Random Reductions in the Boolean Hierarchy are not Robust*

Richard Chang
Pankaj Rohatgi

TR 90-1154
October 1990

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501

*This research was supported in part by NSF Research Grant CCR-88-23053.

Random Reductions in the Boolean Hierarchy are not Robust*

Richard Chang Pankaj Rohatgi

Department of Computer Science
Cornell University
Ithaca, NY 14853

October, 1990

Abstract

We investigate random reductions from complete sets in the Boolean Hierarchy to their complements. We show that under the assumption that the Polynomial Hierarchy is infinite, the error probability of such reductions cannot be significantly lower than a constant. This constant depends on the classes in question. Thus, random reductions in the Boolean Hierarchy are not robust. We also show that the trivial random reductions between classes at the second level of the Boolean Hierarchy are optimal.

1 Introduction

The Boolean Hierarchy (BH) is an interlacing hierarchy of complexity classes built from differences of NP sets. Much like the Polynomial Hierarchy (PH), the k^{th} level of the Boolean Hierarchy is composed of two complementary classes BH(k) and co-BH(k) (analogous to Σ_k^{P} and Π_k^{P} of the Polynomial Hierarchy). Since its original definition [CH86,WW85,CGH+88], much has been discovered about the Boolean Hierarchy. For example, we believe that the Boolean Hierarchy is a proper hierarchy because if it collapses, then the PH collapses to Δ_3^{P} [Kad88,CK90a], and because we adopt as a "working hypothesis" that the Polynomial Hierarchy has infinitely many levels.

In this report, we investigate the role of random reductions in the Boolean Hierarchy. We show that unlike the Polynomial Hierarchy, random reductions in the Boolean Hierarchy are not robust. To illustrate our point, consider L_k, the canonical $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language for Σ_k^{P}. L_k (or rather Σ_k^{P}) is closed under Boolean OR's, Boolean AND's and majority reductions. These properties translate into a certain robustness in the definition of random reductions. For example, when we consider a random reduction (with one-sided error, say) from a set A to L_k, it does not matter if the reduction has an error probability of $1-1/poly$, $1/c$ or $1/exp$—the three types of random reductions are equivalent. The situation is similar for random reductions with two-sided error. Now, recall that if $\overline{L_k}$ randomly reduces to L_k, then the Polynomial Hierarchy collapses [Sch89,TW88]. The robustness of random reductions in the Polynomial Hierarchy allows us to translate this into the broad statement that random reductions cannot complement the complete languages in the PH.

In contrast, the complete languages of the Boolean Hierarchy do not have the robustness properties listed above. So, one cannot immediately establish the equivalence of random reductions with different error bounds. In fact, we show that in certain situations, random reductions with

*This research was supported in part by NSF Research Grant CCR 88-23053.

different error bounds cannot be equivalent unless the PH collapses. Hence, we believe that random reductions in the Boolean Hierarchy are not robust.

To make this claim more precise, consider $\mathrm{L}_{\mathrm{BH}(k)}$, the canonical $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language for $\mathrm{BH}(k)$. We show that

$$\mathrm{L}_{\mathrm{BH}(2)} \leq_{\mathrm{m}}^{\mathrm{bpp}} \overline{\mathrm{L}_{\mathrm{BH}(2)}} \text{ with error } 1/3$$

However,

$$\mathrm{L}_{\mathrm{BH}(2)} \leq_{\mathrm{m}}^{\mathrm{bpp}} \overline{\mathrm{L}_{\mathrm{BH}(2)}} \text{ with error } 1/3 - 1/poly \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$$

These two theorems illustrate an unusual phenomenon. First, notice that unlike the situation with the Polynomial Hierarchy, random reductions *can* complement the complete languages in the Boolean Hierarchy—but only to a certain extent. Beyond a certain error threshold, random reductions cannot complement the complete languages unless the PH collapses. For level 2, this threshold gives a very tight bound on the error probability of random reductions which complement $\mathrm{L}_{\mathrm{BH}(2)}$. That is, there does exist such a random reduction with error 1/3, but not with error less than $1/3 - 1/poly$ unless the PH collapses. In the general case, we show that

$$\mathrm{L}_{\mathrm{BH}(k)} \leq_{\mathrm{m}}^{\mathrm{bpp}} \overline{\mathrm{L}_{\mathrm{BH}(k)}} \text{ with error } \frac{1}{\lfloor \frac{k}{2} \rfloor + 1}$$

but

$$\mathrm{L}_{\mathrm{BH}(k)} \leq_{\mathrm{m}}^{\mathrm{bpp}} \overline{\mathrm{L}_{\mathrm{BH}(k)}} \text{ with error } 1/\mathcal{F}_{k+1} - 1/poly \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$$

where $\mathcal{F}_i$ is the i^{th} Fibonacci number.

2 Definitions and Notation

We assume that the reader is familiar with the classes NP, co-NP, the NP-complete set SAT, the Polynomial time Hierarchy (PH) and the usual probabilistic and nonuniform classes.

Notation Let $\{0,1\}^t$ denote the set of all binary strings of length t.

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 write $\mathrm{BH}(k)$ and co-$\mathrm{BH}(k)$ for the k^{th} levels of the Boolean hierarchy, defined as follows:

$$\mathrm{BH}(1) \stackrel{\mathrm{def}}{=} \mathrm{NP}$$
$$\mathrm{BH}(2k) \stackrel{\mathrm{def}}{=} \{L \mid L = L' \cap \overline{L_2} \text{ where } L' \in \mathrm{BH}(2k-1) \text{ and } L_2 \in \mathrm{NP}\}$$
$$\mathrm{BH}(2k+1) \stackrel{\mathrm{def}}{=} \{L \mid L = L' \cup L_2 \text{ where } L' \in \mathrm{BH}(2k) \text{ and } L_2 \in \mathrm{NP}\}$$
$$\text{co-BH}(k) \stackrel{\mathrm{def}}{=} \{L \mid \overline{L} \in \mathrm{BH}(k)\}$$

From this definition, it is not hard to prove that the following languages are complete for the respective levels of the Boolean Hierarchy [CGH+88]:

Definition We write $L_{BH(k)}$ for the canonical complete language for BH(k) and $L_{co\text{-}BH(k)}$ for the complete language for co-BH(k):

$$
\begin{aligned}
L_{BH(1)} &\stackrel{\text{def}}{=} \text{SAT}\\
L_{BH(2k)} &\stackrel{\text{def}}{=} \{\langle x_1,\ldots,x_{2k}\rangle \mid \langle x_1,\ldots,x_{2k-1}\rangle \in L_{BH(2k-1)} \text{ and } x_{2k} \in \overline{\text{SAT}}\}\\
L_{BH(2k+1)} &\stackrel{\text{def}}{=} \{\langle x_1,\ldots,x_{2k+1}\rangle \mid \langle x_1,\ldots,x_{2k}\rangle \in L_{BH(2k)} \text{ or } x_{2k+1} \in \text{SAT}\}\\
L_{co\text{-}BH(1)} &\stackrel{\text{def}}{=} \overline{\text{SAT}}\\
L_{co\text{-}BH(2k)} &\stackrel{\text{def}}{=} \{\langle x_1,\ldots,x_{2k}\rangle \mid \langle x_1,\ldots,x_{2k-1}\rangle \in L_{co\text{-}BH(2k-1)} \text{ or } x_{2k} \in \text{SAT}\}\\
L_{co\text{-}BH(2k+1)} &\stackrel{\text{def}}{=} \{\langle x_1,\ldots,x_{2k+1}\rangle \mid \langle x_1,\ldots,x_{2k}\rangle \in L_{co\text{-}BH(2k)} \text{ and } x_{2k+1} \in \overline{\text{SAT}}\}
\end{aligned}
$$

The classes BH(2) and co-BH(2) are also known as D^P and co-D^P, respectively [PY82]. From the definitions above we get the following definitions of D^P, co-D^P and their $\leq_m^P$-complete languages SAT$\wedge\overline{\text{SAT}}$ and $\overline{\text{SAT}}\vee$SAT.

Definition

$$
\begin{aligned}
D^P &\stackrel{\text{def}}{=} \{L_1 \cap \overline{L_2} \mid L_1, L_2 \in \text{NP}\}\\
\text{SAT}\wedge\overline{\text{SAT}} &\stackrel{\text{def}}{=} \{(F_1,F_2) \mid F_1 \in \text{SAT} \text{ and } F_2 \in \overline{\text{SAT}}\}\\
\text{co-}D^P &\stackrel{\text{def}}{=} \{\overline{L_1} \cup L_2 \mid L_1, L_2 \in \text{NP}\}\\
\overline{\text{SAT}}\vee\text{SAT} &\stackrel{\text{def}}{=} \{(F_1,F_2) \mid F_1 \in \overline{\text{SAT}} \text{ or } F_2 \in \text{SAT}\}
\end{aligned}
$$

We now define random reductions between sets. These definitions are generalizations of the definitions given in [AM77] and [VV86].

Definition $A \leq_m^{rp} B$ with probability δ, if there exists a polynomial time function f such that

$$
\begin{aligned}
&x \in A \Longrightarrow \text{Prob}_z(\ f(x,z) \in B\ ) \geq \delta\\
&x \notin A \Longrightarrow \text{Prob}_z(\ f(x,z) \notin B\ ) = 1
\end{aligned}
$$

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

Definition $A \leq_m^{bpp} B$ with error ε, if there exists a polynomial time function f such that

$$\text{Prob}_z(\ x \in A \iff f(x,z) \in B\ ) \geq 1 - \varepsilon$$

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

Definition We define the *Fibonacci* numbers inductively as

$$
\begin{aligned}
\mathcal{F}_0 &\stackrel{\text{def}}{=} 1\\
\mathcal{F}_1 &\stackrel{\text{def}}{=} 1\\
\mathcal{F}_{n+2} &\stackrel{\text{def}}{=} \mathcal{F}_n + \mathcal{F}_{n+1}, \quad \text{for } n \geq 2
\end{aligned}
$$

3 Random reductions at Level 2

In this section we consider random reductions at the second level of the Boolean Hierarchy. We show that there are trivial random reductions between the complete sets in $\mathrm{D^P}$ and co-$\mathrm{D^P}$. Moreover, these random reductions are *optimal* in the sense that the existence of significantly better reductions would imply that the PH collapses. Let us first consider $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions from the complete set in $\mathrm{D^P}$ to the complete set in co-$\mathrm{D^P}$.

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

Proof: Consider the random reduction R from $\mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ to $\overline{\mathrm{SAT}} \vee \mathrm{SAT}$ which does the following on input (F_1, F_2) where $n = |(F_1, F_2)|$:

Let k be the number of variables in the formula F_1. Clearly $k \leq n$. Toss k coins in parallel. Assign the value **true** to the i^{th} variable in F_1 iff the i^{th} coin comes up as "heads". If F_1 is **true** under this assignment then output (F_2,**false**). Otherwise, output (**true**,**false**).

Analysis: It is easy to see that if $(F_1, F_2) \notin \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ then R never outputs a member of $\overline{\mathrm{SAT}} \vee \mathrm{SAT}$. If $(F_1, F_2) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ then $F_1 \in \mathrm{SAT}$. Thus, F_1 will have at least one satisfying assignment. Therefore, with probability at least $1/2^k$ (which is at least $1/2^n$) this assignment will be detected by tossing k coins. In that case R will output a member of $\overline{\mathrm{SAT}} \vee \mathrm{SAT}$. Thus, R is a reduction with the desired properties. □

Since R is a trivial reduction, one might suspect that there are more complicated reductions which work with significantly greater probability. The next lemma provides strong evidence that this is not the case.

Lemma 2 If $\mathrm{SAT} \wedge \overline{\mathrm{SAT}} \leq_{\mathrm{m}}^{\mathrm{rp}} \overline{\mathrm{SAT}} \vee \mathrm{SAT}$ with probability $1/p(n)$ for some polynomial p, then the Polynomial Hierarchy collapses.

Proof: (See Proof of **Theorem 2** in [CK90b]) □

Thus, we obtain a tight probability bound on $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions from complete sets in $\mathrm{D^P}$ to sets in co-$\mathrm{D^P}$. Lemma 1 shows that there exists an $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction with probability 1/exp. In contrast, Lemma 2 shows that no $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction can exist with probability 1/*poly* without collapsing the Polynomial Hierarchy. Now, we look at a similar result for $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions from complete sets in co-$\mathrm{D^P}$ to sets in $\mathrm{D^P}$.

Lemma 3 $\overline{\mathrm{SAT}} \vee \mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{rp}} \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ with probability $1/2 + 1/2^{n+2}$.

Proof: Consider the random reduction T from $\overline{\mathrm{SAT}} \vee \mathrm{SAT}$ to $\mathrm{SAT} \wedge \overline{\mathrm{SAT}}$ which does the following on input (F_1, F_2) where $n = |(F_1, F_2)|$:

1. Let k be the number of variables in the formula F_2. Clearly $k \leq n$. Toss k coins in parallel.
2. Assign **true** to the i^{th} variable in F_2 iff the i^{th} coin comes up as "heads". If F_2 is **true** under this assignment, output (**true**,**false**) and stop. Otherwise, go to Step 3.
3. Randomly choose a string S from $\{0,1\}^{n+2}$. Let P be the lexical rank of S in $\{0,1\}^{n+2}$. Clearly $1 \leq P \leq 2^{n+2}$. If $P \leq 2^{n+1} - 1$ then output (F_2,**false**) else output (**true**,F_1).

Analysis: It is easy to see that if $(F_1, F_2) \notin \overline{\text{SAT}} \vee \text{SAT}$ then T never outputs a member of $\text{SAT} \wedge \overline{\text{SAT}}$. If $(F_1, F_2) \in \overline{\text{SAT}} \vee \text{SAT}$ then one of the two cases hold:

1. $F_2 \in \text{SAT}$.

   T can output a member of $\text{SAT} \wedge \overline{\text{SAT}}$ either at Step 2 or at Step 3. In the worst case, when F_2 has only one satisfying assignment then the probability that T outputs an element of $\text{SAT} \wedge \overline{\text{SAT}}$ is at least $1/2^n + (1 - 1/2^n)(1/2 - 1/2^{n+2})$ which is at least $1/2 + 1/2^{n+2}$.

2. $F_2 \in \overline{\text{SAT}}$ and $F_1 \in \overline{\text{SAT}}$.

   In this case note that T never outputs anything at Step 2. At Step 3 it outputs a member of $\text{SAT} \wedge \overline{\text{SAT}}$ i.e. $(\mathbf{true}, F_1)$ with probability $1/2 + 1/2^{n+2}$. □

The trivial $\leq_{\text{m}}^{\text{rp}}$-reduction T works with probability $1/2 + 1/2^{n+2}$. Moreover, the next lemma implies that T is also optimal.

Lemma 4 If $\overline{\text{SAT}} \vee \text{SAT} \leq_{\text{m}}^{\text{rp}} \text{SAT} \wedge \overline{\text{SAT}}$ with probability $1/2 + 1/p(n)$ for some polynomial bound p, then the Polynomial Hierarchy collapses.

Proof: We are given

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

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

We shall use a variation of the *hard/easy* proof technique [Kad88,CK90b] to prove this lemma. We call a string F *easy* if $F \in \overline{\text{SAT}}$ and

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

where π_i is the i^{th} projection function. We call F a *hard* string if $F \in \overline{\text{SAT}}$ and F is not *easy*. We construct an advice function f which on input 0^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 ϕ (which means that there is no hard string of length $|F|$) or some string a of length $|F|$.

Now, we construct an NP machine N. On input $F\#\phi\#x\#z$, N accepts iff $\pi_2(h(x, F, z)) \in \text{SAT}$. Otherwise, if the input is of the form $F\#a\#x\#z$, where $a \neq \phi$, then N accepts iff $\pi_1(h(F, a, z) \in \text{SAT}$. 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: The advice string is empty.
Since $a = f(0^{|F|}) = \phi$, we know that all strings of size $|F|$ which are in $\overline{\text{SAT}}$ are *easy*. Thus, if $F \in \overline{\text{SAT}}$ then F is easy. Therefore,

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

which implies

$$\exists x, |x| = |F|,\ \text{Prob}_z(\ N \text{ accepts } F\#\phi\#x\#z\ ) \geq \frac{1}{2}$$

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,

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

i.e.,

$$\forall x, |x| = |F|, \ \mathrm{Prob}_z(\ N \text{ accepts } F\#\phi\#x\#z\ ) < \frac{1}{2} - \frac{1}{p(n)}$$

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

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

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

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

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

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

If $F \in \mathrm{SAT}$ then $(F, a) \in \mathrm{SAT} \wedge \overline{\mathrm{SAT}}$, and by the definition of the reduction h we know that

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

However, a is a hard string. Therefore,

$$\forall x, |x| = |a|, \ \mathrm{Prob}_z(\ \pi_2(h(x, a, z)) \in \mathrm{SAT}\ ) < \frac{1}{2}$$

In particular, $\mathrm{Prob}_z(\ \pi_2(h(F, a, z)) \in \mathrm{SAT}\ ) < \frac{1}{2}$. Therefore, $\mathrm{Prob}_z(\ \pi_1(h(F, a, z)) \in \overline{\mathrm{SAT}}\ ) \geq \frac{1}{2}$, which implies $\mathrm{Prob}_z(\ \pi_1(h(F, a, z)) \in \mathrm{SAT}\ ) < \frac{1}{2}$. Again, by adding an additional dummy quantifier, we obtain

$$\forall x, |x| = |F|, \ \mathrm{Prob}_z(\ N \text{ accepts } F\#a\#x\#z\ ) < \frac{1}{2}$$

To summarize, we have shown that N behaves in the following manner:
If $f(0^{|F|}) = a = \phi$ then

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

$$F \in \mathrm{SAT} \Longrightarrow \forall x \ \mathrm{Prob}_z(N \text{ accepts } F\#a\#x\#z) \leq \frac{1}{2} - \frac{1}{p(n)}$$

If $f(0^{|F|}) = a \neq \phi$ then

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

$$F \in \text{SAT} \Longrightarrow \forall x \ \text{Prob}_z(N \text{ accepts } F\#a\#x\#z) < \frac{1}{2}$$

where $x \in \{0,1\}^{|F|}$, $z \in \{0,1\}^{q(n)}$ and n is the size of (F, G) for any string G of size $|F|$. We can now apply the results in Section 6 (q.v. Corollary 1) to show that the Polynomial Hierarchy collapses to Σ_3^{P}. □

Thus, we have obtained a bound on the probability of any $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction from complete sets in co-D^{P} to sets in D^{P}. That is, there cannot exist an $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction with probability $1/2 + 1/\text{poly}$, unless the PH collapses. Moreover, by Lemma 3, this bound is tight, since there exists a trivial $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction with probability $1/2 + 1/\exp$. We have shown that the probability bounds of $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reductions at the second level of the BH cannot be significantly greater than some constant, unless the PH collapses. Thus, these reductions are not robust.

We now consider $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reductions from complete sets in D^{P} to sets in co-D^{P}. We will show that these reductions also have similar properties. Lemma 5 states that there exists a $\leq_{\mathrm{m}}^{\mathrm{bpp}}$-reduction with error $1/3 - 1/2^{n+4}$.

Lemma 5 $\text{SAT} \wedge \overline{\text{SAT}} \leq_{\mathrm{m}}^{\mathrm{bpp}} \overline{\text{SAT}} \vee \text{SAT}$ with error $1/3 - 1/2^{n+4}$.

Proof: We modify the $\leq_{\mathrm{m}}^{\mathrm{rp}}$-reduction T from $\overline{\text{SAT}} \vee \text{SAT}$ to $\text{SAT} \wedge \overline{\text{SAT}}$ used in the proof of Lemma 3. On input (F_1, F_2) where $n = |(F_1, F_2)|$ the new reduction T' does the following:

With probability $1/3 - 1/2^{n+4}$ output a trivial member M of $\text{SAT} \wedge \overline{\text{SAT}}$. With the remaining $2/3 + 1/2^{n+4}$ probability, perform the random reduction T on the input (F_1, F_2).

Analysis: If $(F_1, F_2) \in \text{SAT} \wedge \overline{\text{SAT}}$ then T' will output a member of $\overline{\text{SAT}} \vee \text{SAT}$ with probability $2/3 + 1/2^{n+4}$ since T will always output an element of $\overline{\text{SAT}} \vee \text{SAT}$. If, on the other hand, $(F_1, F_2) \in \overline{\text{SAT}} \vee \text{SAT}$ then T' will output the trivial member M of $\text{SAT} \wedge \overline{\text{SAT}}$ with probability $1/3 - 1/2^{n+4}$ and T will output an element of $\text{SAT} \wedge \overline{\text{SAT}}$ with probability at least $(2/3 + 1/2^{n+4})(1/2 + 1/2^{n+2})$. Thus, the total probability that T' outputs a member of $\text{SAT} \wedge \overline{\text{SAT}}$ is at least

$$(1/3 - 1/2^{n+4}) + (2/3 + 1/2^{n+4})(1/2 + 1/2^{n+2})$$

which is at least $2/3 + 1/2^{n+4}$. □

The next lemma implies that it is not possible to have a reduction which is significantly better than T', unless the PH collapses. Since we prove a more general result in the next section, we shall omit the proof.

Lemma 6 If $\text{SAT} \wedge \overline{\text{SAT}} \leq_{\mathrm{m}}^{\mathrm{bpp}} \overline{\text{SAT}} \vee \text{SAT}$ with error $1/3 - 1/p(n)$ for some polynomial p, then the Polynomial Hierarchy collapses.

4 Random Reductions at Higher Levels

At the higher levels of the Boolean Hierarchy, we can show that there exist random reductions between the complete sets and their complements. We will also show that such reductions are not robust, i.e., their error probabilities cannot be reduced below some constant, unless the PH collapses. At Level 2, we were able to show that trivial reductions were close to optimal. However, we have not been able to obtain a similar result for the higher levels. The following lemma states that there are random reductions between the complete sets at the higher levels of the BH which work with high probability.

Lemma 7 $L_{\mathrm{BH}(2k)} \leq^{\mathrm{rp}}_{\mathrm{m}} L_{\text{co-BH}(2k)}$ with probability $1 - 1/k$.

The next theorem states that $\leq^{\mathrm{bpp}}_{\mathrm{m}}$-reductions between complete sets in the BH and their complements cannot have arbitrarily small error probabilities. This result is obtained by generalizing the proof of Lemma 4. This is done by considering $\leq^{\mathrm{bpp}}_{\mathrm{m}}$-reductions instead of $\leq^{\mathrm{rp}}_{\mathrm{m}}$-reductions and by replacing the concept of hard formulas with the concept of hard sequences of formulas. A similar approach was adopted in [CK90a].

Theorem 8 If $L_{\mathrm{BH}(k)} \leq^{\mathrm{bpp}}_{\mathrm{m}} L_{\text{co-BH}(k)}$ with error $1/\mathcal{F}_{k+1} - 1/p(n)$, for some polynomial p, then the PH collapses to Σ^{P}_3.

Note: $\mathcal{F}_{k+1}$ is the $(k+1)^{th}$ *Fibonacci* number according to the definition given earlier.

We will need some definitions and lemmas before we can prove this theorem. We first define what we mean by a *hard* sequence of formulas.

Definition Suppose $L_{\mathrm{BH}(k)} \leq^{\mathrm{bpp}}_{\mathrm{m}} L_{\text{co-BH}(k)}$ with error $1/\mathcal{F}_{k+1} - 1/p(n)$ via some polynomial time function h. Then, we call $\langle 1^m, x_1, \ldots, x_j \rangle$ 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. For all $y_1, \ldots, y_\ell \in \{0,1\}^m$ (where $\ell = k - j$)

$$\mathrm{Prob}_z(\pi_{\ell+1} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in \mathrm{SAT}) < \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}}$$

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 $\leq^{\mathrm{bpp}}_{\mathrm{m}}$-reduction from $L_{\mathrm{BH}(k)}$ to $L_{\text{co-BH}(k)}$, a hard sequence of order j for length m induces an asymmetric probabilistic reduction from $L_{\mathrm{BH}(k-j)}$ to $L_{\text{co-BH}(k-j)}$ for tuples of strings of length m.

Lemma 9 Suppose $L_{\mathrm{BH}(k)} \leq^{\mathrm{bpp}}_{\mathrm{m}} L_{\text{co-BH}(k)}$ with error $1/\mathcal{F}_{k+1} - 1/p(n)$ via some function h and $r(n)$ is the size of the random input to h. Let $q(m)$ be the size of k-tuples of strings of size m, let $t = r(q(m))$ and $\varepsilon = 1/p(q(m))$. Then, the following proposition $P(j)$ holds for all j, $0 \leq j \leq k-1$:

<u>Proposition $P(j)$:</u> If $\langle 1^m, x_1, \ldots, x_j \rangle$ is a hard sequence w.r.t. h, then for all $y_1, \ldots, y_\ell \in \{0,1\}^m$ <u>(where $\ell = k - j$)</u>:

If ℓ is even:

$$\langle y_1, \ldots, y_\ell \rangle \in L_{\mathrm{BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in L_{\text{co-BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \varepsilon$$
$$\langle y_1, \ldots, y_\ell \rangle \in L_{\text{co-BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in L_{\mathrm{BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \varepsilon$$

If ℓ is odd:

$$\langle y_1, \ldots, y_\ell \rangle \in \mathrm{L}_{\text{co-BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\mathrm{BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \varepsilon$$
$$\langle y_1, \ldots, y_\ell \rangle \in \mathrm{L}_{\mathrm{BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\text{co-BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \varepsilon$$

Proof: (by induction on j)

Base Case $P(0)$: This follows trivially from the hypothesis of the lemma and from the fact that $\mathcal{F}_0 = \mathcal{F}_1 = 1$.

Induction Case $P(j+1)$: Suppose $P(j)$ holds. Let $\ell = k - j$ and let $\langle 1^m, x_1, \ldots, x_{j+1} \rangle$ be a hard sequence. Consider the cases where ℓ is even or odd separately.

Case 1: ℓ is even. Since $\langle 1^m, x_1, \ldots, x_j \rangle$ is also a hard sequence, by the induction hypothesis, for all $y_1, \ldots, y_\ell \in \{0,1\}^m$

$$\langle y_1, \ldots, y_\ell \rangle \in \mathrm{L}_{\mathrm{BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\text{co-BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \varepsilon$$
$$\langle y_1, \ldots, y_\ell \rangle \in \mathrm{L}_{\text{co-BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_\ell, x_j, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\mathrm{BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \varepsilon$$

In particular, for $y_\ell = x_{j+1}$ we have

$$\langle y_1, \ldots, y_{\ell-1}, x_{j+1} \rangle \in \mathrm{L}_{\mathrm{BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_{\ell-1}, x_{j+1}, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\text{co-BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \varepsilon$$
$$\langle y_1, \ldots, y_{\ell-1}, x_{j+1} \rangle \in \mathrm{L}_{\text{co-BH}(\ell)}$$
$$\Longrightarrow \mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_{\ell-1}, x_{j+1}, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\mathrm{BH}(\ell)}) \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \varepsilon$$

Using the definitions of $\mathrm{L}_{\mathrm{BH}(\ell)}$ and $\mathrm{L}_{\text{co-BH}(\ell)}$ for even ℓ, for all $y_1, \ldots, y_{\ell-1} \in \{0,1\}^m$

$$\langle y_1, \ldots, y_{\ell-1} \rangle \in \mathrm{L}_{\mathrm{BH}(\ell-1)} \text{ and } x_{j+1} \in \overline{\mathrm{SAT}} \Longrightarrow \tag{1}$$

$$\mathrm{Prob}_{z,|z|=t}\begin{pmatrix} \pi_{(1,\ell-1)} \circ h(\langle y_1, \ldots, y_{\ell-1}, x_{j+1}, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\text{co-BH}(\ell-1)} \\ \text{or} \\ \pi_\ell \circ h(\langle y_1, \ldots, y_{\ell-1}, x_{j+1}, \ldots, x_1 \rangle, z) \in \mathrm{SAT} \end{pmatrix} \geq 1 - \frac{\mathcal{F}_j}{\mathcal{F}_{k+1}} + \varepsilon$$

and

$$\langle y_1, \ldots, y_{\ell-1} \rangle \in \mathrm{L}_{\text{co-BH}(\ell-1)} \text{ or } x_{j+1} \in \mathrm{SAT} \Longrightarrow \tag{2}$$

$$\mathrm{Prob}_{z,|z|=t}\begin{pmatrix} \pi_{(1,\ell-1)} \circ h(\langle y_1, \ldots, y_{\ell-1}, x_{j+1}, \ldots, x_1 \rangle, z) \in \mathrm{L}_{\mathrm{BH}(\ell-1)} \\ \text{and} \\ \pi_\ell \circ h(\langle y_1, \ldots, y_{\ell-1}, x_{j+1}, \ldots, x_1 \rangle, z) \in \overline{\mathrm{SAT}} \end{pmatrix} \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \varepsilon$$

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, $x_{j+1} \in \overline{\mathrm{SAT}}$ and for all $y_1, \ldots, y_{k-j-1} \in \{0,1\}^m$

$$\mathrm{Prob}_{z,|z|=t}(\pi_{k-j}{\circ}h(\langle y_1,\ldots,y_{k-j-1},x_{j+1},\ldots,x_1\rangle,z)\in \mathrm{SAT}) < \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}$$

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

$$\mathrm{Prob}_z(\pi_\ell{\circ}h(\langle y_1,\ldots,y_{\ell-1},x_{j+1},\ldots,x_1\rangle,z)\in \mathrm{SAT}) < \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}$$

So, if $\langle y_1,\ldots,y_{\ell-1}\rangle \in \mathrm{L}_{\mathrm{BH}(\ell-1)}$, then by equation (1) and the fact that $x_{j+1}\in\overline{\mathrm{SAT}}$, we have

$$\mathrm{Prob}_{z,|z|=t}\left(\begin{array}{c}\pi_{(1,\ell-1)}{\circ}h(\langle y_1,\ldots,y_{\ell-1},x_{j+1},\ldots,x_1\rangle,z)\in \mathrm{L}_{\text{co-BH}(\ell-1)}\\ \text{or}\\ \pi_\ell{\circ}h(\langle y_1,\ldots,y_{\ell-1},x_{j+1},\ldots,x_1\rangle,z)\in \mathrm{SAT}\end{array}\right)\geq 1-\frac{\mathcal{F}_j}{\mathcal{F}_{k+1}}+\varepsilon$$

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

$$\mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell-1)}{\circ}h(\langle y_1,\ldots,y_{\ell-1},x_{j+1},\ldots,x_1\rangle,z)\in \mathrm{L}_{\text{co-BH}(\ell-1)})$$
$$\geq 1-\frac{\mathcal{F}_j}{\mathcal{F}_{k+1}}+\varepsilon-\frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} \;\geq 1-\frac{\mathcal{F}_{j+2}}{\mathcal{F}_{k+1}}+\varepsilon$$

(since $\mathcal{F}_{j+2}=\mathcal{F}_j+\mathcal{F}_{j+1}$). Also, if $\langle y_1,\ldots,y_{\ell-1}\rangle\in \mathrm{L}_{\text{co-BH}(\ell-1)}$ then equation (2) implies that

$$\mathrm{Prob}_{z,|z|=t}(\pi_{(1,\ell-1)}{\circ}h(\langle y_1,\ldots,y_{\ell-1},x_{j+1},\ldots,x_1\rangle,z)\in \mathrm{L}_{\mathrm{BH}(\ell-1)})\geq 1-\frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}+\varepsilon$$

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 $\mathrm{L}_{\mathrm{BH}(k)} \leq_{\mathrm{m}}^{\mathrm{bpp}} \mathrm{L}_{\text{co-BH}(k)}$ with error $1/\mathcal{F}_{k+1}-1/p(n)$, then a *maximal* hard sequence for a given length m allows us to differentiate between the cases $y\in\overline{\mathrm{SAT}}$ and $y\in\mathrm{SAT}$, where y is a formula of length m.

Lemma 10 Suppose $\mathrm{L}_{\mathrm{BH}(k)} \leq_{\mathrm{m}}^{\mathrm{bpp}} \mathrm{L}_{\text{co-BH}(k)}$ with error $1/\mathcal{F}_{k+1}-1/p(n)$ via some function h and $r(n)$ is the size of the random input to h. Let $\langle 1^m,x_1,\ldots,x_j\rangle$ be a maximal hard sequence with respect to h, and let $q(m)$ the size of k-tuples of strings of size m. Define $t=r(q(m))$, $\varepsilon = 1/p(q(m))$ and $\ell = k-j$. Then,

$$y\in\overline{\mathrm{SAT}} \Longrightarrow \left(\begin{array}{l}\exists\; y_1,\ldots,y_{\ell-1}\in\{0,1\}^m,\\ \mathrm{Prob}_{z,|z|=t}(\pi_\ell{\circ}h(\langle y_1,\ldots,y_{\ell-1},y,x_j,\ldots,x_1\rangle,z)\in\mathrm{SAT})\geq \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}\end{array}\right)$$

and

$$y\in\mathrm{SAT} \Longrightarrow \left(\begin{array}{l}\forall\; y_1,\ldots,y_{\ell-1}\in\{0,1\}^m,\\ \mathrm{Prob}_{z,|z|=t}(\pi_\ell{\circ}h(\langle y_1,\ldots,y_{\ell-1},y,x_j,\ldots,x_1\rangle,z)\in\overline{\mathrm{SAT}})\geq 1-\frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}+\varepsilon\end{array}\right)$$

By definition of $L_{\text{co-BH}(\ell)}$ we have that

$$\pi_{(1,\ell)} \circ h(\langle y_1, \ldots, y_{\ell-1}, y, x_j, \ldots, x_1 \rangle, z) \in L_{\text{co-BH}(\ell)}$$
$$\Longrightarrow \pi_\ell \circ h(\langle y_1, \ldots, y_{\ell-1}, y, x_j, \ldots, x_1 \rangle, z) \in \overline{\text{SAT}}$$

Thus, we get the required result for odd ℓ:

$$\forall y_1, \ldots, y_{\ell-1} \text{Prob}_{z,|z|=t}(\pi_\ell \circ h(\langle y_1, \ldots, y_{\ell-1}, y, x_j, \ldots, x_1 \rangle, z) \in \overline{\text{SAT}}) \geq 1 - \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} + \varepsilon$$

This completes the proof of the Lemma. □

Now we are in a position to prove the main theorem:

Theorem 8 If $L_{\text{BH}(k)} \leq_m^{\text{bpp}} L_{\text{co-BH}(k)}$ with error $1/\mathcal{F}_{k+1} - 1/p(n)$, for some polynomial p, then the PH collapses to Σ_3^{P}.

Proof: We will use Lemma 10 to prove the theorem. Given a $\leq_m^{\text{bpp}}$-reduction from $L_{\text{BH}(k)}$ to $L_{\text{co-BH}(k)}$, let f be the advice function which on input 0^m outputs the lexically smallest maximal *hard* sequence for length m.

We define an NP machine N which on input $F\#a\#y\#z$ does the following. Suppose a is of the form $\langle 1^m, x_1, \ldots, x_j \rangle$ where $|x_i| = |F| = m$ and suppose that y is of the form $\langle y_1, \ldots, y_{k-1} \rangle$ where $|y_i| = m$. Let z be a bitstring of size t as required by Lemma 10. Then, N accepts iff $\pi_{k-j} \circ h(\langle y_1, \ldots, y_{k-j-1}, F, x_j, \ldots, x_1 \rangle, z) \in \text{SAT}$. It is easy to see that if $a = f(0^{|F|})$ is of order j then by Lemma 10,

$$F \in \overline{\text{SAT}} \Longrightarrow \exists y,\ \text{Prob}_{z,|z|=t}(N \text{ accepts } F\#a\#y\#z) \geq \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}}$$

and

$$F \in \text{SAT} \Longrightarrow \forall y,\ \text{Prob}_{z,|z|=t}(N \text{ accepts } F\#a\#y\#z) \leq \frac{\mathcal{F}_{j+1}}{\mathcal{F}_{k+1}} - \varepsilon$$

Therefore, by results in Section 6 (q.v. Corollary 1), the PH collapses to Σ_3^{P} □

The previous theorem illustrates the limitations of $\leq_m^{\text{bpp}}$-reductions in the Boolean Hierarchy. Using the same techniques we can prove similar results for $\leq_m^{\text{rp}}$-reductions. We will state these results without proof.

Definition For any rational q, let $\lfloor q \rfloor$ denote the largest integer less than or equal to q.

Theorem 11 Suppose $L_{\text{BH}(k)} \leq_m^{\text{rp}} L_{\text{co-BH}(k)}$ with probability $1 - \alpha + 1/p(n)$, where $k \geq 2$, p is a polynomial and α is a rational. Let $\ell = 2 * (\lfloor (k-1)/2 \rfloor) + 1$. If $\alpha \leq 1/\mathcal{F}_\ell$ then the PH collapses.

Theorem 12 Suppose $L_{\text{co-BH}(k)} \leq_m^{\text{rp}} L_{\text{BH}(k)}$ with probability $1 - \alpha + 1/p(n)$, where $k \geq 2$, p is a polynomial and α is a rational. Let $\ell = 2 * (\lfloor k/2 \rfloor)$. If $\alpha \leq 1/\mathcal{F}_\ell$ then the PH collapses.

5 Conclusion

We have shown that random reductions between the complete sets the Boolean Hierarchy and their complements are not robust, unless the PH collapses. We were also able to obtain tight bounds on the error probability of random reductions at the second level of the BH. We believe that it might be possible to obtain tight bounds at the higher levels as well. This remains a challenging open problem.

6 Some Technical Lemmas

In this section, we prove some technical lemmas which show that under certain assumptions, the Polynomial Hierarchy collapses. These lemmas are mostly modifications to familiar theorems in the literature. However, due to the nonuniform nature of the hard/easy formulas argument, it is not possible to cite these theorems directly. We begin with some definitions.

Definition For any class $\mathcal{C}$, $A \in \mathrm{BP}\cdot\mathcal{C}$ if there exists $B \in \mathcal{C}$ and polynomials p and q such that

$$\forall x,\ \mathrm{Prob}_y(x \in A \iff (x,y) \in B) \geq 1/2 + 1/p(|x|)$$

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

Definition Let $\mathcal{C}$ be any class of languages. $A \in \mathcal{C}/poly$ if there exists $B \in \mathcal{C}$ and a function f such that $|f(n)|$ is bounded by a polynomial and

$$\forall x,\ x \in A \iff (x, f(0^{|x|})) \in B$$

f is called the advice function and $f(0^{|x|})$ the advice string. Note that the advice string depends only on the length of x.

Lemma 13 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,

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

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

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

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:

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

$$x \in B \Longrightarrow \text{Prob}_z(N'(x,z) \text{ accepts }) \leq 1 - \frac{1}{2-2m} + \frac{\beta}{2-2m} = \frac{1}{2} - \frac{1}{4(1-m)r}$$

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. So, 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 13 as follows. (The proof is a straightforward modification.)

Lemma 14 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

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

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

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

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

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

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 [Sch86]) to achieve very high probabilities.

Lemma 15 Let N be any NP machine. Suppose there exist two disjoint events, A and B, such that for some polynomials q and r

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

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

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

$$x \in A \Longrightarrow \text{Prob}_z(N'(x,z) \text{ accepts }) > 1 - 2^{-p(n)}$$

$$x \in B \Longrightarrow \text{Prob}_z(N'(x,z) \text{ accepts }) < 2^{-p(n)}$$

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 (q.v. [Bab85]) or by the quantifier structure $[\exists\exists^+\exists/\forall\exists^+\forall]$ (q.v. [Zac86]) are in the class BP$\cdot$NP. Lemma 16 states that the nonuniform versions of such languages are in the class BP$\cdot$(NP/*poly*) which is the same as the class NP/*poly*.

Lemma 16 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:

$$x \in L \Longrightarrow \exists y \ \text{Prob}_z(N(x,y,f(0^n),z) \text{ accepts }) \geq \alpha(n)$$

$$x \notin L \Longrightarrow \forall y \ \text{Prob}_z(N(x,y,f(0^n),z) \text{ accepts }) \leq \beta(n)$$

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, $L \in$ NP/*poly*.

Proof: The goal of the proof is to show that $L \in$ 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$\cdot$(NP/*poly*) expression which, in turn, implies that $L \in$ NP/*poly*.

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

$$A \stackrel{\text{def}}{=} \{(x,a,y) \mid x \in L, \ a = f(0^n), \ y \in \{0,1\}^{p(n)}, \text{ and } \text{Prob}_z(N(x,y,f(0^n),z) \text{ accepts }) \geq \alpha(n)\}$$

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

where $n = |x|$, and z is chosen uniformly over $\{0,1\}^{q(n)}$. Then, a straightforward application of Lemmas 14 and 15 produces an NP machine N' such that

$$x \in L \Longrightarrow \exists y \ \mathrm{Prob}_z(N'(x, y, f(0^n), \alpha(n), \beta(n), z) \text{ accepts }) > 1 - 2^{-2p(n)}$$

$$x \notin L \Longrightarrow \forall y \ \mathrm{Prob}_z(N'(x, y, f(0^n), \alpha(n), \beta(n), z) \text{ accepts }) < 2^{-2p(n)}$$

where $n = |x|$, f is a non-uniform advice function, y is taken from $\{0,1\}^{p(n)}$ and z is chosen uniformly over $\{0,1\}^{q'(n)}$. As a shorthand, we can define a new advice function g:

$$g(0^n) = (f(0^n), \alpha(n), \beta(n))$$

Thus, we have

$$x \in L \Longrightarrow \exists y \ \mathrm{Prob}_z(N'(x, y, g(0^n), z) \text{ accepts }) > 1 - 2^{-2p(n)}$$

$$x \notin L \Longrightarrow \forall y \ \mathrm{Prob}_z(N'(x, y, g(0^n), z) \text{ accepts }) < 2^{-2p(n)}$$

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

$$N''(x, g(0^n), z) \text{ accepts } \iff \exists y, \ N'(x, y, g(0^n), z) \text{ accepts}$$

Now, suppose $x \in L$. Let y_0 be a witness such that $N'(x, y_0, g(0^n), z)$ accepts with high probability. Then, $N''(x, g(0^n), z)$ will also accept with high probability, since N'' will accept by guessing the same y_0. Thus,

$$x \in L \Longrightarrow \mathrm{Prob}_z(N''(x, g(0^n), z) \text{ accepts }) > 1 - 2^{-2p(n)}$$

On the other hand, suppose that $x \notin L$. Then,

$$\mathrm{Prob}_z(\exists y, \ N'(x, y, g(0^n), z) \text{ accepts }) < 2^{-p(n)}$$

To see this, suppose that the probability is greater than $2^{-p(n)}$. Then, let m be the number of pairs (y, z) such that $N'(x, y, g(0^n), z)$ accepts. By assumption, $m > 2^{-p(n)} \cdot 2^{q'(n)} = 2^{q'(n)-p(n)}$. Since there are only $2^{p(n)}$ many different y's, for some particular y_0, there must be more than $m/2^{p(n)} = 2^{q'(n)-2p(n)}$ many z's such that $N'(x, y_0, g(0^n), z)$ accepts. However, this means $\mathrm{Prob}_z(N'(x, y_0, g(0^n), z) \text{ accepts }) > 2^{-2p(n)}$, which violates the condition that $x \notin L$. Thus,

$$x \notin L \Longrightarrow \mathrm{Prob}_z(N''(x, g(0^n), z) \text{ accepts }) < 2^{-p(n)}$$

Combining the two cases, we have

$$\mathrm{Prob}_z(x \in L \iff N''(x, g(0^n), z) \text{ accepts }) < 1 - 2^{-p(n)}$$

Using more standard notation, this statement says $L \in \mathrm{BP}\cdot(\mathrm{NP}/poly)$. Moreover, by a lemma due to Schöning [Sch89], we know that $\mathrm{BP}\cdot(\mathrm{NP}/poly) \subseteq (\mathrm{NP}/poly)/poly = \mathrm{NP}/poly$. Thus, $L \in \mathrm{NP}/poly$.
□

Corollary 1 If the language $\overline{\mathrm{SAT}}$ satisfies the properties in Lemma 16, then the Polynomial Hierarchy collapses to Σ_3^{P}.

Proof: By Lemma 16, $\overline{\mathrm{SAT}} \in \mathrm{NP}/poly$. Then, using Yap's theorem [Yap83], $\mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$. □

Acknowledgements

We are grateful to Juris Hartmanis for his support and guidance. We would also like to thank Desh Ranjan for his comments and suggestions.

References

[AM77] L. M. Adleman and K. Manders. Reducibility, randomness, and intractibility [*sic*]. In *ACM Symposium on Theory of Computing*, pages 151–163, 1977.

[Bab85] L. Babai. Trading group theory for randomness. In *ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[CGH+88] 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.

[CH86] J. Cai and L. A. Hemachandra. The Boolean hierarchy: Hardware over NP. In *Structure in Complexity Theory*, Springer-Verlag *Lecture Notes in Computer Science #223*, pages 105–124, 1986.

[CK90a] 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.

[CK90b] R. Chang and J. Kadin. On the structure of uniquely satisfiable formulas. Technical Report 90-1124, Department of Computer Science, Cornell University, May 1990.

[Kad88] J. Kadin. The polynomial time hierarchy collapses if the Boolean hierarchy collapses. *SIAM Journal on Computing*, 17(6):1263–1282, December 1988.

[PY82] C. H. Papadimitriou and M. Yannakakis. The complexity of facets (and some facets of complexity). In *ACM Symposium on Theory of Computing*, pages 255–260, 1982.

[Sch86] U. Schöning. *Complexity and Structure.* Lecture Notes in Computer Science #211. Springer-Verlag, 1986.

[Sch89] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, 39(1):84–100, 1989.

[TW88] S. Tang and O. Watanabe. On tally relativizations of BP-complexity classes. In *Proceedings of the 3rd Structure in Complexity Theory Conference*, pages 10–18, 1988.

[VV86] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986.

[WW85] K. Wagner and G. Wechsung. On the Boolean closure of NP. In *Proceedings of the 1985 International Conference on Fundamentals of Computation Theory*, Springer-Verlag *Lecture Notes in Computer Science #199*, pages 485–493, 1985.

[Yap83] C. Yap. Some consequences of non-uniform conditions on uniform classes. *Theoretical Computer Science*, 26(3):287–300, 1983.

[Zac86] S. Zachos. Probabilistic quantifiers, adversaries, and complexity classes: An overview. In *Structure in Complexity Theory*, Springer-Verlag *Lecture Notes in Computer Science #223*, pages 383–400, 1986.