$\text{NP} \in \text{co-NP/poly} \rightarrow \Sigma_5^{\text{p}} = \Pi_5^{\text{p}}$

Exposition by William Gasarch

1 Introduction

Recall the definitions of P/poly, NP/poly and co-NP/poly.

Notation 1.1 PTM means Polynomial time bounded Turing Machine.

Def 1.2

1. $A \in \text{P/poly}$ if there exists a PTM M, a function $h : 0^* \rightarrow \{0,1\}^*$, and a polynomial p such that $|h(0^n)| = p(n)$, and

$$A = \{x \mid M(x; h(0^{|x|}) = 1\}.$$

2. $A \in \text{NP/poly}$ if there exists an PTM M, a function $h : 0^* \rightarrow \{0,1\}^*$, and a polynomial p such that $|h(0^n)| = p(n)$, and

$$A = \{x \mid (\exists^p y)[M(x, y; h(0^{|x|})) = 1]\}.$$

3. $A \in \text{co-NP/poly}$ if there exists an PTM M, a function $h : 0^* \rightarrow \{0,1\}^*$, and a polynomial p such that $|h(0^n)| = p(n)$, and

$$A = \{x \mid (\forall^p y)[M(x, y; h(0^{|x|})) = 1]\}.$$

The string $h(0^n)$ is called *advice for strings of length n*.
We leave the proof of the following easy lemma to the reader.

Lemma 1.3 *The following are equivalent:*

1. $NP \subseteq \text{co-NP/poly}$
2. $coNP \subseteq \text{NP/poly}$
3. $SAT \in \text{co-NP/poly}$

4. $TAUT \in$ NP/poly

We will show that

$$\text{NP} \subseteq \text{co-NP/poly} \rightarrow \Sigma_5^{\text{p}} = \Pi_5^{\text{p}}$$

by showing

$$TAUT \in \text{NP/poly} \rightarrow \Sigma_5^{\text{p}} = \Pi_5^{\text{p}}.$$

2 The Complexity of Advice

Lets say $A \in$ NP/poly with advice of length $p(n)$. Then one can ask the following question: given a string w of length $p(n)$ is it good advice for the strings of length n? One can look at the complexity of the set of good advice strings.

We define this formally.

Def 2.1 Let $A \in$ NP/poly. Hence there exists an PTM M, a function $h : 0^* \rightarrow \{0,1\}^*$, and a polynomial p such that $|h(0^n)| = p(n)$, and

$$A = \{x \mid (\exists^p y)[M(x, y; h(0^{|x|}) = 1\}.$$

Let

$$ADV_A = \{(w, n) \mid |w| = p(n) \wedge (\forall x, |x| = n)[x \in A \text{ iff } (\exists^p y)[M(x, y; w) = 1]]]\}.$$

Since testing if $|w|$ is of length $p(n)$ is easily in P we will ignore that part for the purpose of determining the complexity of ADV. Hence we write (informally),

$$ADV_A = \{w \mid (\forall^p x)[x \in A \text{ iff } (\exists^p y)[M(x, y; w) = 1]]\}.$$

Lemma 2.2 *Let A be a coNP set. Assume $A \in$ NP/poly. Let $ADV = ADV_A$. Then $ADV \in \Pi_3^{\text{p}}$.*

Proof:

$$ADV = \{w \mid (\forall^p x)[x \in A \text{ iff } (\exists^p y)[M(x, y; w) = 1]]\}.$$

Since $A \in coNP$ there exists a poly predicate B such that $x \in A$ iff $(\forall^p z)[B(x, z)]$. Hence we can rewrite ADV as the set of all w such that

$$(\forall^p x)[(\forall^p z)[B(x, z)] \text{ iff } (\exists^p y)[M(x, y; w) = 1]]$$

which we rewrite as, omitting the $(\forall^p x)$ for now,

$$[(\forall^p z)[B(x, z)]] \rightarrow [(\exists^p y)[M(x, y; w) = 1]] \bigwedge [(\exists^p y)[M(x, y; w) = 1]] \rightarrow [(\forall^p z)[B(x, z)]]]$$

which we rewrite as

$$[(\exists^p z)[\neg B(x, z)]] \vee [(\exists^p y)[M(x, y; w) = 1]] \bigwedge [(\forall^p y)[M(x, y; w) = 0]] \vee [(\forall^p z)[B(x, z)]]$$

The expression of the form $(\exists^p z)[BLAH] \vee (\exists^p y)[BLAH'$ can be written with one $\exists^p$ and one poly set. We write it as $(\exists^p u)[D(x, y; w]$. Hence we have:

$$(\exists^p u)[D(x, y; w)] \bigwedge [[(\forall^p y)[M(x, y; w) = 0]] \vee [(\forall^p z)[B(x, z)]]]$$

How can we write a $\vee$ of two $(\forall^p)$'s in terms of quantifiers? We can make which of the two parts of the $\vee$ wins another quantifier.

$$(\exists^p u)[D(x, y; w)] \bigwedge [[(\exists b \in \{0, 1\})(\forall^p y)(\forall^p z)[(b = 0 \rightarrow [M(x, y; w) = 0]]) \wedge (b = 1) \rightarrow [B(x, z)]]]$$

The second term is more complicated than the first. Hence, adding the $(\forall^p x)$, we obtain that $ADV \in \Pi_3^{\mathrm{p}}$.

∎

3 Main Theorem

Theorem 3.1 *If* $NP \subseteq$ co-NP/poly *then* $\Pi_5^{\mathrm{p}} = \Sigma_5^{\mathrm{p}}$.

Proof: Assume $NP \subseteq$ co-NP/poly. Then by Lemma 1.3 $TAUT \in$ NP/poly via PTM M. Let $ADV = ADV_{TAUT}$. By Lemma 2.2 $ADV \in \Pi_3^{\mathrm{p}}$.

Let $A \in \Pi_5^{\mathrm{p}}$. Then there exists a $B \in P$ such that

$A =$

$$\{x \mid (\forall^p y_1)(\exists^p y_2)(\forall^p y_3)(\exists^p y_4)(\forall^p y_5)[B(x, y_1, y_2, y_3, y_4, y_5)]\}.$$

By the techniques of the Cook-Levin theorem there exists a function that maps x, y_1, y_2, y_3, y_4 to ϕ_{x,y_1,y_2,y_3,y_4} such that

$A =$

$$\{x \mid (\forall^p y_1)(\exists^p y_2)(\forall^p y_3)(\exists^p y_4)[\phi_{x,y_1,y_2,y_3,y_4} \in TAUT]\}.$$

We want to replace $\phi \in$ TAUT with using the advice. So we begin with the advice:

$A =$

$$\{x \mid (\exists^p w)(\forall^p y_1)(\exists^p y_2)(\forall^p y_3)(\exists^p y_4)[w \in ADV \wedge (\exists^p y_6)[M(\phi, y_6; w) = 1] = 1]\}.$$

Since $ADV \in \Pi_3^{\mathrm{p}}$ let

$$ADV = \{w \mid (\forall^p z_1)(\exists^p z_2)(\forall^p z_3)]C(w, z_1, z_2, z_3) = 1]\}.$$

We can weave this into the definition of A.

$A =$

$$\{x \mid (\exists^p w)(\forall^p y_1, z_1)(\exists^p y_2, z_2)(\forall^p y_3, z_3)(\exists^p y_4, y_6)[C(w, z_1, z_2, z_3 \wedge M(\phi, y_6; w) = 1] = 1]\}.$$

Hence $A \in \Sigma_5^{\mathrm{p}}$.

∎