Polynomialzeitreduktionen

Definition

Es seien $L, L' \in \Sigma^*$. Wir nennen L *polynomiell leichter* als L' bzw. L *polynomiell reduzierbar* auf L', wenn es eine Funktion $f : \Sigma^* \to \Sigma^*$ gibt mit

1. $\forall w \in \Sigma^* : w \in L \Leftrightarrow f(w) \in L'$,
2. f ist in polynomieller Zeit berechenbar.

Wir schreiben $L \preccurlyeq_P L'$.

Beispiel

Jede Variante des Clique-Problems ist polynomiell reduzierbar auf jede Variante des Clique-Problems.

Polynomialzeitreduktionen

Lemma

Es seien $L, L' \in \Sigma^*$. *Dann gilt*

$$L \preccurlyeq_P L' \text{ und } L' \in \mathrm{P} \Rightarrow L \in \mathrm{P}.$$

Die Aussage ist auch richtig, wenn man P *durch* NP *ersetzt.*

Polynomialzeitreduktionen

Lemma (Transitivität)

Es seien $L, L', L'' \in \Sigma^*$. *Dann gilt*

$$L \preccurlyeq_P L' \text{ und } L' \preccurlyeq_P L'' \Rightarrow L \preccurlyeq_P L''.$$

NP-schwer – NP-vollständig

Definition

1. Eine Sprache S heiße NP-*schwer*, wenn für alle $L \in \text{NP}$ gilt $L \preccurlyeq_P S$.
2. Eine Sprache S heiße NP-*vollständig*, wenn
   1. S NP-*schwer* ist und
   2. $S \in \text{NP}$ gilt.

NP-schwer – NP-vollständig

Definition

1. Eine Sprache S heiße NP-*schwer*, wenn für alle $L \in \text{NP}$ gilt $L \preccurlyeq_P S$.
2. Eine Sprache S heiße NP-*vollständig*, wenn
   1. S NP-*schwer* ist und
   2. $S \in \text{NP}$ gilt.

Satz

Es sei $S \in \Sigma^*$. Dann gilt

$$S \text{ NP-schwer/vollständig und } S \in \text{P} \Rightarrow \text{P} = \text{NP}.$$

NP-schwer – NP-vollständig

Definition

1. Eine Sprache S heiße NP-*schwer*, wenn für alle $L \in \text{NP}$ gilt $L \preccurlyeq_P S$.
2. Eine Sprache S heiße NP-*vollständig*, wenn
   1. S NP-*schwer* ist und
   2. $S \in \text{NP}$ gilt.

Satz

Es sei $S \in \Sigma^*$. Dann gilt

$$S \text{ NP-schwer/vollständig und } S \in \text{P} \Rightarrow \text{P} = \text{NP}.$$

Beweis.

1. $\text{P} \subseteq \text{NP}$: ✓
2. $\text{NP} \subseteq \text{P}$:
   - $L \in \text{NP}$ beliebig
   - S NP-schwer $\Rightarrow L \preccurlyeq_P S$
   - $S \in \text{P} \Rightarrow L \in P$ (vgl. 1. Lemma)

□

NP-schwer – NP-vollständig

Andere Formulierung des Satzes

$$\text{P} \neq \text{NP} \text{ und } S \text{ NP-vollständig} \Rightarrow S \notin \text{P}$$

NP-schwer – NP-vollständig

Andere Formulierung des Satzes

$$\text{P} \neq \text{NP} \text{ und } S \text{ NP-vollständig} \Rightarrow S \notin \text{P}$$

Interpretation

Wenn man von einer Sprache S zeigt, dass sie NP-vollständig ist, dann ist dies auf Grund der Vermutung P $\neq$ NP ein starker Grund zur Annahme, dass $S \notin P$, dass also S nicht effizient lösbar ist.

NP-schwer – NP-vollständig

Wie zeigt man, dass eine Sprache NP-schwer ist?

- direkt oder
- mit dem folgenden Lemma:

NP-schwer – NP-vollständig

Wie zeigt man, dass eine Sprache NP-schwer ist?

- direkt oder
- mit dem folgenden Lemma:

Lemma

Es seien $L, S \in \Sigma^*$. *Dann gilt*

$$L \text{ NP-}\textit{schwer und } L \preccurlyeq_P S \Rightarrow S \text{ NP-}\textit{schwer.}$$

NP-schwer – NP-vollständig

Wie zeigt man, dass eine Sprache NP-schwer ist?

- direkt oder
- mit dem folgenden Lemma:

Lemma

Es seien $L, S \in \Sigma^*$*. Dann gilt*

$$L \text{ NP-}\textit{schwer und } L \preccurlyeq_P S \Rightarrow S \text{ NP-}\textit{schwer.}$$

Beweis.

- $L' \in$ NP beliebig
- L NP-schwer $\Rightarrow L' \preccurlyeq_P L$
- zusammen mit $L \preccurlyeq_P S \Rightarrow L' \preccurlyeq_P S$ (Transitivität von $\preccurlyeq_P$) □

P-UNIV

Definition

$$\text{P-UNIV} = \{\text{cod}(M)\,\$\,w\,\$\,1^m \mid \text{nichtdet.TM } M \text{ akzeptiert } w \text{ in} \leq m \text{ Schritten}\}$$

P-UNIV

Definition

P-UNIV $=$

$\{\text{cod}(M)\,\$\,w\,\$\,1^m \mid \text{nichtdet.TM } M \text{ akzeptiert } w \text{ in} \leq m \text{ Schritten}\}$

Satz

P-UNIV *ist* NP-*vollständig.*

P-UNIV

Definition

P-UNIV $=$

$\{\text{cod}(M)\,\$\,w\,\$\,1^m \mid \text{nichtdet.TM } M \text{ akzeptiert } w \text{ in} \leq m \text{ Schritten}\}$

Satz

P-UNIV *ist* NP-*vollständig.*

Beweis.

1. P-UNIV $\in$ NP: Simuliere M auf Eingabe w für m richtig geratene Schritte.

□

P-UNIV

Definition

P-UNIV $=$

$\{\text{cod}(M)\,\$\,w\,\$\,1^m \mid \text{nichtdet.TM } M \text{ akzeptiert } w \text{ in} \leq m \text{ Schritten}\}$

Satz

P-UNIV *ist* NP*-vollständig.*

Beweis.

1. P-UNIV $\in$ NP: Simuliere M auf Eingabe w für m richtig geratene Schritte.
2. $L \preccurlyeq_P$ P-UNIV für jedes $L \in$ NP: L wird von einer nichtdet. TM M mit Laufzeit $\leq c \cdot n^k$ akzeptiert. Baue TM F, die als Ausgabe $\text{cod}(M)\,\$\,w\,\$\,1^{c \cdot n^k}$ produziert. F hat Laufzeit $O(n^k)$. □

MERF – Mehrwertige Erfüllbarkeit

MERF

Instanz:

- Variablen $Y_1, \ldots, Y_n$ mit (endlichen) Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form
  - $Y_i = a$
  - $Y_i \neq a$
  - $Y_i = Y_j$
  - $Y_i \neq Y_j$

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

MERF – Mehrwertige Erfüllbarkeit

MERF

Instanz:
- Variablen $Y_1, \ldots, Y_n$ mit (endlichen) Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form
  - $Y_i = a$
  - $Y_i \neq a$
  - $Y_i = Y_j$
  - $Y_i \neq Y_j$

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

Definition

$$\text{MERF} = \{\text{cod}(Y_1) \cdots \text{cod}(Y_n) \,\$\, \text{cod}(B_1) \cdots \text{cod}(B_n) \,\$\, \text{cod}(F) \mid F \text{ erfüllbar}\}$$

MERF – Mehrwertige Erfüllbarkeit

MERF

Instanz:
- Variablen $Y_1, \ldots, Y_n$ mit (endlichen) Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form
  - $Y_i = a$
  - $Y_i \neq a$
  - $Y_i = Y_j$
  - $Y_i \neq Y_j$

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

Definition

$$\text{MERF} = \{\text{cod}(Y_1) \cdots \text{cod}(Y_n) \,\$\, \text{cod}(B_1) \cdots \text{cod}(B_n) \,\$\, \text{cod}(F) \mid F \text{ erfüllbar}\}$$

Satz

MERF *ist* NP-*vollständig.*

$$MERF = \{ \langle Y_1 \rangle \langle Y_2 \rangle \dots \langle Y_n \rangle \$ \langle B_1 \rangle \dots \langle B_n \rangle \$ \langle Formel \rangle \mid$$

mehrwertige ⟨FORMEL⟩ ist erfüllbar $\}$

ist NP-vollständig.

z.B: $X_1, X_2, X_3 \; \$\{1,2,3\},\{4,5\},\{1,3,5\}\$$

$$((X_1 = 3 \wedge X_3 \neq 3) \vee (X_2 = 4 \vee X_1 = 1 \vee X_3 \neq 1)) \wedge X_2 = 5$$

Bew: (i) $MERF \in NP$ "errate" erfüllende Belegung und verifiziere

(ii) $\forall L \in NP : L \leq_p MERF$

$L \in NP \Rightarrow \exists$ TM M_L mit $L(M_L) = L$

g ... worst case Laufzeit

$g(n) \leq c \cdot n^k \quad \forall n \in \mathbb{N}$

$c, k \in \mathbb{N}$ (Konstant)

$M_L = (\Sigma, \Gamma, Q, s, F, \delta, \Delta)$

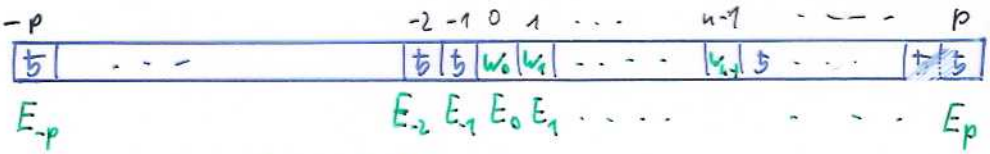
geg $w \in \Sigma^*$

Wollen MERF-Formel F_w

F_w erfüllbar $\Leftrightarrow$ $w \in L$

w wird von M_L akzeptiert

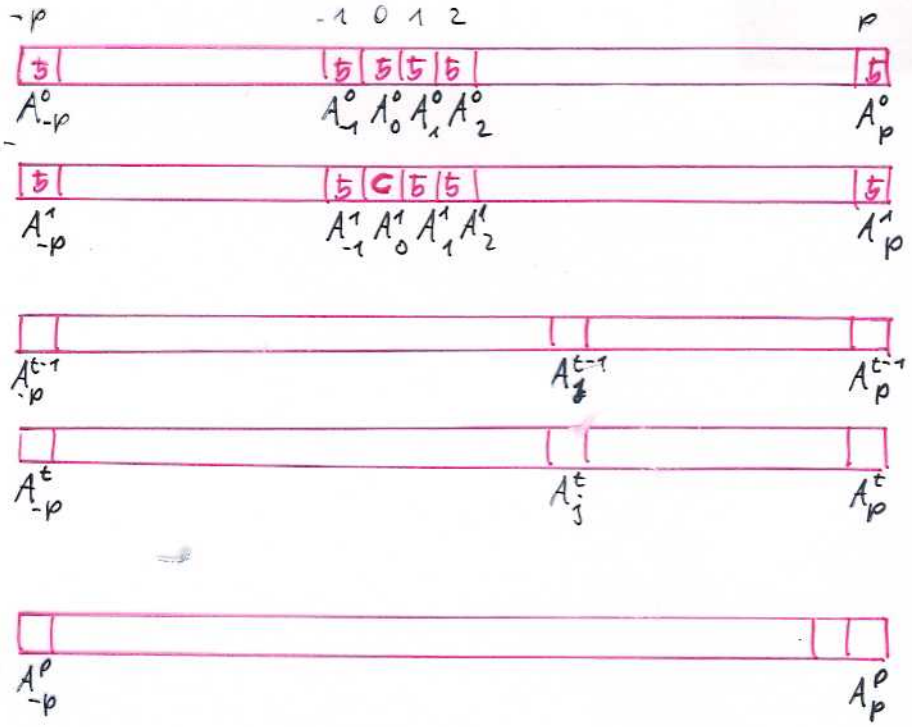
$p = g(|w|)$



Eingabeband

Schritt t	Zustand	E-Kopf Pos.	A-Kopf Pos
0	z^0	I^0	j^0
1	z^1	I^1	j^1
⋮			
$t-1$	z^{t-1}	I^{t-1}	j^{t-1}
t	z^t	I^t	j^t
⋮			
p	z^p	I^p	j^p

A-Bandinhalt



F_w = Anfang $\wedge$ „Übergänge" $\wedge$ Ende

$$\text{Anfang} = (z^0 = s) \wedge (I^0 = 0) \wedge (j^0 = 0) \wedge \big((E_{-p} = \text{b}) \wedge \ldots \wedge (E_{-1} = \text{b}) \wedge (E_0 = w_0) \wedge \ldots \wedge (E_{n-1} = w_{n-1}) \wedge (E_n = \text{b}) \wedge \ldots \wedge (E_p = \text{b})\big) \wedge \big((A^0_{-p} = \text{b}) \wedge \ldots \wedge (A^0_p = \text{b})\big)$$

$$\text{„Übergänge"} = \bigwedge_{1 \le t \le p} \text{„}U^t\text{"} \qquad \text{„}U^t\text{"} = \bigvee_{\substack{-p \le i \le p \\ -p \le j \le p}} \text{„}U^t_{ij}\text{"}$$

$$\text{„}U^t_{ij}\text{"} = (I^{t-1} = i) \wedge (j^{t-1} = j) \wedge \bigwedge_{\substack{-p \le \ell \le p \\ \ell \ne j}} (A^t_\ell = A^{t-1}_\ell) \wedge \bigvee_{(q, a, B, q', \lambda, 3', \mu) \in \Delta} \Big((z^{t-1} = q) \wedge (E_i = a) \wedge (A^{t-1}_j = B) \wedge (z^t = q') \wedge (I^t = i + \lambda) \wedge (A^t_j = B') \wedge (j^t = j + \mu)\Big)$$