Berechenbarkeit & Komplexität Modulkonferenz 23.01.24

$P \subseteq NP \cap coNP \overset{?}{\subseteq} P$

Faktorisieren $= \{ \langle n,k \rangle \mid n,k \in \mathbb{N} \wedge \exists_{q \in \mathbb{N}}\ q \mid n \wedge 1 < q \leq k \}$

n hat Teiler $1 < q \leq k$

Fak $\in NP$: ja Zertifikat: q selbst → poly $(|\langle n,k \rangle|)$ groß
→ in poly-Zeit v. DTM überprüfbar

Fak $\in coNP$: nein Zertifikat: Primfaktorzerlegung von n
poly $(|\langle n \rangle|)$ groß weil max $\log n$ Primfaktoren jeder $\leq n$

Reduktionsfunktion

$$f: \Sigma^* \to \Sigma^*$$

$$f(\langle \varphi \rangle) = \langle g, k \rangle \qquad f(\varphi) = (g, k)$$

X NP-vollständiges Problem in coNP? Dann $NP = coNP$

$NP \subseteq coNP$

$coNP \subseteq NP$

$$\frac{L \in NP}{L \leq_m^P X \wedge X \in coNP \Rightarrow L \in coNP}$$

$$\frac{L \in coNP}{\overline{L} \in NP \Rightarrow \overline{L} \in coNP \Leftrightarrow L \in NP}$$

"Kollaps der Polynomzeithierarchie"

$$TAUT = \{\langle\varphi\rangle \mid \forall_{\text{Belegungen } \beta \text{ d. Var. in } \varphi} \ \beta \text{ erfüllt } \varphi\}$$

$$\overline{TAUT} = \Sigma^* \setminus TAUT$$

$$= \underbrace{\{x \in \Sigma^* \mid x \text{ codiert keine Formel}\}}_{\in P} \cup \underbrace{\{\langle\varphi\rangle \mid \langle\varphi\rangle \notin TAUT\}}$$

$$\{\langle\varphi\rangle \mid \exists_{\text{Bel. } \beta} \ \beta \text{ erfüllt } \varphi \text{ nicht}\}$$
$$\in NP$$

$$\in NP \quad (\text{insbesondere: } \forall L \in P, L' \in NP \ L \cup L' \in NP)$$

$\overline{SAT} = \{\langle\varphi\rangle \mid \varphi \text{ unerfüllbar}\} = UNSAT$ coNP-vollständig

TODO: ja-Zertifikat für X ist nein-Zertifikat für $\overline{X}$

Definitionen von NP

① $L \in NP \Leftrightarrow L$ kann von NTM in polynomieller Zeit entschieden werde
(χ_L kann in poly Zeit berechnet)

② $L \in NP \Leftrightarrow \overline{L} \in coNP$

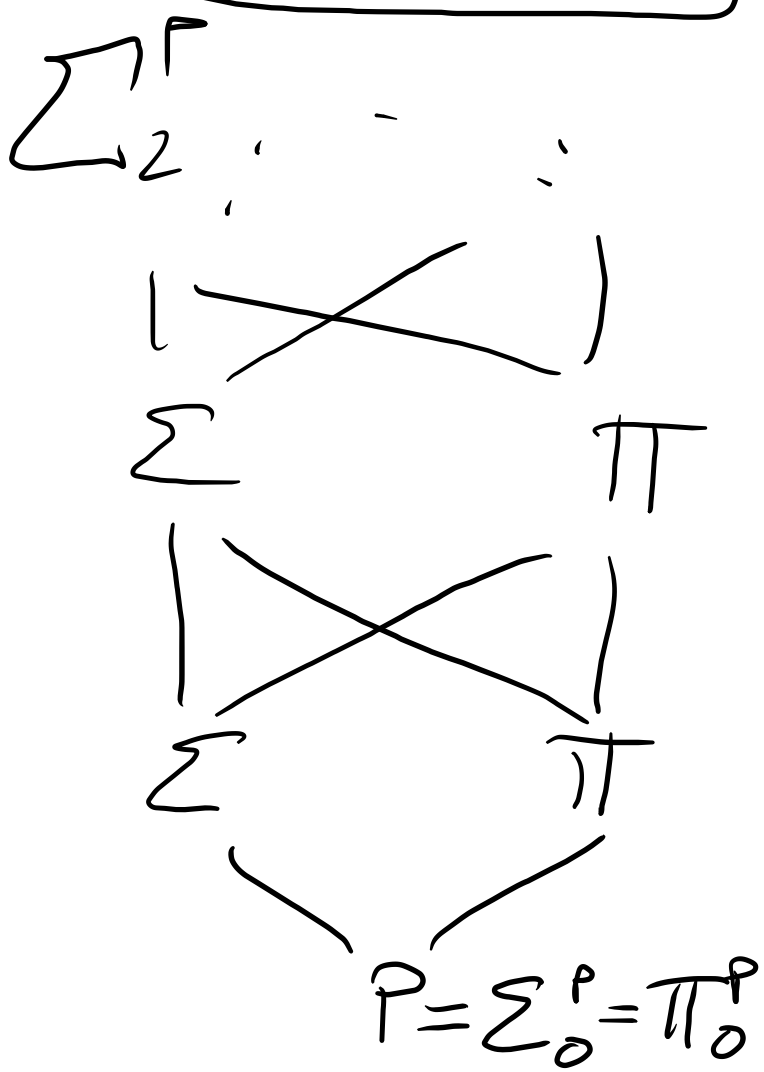
③ $L \in NP \Leftrightarrow \exists$ DTM M sodass $\forall_{x \in \Sigma^*} \left(\exists_{u \in \Sigma^*} |u| \leq poly(|x|) \right.$
$\left. \& \; \langle u, x \rangle \in T(M) \Leftrightarrow x \in L \right)$

④ $L \in NP \Leftrightarrow L \leq_m^P SAT$

$$VC^* = \{\langle G,k\rangle \mid \text{jedes kleinste VC in } G \text{ hat Größe } = k\}$$

$$= \{\langle G,k\rangle \mid \underbrace{\exists_{VC\ X \subseteq G}\ |X| \leq k}_{\in NP?} \wedge \underbrace{\forall_{VC\ X \subseteq G}\ |X| \geq k}_{\in coNP?}\}$$

TPSPACE



NP	$\exists_x P(x)$	
coNP	$\forall_x P(x)$	
Σ_2^P	$\exists_x \forall_y P(x,y)$	$\Pi_2^P \forall_x \exists_y P(x,y)$
Σ_3^P	$\exists_x \forall_y \exists_z P(x,y,z)$	$\Pi_3^P \forall_x \exists_y \forall_z P(x,y,z)$
⋮		
PSPACE		