Teilformeln von Φ

TECHNISCHE UNIVERSITÄT DARMSTADT

$\Phi_{\underline{w}}(V_0,..,V_T) := \mathbf{Config}(V_0) \wedge \mathbf{Config}(V_1) \wedge \ldots \wedge \mathbf{Config}(V_T)$
$\wedge\ \mathbf{Start}_{\underline{w}}(V_0) \wedge \mathbf{Succ}(V_0,V_1) \wedge \ldots \wedge \mathbf{Succ}(V_{T-1},V_T) \wedge \mathbf{Akz}(V_T)$

Boole'sche Variablen von Φ und ihre intuitive Bedeutung:

$d_{s,a,t}$: „Nach Schritt t steht in Bandzelle s das Symbol a“ $a \in \Gamma,\ q \in Q$

$h_{s,t}$: „Nach Schritt t steht der Kopf auf Zelle s“ $s=1..S(|\underline{w}|)$

$z_{q,t}$: „Nach Schritt t ist die Maschine im Zustand q“ $t=0\ldots T(|\underline{w}|)$

$\boldsymbol{V_t}$:= der Teil der Variablen, die zum Rechenschritt #t gehören
$= \{ d_{s,a,t} : a \in \Gamma, s \le S \} \cup \{ h_{s,t} : s \le S \} \cup \{ z_{q,t} : q \in Q \}$

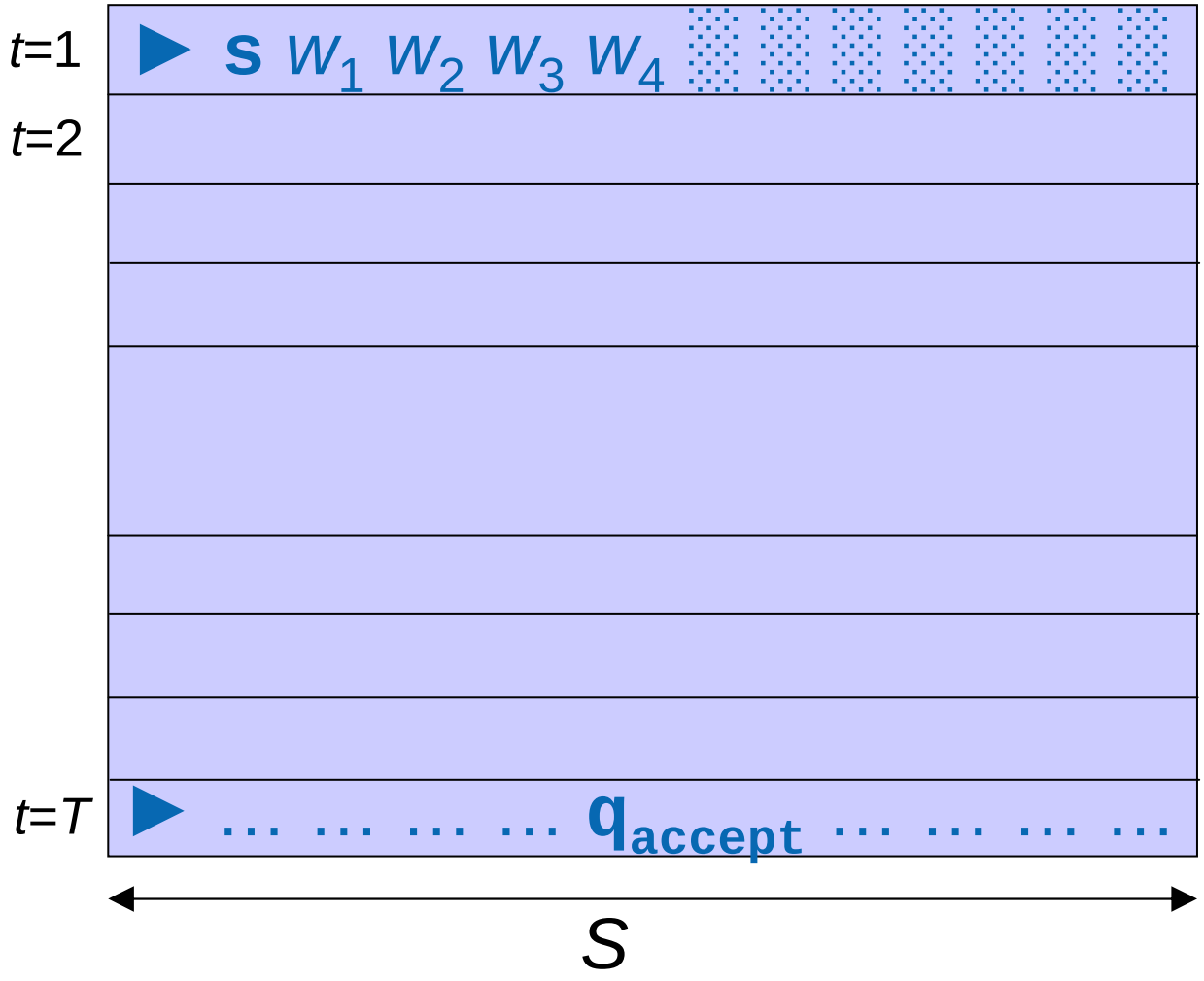
Config(V_t) : wird **wahr** genau für die Belegungen von V_t ,
die eine Konfiguration beschreiben.

Succ(V_t, V_{t+1}) : wird **wahr** genau für die Belegungen von $V_t \cup V_{t+1}$,
die Konfigurationen K und K' beschreiben mit $K \vdash K'$.

$\mathbf{Start}_{\underline{w}}(V_0)$: wird **wahr** genau für Belegung, die $q_0\underline{w}$ beschreibt.

Akz(V_T) **wahr** für Belegung, die einen akz. Endzustand beschreibt

Skizze zum Beweis



Start(V_1,$\underline{w}$)
Succ(V_1,V_2)
Succ(V_2,V_3)

T

Succ(V_{T-1},V_T)
Akz(V_T)

Config(V_1) > … > Config(V_T)

Gibt es solch eine Rechnung auf der NTM?

Gibt es so eine Belegung?

Config(V), Start$_{\underline{w}}$, Akz

TECHNISCHE UNIVERSITÄT DARMSTADT

wahr für Belegungen, die eine Konfiguration beschreiben

$V = \{ d_{s,a} : a \in \Gamma,\ s \le S \} \cup \{ h_s :\ s \le S \} \cup \{ z_q : q \in Q \}$

$d_{s,a}$: „in Bandzelle #s steht das Symbol a“

h_s : „Kopf steht auf Zelle #s“ z_q : „N ist in Zustand q“

Abkürzung **uniq**$(x_1,\ldots,x_r) := (x_1 \vee \ldots \vee x_r) \wedge \bigwedge_{i \neq j} (\neg x_i \vee \neg x_j)$

wahr $\Leftrightarrow$ genau ein x_i ist **wahr**, Länge $O(r^2)$.

Config(V) :=

$\quad$ **uniq**$(h_1,\ldots,h_S) \wedge$ **uniq**$(z_q : q \in Q) \wedge \bigwedge_{s \le S}$ **uniq**$(d_{s,a} : a \in \Gamma)$

hat Länge $O(S^2+|Q|^2+S\cdot|\Gamma|^2) = O(S^2)$, da NTM N fixiert.

Start$_{\underline{w}}(V) := h_1 \wedge z_s \wedge d_{1,w_1} \wedge \ldots \wedge d_{n,w_n} \wedge d_{n+1,B} \wedge \ldots \wedge d_{S,B}$

Akz$(V) := z_{q_+}$ Länge $O(S)$

Start$_{\underline{w}}(V)$: wird **wahr** genau für Belegung, die $q_0\underline{w}$ beschreibt.

Succ(V_t, V_{t+1})

wahr genau für die Belegungen, die aufeinanderfolgende Konfigurationen beschreiben

Abkürzungen: „$x=y$“ $\Leftrightarrow$ $(x \vee \neg y) \wedge (\neg x \vee y)$

$\gamma_{s,q,a,p,b,\mathrm{L}}$:= „$(h_{s,t} \wedge z_{q,t} \wedge d_{s,a,t}) \Rightarrow (z_{p,t+1} \wedge d_{s,b,t+1} \wedge h_{s-1,t+1})$“

$\gamma_{s,q,a,p,b,\mathrm{N}}(V_t, V_{t+1})$ und $\gamma_{s,q,a,p,b,\mathrm{R}}(V_t, V_{t+1})$ analog

„Kopf steht auf Bandzelle #s oder Zelle #s bleibt unverändert“

$$\mathbf{Succ}(V_t, V_{t+1}) := \bigwedge_{s \le S} \bigwedge_{a \in \Gamma} \left(h_{s,t} \vee \text{„}d_{s,a,t} = d_{s,a,t+1}\text{“} \right)$$

$$\wedge \bigwedge_{s \le S} \bigvee_{(p,b,X) \in \delta(q,a)} \gamma_{s,q,a,p,b,X}(V_t, V_{t+1})$$

$d_{s,a,t}$: „Nach Schritt t steht in Bandzelle s das Symbol a“ $a \in \Gamma$, $q \in Q$

$h_{s,t}$: „Nach Schritt t steht der Kopf auf Zelle #s“ $s=1..S$

$z_{q,t}$: „Nach Schritt t ist die Maschine im Zustand q“ $t=0\ldots T$

Zusammenfassung des Beweises

Config(V_t) : wird **wahr** genau für die Belegungen von V_t , die eine Konfiguration beschreiben.

Succ(V_t, V_{t+1}) : wird **wahr** genau für die Belegungen von $V_t \cup V_{t+1}$, die Konfigurationen K und K' beschreiben mit $K \vdash K'$.

Start$_{\underline{w}}$(V_0) : wird **wahr** genau für Belegung, die $q_0\underline{w}$ beschreibt.

Akz(V_T) **wahr** für Belegung, die einen akz. Endzustand beschreibt

Jeweils berechenbar aus $\underline{w}$ in polynom. Zeit

$$\Phi_{\underline{w}}(V_0,..,V_T) := \mathbf{Config}(V_0) \wedge \mathbf{Config}(V_1) \wedge \ldots \wedge \mathbf{Config}(V_T) \wedge \mathbf{Start}_{\underline{w}}(V_0) \wedge \mathbf{Succ}(V_0,V_1) \wedge \ldots \wedge \mathbf{Succ}(V_{T-1},V_T) \wedge \mathbf{Akz}(V_T)$$

Berechenbar in polynom. Zeit und gilt:

N akzeptiert $\underline{w}$ $\Leftrightarrow$ $\Phi_{\underline{w}}$ ist erfüllbar

NP-vollständige Probleme

Def. (Erinnerung): A heißt $\mathcal{NP}$-vollständig, falls $A \in \mathcal{NP}$ und für jedes $L \in \mathcal{NP}$ gilt: $L \leqslant_p A$

Cook-Levin: $\mathbf{SAT}$ ist $\mathcal{NP}$-vollständig.

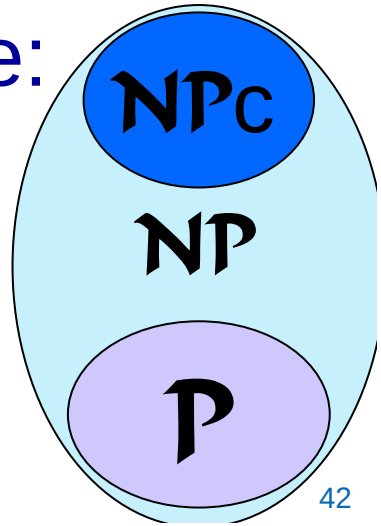
Wissen: $\mathbf{CLIQUE} \equiv_p \mathbf{IS} \leqslant_p \mathbf{SAT} \equiv_p \mathbf{3SAT} \leqslant_p \mathbf{IS}$.

$\Rightarrow$ auch $\mathbf{CLIQUE}$, $\mathbf{IS}$, $\mathbf{3SAT}$ sind $\mathcal{NP}$-vollständig

Lemma. Sei A $\mathcal{NP}$-vollständig und gelte:

- $B \in \mathcal{NP}$
- $A \leqslant_p B$

Dann ist auch B ist $\mathcal{NP}$-vollständig.



SubsetSum $\mathcal{NP}$-*vollständig*

TECHNISCHE UNIVERSITÄT DARMSTADT

Complexity Theory

$\{ \langle a_1,\ldots,a_N,b\rangle \mid a_1,\ldots,a_N,b\in\mathbb{N}, \exists\alpha_1,\ldots,\alpha_N\in\{0,1\} : \; b=\Sigma_i\, a_i\cdot\alpha_i \}$

SubsetSum$\in\mathcal{NP}$ √ Zeige: **3SAT $\leqslant_p$ SubsetSum**

In polynom. Zeit: 3KNF Φ $\rightarrow$ $X\subseteq\mathbb{N}$ und $b\in\mathbb{N}$ mit:

$\exists$erfüllend. Belegung von Φ $\Leftrightarrow$ $\exists Y\subseteq X$: $b=\Sigma_{a\in Y}\, a$

Bsp $\Phi = (x_1 \vee \neg x_3 \vee x_5) \wedge (\neg x_1 \vee x_5 \vee x_4) \wedge (\neg x_2 \vee \neg x_2 \vee \neg x_5)$

v_1 :=	100	10000	v_1' := 010	10000	b := 444 11111
v_2 :=	000	01000	v_2' := 002	01000	c_1:= 100 00000
v_3 :=	000	00100	v_3' := 100	00100	d_1:= 200 00000
v_4 :=	010	00010	v_4' := 000	00010	c_2:= 010 00000
v_5 :=	110	00001	v_5' := 001	00001	d_2:= 020 00000
					c_3:= 001 00000

m Klauseln in *n* Var. $\rightarrow$ 2*n*+2*m*+1 Werte à *n*+*m* Dez.ziffern

Integer Linear Program

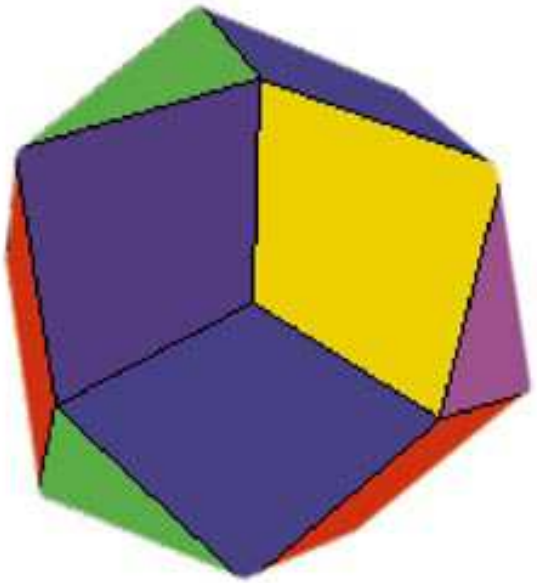
Ein lineares Programm ist ein lin. Ungleichungssystem der Form $A \cdot \underline{y} \leq \underline{b}$ mit $m \times n$–Matrix A und m-dim Vektor b.

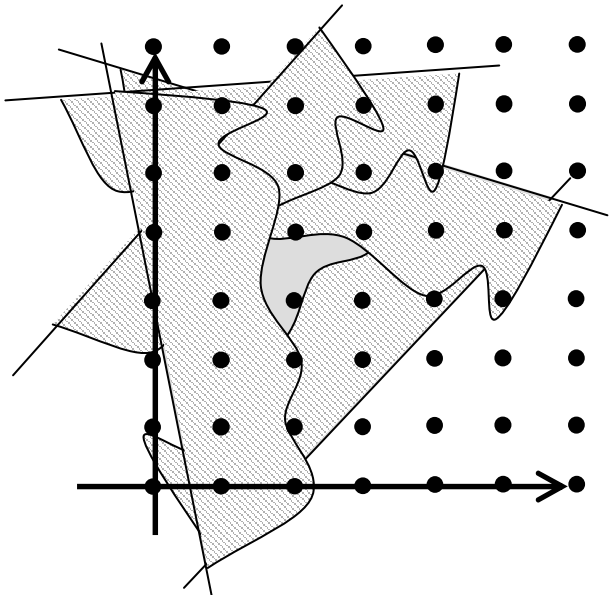
Geometrische Intuition:

$\{\underline{y} \in \mathbb{R}^n \mid \underline{a} \cdot \underline{y} \leq \beta\}$ ist Halbraum,

d.h $\{\underline{y} \in \mathbb{R}^n \mid \underline{a} \cdot \underline{y} \leq \beta\}$ Polytop.

„Enthält es ganz-zahlige Punkte?“





$\mathcal{NP}$-*vollständige Probleme*

SAT $\equiv_p$ **3SAT** $\equiv_p$ **IS** $\equiv_p$ **CLIQUE** $\equiv_p$ **VC** $\equiv_p$ **SubsetSum** $\equiv_p$ **ILP**

$\mathcal{NP}$-vollständige Probleme sind polynomialzeitäquivalent:

$A, B \in \mathcal{NP}$ und $A \leqslant_p B \leqslant_p A$.

Außerdem $\mathcal{NP}$-vollständig:

- Hamiltonkreis (**HC**),
- Travelling Salesperson (**TSP**)

(Beweise in den Übungen)

- und noch über 300 weitere: