Beko Modulkonferenz 26.01.23

$\leq$ $\leq_m^P$

Tee Problem: gg. n Liter Wasser & k Teeblätter
können Sie n Liter Tee kochen?

Wasser Problem: gg n Liter Wasser
können Sie die kochen?

Super Wasser Problem: gg n L. Wasser
können Sie, die kochen & im Lotto gewinnen

Wasser Problem $\leq_m^P$ Tee Problem $\leq$ SW Problem

f: Bottich Wasser ohne Teeblätter

Tee Problem $\leq_m^P$ Wasser Problem

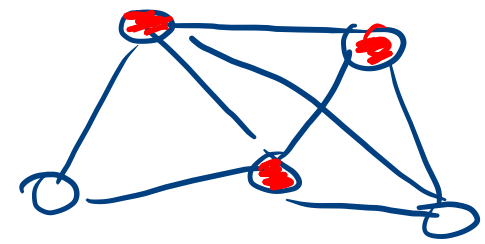
f: schmeiß die Teeblätter in den Bottich

„schwerer im Sinne $\leq$"

SW Problem $\not\leq$ Tee Problem

VC $L_{VC} = \{\langle G, k\rangle \mid k \in \mathbb{N}$, G hat Knotenüberdeckung der Größe $\leq k\}$

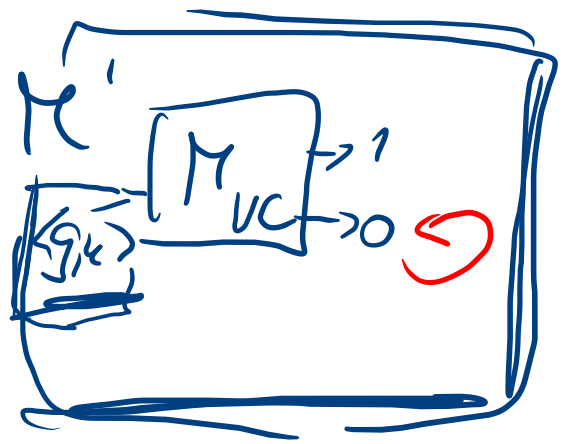
$Q: \exists X \subseteq V(G),\ |X| \leq k,\ \forall_{uv \in E(G)}\ u \in X \vee v \in X$



$VC \leq_m^P H_0$

$f: (G, k) \to \pi$

G hat VC der Größe $\leq k \iff \pi$ hält auf ε



Falls. VC entscheidbar $\rightsquigarrow \exists$ TM M_{VC}

π' hält $\iff M_{VC}$ hält mit Ausgabe 1

$\iff \langle G, k\rangle \in VC$

- f polynomiell berechenbar

$H_0 \not\leq_m^P VC$ da H_0 unentscheidbar

NP

(1) Guess & check: $L \in NP \Leftrightarrow \exists$ poly-time DTM M s.d.

$x \in L \Leftrightarrow \exists \underbrace{u \in \Sigma^{poly(|x|)}}$ $\langle u, x \rangle \in T(M)$

(2) $L \in NP \Leftrightarrow \exists$ poly-time NTM M s.d. $L = T(M)$

(3) $L \in NP \Leftrightarrow \overline{L} \in coNP$

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

„$\Rightarrow$" da SAT NP-vollständig

„$\Leftarrow$" Lemma Folie 49

$NP = \{ L \mid L \leq_m^P SAT \}$

NP & coNP

Independent Set $\rightsquigarrow \in NP$

In: $G, k \in \mathbb{N}$

Q: $\exists X \subseteq V(G),\ |X| \geq k\ .\ \forall_{uv \in E(G)}\ u \notin X \vee v \notin X$

Independent Set $\rightsquigarrow \in coNP$

In: $G, k \in \mathbb{N}$

Q: $\forall X \subseteq V(G),\ |X| < k \vee \exists_{uv \in E(G)}\ u \in X \wedge v \in X$

gibt es ein IS der Größe $\geq k$?

↳ keine Ja-Zertifikate

haben alle IS in G Größe $< k$?

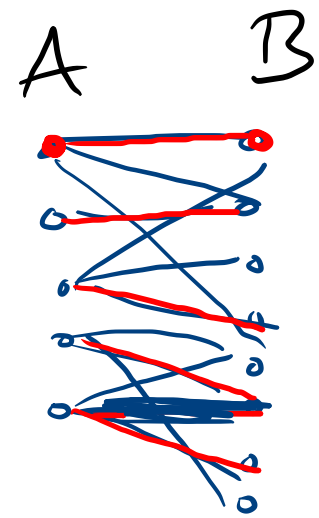
↳ keine Nein-Zertifikate

genau so

Es gibt keine „kurzen" Beweise dafür dass eine aussagenlogische Formel eine Tautologie ist

$\exists L \in NP \cap coNP$ mit $L \notin P$

$\Rightarrow P \subsetneq NP \cap coNP$



① In: bipartiter Graph $G=(A \dot\cup B, E)$

Q: $\exists$ Matching der Größe $|A|$ in G?

$\hookrightarrow X \subseteq E(G)$ sd. $uv, xy \in X$ $\{u,v\} \cap \{x,y\} = \emptyset$

$\in NP$: X ist kurzes Zertifikat

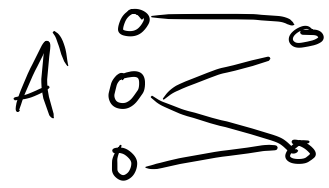
$\in coNP$: Hall's Theorem

jeder Knoten aus A hat Kante

bipartiter Graph $G=(A \dot\cup B, E)$ hat "A-sättiges" Matching

$\Leftrightarrow$

$\forall A' \subseteq A \quad |N(A')| \geq |A'|$



Nein-Zertifikat: $A' \subseteq A$ mit $|N(A')| < |A'|$

Faktorisierung

In: $n, k \in \mathbb{N}$

Q: hat n einen Teiler $g \leq k$ mit $g \neq 1$

$\in NP$: Ja-Zertifikat: g

$\in coNP$: Nein-Zertifikat: Primfaktorzerlegung a_i von n

Verifizierung: ① alle $a_i > k$

② $\prod_i a_i = n$

③ alle a_i prim

Bemerkung

Falls es ein coNP-vollständiges Problem $Q \in \text{co}NP$

dann $NP = \text{co}NP$

$NP \subseteq \text{co}NP$

Bew: ① $NP \subseteq \text{co}NP \iff NP = \text{co}NP$

"$\Leftarrow$" $NP \subseteq \text{co}NP \Rightarrow \text{co}NP \subseteq NP$

"$\Rightarrow$"

Sei $L \in \text{co}NP \iff \overline{L} \in NP \Rightarrow \overline{L} \in \text{co}NP \iff L \in NP$

② Sei $SAT \in \text{co}NP$

Satz $A \leq_m^P B \iff \overline{A} \leq_m^P \overline{B}$

$L \in NP \Rightarrow L \leq_m^P SAT \Rightarrow \overline{L} \leq_m^P \overline{SAT}$ $\in NP$ laut Annahme

$\Rightarrow \overline{L} \in NP \Rightarrow L \in \text{co}NP$