## Notes for Lecture 4

Today we give the definition of the polynomial hierarchy and prove two results about boolean circuits and randomized algorithms.

## 1 Polynomial hierarchy

Remark 1 (Definition of NP and coNP) A problem is in NP if and only if there is a polynomial time computable $F(\cdot, \cdot)$ and a polynomial time bound $p()$ such that

$$
x \text { is a } Y E S \text {-instance } \Leftrightarrow \exists y . y \in\{0,1\}^{p(|x|)} \wedge F(x, y)
$$

coNP is the class of problems whose complement (switch YES-instance to NO-instance) is in NP. Formally, a problem is in coNP if and only if there is a polynomial time computable $F(\cdot, \cdot)$ and a polynomial time bound $p()$ such that

$$
x \text { is a YES-instance } \Leftrightarrow \forall y: y \in\{0,1\}^{p(|x|)}, F(x, y)
$$

The polynomial hierarchy starts with familiar classes on level one: $\Sigma_{1}=\mathbf{N P}$ and $\Pi_{1}=c o \mathbf{N P}$. For all $i \geq 1$, it includes two classes, $\Sigma_{i}$ and $\Pi_{i}$, which are defined as follows:

Definition $2 \Sigma_{k}$ is the class of all problems such that there is a polynomial time computable $F(\cdot, \ldots, \cdot)$ and $k$ polynomials $p_{1}(), \ldots, p_{k}()$ such that

$$
\begin{gathered}
x \text { is a YES-instance } \Leftrightarrow \\
\exists y_{1} \in\{0,1\}^{p_{1}(|x|)} \cdot \forall y_{2} \in\{0,1\}^{p_{2}(|x|)} . \ldots \\
\ldots \underset{k \text { is odd/even }}{\forall / \exists} y_{k} \in\{0,1\}^{p_{k}(|x|)} \cdot F\left(x, y_{1}, \ldots, y_{k}\right)
\end{gathered}
$$

Definition $3 \Pi_{k}$ is the class of all problems such that there is a polynomial time computable $F(\cdot, \ldots, \cdot)$ and $k$ polynomials $p_{1}(), \ldots, p_{k}()$ such that

$$
\begin{gathered}
x \text { is a YES-instance } \Leftrightarrow \\
\forall y_{1} \in\{0,1\}^{p_{1}(|x|)} \cdot \exists y_{2} \in\{0,1\}^{p_{2}(|x|)} . \ldots \\
\ldots \underset{k \text { is odd/even }}{\forall / \exists} y_{k} \in\{0,1\}^{p_{k}(|x|)} \cdot F\left(x, y_{1}, \ldots, y_{k}\right)
\end{gathered}
$$

One thing that is easy to see is that $\Pi_{k}=\operatorname{co} \Sigma_{k}$. Also, note that, for all $i \leq k-1$, $\Pi_{i} \subseteq \Sigma_{k}$ and $\Sigma_{i} \subseteq \Sigma_{k}$. These subset relations hold for $\Pi_{k}$ as well. This can be seen by noticing that the predicates $F$ do not need to "pay attention to" all of their arguments, and so can represent classes lower on the hierarchy which have a smaller number of them.

Exercise $1 \forall k . \Sigma_{k}$ has a complete problem.

One thing that is easy to see is that $\Pi_{k}=\operatorname{co} \Sigma_{k}$. Also, note that, for all $i \leq k-1$, $\Pi_{i} \subseteq \Sigma_{k}, \Sigma_{i} \subseteq \Sigma_{k}, \Pi_{i} \subseteq \Pi_{k}, \Sigma_{i} \subseteq \Pi_{k}$. This can be seen by noticing that the predicates $F$ do not need to "pay attention to" all of their arguments, and so a statement involving $k$ quantifiers can "simulate" a statement using less than $k$ quantifiers.

Theorem 4 Suppose $\Pi_{k}=\Sigma_{k}$. Then $\Pi_{k+1}=\Sigma_{k+1}=\Sigma_{k}$.
Proof: For any language $L \in \Sigma_{k+1}$, we have that there exist polynomials $p_{1}, \ldots, p_{k+1}$ and a polynomial time computable function F such that

$$
x \in L \Leftrightarrow \exists y_{1} \cdot \forall y_{2} . \ldots Q_{k+1} y_{k+1} \cdot F\left(x, y_{1}, \ldots, y_{k+1}\right)=1
$$

where we did not explicitly stated the conditions $y_{i} \in\{0,1\}^{p_{i}(|x|)}$. Let us look at the right hand side of the equation. What is following $\exists y_{1}$ is a $\Pi_{k}$ statement. Thus, there is a $L^{\prime} \in \Pi_{k}$ such that

$$
x \in L \Leftrightarrow \exists y_{1} \in\{0,1\}^{p_{1}(|x|)} \cdot\left(x, y_{1}\right) \in L^{\prime}
$$

Under the assumption that $\Pi_{k}=\Sigma_{k}$, we have $L^{\prime} \in \Sigma_{k}$, which means that there are polynomials $p_{1}^{\prime}, \ldots, p_{k}^{\prime}$ and a polynomial time computable $F^{\prime}$ such that

$$
\left(x, y_{1}\right) \in L^{\prime} \Leftrightarrow \exists z_{1} \cdot \forall z_{2} \ldots Q_{k} z_{k} \cdot F^{\prime}\left(\left(x, y_{1}\right), z_{1}, \ldots, z_{k}\right)=1
$$

where we omitted the conditions $z_{i} \in\{0,1\}^{p_{i}^{\prime}(|x|)}$. So now we can show that

$$
\begin{aligned}
x \in L & \Leftrightarrow \exists y_{1} \cdot\left(x, y_{1}\right) \in L^{\prime} \\
& \Leftrightarrow \exists y_{1} \cdot\left(\exists z_{1} \cdot \forall z_{2} \ldots Q_{k} z_{k} \cdot F^{\prime}\left(\left(x, y_{1}\right), z_{1}, \ldots, z_{k}\right)=1\right) \\
& \left.\Leftrightarrow \exists\left(y_{1}, z_{1}\right) \cdot \forall z_{2} \ldots Q_{k} z_{k} \cdot F^{\prime \prime}\left(x,\left(y_{1}, z_{1}\right), z_{2}, \ldots, z_{k}\right)=1\right)
\end{aligned}
$$

And so $L \in \Sigma_{k}$.
Now notice that if $\mathcal{C}_{1}$ and $\mathcal{C}_{2}$ are two complexity classes, then $\mathcal{C}_{1}=\mathcal{C}_{2}$ implies $\operatorname{coC}_{1}=$ $\operatorname{coC}_{2}$. Thus, we have $\Pi_{k+1}=\operatorname{co} \Sigma_{k+1}=\operatorname{co} \Sigma_{k}=\Pi_{k}=\Sigma_{k}$. So we have $\Pi_{k+1}=\Sigma_{k+1}=\Sigma_{k}$.

## $2 \quad \mathrm{BPP} \subseteq \Sigma_{2}$

This result was first shown by Sipser and Gács. Lautemann gave a much simpler proof which we give below.

Lemma 5 If $L$ is in BPP then there is an algorithm $A$ such that for every $x$,

$$
\underset{r}{\mathbb{P}}(A(x, r)=\text { right answer }) \geq 1-\frac{1}{3 m},
$$

where the number of random bits $|r|=m=|x|^{O(1)}$ and $A$ runs in time $|x|^{O(1)}$.

Proof: Let $\hat{A}$ be a BPP algorithm for $L$. Then for every $x$,

$$
\underset{r}{\mathbb{P}}(\hat{A}(x, r)=\text { wrong answer }) \leq \frac{1}{3},
$$

and $\hat{A}$ uses $\hat{m}(n)=n^{o(1)}$ random bits where $n=|x|$.
Do $k(n)$ repetitions of $\hat{A}$ and accept if and only if at least $\frac{k(n)}{2}$ executions of $\hat{A}$ accept. Call the new algorithm $A$. Then $A$ uses $k(n) \hat{m}(n)$ random bits and

$$
\underset{r}{\mathbb{P}}(A(x, r)=\text { wrong answer }) \leq 2^{-c k(n)} .
$$

We can then find $k(n)$ with $k(n)=\Theta(\log \hat{m}(n))$ such that $\frac{1}{2^{\operatorname{ck(n)}} \leq \frac{1}{3 k(n) m(n)} .}$
Theorem $6 \mathrm{BPP} \subseteq \Sigma_{2}$.
Proof: Let $L$ be in BPP and $A$ as in the claim. Then we want to show that

$$
x \in L \Longleftrightarrow \exists y_{1}, \ldots, y_{m} \in\{0,1\}^{m} \forall z \in\{0,1\}^{m} \bigvee_{i=1}^{m} A\left(x, y_{i} \oplus z\right)=1
$$

where $m$ is the number of random bits used by $A$ on input $x$.
Suppose $x \in L$. Then

$$
\begin{aligned}
& \mathbb{P}_{y_{1}, \ldots, y_{m}}\left(\exists z A\left(x, y_{1} \oplus z\right)=\cdots=A\left(x, y_{m} \oplus z\right)=0\right) \\
& \leq \sum_{z \in\{0,1\}^{m}} \underset{y_{1}, \ldots, y_{m}}{\mathbb{P}}\left(A\left(x, y_{1} \oplus z\right)=\cdots=A\left(x, y_{m} \oplus z\right)=0\right) \\
& \leq 2^{m} \frac{1}{(3 m)^{m}} \\
& <1
\end{aligned}
$$

So

$$
\begin{aligned}
\underset{y_{1}, \ldots, y_{m}}{\mathbb{P}}\left(\forall z \bigvee_{i} A\left(x, y_{i} \oplus z\right)\right) & =1-\underset{y_{1}, \ldots, y_{m}}{\mathbb{P}}\left(\exists z A\left(x, y_{1} \oplus z\right)=\cdots=A\left(x, y_{m} \oplus z\right)=0\right) \\
& >0
\end{aligned}
$$

So a sequence $\left(y_{1}, \ldots, y_{m}\right)$ exists, such that $\forall z . \bigvee_{i} A\left(x, y_{i} \oplus z\right)=1$.
Conversely suppose $x \notin L$. Then fix a sequence $\left(y_{1}, \ldots, y_{m}\right)$. We have

$$
\begin{aligned}
\underset{z}{\mathbb{P}}\left(\bigvee_{i} A\left(x, y_{i} \oplus z\right)\right) & \leq \sum_{i} \underset{z}{\mathbb{P}}\left(A\left(x, y_{i} \oplus z\right)=1\right) \\
& \leq m \cdot \frac{1}{3 m} \\
& =\frac{1}{3} .
\end{aligned}
$$

So

$$
\begin{aligned}
\underset{z}{\mathbb{P}}\left(A\left(x, y_{1} \oplus z\right)=\cdots=A\left(x, y_{m} \oplus z\right)=0\right) & =\underset{z}{\mathbb{P}}\left(\bigvee_{i} A\left(x, y_{i} \oplus z\right)=0\right) \\
& \geq \frac{2}{3} \\
& >0 .
\end{aligned}
$$

So for all $y_{1}, \ldots, y_{m} \in\{0,1\}^{m}$ there is a $z$ such that $\bigvee_{i} A\left(x, y_{i} \oplus z\right)=0$.

## 3 The Karp-Lipton Theorem

Theorem 7 (Karp-Lipton) If $\mathbf{N P} \subseteq \operatorname{SIZE}\left(n^{O(1)}\right)$ then $\Sigma_{2}=\Pi_{2}$ and therefore the polynomial hierarchy would collapse to its second level.

Before proving the above theorem, we first show a result that contains some of the ideas in the proof of the Karp-Lipton theorem.

Lemma 8 If $\mathbf{N P} \subseteq \operatorname{SIZE}\left(n^{O(1)}\right)$ then for every polynomial time computable $F(\cdot, \cdot)$ and every polynomial $p(\cdot)$, there is a family of polynomial size circuits such that

$$
C_{|x|}(x)=\left\{\begin{array}{l}
y: F(x, y)=1 \quad \text { if such a } y \text { exists } \\
\text { a sequence of zeroes } \quad \text { if otherwise }
\end{array}\right.
$$

Proof: We define the circuits $C_{n}^{1}, \ldots, C_{n}^{p(n)}$ as follows:
$C_{n}^{i}$, on input x and bits $b_{1}, \ldots, b_{i-1}$, outputs 1 if and only if there is a satisfying assignment for $F(x, y)=1$ where $y_{1}=b_{1}, \ldots, y_{i-1}=b_{i-1}, y_{i}=1$.

Also, each circuit realizes an NP computation, and so it can be built of polynomial size. Consider now the sequence $b_{1}=C_{n}^{1}(x), b_{2}=C_{n}^{2}\left(b_{1}, x\right), \ldots, b_{p(n)}=C_{n}^{p(n)}\left(b_{1}, \ldots, b_{p(n)-1}, x\right)$, as shown in the following picture:


The reader should be able to convince himself that this is a satisfying assignment for $F(x, y)=1$ if it is satisfiable, and a sequence of zeroes otherwise.

We now prove the Karp-Lipton theorem.
Proof: [Of Theorem ??] We will show that if $\mathbf{N P} \subseteq \operatorname{SIZE}\left(n^{O(1)}\right)$ then $\Pi_{2} \subseteq \Sigma_{2}$. By a result in a previous lecture, this implies that $\forall k \geq 2 \Sigma_{k}=\Sigma_{2}$.

Let $L \in \Pi_{2}$, then there is a polynomial $p(\cdot)$ and a polynomial-time computable $F(\cdot)$ such that

$$
x \in L \leftrightarrow \forall y_{1} \cdot\left|y_{1}\right| \leq p(|x|) \exists y_{2} \cdot\left|y_{2}\right| \leq p(|x|) \cdot F\left(x, y_{1}, y_{2}\right)=1
$$

By using Lemma ??, we can show that, for every $n$, there is a circuit $C_{n}$ of size polynomial in $n$ such that for every $x$ of length $n$ and every $y_{1},\left|y_{1}\right| \leq p(|x|)$,

$$
\exists y_{2} \cdot\left|y_{2}\right| \leq p(|x|) \wedge F\left(x, y_{1}, y_{2}\right)=1 \text { if and only if } F\left(x, y_{1}, C_{n}\left(x, y_{1}\right)\right)=1
$$

Let $q(n)$ be a polynomial upper bound to the size of $C_{n}$.
So now we have that for inputs $x$ of length $n$,

$$
x \in L \leftrightarrow \exists C .|C| \leq q(n) . \forall y_{1} \cdot\left|y_{1}\right| \leq p(n) . F\left(x, y_{1}, C\left(x, y_{1}\right)\right)=1
$$

which shows that $L$ is in $\Sigma_{2}$.

