3.2 NP-Vollständigkeit

Def Seien $A \subseteq \Sigma^*$ und $B \subseteq \Gamma^*$ Sprachen.

Dann heißt A auf B reduzierbar in polynomieller Zeit ("polynomial reduzierbar"), symbolisch $A \leq_p B$, falls es eine totale und in polynomieller Laufzeit berechenbare Funktion $f: \Sigma^* \to \Gamma^*$ gibt, sodass für alle $w \in \Sigma^*$:

$$w \in A \text{ gdw. } f(w) \in B$$

Bem: Spezialisierung des allgemeinen Reduktionsbegriffs.

Lemma Falls $A \leq_p B$ und $B \in P$ ($B \in NP$), so ist auch $A \in P$ ($A \in NP$).

Bew: Sei $A \leq_p B$ mittels f jeweils, wobei

M_f die TM, die f in Zeit $p(n)$ berechnet.

χ_B wird durch M_B in $q(n)$ Zeit berechnet.

p, q sind Polynome

$\rightarrow M_f \rightarrow M_B \rightarrow$ berechnet χ_A in Zeit:

$$p(|w|) + q(|f(w)|) \leq p(|w|) + q(p(|w|))$$

$\leq$

Polynom

D.h. die Laufzeit kann durch ein Polynom abgeschätzt werden. Das gilt sowohl für det. als auch für nicht-det. TMs. Damit folgt, dass $A \in P$ ($A \in NP$).

□

Exkurs:

$$P = \bigcup_{p \text{ Polynome}} TIME(p(n))$$

$$NP = \bigcup_{p \text{ Polynome}} NTIME(p(n))$$

$$P \subseteq NP$$

?

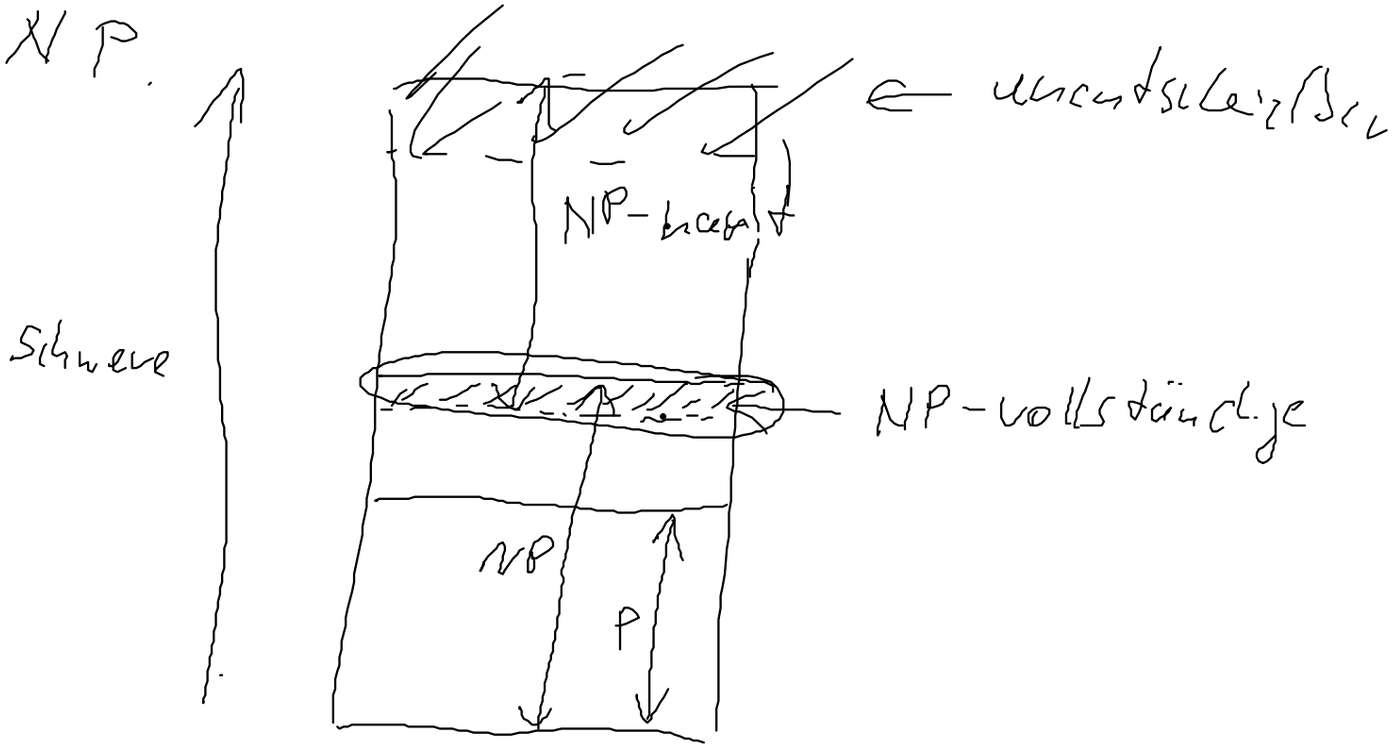
Beobachtung: $\leq_p$ ist transitiv und reflexiv ($\hat{=}$ Quasiordnung)

Frage: Wie findet man schwerste Probleme?

Def Eine Sprache A heißt NP-hard, falls für alle Sprachen $L \in NP$ gilt: $L \leq_p A$. Eine Sprache A heißt NP-vollständig, falls A NP-hard ist und $A \in NP$.

$P = NP$

$\Rightarrow N = 1$



Satz Sei A NP-vollständig. Dann gilt:

$A \in P$ gdw. $P = NP$.

Bew: $\Leftarrow$: Falls $P = NP$, dann folgt $A \in P$, weil $A \in NP$.

$\Rightarrow$: Sei $A \in P$ und sei $L \in NP$ beliebig. Da A NP-hard, gilt $L \leq_p A$. Mit obigem Lemma folgt $L \in P$. Da L beliebig, gilt $P = NP$. $\square$

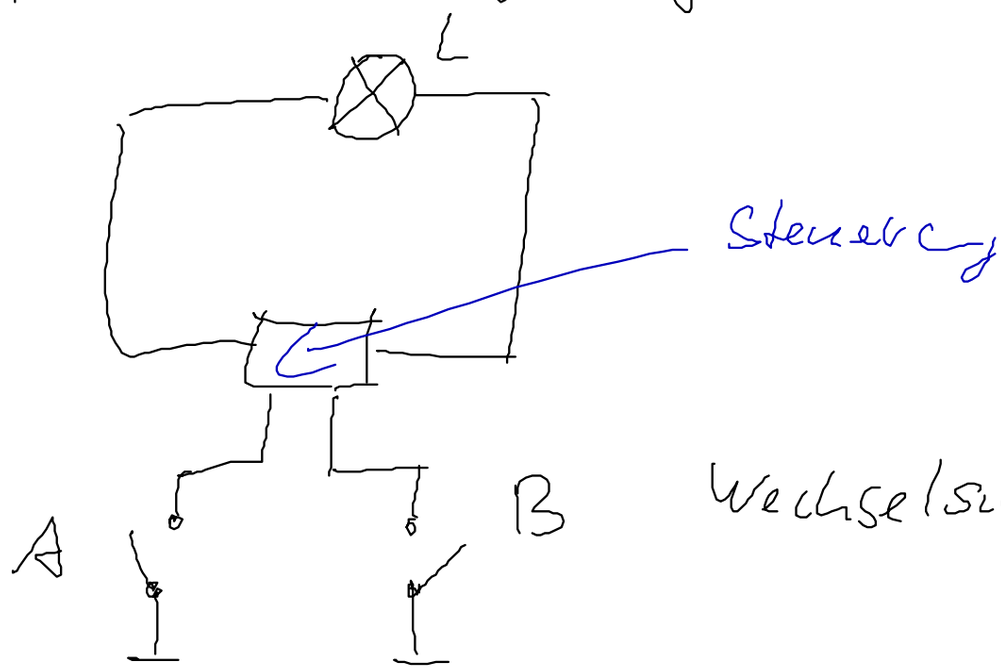
Frage: Wie identifiziere wir die erste NP-vollständige Sprache. SAT

Def.: Das Erfüllbarkeitsproblem der Aussagenlogik ist definiert durch:

Gegeben: Ein Formel F der Aussagenlogik

Gefragt: Ist F erfüllbar (ev. eine Belegung, die die Formel F wahr macht)?

Exkurs: Modellierung dynamischer Systeme mit Hilfe von Aussagenlogik



Wird ein Schalter bewegt, dann ändert sich der Status von L.

Initial: alle Schalter sind aus (offen) und das Licht ist auch aus

Frage: Gibt es eine Folge Schaltungen, so dass eine Situation erreicht wird, in der beide Schalter an sind und die Lampe ist aus?

Formalisierung mit Hilfe der Aussagenlogik

- Indizierte Variablen mit Zeitpunkten
- Änderungen formulieren
- Erfüllende Belegung $\hat{=}$ mögliche Abfolge von Zeitpunkten

Zeitpunkt 0 1 2 ... 3

$L_0 = F$ $L_1 = T$ $L_2 = T$ | $L_3 = F$

$A_0 = F$ $A_1 = T$ $A_2 = T$ | $A_3 = T$

$B_0 = F$ $B_1 = F$ $B_2 = F$ | $B_3 = T$

Anfangsbed.: $\neg L_0 \wedge \neg A_0 \wedge \neg B_0$

Übergänge: $((A_i \leftrightarrow \neg A_{i+1}) \wedge (B_i \leftrightarrow B_{i+1})) \rightarrow (L_i \leftrightarrow \neg L_{i+1})$

$\neg((A_i \leftrightarrow A_{i+1}) \wedge (B_i \leftrightarrow \neg B_{i+1})) \rightarrow (L_i \leftrightarrow \neg L_{i+1})$

$((A_i \leftrightarrow A_{i+1}) \wedge (B_i \leftrightarrow B_{i+1})) \rightarrow (L_i \leftrightarrow L_{i+1})$

$\neg((A_i \leftrightarrow \neg A_{i+1}) \wedge (B_i \leftrightarrow B_{i+1}))$

k Formeln jeweils

Notation: $G(x_1, \dots, x_n)$ modelliert $x_1, \dots, x_n$ Boolesche Var. sind, Soll wahr sein gdw. genau eines der x_i wahr ist.

Größe der Formel $O(n^2)$

$$G(x_1, \dots, x_n) = \underbrace{\bigvee_{i=1}^{n} x_i}_{\text{mind. 1 } x_i} \wedge \underbrace{\left(\bigwedge_{j=1}^{n-1} \bigwedge_{\ell=j+1}^{n} \neg(x_j \wedge x_\ell) \right)}_{\text{nicht zwei gleichzeitig wahr.}}$$

mind. 1 x_i soll wahr sein

nicht zwei gleichzeitig wahr.

Satz (Cook)

SAT ist NP-vollständig.

Bew: SAT $\in$ NP: Rate Belegung und überprüfe, ob die Belegung die Formel wahr macht. Kann in poly-Zeit auf NTM abgearbeitet werde.

SAT ist NP-hart: Generische Reduktion. Sei $L \in NP$ beliebig.

Zu zeigen $L \leq_p SAT$

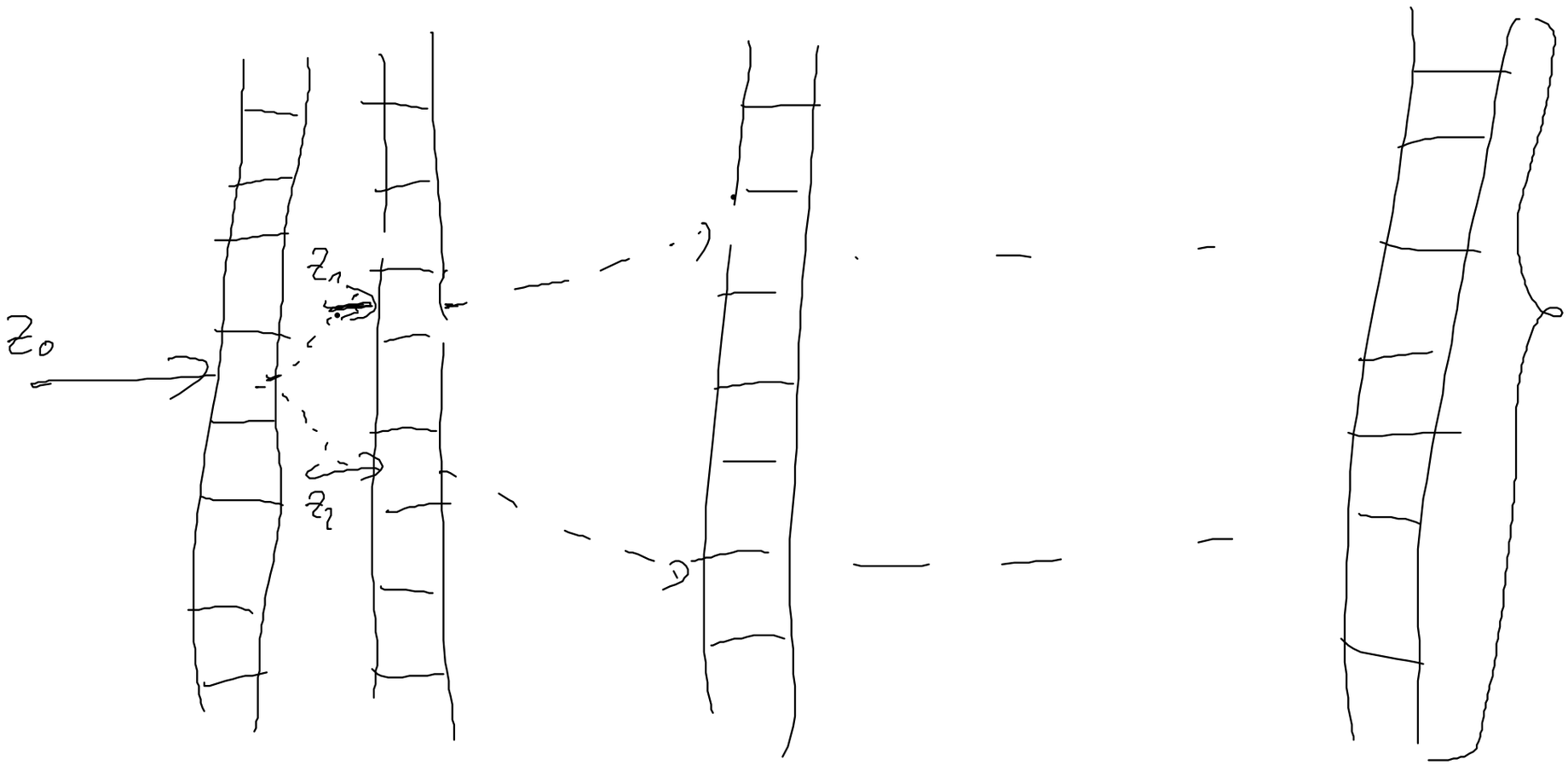
Sei M_L die nicht-det. TM die L akzeptiert mit Laufzeit $p(n)$, wobei n Eingabelänge ist.

Sei $w \in \Sigma^*$ $\longrightarrow$ es zeige eine Formel F_w mit

die baue ich Rechnung

$$w \in L \text{ gdw } F_w \in SAT$$

Zeitpunkte 0 1 i p(n)



Aufgaben