§4 Such- und Entscheidungsprobleme

<u>bislang:</u> haben nur Entscheidungsprobleme / Sprachen betrachtet; diese waren in der Theorie einfacher zu behandeln.

In der Praxis sind Suchprobleme wichtiger, z.B. wollen wir nicht nur wissen, ob eine 3-SAT Formel erfüllbar ist, wir wollen auch eine erfüllende Belegung finden.

Aber beide Probleme sind polynomialzeit-äquivalent. D.h.

<u>Satz</u> Falls $SAT \in P$, dann gibt es polynomialzeit-Algorithmus, der bei Eingabe einer erfüllbaren Formel F mit atomaren Formeln $A_1, \dots, A_m$ eine erfüllende Belegung berechnet.

<u>Bew.:</u> Sei M eine poly. Zeit beschr. TM, die SAT entscheidet. Verwende M, um zu entscheiden, ob die Formel F_0 und die Formel F_1 erfüllbar ist. Dabei entsteht F_0 aus F, indem $A_1 = 0$ gesetzt wird, genauso F_1, indem $A_1 = 1$ gesetzt wird. Man kann F_0 und F_1 als KNF schreiben, und man kann F_0, F_1 in poly. Zeit aus F berechnen.

Da F erfüllbar ist, ist F_0 oder F_1 erfüllbar, OE F_1. Setze nun $A_2 = 0$ bzw. $A_2 = 1$ und bestimme KNF F_{10} bzw. F_{11} und wende M an. Nun kann man mit Hilfe von $2m$ Aufrufen von M eine erfüllende Belegung von F bestimmen. $\boxtimes$

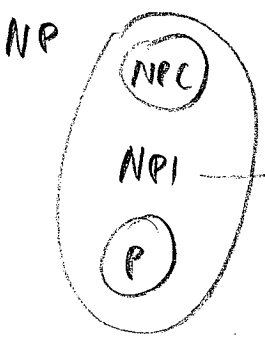
§5 NP-unvollständige Probleme

Im Szenario $P \neq NP$ gibt es viele Probleme, die in P liegen, und viele, die NP-vollständig sind.

<u>Natürliche Frage</u>: Ist $NP \setminus P = NPC$?

<u>Antwort</u>: Nein, falls $P \neq NP$ (Satz von Ladner)

Nein, falls $P = NP$ (trivial)



NP-incomplete, NP-intermediate

<u>Satz</u> (Ladner, 1975)

Falls $P \neq NP$, dann gibt es eine Sprache $L \in NP \setminus P$, die nicht NP-vollständig ist.

<u>Bew.</u>: (durch eine Variante des Diagonalarguments)

Seien $M_1, M_2, \ldots$ TMs, so dass M_i bei Eingabe von x in Zeit $|x|^i$ läuft und für jede Sprache $L \in P$ gibt es ein Index i, so dass die TM M_i die Sprache L erkennt.

Genauso seien $f_1, f_2, \ldots$ Fkten, die in Zeit $|x|^i$ berechenbar sind, und die alle poly. Zeit berechenbaren Fkt.en enthalten.

Definiere

$$L = \{ \langle F \rangle : \langle F \rangle \in SAT,\ f(|\langle F \rangle|) \text{ ist gerade} \}$$

$$\subseteq SAT,$$

wobei $f : \mathbb{N} \to \mathbb{N}$ induktiv definiert wird:

$\underline{f(0) = f(1) = 2.}$

$\underline{n \to n+1}$:

1. Falls $(\log n)^{f(n)} \geq n$, dann $f(n+1) = n$

2. Sonst:

   (a) $f(n)$ gerade, $f(n) = 2i$.

   Setze $f(n+1) = f(n) + 1$, falls es eine Formel F gibt mit $|\langle F \rangle| \leq \log n$ und

   (i) M_i akzeptiert $\langle F \rangle$ und $\langle F \rangle \notin L$. oder

   (ii) M_i verwirft $\langle F \rangle$ und $\langle F \rangle \in L$.

Sonst setze $f(n+1) = f(n)$.

(b) $f(n)$ ungerade, $f(n) = 2i+1$

Setze $f(n+1) = f(n)+1$, falls es eine Formel F gibt mit $|\langle F\rangle| \leq \log n$ und

(i) $\langle F\rangle \in SAT$ und $f_i(\langle F\rangle) \notin L$

(ii) $\langle F\rangle \notin SAT$ und $f_i(\langle F\rangle) \in L$.

Die Fkt. $f(n)$ ist wohldefiniert und man kann sie polynomiell zeitbeschränkt in n berechnen, weil nur Formeln F mit $|\langle F\rangle| \leq \log n$ betrachtet werden und im Fall (b) gilt

$$|x|^i \leq (\log n)^i \leq (\log n)^{f(n)} < n.$$

<u>Das</u> impliziert auch, dass $L \in NP$ ist.

<u>Beh.</u> Die Fkt. f ist monoton wachsend und unbeschränkt.

<u>Bew.</u> klar nach Def.: f ist monoton wachsend.

Ang. f ist beschränkt, d.h. $\exists N : f(n) = m$ für alle $n \geq N$.

<u>1. Fall:</u> m gerade, $m = 2i$.

Dann liefern nur endlich viele Werte n den Fkt.wert $f(n) < 2i$, insbesondere sind nur endlich viele Fkt.werte ungerade. Also ist $SAT \setminus L$ endlich, also in P. Gleichzeitig erkennt die poly. zeitbeschränkte TM M_i die Sprache L, also auch $L \in P$.

Zusammen $SAT = L \cup SAT \setminus L \in P$, im Widerspruch zu $P \neq NP$.

<u>2. Fall:</u> m ungerade, $m = 2i+1$

Dann liefern nur endlich viele Werte n den Fkt.wert $f(n) < 2i+1$, insbesondere sind nur endlich viele Fkt.werte gerade. Also ist L endlich, also in P.

Gleichzeitig ist f_i ein polynomielle Reduktion $SAT \leq_p L$. Also $SAT \in P$, im Widerspruch zu $P \neq NP$.

$\boxtimes$

Da f unbeschränkt wächst, werden alle poly. zeitbeschränkten TMs ausgeschlossen, die L entscheiden könnten, d.h. $L \notin P$. Genauso werden alle polynomiellen Reduktionen $SAT \leq_p L$ ausgeschlossen, d.h. $L \notin NPC$. $\boxtimes$

Die im Beweis konstruierte Sprache L ist sehr künstlich und nur eine Ausdünnung von SAT. Nur wenige Kandidaten für NP-unvollständige Sprachen sind bekannt, z.B. GI (Graphenisomorphie) oder

$$FACTORING = \{ \langle N, L, U \rangle : \exists p \text{ prim}, p \in [L, U], \text{ und } p \mid N \}.$$