P-UNIV

Definition

P-UNIV =

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

P-UNIV

Definition

P-UNIV =

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

Satz

P-UNIV *ist* NP-*vollständig.*

P-UNIV

Definition

P-UNIV =

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

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 $\mathrm{cod}(M)\,\$\,w\,\$\,1^{c \cdot n^k}$ 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.*

SMERF – Simple Mehrwertige Erfüllbarkeit

SMERF

Gegeben:
- Variablen $Y_1, \ldots, Y_n$ mit Wertebereichen $B_1, \ldots, B_n$
- Formel F, die als $\wedge$ und $\vee$ von Termen der Form $Y_i = a$ aufgebaut ist.
  (Terme der Form $Y_i \neq a$, $Y_i = Y_j$ und $Y_i \neq Y_j$ sind nicht erlaubt.)

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

SMERF – Simple Mehrwertige Erfüllbarkeit

SMERF

Gegeben:
- Variablen $Y_1, \ldots, Y_n$ mit Wertebereichen $B_1, \ldots, B_n$
- Formel F, die als $\wedge$ und $\vee$ von Termen der Form $Y_i = a$ aufgebaut ist.
  (Terme der Form $Y_i \neq a$, $Y_i = Y_j$ und $Y_i \neq Y_j$ sind nicht erlaubt.)

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

Satz

SMERF *ist* NP-*vollständig.*

SAT – Boole'sche Erfüllbarkeit

SAT

Gegeben: Boole'sche Formel F in Boole'schen Variablen
Beispiel: $(X_1 \vee X_2 \vee \overline{X_3}) \wedge (X_3 \vee \overline{X_4})$

Frage: Ist F erfüllbar, d. h. gibt es Wahrheitsbelegungen der Variablen, so dass F wahr ist?

SAT – Boole'sche Erfüllbarkeit

SAT

Gegeben: Boole'sche Formel F in Boole'schen Variablen
Beispiel: $(X_1 \vee X_2 \vee \overline{X_3}) \wedge (X_3 \vee \overline{X_4})$

Frage: Ist F erfüllbar, d. h. gibt es Wahrheitsbelegungen der Variablen, so dass F wahr ist?

Satz

SAT *ist* NP-*vollständig.*

3-SAT

3-SAT

Gegeben: Boole'sche Formel F in KNF (konjunktiver Normalform) mit ≤ 3 Literalen pro Klausel, d. h.

- $F = K_1 \wedge \cdots \wedge K_i \wedge \cdots \wedge K_m$
- $K_i = (L_{i1} \vee \cdots \vee L_{ij} \vee \cdots \vee L_{it})$
- Jedes Literal L_{ij} ist eine Variable X_k oder deren Negation $\overline{X_k}$

Frage: Ist F erfüllbar, d. h. gibt es Wahrheitsbelegungen der Variablen, so dass F wahr ist?

3-SAT

3-SAT

Gegeben: Boole'sche Formel F in KNF (konjunktiver Normalform) mit ≤ 3 Literalen pro Klausel, d. h.

- $F = K_1 \wedge \cdots \wedge K_i \wedge \cdots \wedge K_m$
- $K_i = (L_{i1} \vee \cdots \vee L_{ij} \vee \cdots \vee L_{it})$
- Jedes Literal L_{ij} ist eine Variable X_k oder deren Negation $\overline{X_k}$

Frage: Ist F erfüllbar, d. h. gibt es Wahrheitsbelegungen der Variablen, so dass F wahr ist?

Satz

3-SAT *ist* NP-*vollständig.*

$$\text{MERF} = \{ \langle Y_1 \rangle \langle Y_2 \rangle \ldots \langle Y_n \rangle \,\$\, \langle B_1 \rangle \ldots \langle B_n \rangle \,\$\, \langle \text{Formel} \rangle \mid$$

mehrwertige $\langle$FORMEL$\rangle$ 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) $\forall L \in NP : L \leq_p \text{MERF}$

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

$g \ldots$ worst case Laufzeit

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

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

$M_L = (\Sigma, \Gamma, Q, s, F, \not{b}, \Delta)$

geg $w \in \Sigma^*$

Wollen MERF-Formel F_w

F_w erfüllbar $\Longleftrightarrow$ $w \in L$

w wird von M_L akzeptiert

$p = g(|w|)$

$-p$	…	-2	-1	0	1	…	$n-1$	…	p
$\not{b}$	…	$\not{b}$	$\not{b}$	w_0	w_1	…	w_{n-1}	$\not{b}$ …	$\not{b}$
E_{-p}		E_{-2}	E_{-1}	E_0	E_1	…		…	E_p

Eingabeband

Schritt t	Zustand	E-Kopf Pos.	A-Kopf Pos	A-Bandinhalt
				$-p \quad -1 \ 0 \ 1 \ 2 \quad p$
0	Z^0	I^0	J^0	$\not{b}$ … $\not{b}\ \not{b}\ \not{b}\ \not{b}$ … $\not{b}$; $A^0_{-p} \quad A^0_{-1} A^0_0 A^0_1 A^0_2 \quad A^0_p$
1	Z^1	I^1	J^1	$\not{b}$ … $\not{b}$ C $\not{b}\ \not{b}$ … $\not{b}$; $A^1_{-p} \quad A^1_{-1} A^1_0 A^1_1 A^1_2 \quad A^1_p$
⋮				
$t-1$	Z^{t-1}	I^{t-1}	J^{t-1}	$A^{t-1}_{-p} \quad A^{t-1}_j \quad A^{t-1}_p$
t	Z^t	I^t	J^t	$A^t_{-p} \quad A^t_j \quad A^t_p$
⋮				
p	Z^p	I^p	J^p	$A^p_{-p} \quad A^p_p$

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

$$\text{Anfang} = (Z^0 = s) \wedge (I^0 = 0) \wedge (J^0 = 0) \wedge ((E_{-p} = \not{b}) \wedge \ldots \wedge (E_{-1} = \not{b}) \wedge (E_0 = w_0) \wedge \ldots \wedge (E_{n-1} = w_{n-1})$$
$$\wedge (E_n = \not{b}) \wedge \ldots \wedge (E_p = \not{b}))$$
$$\wedge ((A^0_{-p} = \not{b}) \wedge \ldots \wedge (A^0_p = \not{b}))$$

$$\text{Übergänge} = \bigwedge_{1 \leq t \leq p} Ü^t \qquad Ü^t = \bigvee_{\substack{-p \leq i \leq p \\ -p \leq j \leq p}} Ü^t_{ij}$$

$$Ü^t_{ij} = (I^{t-1} = i) \wedge (J^{t-1} = j) \wedge \bigwedge_{\substack{-p \leq l \leq p \\ l \neq j}} (A^t_l = A^{t-1}_l) \wedge$$
$$\wedge \bigvee_{(q, a, B, q', \lambda, B', \mu) \in \Delta} \Big((Z^{t-1} = q) \wedge (E_i = a) \wedge (A^{t-1}_j = B) \wedge (Z^t = q') \wedge (I^t = i + \lambda) \wedge$$
$$\wedge (A^t_j = B') \wedge (J^t = j + \mu) \Big)$$