless PH $\subseteq \Delta_3^{\mathrm{P}}$.

Proof: Parts 1 and 3 follow from Theorem 4 and Part 2 follows from Theorem 11. □

5 The Boolean Hierarchy

5.1 Some Properties

The Boolean Hierarchy (BH) is the closure of NP and co-NP under Boolean operations [7]. Like the Polynomial Hierarchy, the k^{th} level of this hierarchy consists of two complementary classes BH_k and co-BH_k. It follows from definition that $\mathrm{BH}_1 = \mathrm{NP}$ and $\mathrm{BH}_2 = \mathrm{D^P}$. We will use BL_k and co-BL_k to denote the canonical $\leq_\mathrm{m}^\mathrm{P}$-complete languages for BH_k and co-BH_k, respectively. (See Appendix A.)

It has been shown that $\mathrm{BH}_k \neq$ co-BH_k, unless PH collapses [8, 10]. In this section, we look for the probability threshold of randomized reductions that preserve this structure. That is, we insist that randomized reductions should not be able to reduce BL_k to co-BL_k. So far, we have discussed $\leq_\mathrm{m}^\mathrm{rp}$-completeness of BH_1, co-BH_1, BH_2 and co-BH_2. For ease of presentation and completeness, we now consider randomized reductions with two-sided error.

Definition: $A \leq_\mathrm{m}^\mathrm{bpp} B$ with probability ε, if there exists a polynomial time function f such that

$$\mathrm{Prob}_z[\ x \in A \iff f(x,z) \in B\ ] \geq \varepsilon$$

where z is chosen uniformly at random from $\{0,1\}^{q(|x|)}$, for some polynomial q.

As it turns out, $\leq_\mathrm{m}^\mathrm{bpp}$-reductions in the classes BH_1, co-BH_1, BH_2 and co-BH_2 exhibit threshold behaviors in much the same way that $\leq_\mathrm{m}^\mathrm{rp}$-reductions do. For example, the trivial singleton set $\{1\}$ is complete for NP under $\leq_\mathrm{m}^\mathrm{bpp}$-reductions with probability $1/2 + 1/exp$. So, the $\leq_\mathrm{m}^\mathrm{bpp}$-threshold for NP is bounded below by $1/2+1/exp$. Moreover, by the results of Boppana, Håstad and Zachos, $\overline{\mathrm{SAT}} \not\leq_\mathrm{m}^\mathrm{bpp} \mathrm{SAT}$ with probability $1/2 + 1/poly$, unless PH collapses [6, 23]. So, the $\leq_\mathrm{m}^\mathrm{bpp}$-threshold for NP is between $1/2+1/exp$ and $1/2+1/poly$. Since $\leq_\mathrm{m}^\mathrm{bpp}$-reductions are symmetrical, this is also the probability threshold for co-NP. In Lemma 13 and Theorem 14, we establish that the $\leq_\mathrm{m}^\mathrm{bpp}$-threshold for $\mathrm{D^P}$ and co-$\mathrm{D^P}$ is $2/3 + 1/poly$. (Lemma 13 follows from Lemma 9 and Theorem 14 from Theorem 16.)

Lemma 13. $\mathrm{SAT}\wedge\overline{\mathrm{SAT}} \leq_\mathrm{m}^\mathrm{bpp} \overline{\mathrm{SAT}}\vee\mathrm{SAT}$ with probability $2/3 + 2^{-n^2}$.

Theorem 14. $\mathrm{SAT}\wedge\overline{\mathrm{SAT}} \not\leq_\mathrm{m}^\mathrm{bpp} \overline{\mathrm{SAT}}\vee\mathrm{SAT}$ with probability $2/3 + 1/p(n)$, for any polynomial $p(n)$, unless PH collapses.

5.2 Fibonacci Numbers

In this section, we show that at the higher levels of the Boolean Hierarchy randomized reductions continue to exhibit threshold behavior. The next lemma shows that below the probability threshold, BL_{2k} can be randomly reduced to the simpler language BL_{2k-2}.

Lemma 15. $\mathrm{BL}_{2k} \leq_\mathrm{m}^\mathrm{rp} \mathrm{BL}_{2k-2}$ with probability $1 - 1/k$.

Proof: A set is in BH_{2k} iff it can be expressed as a union of k $\mathrm{D^P}$ sets (q.v. normal forms for the Boolean Hierarchy [7]). Thus, we can reduce BL_{2k} to BL_{2k-2} by randomly omitting one of the $\mathrm{D^P}$ sets from the union. This type of reduction works with probability $1 - 1/k$. □

Since $\mathrm{BL}_{2k} \not\leq_\mathrm{m}^\mathrm{P} \mathrm{BL}_{2k-2}$ unless PH collapses, $1 - 1/k$ is a lower bound on the threshold for BH_{2k}. Note that a bound of $1 - 1/k$ implies that the reduction behaves correctly for a large fraction of the random trials. For robust complexity classes, a probability bound of 7/8 or 99/100 may seem reasonable. However, completeness for BH_{2k} under $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions with probability $1 - 1/k$ does not make sense. One can easily extend this lemma to cover all classes in the Boolean Hierarchy and to $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reductions.

The following theorems state that randomized reductions cannot reduce BL_k to its complement with probability above the threshold. The proofs of these theorems rely on complicated *hard/easy* arguments in conjunction with results about nonuniform versions of Merlin-Arthur-Merlin games. Note that the threshold is expressed in terms of *Fibonacci numbers*.[3] The role that the Fibonacci numbers play in these proofs is similar to their role in the proof that Euclid's Algorithm takes the largest number of steps to compute the greatest common divisor of two successive Fibonacci numbers [12]. (The proof of Theorem 16 is presented in Appendix A. The proofs of Theorems 17 and 18 are similar.)

Theorem 16. If $\mathrm{BL}_k \leq_{\mathrm{m}}^{\mathrm{bpp}} \text{co-}\mathrm{BL}_k$ with probability $1 - 1/\mathcal{F}_{k+1} + 1/p(n)$ for some polynomial p, then PH collapses.

Theorem 17. Suppose $\mathrm{BL}_k \leq_{\mathrm{m}}^{\mathrm{rp}} \text{co-}\mathrm{BL}_k$ with probability $1 - \alpha + 1/\mathit{poly}$, where $k \geq 2$ and α is a rational. Let $\ell = 2 * (\lfloor (k-1)/2 \rfloor) + 1$. If $\alpha \leq 1/\mathcal{F}_\ell$ then PH collapses.

Example: Let $k = 4$. Then $\ell = 3$ and $\mathcal{F}_\ell = 3$. Then, we obtain the corollary

$\mathrm{BL}_4 \not\leq_{\mathrm{m}}^{\mathrm{rp}} \text{co-}\mathrm{BL}_4$ with probability $2/3 + 1/\mathit{poly}$, unless PH collapses.

Theorem 18. Suppose $\text{co-}\mathrm{BL}_k \leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{BL}_k$ with probability $1 - \alpha + 1/\mathit{poly}$, where $k \geq 2$ and α is a rational. Let $\ell = 2 * (\lfloor k/2 \rfloor)$. If $\alpha \leq 1/\mathcal{F}_\ell$ then PH collapses.

Example: Let $k = 4$. Then $\ell = 4$ and $\mathcal{F}_\ell = 5$. Then, we obtain the corollary

$\text{co-}\mathrm{BL}_4 \not\leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{BL}_4$ with probability $4/5 + 1/\mathit{poly}$, unless PH collapses.

From these theorems we can conclude that for BH_k and $\text{co-}\mathrm{BH}_k$, completeness under randomized reductions makes sense only when the probabilities are beyond certain thresholds. At higher levels of the Boolean Hierarchy, Lemma 15 and Theorems 16, 17 and 18 provide a range where the actual thresholds lie. Further work will be required to determine the exact values of these thresholds.

5.3 Bounded Query Classes

The bounded query class $\mathrm{P}^{\mathrm{SAT}\|[k]}$ consists of all the languages recognized by polynomial time Turing machines which ask at most k parallel (or non-adaptive) queries to the SAT oracle. Alternatively, it is the class of languages k-truth-table reducible to SAT. The k^{th} level of the Query Hierarchy is the class $\mathrm{P}^{\mathrm{SAT}\|[k]}$. Since the Query Hierarchy is intertwined with the Boolean Hierarchy [3]

$\mathrm{BH}_k \subseteq \mathrm{P}^{\mathrm{SAT}\|[k]} \subseteq \mathrm{BH}_{k+1}$,

the Query Hierarchy has infinitely many levels, unless PH collapses. In other words, we believe that each additional query to SAT allows the machine to recognize new languages. In the Query Hierarchy, we look for randomized reductions which preserve the additional query property. Since the Boolean Hierarchy is closely linked to the bounded query hierarchies, the thresholds for $\mathrm{P}^{\mathrm{SAT}\|[k]}$ can be derived from the thresholds for BH_k and $\text{co-}\mathrm{BH}_k$.

[3] We denote the i^{th} Fibonacci number as $\mathcal{F}_i$ and adopt the convention that $\mathcal{F}_0 = \mathcal{F}_1 = 1$.

The class $\mathrm{P}^{\mathrm{SAT}[\log n]}$, where the machines are allowed $O(\log n)$ serial queries, is the limiting class of the Query Hierarchy. We have shown in Section 3 that $1/\mathit{poly}$ is a lower bound on the threshold. An upper bound on the threshold is $1 - 1/\alpha(n)$ where $\alpha(n)$ is the inverse Ackermann function or any slowly growing function. This is an upper bound because a set, A, complete for $\mathrm{P}^{\mathrm{SAT}[\log n]}$ under this kind of randomized reduction cannot be in the Query Hierarchy, unless PH collapses. These bounds are not very good, since the lower bound tends toward 0 and the upper bound, 1. However, tighter bounds would have to depend on new results on the complexity of $\mathrm{P}^{\mathrm{SAT}[\log n]}$.

References

[1] L. M. Adleman and K. Manders. Reducibility, randomness, and intractibility [*sic*]. In *ACM Symposium on Theory of Computing*, pages 151–163, 1977.

[2] L. Babai and S. Moran. Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36:254–276, 1988.

[3] R. Beigel. Bounded queries to SAT and the Boolean hierarchy. Technical Report 7, Department of Computer Science, The Johns Hopkins University, 1987. To appear in *Theoretical Computer Science.*

[4] R. Beigel. NP-hard sets are p-superterse unless R = NP. Technical Report 4, Department of Computer Science, The Johns Hopkins University, 1988.

[5] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 55(1–3):80–88, 1982.

[6] R. Boppana, J. Håstad, and S. Zachos. Does co-NP have short interactive proofs? *Information Processing Letters*, 25(2):127–132, 1987.

[7] J. Cai, T. Gundermann, J. Hartmanis, L. Hemachandra, V. Sewelson, K. Wagner, and G. Wechsung. The Boolean hierarchy I: Structural properties. *SIAM Journal on Computing*, 17(6):1232–1252, December 1988.

[8] R. Chang and J. Kadin. The Boolean hierarchy and the polynomial hierarchy: a closer connection. In *Proceedings of the 5th Structure in Complexity Theory Conference*, pages 169–178, July 1990.

[9] R. Chang and J. Kadin. On computing Boolean connectives of characteristic functions. Technical Report TR 90-1118, Cornell Department of Computer Science, May 1990. To appear in *Mathematical Systems Theory.*

[10] J. Kadin. The polynomial time hierarchy collapses if the Boolean hierarchy collapses. *SIAM Journal on Computing*, 17(6):1263–1282, December 1988.

[11] J. Kadin. $\mathrm{P}^{\mathrm{NP}[\log n]}$ and sparse Turing complete sets for NP. *Journal of Computer and System Sciences*, 39:282–298, December 1989.

[12] D. E. Knuth. *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming.* Addison-Wesley, Second edition, 1973.

[13] M. W. Krentel. The complexity of optimization problems. *Journal of Computer and System Sciences*, 36(3):490–509, 1988.

[14] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pages 2–10, 1990.

[15] C. Papadimitriou and M. Yannakakis. The complexity of facets (and some facets of complexity). *Journal of Computer and System Sciences*, 28(2):244–259, April 1984.

[16] C. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *Sixth GI Conference on Theoretical Computer Science*, volume 145 of *Lecture Notes in Computer Science*, pages 269–276. Springer-Verlag, 1983.

[17] U. Schöning. *Complexity and Structure*, volume 211 of *Lecture Notes in Computer Science*. Springer-Verlag, 1985.

[18] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, 39(1):84–100, 1989.

[19] S. Toda. On the computational power of PP and $\oplus$P. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pages 514–519, 1989.

[20] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986.

[21] C. Yap. Some consequences of non-uniform conditions on uniform classes. *Theoretical Computer Science*, 26(3):287–300, 1983.

[22] S. Zachos. Probabilistic quantifiers, adversaries, and complexity classes: An overview. In *Structure in Complexity Theory*, volume 223 of *Lecture Notes in Computer Science*, pages 383–400. Springer-Verlag, 1986.

[23] S. Zachos and H. Heller. A decisive characterization of BPP. *Information and Control*, 69(1–3):125–135, 1986.

A Proof of Theorem 16

In this section we give the complete proof of Theorem 16. We will need the following notational devices and definitions.

Notation: Let $\langle x_1, \ldots, x_k \rangle$ be any k-tuple. When the individual strings in the tuple are not significant, we will substitute $\vec{x}$ for $\langle x_1, \ldots, x_k \rangle$. Also, we write $\vec{x}^R$ for $\langle x_k, \ldots, x_1 \rangle$, the reversal of the tuple. Finally, we will use $\{0,1\}^{m \times k}$ to denote the set of k-tuples of strings of length m.

Notation: We will write π_j for the j^{th} projection function, and $\pi_{(i,j)}$ for the function that selects the i^{th} through j^{th} elements of a k-tuple. For example,

$$\pi_j(\langle x_1, \ldots, x_k \rangle) = x_j$$
$$\pi_{(i,j)}(\langle x_1, \ldots, x_k \rangle) = \langle x_i, \ldots, x_j \rangle$$

Definition: We use the following definition for the levels of the Boolean Hierarchy.

$$\mathrm{BH}_1 = \mathrm{NP},$$
$$\mathrm{BH}_{2k} = \{\ L_1 \cap \overline{L_2} \mid L_1 \in \mathrm{BH}_{2k-1} \text{ and } L_2 \in \mathrm{NP}\ \},$$
$$\mathrm{BH}_{2k+1} = \{\ L_1 \cup L_2 \mid L_1 \in \mathrm{BH}_{2k} \text{ and } L_2 \in \mathrm{NP}\ \},$$
$$\text{co-}\mathrm{BH}_k = \{\ L \mid \overline{L} \in \mathrm{BH}_k\ \}.$$

Definition: BL_k and co-BL_k, defined below, are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for BH_k and co-BH_k, respectively.

$$\mathrm{BL}_1 = \mathrm{SAT},$$
$$\mathrm{BL}_{2k} = \{\ \langle x_1, \ldots, x_{2k} \rangle \mid \langle x_1, \ldots, x_{2k-1} \rangle \in \mathrm{BL}_{2k-1} \text{ and } x_{2k} \in \overline{\mathrm{SAT}}\ \},$$
$$\mathrm{BL}_{2k+1} = \{\ \langle x_1, \ldots, x_{2k+1} \rangle \mid \langle x_1, \ldots, x_{2k} \rangle \in \mathrm{BL}_{2k} \text{ or } x_{2k+1} \in \mathrm{SAT}\ \},$$
$$\text{co-}\mathrm{BL}_k = \overline{\mathrm{BL}_k}.$$

We now define a *hard* sequence of formulas.

Definition: Suppose $\mathrm{BL}_k \leq_{\mathrm{m}}^{\mathrm{bpp}}$ co-BL_k with probability $1 - 1/\mathcal{F}_{k+1} + 1/p(n)$ via some polynomial time function h. Then, we call $\langle 1^m, x_1, \ldots, x_j \rangle = \langle 1^m, \vec{x} \rangle$ a *hard sequence* with respect to h if $j = 0$ or if all of the following hold:

1. $1 \leq j \leq k - 1$.

2. $|x_j| = m$.

3. $x_j \in \overline{\mathrm{SAT}}$.

4. $\langle 1^m, x_1, \ldots, x_{j-1} \rangle$ is a hard sequence with respect to h.

5. $\forall \vec{y} = \langle y_1, \ldots, y_\ell \rangle \in \{0,1\}^{m \times \ell}$ $\mathrm{Prob}_z[\ \pi_{\ell+1} \circ h(\vec{y}, \vec{x}^R, z) \in \mathrm{SAT}\ ] < \mathcal{F}_j / \mathcal{F}_{k+1}$ where $\ell = k - j$.

If $\langle 1^m, x_1, \ldots, x_j \rangle$ is a hard sequence, then we refer to j as the *order* of the sequence and say that it is a hard sequence for length m. Also, we will call a hard sequence *maximal* if it cannot be extended to a hard sequence of higher order.

The following lemma shows that given a $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reduction from BL_k to co-BL_k, a hard sequence of order j for length m induces an asymmetric probabilistic reduction from BL_{k-j} to co-BL_{k-j} for tuples of strings of length m.

Lemma 19. Suppose $\mathrm{BL}_k \le_{\mathrm{m}}^{\mathrm{bpp}} \text{co-BL}_k$ with probability $1 - 1/\mathcal{F}_{k+1} + 1/p(n)$ via some function h and $r(n)$ is the size of the random input to h. Let $q(m)$ be the size of the tuples in $\{0,1\}^{m\times k}$, let $t = r(q(m))$ and $\epsilon = 1/p(q(m))$. Then, the following proposition $P(j)$ holds for all j, $0 \le j \le k-1$:

<u>PROPOSITION $P(j)$:</u> Let $\langle 1^m, x_1, \ldots, x_j\rangle = \langle 1^m, \vec{x}\rangle$ be a hard sequence w.r.t. h and let $\ell = k - j$. Then, for all $\vec{y} = \langle y_1, \ldots, y_\ell\rangle \in \{0,1\}^{m\times\ell}$, ℓ is even implies that

$$\vec{y} \in \mathrm{BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}, \vec{x}^R, z) \in \text{co-BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon,$$

$$\vec{y} \in \text{co-BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}, \vec{x}^R, z) \in \mathrm{BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

Also, ℓ is odd implies that

$$\vec{y} \in \text{co-BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}, \vec{x}^R, z) \in \mathrm{BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon,$$

$$\vec{y} \in \mathrm{BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}, \vec{x}^R, z) \in \text{co-BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon,$$

where $g = \pi_{(1,\ell)} \circ h$ and the probability is computed over all z, $|z| = t$.

Proof: (by induction on j)

<u>BASE CASE $P(0)$:</u> This follows trivially from the hypothesis of the lemma and from the fact that $\mathcal{F}_0 = \mathcal{F}_1 = 1$.

<u>INDUCTION CASE $P(j+1)$:</u> Suppose $P(j)$ holds. Let $\ell = k - j$ and let $\langle 1^m, x_1, \ldots, x_{j+1}\rangle = \langle 1^m, \vec{x}\,'\rangle$ be a hard sequence. Consider the cases where ℓ is even or odd separately.

<u>CASE 1:</u> ℓ is even. Since $\langle 1^m, x_1, \ldots, x_j\rangle = \langle 1^m, \vec{x}\rangle$ is also a hard sequence, by the induction hypothesis, for all $\vec{y} = \langle y_1, \ldots, y_\ell\rangle \in \{0,1\}^{m\times\ell}$

$$\vec{y} \in \mathrm{BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}, \vec{x}^R, z) \in \text{co-BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon,$$

$$\vec{y} \in \text{co-BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}, \vec{x}^R, z) \in \mathrm{BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon,$$

where again $g = \pi_{(1,\ell)} \circ h$ and the probability is computed over all z, $|z| = t$. In particular, for $y_\ell = x_{j+1}$ and $\vec{y}\,' = \langle y_1, \ldots, y_{\ell-1}\rangle$ we have

$$\langle y_1, \ldots, y_{\ell-1}, x_{j+1}\rangle \in \mathrm{BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}\,', \vec{x}\,'^R, z) \in \text{co-BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon,$$

$$\langle y_1, \ldots, y_{\ell-1}, x_{j+1}\rangle \in \text{co-BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ g(\vec{y}\,', \vec{x}\,'^R, z) \in \mathrm{BL}_\ell\ ] \ge 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

Using the definitions of BL_ℓ and co-BL_ℓ for even ℓ, for all $\vec{y}\,' = \langle y_1, \ldots, y_{\ell-1}\rangle \in \{0,1\}^{m\times(\ell-1)}$

$$\vec{y}\,' \in \mathrm{BL}_{\ell-1} \text{ and } x_{j+1} \in \overline{\mathrm{SAT}} \Longrightarrow$$
$$\mathrm{Prob}_z\left[\begin{array}{c} \pi_{(1,\ell-1)} \circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{co-BL}_{\ell-1} \\ \text{or } \pi_\ell \circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \mathrm{SAT} \end{array}\right] \ge 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon, \tag{1}$$

and

$$\vec{y}\,' \in \text{co-BL}_{\ell-1} \text{ or } x_{j+1} \in \text{SAT} \implies \text{Prob}_z\left[\begin{array}{c} \pi_{(1,\ell-1)}\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{BL}_{\ell-1} \\ \text{and } \pi_\ell\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \overline{\text{SAT}} \end{array}\right] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon. \tag{2}$$

Since $\langle 1^m, x_1, \ldots, x_{j+1}\rangle$ is a hard sequence, we know conditions 1 and 5 of the definition hold. That is, $x_{j+1} \in \overline{\text{SAT}}$ and for all $\vec{y}\,' = \langle y_1, \ldots, y_{k-j-1}\rangle \in \{0,1\}^{m\times(k-j-1)}$

$$\text{Prob}_z[\ \pi_{k-j}\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{SAT}\ ] < \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}},$$

i.e., for $\ell = k - j$,

$$\text{Prob}_z[\ \pi_\ell\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{SAT}\ ] < \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}.$$

So, if $\vec{y}\,' \in \text{BL}_{\ell-1}$, then by equation (1) and the fact that $x_{j+1} \in \overline{\text{SAT}}$, we have

$$\text{Prob}_z[\ \pi_{(1,\ell-1)}\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{co-BL}_{\ell-1} \text{ or } \pi_\ell\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{SAT}\ ] \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon.$$

Moreover, by condition 5 described above, we can say that

$$\text{Prob}_z[\ \pi_{(1,\ell-1)}\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{co-BL}_{\ell-1}\ ] \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \epsilon - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} = 1 - \frac{\mathcal{F}_{j+2}}{\mathcal{F}_{k+1}} + \epsilon,$$

(since $\mathcal{F}_{j+2} = \mathcal{F}_j + \mathcal{F}_{j+1}$). Conversely, if $\vec{y}\,' \in \text{co-BL}_{\ell-1}$ then equation (2) implies that

$$\text{Prob}_z[\ \pi_{(1,\ell-1)}\circ h(\vec{y}\,', \vec{x}\,'^R, z) \in \text{BL}_{\ell-1}\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

Thus, we have proved $P(j+1)$ for the case when $\ell = k - j$ is even.

CASE 2: $\ell = k - j$ is odd. Using a proof similar to the proof of Case 1 we can show that $P(j+1)$ holds in this case as well. This completes the proof of the Lemma. □

The next lemma states that if $\text{BL}_k \leq_{\text{m}}^{\text{bpp}} \text{co-BL}_k$ with probability $1 - 1/\mathcal{F}_{k+1} + 1/p(n)$, then a *maximal* hard sequence for a given length m allows us to differentiate between the cases where $y \in \overline{\text{SAT}}$ and where $y \in \text{SAT}$ for any formula y of length m.

Lemma 20. Suppose $\text{BL}_k \leq_{\text{m}}^{\text{bpp}} \text{co-BL}_k$ with probability $1 - 1/\mathcal{F}_{k+1} + 1/p(n)$ via some function h and $r(n)$ is the size of the random input to h. Let $\langle 1^m, x_1, \ldots, x_j\rangle = \langle 1^m, \vec{x}\rangle$ be a maximal hard sequence with respect to h, and let $q(m)$ be the size of the tuples in $\{0,1\}^{m\times k}$. Define $t = r(q(m))$, $\epsilon = 1/p(q(m))$ and $\ell = k - j$. Then,

$$y \in \overline{\text{SAT}} \Longrightarrow \exists\ \vec{y}\,' \in \{0,1\}^{m\times(\ell-1)},\ \text{Prob}_z[\ g(\vec{y}\,', y, \vec{x}^R, z) \in \text{SAT}\ ] \geq \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}$$

and

$$y \in \text{SAT} \Longrightarrow \forall\ \vec{y}\,' \in \{0,1\}^{m\times(\ell-1)}, \text{Prob}_z[\ g(\vec{y}\,', y, \vec{x}^R, z) \in \overline{\text{SAT}}\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon$$

where $g = \pi_\ell\circ h$ and the probability is computed over all z, $|z| = t$.

Proof:
Suppose $j = k-1$, i.e., ($\vec{y}\,'$ is the empty sequence). Then, by Lemma 19, for all $y \in \{0,1\}^m$

$$y \in \overline{\mathrm{SAT}} \Longrightarrow \mathrm{Prob}_z[\ \pi_1 \circ h(y, \vec{x}^R, z) \in \mathrm{SAT}\ ] \geq 1 - \frac{\mathcal{F}_{k-1}}{\mathcal{F}_{k+1}} = \frac{\mathcal{F}_k}{\mathcal{F}_{k+1}},$$

and

$$y \in \mathrm{SAT} \Longrightarrow \mathrm{Prob}_z[\ \pi_1 \circ h(y, \vec{x}^R, z) \in \overline{\mathrm{SAT}}\ ] \geq 1 - \frac{\mathcal{F}_k}{\mathcal{F}_{k+1}} + \epsilon.$$

Thus, the lemma holds when $j = k-1$ (i.e. when $\vec{y}\,'$ is the empty sequence).

Consider the case when $j < k-1$. Let $\ell = k - j$. Suppose $y \in \overline{\mathrm{SAT}}$. Since $\langle 1^m, x_1, \ldots, x_j \rangle$ is maximal, $\langle 1^m, x_1, \ldots, x_j, y \rangle$ is not a hard sequence. However, we know that $j+1 \leq k-1$, $|y| = m$, $y \in \overline{\mathrm{SAT}}$ and $\langle 1^m, x_1, \ldots, x_j \rangle$ is a hard sequence. So, $\langle 1^m, x_1, \ldots, x_j, y \rangle$ must fail to be a hard sequence by failing to satisfy condition 5 of the definition of hard sequences. Thus,

$$\exists\ \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)},\ \mathrm{Prob}_z[\ \pi_\ell \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \mathrm{SAT}\ ] \geq \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}.$$

Conversely, suppose $y \in \mathrm{SAT}$. Let $\ell = k - j$. By Lemma 19, for all $\vec{y} \in \{0,1\}^{m \times \ell}$, if ℓ is even:

$$\vec{y} \in \text{co-BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ \pi_{(1,\ell)} \circ h(\vec{y}, \vec{x}^R, z) \in \mathrm{BL}_\ell\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon$$

and if ℓ is odd:

$$\vec{y} \in \mathrm{BL}_\ell \Longrightarrow \mathrm{Prob}_z[\ \pi_{(1,\ell)} \circ h(\vec{y}, \vec{x}^R, z) \in \text{co-BL}_\ell\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

Now let us consider the even and odd cases separately. If ℓ is even, then by the definition of co-BL$_\ell$, we know that $y \in \mathrm{SAT} \Longrightarrow \forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)}$, $\langle \vec{y}\,', y \rangle \in \text{co-BL}_\ell$. Therefore,

$$\forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)},\ \mathrm{Prob}_z[\ \pi_{(1,\ell)} \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \mathrm{BL}_\ell\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

Also, by the definition of BL$_\ell$, we know that $\langle u_1, \ldots, u_\ell \rangle \in \mathrm{BL}_\ell \Longrightarrow u_\ell \in \overline{\mathrm{SAT}}$. Thus,

$$\forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)}, [\ \pi_{(1,\ell)} \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \mathrm{BL}_\ell \Longrightarrow \pi_\ell \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \overline{\mathrm{SAT}}\ ].$$

So, we get the required result

$$\forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)},\ \mathrm{Prob}_z[\ \pi_\ell \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \overline{\mathrm{SAT}}\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

In the other case, when ℓ is odd, by unfolding the definition of BL$_\ell$, we know that $y \in \mathrm{SAT} \Longrightarrow \forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)}$, $\langle \vec{y}\,', y \rangle \in \mathrm{BL}_\ell$. Therefore,

$$\forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)},\ \mathrm{Prob}_z[\ \pi_{(1,\ell)} \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \text{co-BL}_\ell\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

By definition of co-BL$_\ell$ we have that

$$\pi_{(1,\ell)} \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \text{co-BL}_\ell \Longrightarrow \pi_\ell \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \overline{\mathrm{SAT}}.$$

Thus, we get the required result for odd ℓ.

$$\forall \vec{y}\,' \in \{0,1\}^{m \times (\ell-1)},\ \mathrm{Prob}_z[\ \pi_\ell \circ h(\vec{y}\,', y, \vec{x}^R, z) \in \overline{\mathrm{SAT}}\ ] \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \epsilon.$$

This completes the proof of the Lemma. □

Now we are in a position to prove Theorem 16.

Theorem 16. If $\mathrm{BL}_k \le_{\mathrm{m}}^{\mathrm{bpp}} \text{co-}\mathrm{BL}_k$ with probability $1 - 1/\mathcal{F}_{k+1} + 1/p(n)$, for some polynomial p, then PH collapses.

Proof: Using Lemma 20 and given a $\le_{\mathrm{m}}^{\mathrm{bpp}}$-reduction from BL_k to co-BL_k, let f be the advice function gives the lexically smallest maximal *hard* sequence. Define an NP machine N which on input $\langle F, H, \vec{y}, z\rangle$, parses H as $\langle 1^m, x_1, \ldots, x_j\rangle$ where $|x_i| = |F| = m$, divides $\vec{y}$ into $\langle y_1, \ldots, y_{k-j-1}\rangle$ where $|y_i| = m$, and interprets z as bitstring of size t as required by Lemma 20. Then, N accepts iff $\pi_{k-j} \circ h(y_1, \ldots, y_{k-j-1}, F, x_j, \ldots, x_1, z) \in \mathrm{SAT}$. If $H = f(1^{|F|})$ is of order j then by Lemma 20,

$$F \in \overline{\mathrm{SAT}} \Longrightarrow \exists \vec{y} \in \{0,1\}^{m\times(k-j-1)},\ \mathrm{Prob}_z[\ N(F, H, \vec{y}, z) \text{ accepts }] \ge \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}},$$

and

$$F \in \mathrm{SAT} \Longrightarrow \forall \vec{y} \in \{0,1\}^{m\times(k-j-1)},\ \mathrm{Prob}_z[\ N(F, H, \vec{y}, z) \text{ accepts }] \le \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} - \epsilon.$$

Thus, there exists a nonuniform Merlin-Arthur-Merlin game [2] for $\overline{\mathrm{SAT}}$. In the next section of the appendix, we show that this condition collapses PH to Σ_3^{P}. □

B Nonuniform Merlin-Arthur-Merlin Games

A Merlin-Arthur-Merlin game begins with an existential move by Merlin, followed by a probabilistic move by Arthur and another existential move by Merlin. Languages which have Merlin-Arthur-Merlin games are exactly those recognized by $\exists\cdot$BP$\cdot$NP machines. In this section, we prove some technical lemmas which show that under certain assumptions, NP/*poly* = co-NP/*poly* and PH collapses. These lemmas are mostly modifications to familiar theorems in the literature [2]. However, due to the nonuniform nature of the hard/easy argument, it is not possible to cite these theorems directly. We need to show that these theorems hold even for nonuniform probabilistic bounds. The theorems and lemmas in this section are geared towards normalizing probabilistic NP machines so they fit the standard definitions. The first lemma shows that we can always reprogram a probabilistic NP machine so its probability bounds are centered at 1/2.

Lemma 21. Let N be any NP machine. Let A and B be two disjoint events such that for some polynomial q and rational constants α, β and r

$$x \in A \Longrightarrow \mathrm{Prob}_z[\ N(x,z) \text{ accepts }] \geq \alpha$$

$$x \in B \Longrightarrow \mathrm{Prob}_z[\ N(x,z) \text{ accepts }] \leq \beta,$$

where z is chosen uniformly over $\{0,1\}^{q(|x|)}$ and $\alpha - \beta \geq 1/r$. Then, there is an NP machine N', a polynomial q' and a constant r' such that

$$x \in A \Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] \geq \frac{1}{2} + \frac{1}{r'}$$

$$x \in B \Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] \leq \frac{1}{2} - \frac{1}{r'}\ ,$$

where z is chosen uniformly over $\{0,1\}^{q'(|x|)}$.

Proof: The idea of behind the proof is quite simple. Let $m = (\alpha + \beta)/2$. The probabilities α and β are centered around m. We simply have to shift these probabilities so they are centered around 1/2.

First, assume that $m > 1/2$. In this case, the machine N accepts too often, so we simply need to add more cases where the machine rejects. Let $q'(n) = q(n) + c$, where c is roughly twice the number of bits required to specify α and β in binary. The new machine N' does the following on input (x, z) where $|z| = q'(n)$ and $n = |x|$.

1. Divide z into two parts v and w of lengths $q(n)$ and c respectively.
2. Interpret w as a number between 0 and 2^c.
3. If $w/2^c < 1/(2m)$, then simulate $N(x, v)$.
4. Otherwise, reject the input string.

Analysis: Now we claim that N' accepts and rejects with the prescribed probabilities. If $x \in A$, then the probability that $N'(x,z)$ accepts is the probability that N' reaches step 3, simulates $N(x, v)$, and $N(x, v)$ accepts. Thus,

$$x \in A \Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] \geq \frac{\alpha}{2m} \geq \frac{1}{2m}\left(m + \frac{1}{2r}\right) = \frac{1}{2} + \frac{1}{4mr}\ .$$

Similarly, we can calculate the probability that $N'(x,z)$ accepts when $x \in B$.

$$x \in B \Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] \leq \frac{\beta}{2m} \leq \frac{1}{2m}\left(m - \frac{1}{2r}\right) = \frac{1}{2} - \frac{1}{4mr} \ .$$

Thus, if we let $r' = 4r$, we have satisfied the statement of the lemma (since $1/2 < m \leq 1$). Note that in the preceding calculations, we used $1/(2m)$ as the probability that $w/2^c < 1/(2m)$. There is an inherent error in this estimation, but the error can be made arbitrary small by increasing c.

Finally, we consider the case where $m < 1/2$. In this case, we simply need to increase the probability of accepting. So, $N'(x,z)$ would simulate $N(x,v)$ with probability $1/(2-2m)$ and accept outright in the remaining cases. A similar analysis yields:

$$\begin{aligned} x \in A \Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] &\geq 1 - \frac{1}{2-2m} + \frac{\alpha}{2-2m} \\ &= \frac{1}{2} + \frac{1}{4(1-m)r} \end{aligned}$$

$$\begin{aligned} x \in B \Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] &\leq 1 - \frac{1}{2-2m} + \frac{\beta}{2-2m} \\ &= \frac{1}{2} - \frac{1}{4(1-m)r} \ . \end{aligned}$$

Again, since $1/2 < 1 - m \leq 1$, we satisfy the statement of the lemma by letting $r' = 4r$. □

Note that the preceding proof did not use the fact that α and β are constants. In fact, since r' did not depend on m, it is not even necessary for $1/\alpha$ and $1/\beta$ to be polynomially bounded. The only important point is that α and β can be represented in c bits. In order to generalize this lemma, we need the following definition.

Definition: A function γ is a *nice* nonuniform probability bound if there exists a polynomial d such that for all n, $0 \leq \gamma(n) \leq 1$ and $|\gamma(n)| \leq d(n)$.

Using the definition of nice probability bounds, we can restate Lemma 21 as follows. We will not repeat the proof for this lemma because it is a straightforward modification of the proof for Lemma 21.

Lemma 22. Let N be any NP machine and let the functions α and β be nice nonuniform probability bounds. Suppose there exist two disjoint events A and B such that for some polynomial q and r

$$x \in A \Longrightarrow \mathrm{Prob}_z[\ N(x,z) \text{ accepts }] \geq \alpha(n)$$
$$x \in B \Longrightarrow \mathrm{Prob}_z[\ N(x,z) \text{ accepts }] \leq \beta(n),$$

where $n = |x|$, z is chosen uniformly over $\{0,1\}^{q(n)}$ and $\alpha(n) - \beta(n) > 1/r(n)$. Then, there is an NP machine N' and polynomials q' and r' such that

$$x \in A \Longrightarrow \mathrm{Prob}_z[\ N'(x,\alpha(n),\beta(n),z) \text{ accepts }] \geq \frac{1}{2} + \frac{1}{r'(n)}$$
$$x \in B \Longrightarrow \mathrm{Prob}_z[\ N'(x,\alpha(n),\beta(n),z) \text{ accepts }] \leq \frac{1}{2} - \frac{1}{r'(n)} \ ,$$

where $n = |x|$ and z is chosen uniformly over $\{0,1\}^{q'(n)}$.

In the next lemma we use the standard amplification techniques (q.v. Lemma 3.4 in [17]) to achieve very high probabilities.

Lemma 23. Let N be any NP machine. Suppose there exist two disjoint events, A and B, such that for some polynomials q and r

$$\begin{aligned} x \in A &\Longrightarrow \mathrm{Prob}_z[\ N(x,z) \text{ accepts }] \geq \frac{1}{2} + \frac{1}{r(n)} \\ x \in B &\Longrightarrow \mathrm{Prob}_z[\ N(x,z) \text{ accepts }] \leq \frac{1}{2} - \frac{1}{r(n)}\ , \end{aligned}$$

where $n = |x|$ and z is chosen uniformly over $\{0,1\}^{q(n)}$. Then, for any polynomial p, there is an NP machine N' and a polynomial q' such that

$$\begin{aligned} x \in A &\Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] > 1 - 2^{-p(n)} \\ x \in B &\Longrightarrow \mathrm{Prob}_z[\ N'(x,z) \text{ accepts }] < 2^{-p(n)}, \end{aligned}$$

where $n = |x|$ and z is chosen uniformly over $\{0,1\}^{q'(n)}$.

The next lemma gives an alternate characterization of of the class NP/*poly*. It is known that languages which can be characterized by Merlin-Arthur-Merlin games [2] or by the quantifier structure $(\exists\exists^+\exists/\forall\exists^+\forall)$ [22] are in the class BP·NP. Lemma 24 states that the nonuniform versions of such languages are in the class BP·(NP/*poly*) which is the same as the class NP/*poly*.

Lemma 24. Let N be an NP machine and let p, q and r be polynomials. Let the functions α and β be nice nonuniform probability bounds. Suppose that a language L satisfies the following:

$$x \in L \Longrightarrow \exists y\ \mathrm{Prob}_z[\ N(x,y,f(1^n),z) \text{ accepts }] \geq \alpha(n)$$

$$x \notin L \Longrightarrow \forall y\ \mathrm{Prob}_z[\ N(x,y,f(1^n),z) \text{ accepts }] \leq \beta(n),$$

where $n = |x|$, $\alpha(n) - \beta(n) > 1/r(n)$, f is an advice function, y is taken from $\{0,1\}^{p(n)}$ and z is chosen uniformly over $\{0,1\}^{q(n)}$. Then, $L \in \mathrm{NP}/poly$.

Proof: The goal of the proof is to show that $L \in \mathrm{NP}/poly$. The proof starts by invoking the previous lemmas to center and amplify the probability bounds. After the probability bounds has been sufficiently amplified, the $\exists$ and $\forall$ quantifiers can be moved inside the probability quantifier. This finally results in a BP·(NP/*poly*) expression which, in turn, implies that $L \in \mathrm{NP}/poly$.

First, we define the events A and B as follows:

$$\begin{aligned} A \overset{\text{def}}{=} \{\ (x,a,y) \mid x \in L,\ a = f(1^n),\ y \in \{0,1\}^{p(n)},\ \text{and} \\ \mathrm{Prob}_z[\ N(x,y,f(1^n),z) \text{ accepts }] \geq \alpha(n)\ \} \end{aligned}$$

$$B \overset{\text{def}}{=} \{\ (x,a,y) \mid x \notin L,\ a = f(1^n),\ \text{and } y \in \{0,1\}^{p(n)}\ \}.$$

where $n = |x|$, and z is chosen uniformly over $\{0,1\}^{q(n)}$. Then, a straightforward application of Lemmas 22 and 23 produces an NP machine N' such that

$$x \in L \Longrightarrow \exists y\ \mathrm{Prob}_z[\ N'(x,y,f(1^n),\alpha(n),\beta(n),z) \text{ accepts }] > 1 - 2^{-2p(n)}$$

$$x \notin L \Longrightarrow \forall y\ \mathrm{Prob}_z[\ N'(x,y,f(1^n),\alpha(n),\beta(n),z) \text{ accepts }] < 2^{-2p(n)},$$

where $n = |x|$, f is a nonuniform advice function, y is taken from $\{0,1\}^{p(n)}$ and z is chosen uniformly over $\{0,1\}^{q'(n)}$. To shorten the notation, we define a new advice function g:

$$g(1^n) = (f(1^n), \alpha(n), \beta(n)).$$

Thus, we have

$$x \in L \Longrightarrow \exists y \ \mathrm{Prob}_z[\ N'(x, y, g(1^n), z) \text{ accepts }] > 1 - 2^{-2p(n)}$$

$$x \notin L \Longrightarrow \forall y \ \mathrm{Prob}_z[\ N'(x, y, g(1^n), z) \text{ accepts }] < 2^{-2p(n)}.$$

In the next step, we construct a new NP machine N'' such that

$$N''(x, g(1^n), z) \text{ accepts } \iff \exists y,\ N'(x, y, g(1^n), z) \text{ accepts }.$$

(N'' simply guesses the witness y.) Now, suppose that $x \in L$. Let y_0 be a witness such that $N'(x, y_0, g(1^n), z)$ accepts with high probability. Then, $N''(x, g(1^n), z)$ will also accept with high probability, since N'' will accept by guessing the same y_0. Thus,

$$x \in L \Longrightarrow \mathrm{Prob}_z[\ N''(x, g(1^n), z) \text{ accepts }] > 1 - 2^{-2p(n)}.$$

Conversely, suppose that $x \notin L$. Then, by counting the pairs (y, z) such that $N'(x, y, g(1^n), z)$ accepts, it follows that

$$\mathrm{Prob}_z[\ \exists y,\ N'(x, y, g(1^n), z) \text{ accepts }] < 2^{-p(n)}.$$

Combining the two cases, we have

$$\mathrm{Prob}_z[\ x \in L \iff N''(x, g(1^n), z) \text{ accepts }] > 1 - 2^{-p(n)}.$$

Using more standard notation, this statement says $L \in \mathrm{BP}\cdot(\mathrm{NP}/\textit{poly})$. Moreover, by a lemma due to Schöning (q.v. [18] Corollary 3.6), we know that $\mathrm{BP}\cdot(\mathrm{NP}/\textit{poly}) \subseteq (\mathrm{NP}/\textit{poly})/\textit{poly} = \mathrm{NP}/\textit{poly}$. Thus, $L \in \mathrm{NP}/\textit{poly}$. □

Corollary 25. If the language $\overline{\mathrm{SAT}}$ satisfies the properties in Lemma 24, then $\mathrm{NP}/\textit{poly} = \text{co-}\mathrm{NP}/\textit{poly}$ and $\mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$.

Proof: By Lemma 24, $\overline{\mathrm{SAT}} \in \mathrm{NP}/\textit{poly}$. Then, using Yap's theorems [21], it follows that $\mathrm{NP}/\textit{poly} = \text{co-}\mathrm{NP}/\textit{poly}$ and $\mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$. □