Polynomialzeitreduktion

Def.: Sei $L_1, L_2 \subset \Sigma^*$. Falls es eine totale, *in polynomieller Zeit* berechenbare Funktion $f : \Sigma^* \to \Sigma^*$ gibt, mit

$$\forall w \in \Sigma^* : w \in L_1 \text{ gdw. } f(w) \in L_2,$$

so heisst L_1 auf L_2 *polynomiell reduzierbar mittels* f

"$L_1 \leq_p L_2$"

Eigenschaften der Polynomzeitreduktion

Satz: Sei $L_1, L_2 \subset \Sigma^*$ mit $L_1 \leq_p L_2$. Dann gilt

- $L_2 \in P \to L_1 \in P$

Bew.:

- $L_1 \leq_p L_2$ mittels f → es gibt dtm T mit $f_T = f$ und $t_T(n) \leq n^r$ für ein $r > 0$
- $L_2 \in P$ → es gibt dtm M mit $L(M) = L_2$ und $t_M(n) \leq n^s$ für ein $s > 0$
- Konstruiere dtm N mit $L(N) = L_1$
  - berechne mittels T den Wert $f(w)$ bei Eingabe w
  - entscheide mittels M, ob $f(w) \in L_2$

→ $t_M(n) = O(n^{rs})$

Beispiel Polynomialzeitreduktion

Satz: HAMILTON $\leq_p$ SUBGRAPHISO

Bew.:

- Funktion f mit

  $f(\langle G \rangle) := \langle G,C \rangle$ wobei C = Kreis mit $|V(G)|$ Knoten

  ist in polynomieller Zeit berechenbar
- es ist $\langle G \rangle \in$ HAMILTON gdw. $\langle G,C \rangle \in$ SUBGRAPHISO

NP-Vollständigkeit

Def.: $L \subset \Sigma^*$ heisst

- *NP-schwer*, falls $\forall L' \in$ **NP** : $L' \leq_p L$
- *NP-vollständig*, falls $L \in$ **NP** und L **NP**-schwer ist

NPH := {$L \subset \Sigma^*$ | L ist **NP**-schwer}

NPC := {$L \subset \Sigma^*$ | L ist **NP**-vollständig}

L ist **NP**-vollständig → L ist "schwerstes" Problem in **NP**

Polynomzeitreduktionen in NP

Satz:

1. Sei $L \in NPC$. Dann gilt $L \in P$ gdw. $P=NP$
2. Sei $L_1, L_2 \in NP$ mit $L_1 \leq_p L_2$. Dann gilt $L_1 \in NPC \rightarrow L_2 \in NPC$

Bew.: *(→ Übung)*

NP-Vollständige Sprachen

Satz (Cook '71): $SAT \in NPC$

Bew.:

- $SAT \in NP$ (s.o.)

- sei $L \in NP$ beliebig → es gibt ntm M mit $L=L(M)$ und $t_M(n) \leq n^r$ für ein $r>0$

  z.z. $L \leq_p SAT$, d.h. es gibt dtm R mit
  - $t_R(n) \leq n^s$ für ein $s>0$ und
  - $\forall w \in \Sigma^*$: $w \in L$ gdw. $f_R(w) \in SAT$

Satz von Cook (Bew.)

Sei $M=(Q,\Sigma,\Gamma,\delta,q_0,\underline{b},F)$ mit $Q = \{z_1,\ldots, z_k\}$ und $\Gamma = \{a_1,\ldots,a_l\}$

Ziel: R konstruiert bei Eingabe $w=w_1\ldots w_n \in \Sigma^*$ eine boolesche Formel $f_R(w)$ für die gilt:

$w \in L$ gdw. $f_R(w)$ beschreibt einen akzeptierenden Berechnungspfad von M

Satz von Cook (Bew.)

Variablen aus denen $f_R(w)$ zusammengesetzt ist:

Variablen	Indizes	Bedeutung
$zust_{t,z}$	$t \in \{0,\ldots,n^r\}$ $z \in Q$	$zust_{t,z} = 1$ gdw. nach t Schritten ist M im Zustand z
$pos_{t,i}$	$t \in \{0,\ldots,n^r\}$ $i \in \{-n^r,\ldots,0,\ldots,n^r\}$	$pos_{t,i} = 1$ gdw. nach t Schritten ist der Kopf von M in Zelle i
$band_{t,i,a}$	$t \in \{0,\ldots,n^r\}$ $i \in \{-n^r,\ldots,0,\ldots,n^r\}$ $a \in \Gamma$	$band_{t,i,a} = 1$ gdw. nach t Schritten ist Zelle i mit a beschriftet

Satz von Cook (Bew.)

$$f_R(w) := B \wedge A(w) \wedge Ü \wedge Ü^* \wedge E$$

- B beschreibt "Randbedingungen" gültiger Berechnungen von M
- $A(w)$ beschreibt die Anfangskonfiguration von M auf w
- $Ü$, $Ü^*$ beschreiben die Überführungsrelation von M
- E beschreibt das Akzeptanzkriterium von M

Satz von Cook (Bew.)

Randbedingungen B: Zu jedem Zeitpunkt $0 \leq t \leq n^r$ gibt es

- *genau einen* Zustand
- *genau eine* Kopfposition
- *genau ein* Zeichen in jeder Bandzelle

Hilfsformel:

$$G(x_1,\ldots,x_m) := (x_1 \vee \ldots \vee x_m) \wedge (\wedge_{i \neq j}(\neg x_i \vee \neg x_j))$$

- $G(x_1,\ldots,x_m)$ wahr gdw. *genau eine* der Variablen $x_1,\ldots,x_m$ ist wahr
- Länge von $G(x_1,\ldots,x_m) = O(m^2)$

Satz von Cook (Bew.)

Randbedingungen B: Zu jedem Zeitpunkt $0 \le t \le n^r$ gibt es

- *genau einen* Zustand
- *genau eine* Kopfposition
- *genau ein* Zeichen in jeder Bandzelle

$$B := \wedge_{0 \le t \le n^r} [G(zust_{t,z_1}, \ldots, zust_{t,z_k}) \wedge G(pos_{t,-n^r}, \ldots, pos_{t,n^r}) \wedge (\wedge_{-n^r \le i \le n^r} G(band_{t,i,a_1}, \ldots, band_{t,i,a_l}))]$$

- Länge von $B = O(n^r(k^2+n^{2r}+n^r l^2)) = O(n^{3r})$

Satz von Cook (Bew.)

Anfangskonfiguration $A(w)$: Zum Zeitpunkt $t=0$

- ist M im Zustand q_0
- zeigt der Kopf auf die erste Bandzelle
- sind die ersten n Bandzellen mit der Eingabe w beschriftet und alle anderen Bandzellen leer

$$A(w) := zust_{0,q_0} \wedge pos_{0,1} \wedge (\wedge_{-n^r \le i \le 0} band_{0,i,\underline{b}}) \wedge (\wedge_{1 \le i \le n} band_{0,i,w_i}) \wedge (\wedge_{n+1 \le i \le n^r} band_{0,i,\underline{b}})$$

- Länge von $A(w) = O(n^r)$

Satz von Cook (Bew.)

Überführungsrelation Ü: Für $a \in \Gamma$ und $z \in Q$ beschreibt $Ü_{a,z}$ zu jedem Zeitpunkt $0 \leq t \leq n^r$ die möglichen Übergange von M, wenn an der Bandposition $-n^r \leq i \leq n^r$ im Zustand z das Symbol a gelesen wird:

$$Ü_{a,z} := \bigwedge_{0 \leq t < n^r, -n^r \leq i \leq n^r} [(zust_{t,z} \wedge pos_{t,i} \wedge band_{t,i,a}) \Rightarrow \bigvee_{(z',a',y) \in \delta(z,a)} (zust_{t+1,z'} \wedge pos_{t+1,i+y} \wedge band_{t+1,i,a'})]$$

$$Ü := \bigwedge_{a \in \Gamma, z \in Q} Ü_{a,z}$$

- Länge von Ü = $O(n^{2r})$

Satz von Cook (Bew.)

Überführungsrelation Ü*: Für $a \in \Gamma$ beschreibt $Ü^*_a$ zu jedem Zeitpunkt $0 \leq t \leq n^r$, dass an der Bandposition $-n^r \leq i \leq n^r$ sich nichts ändert, wenn der Kopf sich nicht an dieser Position befindet

$$Ü_a^* := \bigwedge_{0 \leq t < n^r, -n^r \leq i \leq n^r} [(\neg pos_{t,i} \wedge band_{t,i,a}) \Rightarrow band_{t+1,i,a}]$$

$$Ü^* := \bigwedge_{a \in \Gamma} Ü_a^*$$

- Länge von Ü* = $O(n^{2r})$

Satz von Cook (Bew.)

Akzeptanzkriterium: Zum Zeitpunkt $t=n^r$

- ist M in einem akzeptierenden Zustand $z \in F$

$$E := \vee_{z \in F} zust_{n^r,z}$$

- Länge von $E = O(1)$

Satz von Cook (Bew.)

$$f_R(w) := B \wedge A(w) \wedge Ü \wedge Ü^* \wedge E$$

Bem.:

- Länge von $f_R(w) = O(n^{3r})$ (*polynomiell* in $n=|w|$)
- f_R kann in polynomieller Zeit berechnet werden

Satz von Cook (Bew.)

Bem.: $w \in L$ gdw. $f_R(w)$ ist erfüllbar

"→": $w \in L$ → es gibt eine akzeptierende Berechnung von M der Länge $\leq n^r$ auf der Eingabe w

Die Belegung der Variablen von $f_R(w)$ gemäss dieser Berechnung erfüllt die Formel

"←": $f_R(w)$ ist erfüllbar → es gibt eine Belegung der Variablen von $f_R(w)$ die die Formel erfüllt

Diese erfüllende Belegung beschreibt eine akzeptierende Berechnung von M der Länge $\leq n^r$ auf der Eingabe w

Bemerkung zum Satz von Cook

CNFSAT = {<F> | F ist erfüllbare aussagenlogische Formel in konjunktiver Normalform}

Satz: CNFSAT $\in$ **NPC**

Bew.: Geeignete Modifikation im obigen Beweis *(→ Übung)*