18.405J/6.841J Advanced Complexity Theory	March 9, 1998
Lecture 9	
Lecturer: Daniel A. Spielman	*Scribe: Eric krevice Prebys*

1 Introduction

In the last class we saw that **BPP** was contained in **P/poly**. We also saw that the definition of **BPP** is equivalent to the following :

Definition 1 $\mathbf{L} \in \mathbf{BPP}$ *if* $\exists A \in \mathbf{P}, f(n) \leq n^{O(1)}$ *such that*

$$w \in \mathbf{L} \implies \Pr_{r \in \{0,1\}^{f(n)}}[(w,r) \in A] > 1 - 2^{-n}$$

$$w \notin \mathbf{L} \implies \Pr_{r \in \{0,1\}^{f(n)}}[(w,r) \in A] < 1 - 2^{-n}$$

In this class, we will show that **BPP** is contained in Σ_2^P. This will show that randomization is no more powerful than the **PH**.

2 BPP is in Σ_2^P

It will also be useful to look at how **BPP** fits into the polynomial hierarchy. Figure 1 illustrates what is known about the relationship between **P**, **RP**, **coRP**, **BPP**, **NP** and **coNP**. It also illustrates the following theorem:

Theorem 2 $\mathbf{BPP} \subseteq \Sigma_2^P$

Proof Idea This proof was originally done by Michael Sipser, later it was improved by Clemens Lautemann. Throughout, $n = |w|$.

We want to create a Σ_2^P machine which solves an arbitrary $\mathbf{L} \in \mathbf{BPP}$.

Let

$$R_w = \{r \in \{0,1\}^{f(n)} \mid (r,w) \in A\}.$$

Now we can rephrase definition 1 as : $\mathbf{L} \in \mathbf{BPP}$ if $\exists A \in \mathbf{P}, f(n) \leq n^{O(1)}$ such that

$$w \in \mathbf{L} \implies |R_w| \geq (1 - 2^{-n})2^{f(n)}$$

$$w \notin \mathbf{L} \implies |R_w| \leq 2^{-n}2^{f(n)}$$

How can a Σ_2^P machine tell if $|R_w|$ is very large or very small? If we translate R_w enough times, when $w \in \mathbf{L}$ the union of all the translations covers all of $\{0,1\}^{f(n)}$, but when $w \notin \mathbf{L}$, the union of translations still covers very little.

■

Proof If $x, y \in \{0,1\}^m$, then we define $x \oplus y$ as the componentwise XOR of x and y. For a set $S \in \{0,1\}^m$, and vector $t \in \{0,1\}^m$, then to translate s by t we define $S \oplus t = \{\phi \oplus t \mid \phi \in S\}$.

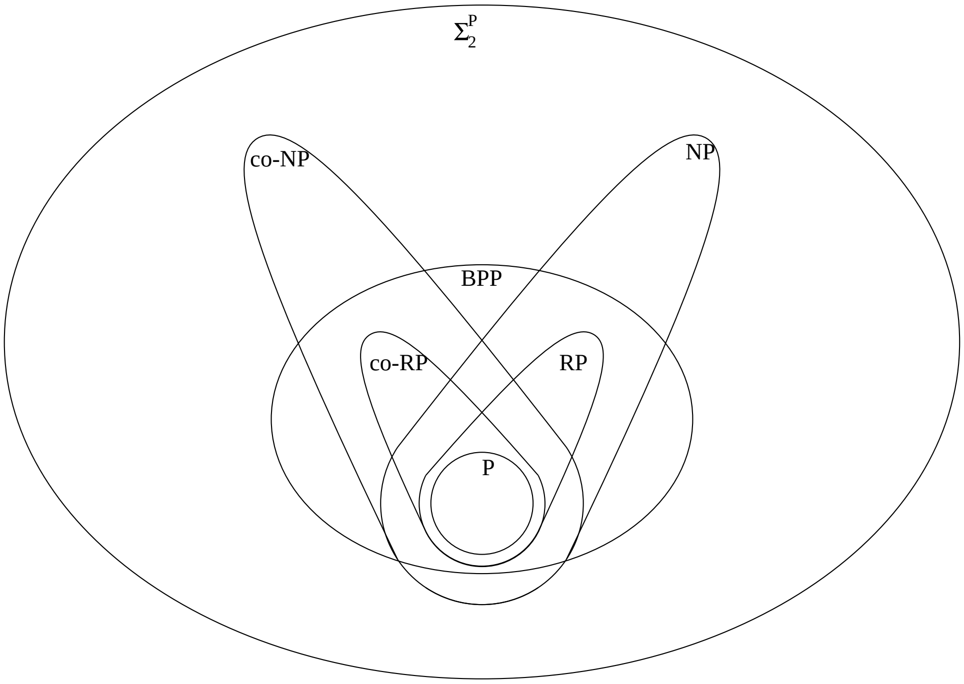

Figure 1: The containments of some complexity classes

Claim 3 *If $R_w \geq (1-2^{-n})2^{f(n)}$ then $\exists t_1, ..., t_{f(n)}$ such that $\bigcup_i (R_w \oplus t_i) = \{0,1\}^{f(n)}$.*

If $R_w \leq 2^{-n}2^{f(n)}$ then $\forall t_1, ..., t_{f(n)}$, we have $|\bigcup_i (R_w \oplus t_i)| \leq f(n)2^{-n}2^{f(n)} < 2^{f(n)}$ for all n greater than some n_0.

Now we will see why this claim implies $\mathbf{L} \in \Sigma_2^P$.

First consider $w \in \mathbf{L}$. By the claim, we have $|R_w| \geq (1-2^{-n})2^{f(n)}$ which implies that $\exists t_1, ..., t_{f(n)}$ such that $\forall x \in \{0,1\}^{f(n)}$, $x \in \bigcup_i (R_w \oplus t_i)$.

Now consider $w \notin \mathbf{L}$. By the claim, we have $|R_w| \leq 2^{-n}2^{f(n)}$ which implies that $\forall t_1, ..., t_{f(n)}$, $\exists x \in \{0,1\}^{f(n)}$, such that $x \notin \bigcup_i (R_w \oplus t_i)$.

To see that this gives us the proof we must observe that these two are contradictions, which they obviously are.

We must also check if we can test if $x \in \bigcup_i (R_w \oplus t_i)$ in polynomial time. We must check if $(w, x \oplus t_i) \in A, A \in \mathbf{P}$. We can check this since there are only a polynomial number of t_i.

Now we will describe a Σ_2^P machine for deciding $\mathbf{L}$:

$\exists$ choose $t_i, ..., t_{f(n)}$

$\forall$ choose $x \in \{0,1\}^{f(n)}$

Accept if $\exists_{1 \leq i \leq f(n)} (w, x \oplus t_i) \in A$

Since $A \in \mathbf{P}$ this can all be done in polynomial time. This machine works since clearly $w \in \mathbf{L}$ is accepted and $w \notin \mathbf{L}$ is rejected.

Now we will prove the claim. To prove the first part, we essentially need to show :

$$
\begin{aligned}
\text{If} \quad & |R_w| \leq 2^{-n}2^{f(n)}, \text{ and } \forall t_1, ..., t_{f(n)}, \text{ and } \forall n > \text{ some } n_0 \\
& |\bigcup_i (R_w \oplus t_i)| \leq f(n)2^{-n}2^{f(n)} < 2^{f(n)} \\
\implies \quad & |\bigcup_i (R_w \oplus t_i)| \neq |\{0,1\}^{f(n)}|
\end{aligned}
$$

The proof is simple.

$$
\left|\bigcup_i (R_w \oplus t_i)\right| \leq \sum_i |(R_w \oplus t_i)| \leq f(n)|R_w|
$$

Now we must prove the second part :

If $R_w \geq (1 - 2^{-n})2^{f(n)}$ then $\exists t_1, ..., t_{f(n)}$ such that $\forall x \in \{0,1\}^{f(n)}, x \in \bigcup_i (R_w \oplus t_i)$.

To prove this, we will show

$$
\Pr_{t_1,...,t_{f(n)} \in \{0,1\}^{f(n)}} [\forall x, x \in \bigcup_i (R_w \oplus t_i)] > 0.
$$

We have :

$$
\begin{aligned}
\Pr_{t_1,...,t_{f(n)} \in \{0,1\}^{f(n)}} [\forall x, x \in \bigcup_i (R_w \oplus t_i)] &= \\
&= 1 - \Pr_{t_1,...,t_{f(n)} \in \{0,1\}^{f(n)}} [\exists x \mid \bigwedge_i (x \notin R_w \oplus t_i)] \\
&\geq 1 - \sum_{x \in \{0,1\}^{f(n)}} \Pr_{t_1,...,t_{f(n)}} [\bigwedge_i (x \notin (R_w \oplus t_i))] \\
&= 1 - \sum_x \prod_{i=1}^{f(n)} \Pr_{t_1,...,t_{f(n)} \in \{0,1\}_{f(n)}} [x \notin (R_w \oplus t_i)] \\
&= 1 - 2^{f(n)}(2^{-n})^{f(n)} \\
&= 1 - \frac{1}{2^{(n-1)f(n)}} > 0 \text{ for } n > 1.
\end{aligned}
$$

■

Since **BPP** is closed under complement and **BPP** $\subseteq \Sigma_2^P$, we know that **BPP** must be contained in Π_2^P. If $\Pi_2^P \subseteq$ **BPP**, then **PH** would collapse.

Next, will be a theorem proved by Valiant and Vazirani. The theorem shows that, if you could efficiently solve instances of **SAT** knowing that there is only one or no solutions, then you could efficiently solve **SAT** in general.

Theorem 4 *There exists a random polynomial time Turing machine M that on input w produces $w_1, ..., w_{|w|}$ with the following properties :*

If $w \in \mathbf{SAT}$ *then*

$\Pr[\exists i \mid w_i \in \mathbf{SAT}$ *and* w_i *has exactly 1 satisfying assignment* $] > \frac{1}{8}$

If $w \notin \mathbf{SAT}$ *then* $w_i \notin \mathbf{SAT}$.

(Up to some randomization, solving general **SAT** *is no more difficult.)*

Definition 5 *For a predicate* Q,

$$\mathbf{USAT}_Q(w) = \begin{cases} 0 & \text{if } w \notin \mathbf{SAT} \\ 1 & \text{if } w \in \mathbf{SAT}, \text{ and } w \text{ has unique satisfying assignment} \\ Q(w) & \text{o.w.} \end{cases}$$

Corollary 6 *If there exists* Q *such that* $\mathbf{USAT}_Q \in \mathbf{RP}$ *then* $\mathbf{NP} \subseteq \mathbf{RP}$.

Proof of Theorem 4: We will do a reduction. Let $H_{k,n}$ be a set of functions from $\{0,1\}^n \longrightarrow \{0,1\}^k$ such that $\forall x \neq y \in \{0,1\}^n, a, b \in \{0,1\}^k$. Then we have

$$\Pr_{h \in H_{k,n}}[(h(x) = a) \wedge (h(y) = b)] = 2^{-2k}$$

The reduction is that given a **CNF** $\phi(x_1, ..., x_n)$, we choose $h_i \in H_{i,n}$ for $1 \leq i \leq n$ and output **CNF**s $\phi_i = \phi \wedge \phi_{h_i}$ which corresponds to $\phi(x_1, ..., x_n) \wedge (h_i(x_i, ..., x_n) = \bar{0})$.

To make this reduction, we assume the following lemma, which is easy to prove:

Lemma 7 *Given* h_i, *in polynomial time we can construct a* **CNF** ϕ_{h_i} *satisfying the following :*

If $h_i(x_1, ..., x_n) = \bar{0}$

then there exists unique $y_1, ..., y_m$ *such that* $\phi_{h_1}(\bar{x}, \bar{y})$ *is satisfied.*

If $h_i(x_1, ..., x_n) \neq \bar{0}$

then there does not exist $y_1, ..., y_m$ *such that* $\phi_{h_i}(\bar{x}, \bar{y})$ *is satisfied.*

To prove the Theorem we need to show two things. We must show that $\phi \notin \mathbf{SAT} \implies \phi_i \notin \mathbf{SAT}$. This is clear.

We must also show that

$$\phi \in \mathbf{SAT} \implies \Pr[\exists i \mid \phi_i \text{ has unique } \mathbf{SAT} \text{ assignment}] > \frac{1}{8}.$$

Let $S =$ the set of satisfying assignments of ϕ. Choose i such that $2^{i-2} \leq |S| \leq 2^{i-1}$. Now we can make the following claim.

Claim 8

$$\Pr_{h_i}[|S \cap h_i^{-1}(0)| = 1] \geq \frac{1}{8}$$

$$\Pr_{h_i}[|S \cap h_i^{-1}(0)| = 1] = \tag{1}$$

$$= \Pr_{h_i}[(\exists a \in S \mid h_i(a) = 0) \wedge \forall_{((b \neq a) \wedge (b \in S))} h_i(b) \neq 0] \tag{2}$$

To be continued next lecture...

■