Chapter 3 - Inside **NP**

- co-classes and co-**NP**
- existence of languages that are neither in **P** nor **NP**-complete
- Relations between classes **P**, **NP**, and co-**NP**

Between **P** and **NP**

- **NPC** $:=$ class of **NP**-complete problems
- Write $L_1 =_p L_2$, if $L_1 \leq_p L_2$ and $L_2 \leq_p L_1$

Theorem 3.1 (Ladner)

If $\mathbf{P} \neq \mathbf{NP}$*, then there is a language* $L \in \mathbf{NP}$*, that is neither in* **P** *nor in* **NPC***.*

Co-classes

Definition 3.2

Let **C** *be a class of languages. The class co-***C** *is defined by*

$$\textit{co-}\mathbf{C} := \left\{ L \,\middle|\, \textit{the complement } \bar{L} \textit{ of } L \textit{ is in } \mathbf{C} \right\}.$$

In particular,

$$\textit{co-}\mathbf{NP} := \left\{ L \,\middle|\, \textit{the complement } \bar{L} \textit{ of } L \textit{ is in } \mathbf{NP} \right\}.$$

Remarks

- Note that co-**C** is (in general) not the complement of **C**.
- For complement $\bar{L}$ of language L, ignore malformed elements.
- $\mathbf{P} = \text{co-}\mathbf{P}$ and $\mathbf{PSPACE} = \text{co-}\mathbf{PSPACE}$

NP and co-NP

Example

- A tautology is a Boolean formula ϕ that is true for all assignments to its variables.
- $\mathit{TAUT} := \{\langle\phi\rangle \mid \phi \text{ is a tautology}\}$
- $\mathit{TAUT} \in \text{co-}\mathbf{NP}$

Theorem 3.3

If $\mathbf{NP} \neq \textit{co-}\mathbf{NP}$*, then* $\mathbf{P} \neq \mathbf{NP}$*.*

Alternative characterizations for **NP** and co-**NP**

Theorem 3.4

$L \subseteq \Sigma^*$ is in **NP***, if and only if $k \in \mathbb{N}$ and $A \in \mathbf{P}$ exist with*

$$L = \left\{ x \in \Sigma^* \,\middle|\, \exists z \in \{0,1\}^{|x|^k} : (x,z) \in A \right\}.$$

Corollary 3.5

*$L \subseteq \Sigma^*$ is in co-***NP***, if and only if $k \in \mathbb{N}$ and $B \in \mathbf{P}$ exist with*

$$L = \left\{ x \in \Sigma^* \,\middle|\, \forall z \in \{0,1\}^{|x|^k} : (x,z) \in B \right\}.$$

co-**NP**-completeness

Definition 3.6

*A language B is co-**NP**-complete, if it satisfies two conditions:*

1. $B \in$ *co-**NP**, and*
2. *every language $A \in$ co-**NP** is polynomial time reducible to B.*

*We denote by co-**NPC** the class of co-**NP**-complete languages.*

P, **NP**, and co-**NP**

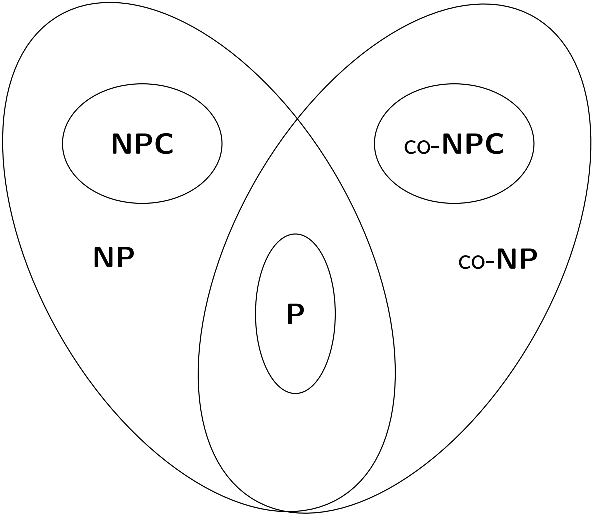
Theorem 3.7

If there is a **NP***-complete language* A *that is in co-***NP***, then* **NP** $=$ *co-***NP***.*

Corollary 3.8

If **NP** $\neq$ *co-***NP***, then languages in* **NP** $\cap$ *co-***NP** *are not* **NP***-complete.*

Conjectured relations between **P**, **NP**, co-**NP**



Ladner's theorem

Theorem 3.1 (Ladner)

If $\mathbf{P} \neq \mathbf{NP}$*, then there is a language* $L \in \mathbf{NP}$*, that is neither in* $\mathbf{P}$ *nor in* $\mathbf{NPC}$*.*

A strange variant of SAT

- M_i TM with Gödel number i.
- For $H : \mathbb{N} \to \mathbb{N}$ define language SAT_H as follows:

$$SAT_H := \left\{ \psi 01^{n^{H(n)}} : \psi \in SAT \text{ und } |\psi| = n \right\}$$

- $$SAT_H(x) := \begin{cases} 1, & \text{if } x \in SAT_H \\ 0, & \text{if } x \notin SAT_H \end{cases}$$

- Use specific $H : \mathbb{N} \to \mathbb{N}$ defined as follows:

  $H(n)$ is the smallest number $i < \log\log(n)$ such that for every $x \in \{0,1\}^*$ with $|x| \leq \log(n)$ the Turing machine M_i outputs $SAT_H(x)$ within $i|x|^i$ steps. If there is no such number i, then $H(n) = \log\log(n)$.

Properties of H and SAT_H

Lemma 3.9

1. *H is well-defined.*
2. *H can be computed in time $\mathcal{O}(n^3)$.*

Lemma 3.10

1. *If $SAT_H \in \mathbf{P}$, then there is a constant $C \in \mathbb{N}$ such that $H(n) \leq C$ for all n.*
2. *If $SAT_H \notin \mathbf{P}$, then for every $C \in \mathbb{N}$ there are only finitely many $n \in \mathbb{N}$ with $H(n) \leq C$. In particular,*

$$\lim_{n \to \infty} H(n) = \infty.$$

The final steps of the proof

Case $SAT_H \in \mathbf{P}$

$\Rightarrow$ $H(n) \leq C$ for some constant C (Lemma 3.10)

$\Rightarrow$ For all Boolean formulas ψ

$$\left|\psi 0 1^{|\psi|^{H(|\psi|)}}\right| \leq |\psi|^{C+1}.$$

$\Rightarrow$ $SAT \in \mathbf{P}$ and $\mathbf{P} = \mathbf{NP}$. $\lightning$

The final steps of the proof

Case $SAT_H \in \mathbf{NPC}$

- $\Rightarrow$ There is a polynomial time reduction f from SAT to SAT_H. Assume f can be computed in time n^C.
- $\Rightarrow$ There is $n_0 \in \mathbb{N}$ with $H(n) \geq 2C$ for all $n \geq n_0$ (Lemma 3.10)
- $\Rightarrow$ For all ϕ with $|\phi| > n_0^2$, if $f(\phi) = \psi 01^{|\psi|^{H(|\psi|)}}$, then $|\psi| \leq \sqrt{|\phi|}$.
- $\Rightarrow$ $SAT \in \mathbf{P}$ and $\mathbf{P} = \mathbf{NP}$. $\lightning$