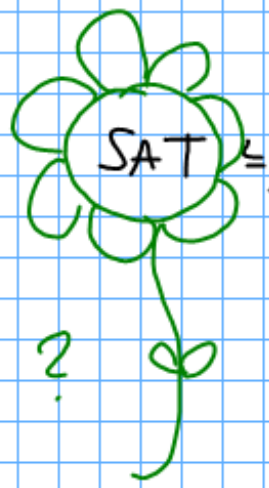
VL 12, 26.1.12



$SAT \leq_p 3\text{-}SAT \leq_p$ Clique $\leq_p$ Stabile Menge $\leq_p$ Vertex Cover

$\leq_p$ DiR. Ham. Cycle $\leq_p$ Ham. Cycle $\leq_p$ TSP ....

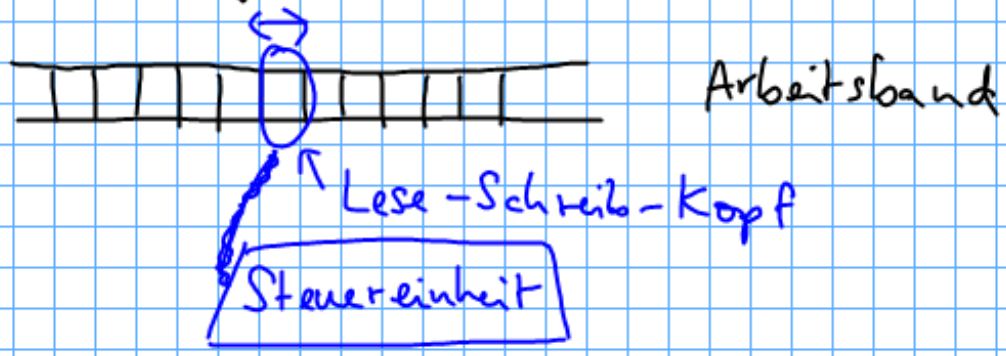
Aber ist denn SAT jetzt „schwer"?

oder

?

Def 5.13 Turingmaschine (Turing, 1912–1954)

Idee:



a) Eine nicht-deterministische Turingmaschine (NTM) wird durch ein 6-Tupel $M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ beschrieben, wobei

Z endl. Menge von Zuständen,

Σ das Eingabealphabet (mit $\sqcup \notin \Sigma$)

Γ das Arbeitsalphabet (mit $\Sigma \cup \{\sqcup\} \subset \Gamma$)

$\delta: Z \times \Gamma \longrightarrow \mathcal{P}(Z \times \Gamma \times \{L, R, N\})$ die Überführungsfunktion

$q_0 \in Z$ der Startzustand

$E \subset Z$ die Menge der Endzustände ist.

b) M heißt deterministische Turingmaschine (DTM),

wenn $\forall (q,a) \in Z \times \Gamma$ gilt: $|\delta(q,a)| \leq 1$

c) Für $(q', a', D) \in \delta(q,a)$ schreiben wir

auch $(q,a) \longrightarrow (q', a', D)$.

Es bedeutet: wenn q der aktuelle Zustand von M

ist und sich der Kopf auf einem mit a beschrifteten

Feld befindet, dann kann M in den Zustand

q' übergehen, das Symbol a durch a' ersetzen,

und den Kopf ein Feld nach links $(D = L)$, nach

rechts $(D = R)$ oder gar nicht $(D = N)$ bewegen.

d) Eine Konfiguration von M ist ein 4-Tupel

$K = (q, u, a, v) \in Z \times \Gamma^+ \times \Gamma \times \Gamma^*$ und besagt,

dass q der momentane Zustand von M ist,

das Band mit $\ldots \sqcup\sqcup u\boxed{a}v\sqcup\sqcup \ldots$ beschriftet

ist und der Kopf gerade auf dem Zeichen a steht.

Die Startkonfiguration bei Eingabe $x = x_1 \dots x_n \in \Sigma^* \setminus \{\varepsilon\}$ ist gegeben durch $K_x = (q_0, \varepsilon, x_1, x_2 \dots x_n)$

und für $x = \varepsilon$ durch $K_x = (q_0, \varepsilon, \sqcup, \varepsilon)$.

Schreibe $K \vdash K'$ wenn sich die Konfiguration K' aus der Konfiguration K durch einen Übergang der TM ergibt.

Schreibe $K \vdash^t K'$, wenn es Konfig. $K_1, \dots, K_{t-1}$ mit $K \vdash K_1 \vdash K_2 \vdash \dots \vdash K_{t-1} \vdash K'$ gibt.

Schreibe $K \vdash^* K'$, wenn es $t \in \mathbb{N}$ mit $K \vdash^t K'$ gibt.

e) Die von M akzeptierte Sprache ist definiert als

$$L(M) = \{ x \in \Sigma^* : \exists \text{ Konfig } K' \in E \times \Gamma^* \times Q \times \Gamma^* \text{ mit } K \vdash^* K' \}.$$

Bsp 5.14

$M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ mit $Z = \{q_0, q_1, q_2, q_3\}$,
$\Sigma = \{a, b\}$, $\Gamma = \{a, b, A, B, \sqcup\}$, $E = \{q_3\}$
und δ enthält die folgenden Anweisungen:

1) $(q_0, a) \to (q_0, A, R)$
2) $(q_0, b) \to (q_0, B, R)$
3) $(q_0, \sqcup) \to (q_1, \sqcup, L)$
4) $(q_1, A) \to (q_2, A, R)$
5) $(q_1, B) \to (q_3, B, R)$

Bsp-Rechnung:
Eingabe aab

$(q_0, \varepsilon, a, ab) \overset{1)}{\vdash} (q_0, A, a, b)$
$\overset{1)}{\vdash} (q_0, AA, b, \varepsilon)$ $\overset{2)}{\vdash} (q_0, AAB, \sqcup, \varepsilon)$
$\overset{3)}{\vdash} (q_1, AA, B, \varepsilon)$ $\overset{5)}{\vdash} (q_3, AAB, \sqcup, \varepsilon)$
$\in E \times \Gamma^* \times \Gamma \times \Gamma^*$

$$L(M) = \{x = x_1 \dots x_n \in \Sigma^* : x_n = b\}.$$

Bem: „Turing-berechenbar"
Church-Turing-These: Die Klasse der Turing-berechenbaren Probleme ist identisch mit der Klasse der intuitiv berechenbaren Probleme.

Def 5.15

a) Betrachte eine Funktion $f: \Sigma^* \to \Gamma^* \cup \{?\}$.
Für $x \in \Sigma^*$ mit $f(x) = ?$ sagen wir $f(x)$ ist „undefiniert", $\mathrm{dom}(f) := \{x \in \Sigma^* : f(x) \neq ?\}$.

b) Eine DTM M berechnet f, falls

$\forall x \in \mathrm{dom}(f)$: M gibt bei Eingabe x das Wort $f(x)$ aus und „stoppt"

$\forall x \in \Sigma^* \setminus \mathrm{dom}(f)$: M hält bei Eingabe von x nicht an.

c) Die Laufzeit einer NTM M bei Eingabe x ist def. als

$$\mathrm{time}_M(x) := \begin{cases} \max\{t \in \mathbb{N}_0 : \exists \text{ Konfig. } K \; k_x \vdash^t K\} \\ \infty \quad \text{falls} \end{cases}$$

↑ diese Menge unendlich ist

d) Sei $t: \mathbb{N} \to \mathbb{N}$. Dann heißt M $t(n)$-zeitbeschränkt, wenn $\mathrm{time}_M(x) \leq t(|x|)$ für alle Eingaben x gilt.

↑ Länge der Eingabe

e) $P := \bigcup_{k:=1}^{\infty} \{ L(M) : M \text{ ist eine } n^k\text{-zeitbeschränkte DTM} \}$

$NP := \bigcup_{k:=1}^{\infty} \{$ NTM $\}$

Bsp 5.16 $k \in \mathbb{N}$

$k\text{-COL} := \{ \langle G \rangle : G \text{ ist } k\text{-färbbarer Graph}, \langle G \rangle \text{ ist seine Codierung als 0,1-Adjazenzmatrix} \}$

$1\text{-COL} \in P$, denn man kann mit einer DTM in $O(|\text{Eingabe}|)$ überprüfen, ob der Graph leer ist.

$2\text{-COL} \in P$, denn .... #A!

Bsp 5.17

3-COL $\in$ NP, denn wir können die folgende NTM M konstruieren:

1. Gebe jedem Knoten eine der Farben 1, 2, oder 3 (nicht-deterministisch!)
2. Überprüfe, ob alle Kanten nicht-einfarbig sind:
   falls ja, gehe in Zustand $q_Y \in E$
   falls nein, gehe in Zustand $q_N \in Z \setminus E$ und „bleibe da stehen".

Dann gilt: $L(M)$ = 3-COL, denn genau die Codierungen von 3-färbbaren Graphen können akzeptiert werden.

Def 5.18 Betrachte $A \subset \Sigma^*$ und $B \subset \Gamma^*$.

a) $A \leq_p B$: $\Leftrightarrow \exists k \in \mathbb{N}$ Funktion $f: \Sigma^* \to \Gamma^*$ mit
vgl Def 5.5
$\forall x \in \Sigma^*: \quad x \in A \Leftrightarrow f(x) \in B$
und f durch eine $t(n)$-zeitbeschränkte DTM berechnet werden kann, wobei $t(n) \leq n^k$.

b) B heißt NP-schwer, wenn: $\forall A \in NP: A \leq_p B$.

c) B heißt NP-vollständig (Kurz $\in NPC$), wenn gilt:
$B \in NP$ und NP-schwer.

Prop 5.19 Wenn $A \leq_p B$ und $B \in P$, dann auch $A \in P$.

Bew: ~~Sch~~ klar.

Prop 5.20

a) $P \subseteq NP$

b) Die Relation $\leq_p \subseteq NP \times NP$ ist transitiv.

c) Wenn $A \leq_p B$ und A NP-schwer ist, dann ist auch B NP-schwer.

d) Wenn es ein $A \in P$ gibt, so dass A NP-schwer ist, dann $P = NP$.

Bew: a) Klar, weil jede DTM auch NTM ist.

b) $A \leq_p B$, $B \leq_p C \Rightarrow A \leq_p C$ klar.

c) Sei $L \in NP$ beliebig. z.z: $L \leq_p B$.

$L \leq_p A \leq_p B$ (b)

$L \leq_p A$: Weil A NP-schwer

d) Sei $L \in NP$ beliebig. z.z: $L \in P$.

Da A NP schwer, gilt $L \leq_p A$. Da $A \in P$, muss nach 5.19 auch $L \in P$ sein.