

Satz von Cook und Levin satisfiability

propositional logic

Das Erfüllbarkeitsproblem SAT (gag. auss. Formel, ist sie erfüllbar?) ist NP-vollständig.

sogar: 3-SAT ist NP-vollständig

↳ Erfüllbarkeitsproblem für CNF-Formeln mit  $\leq 3$  Literale pro Klausel

Definitionen:

Ein Problem ist eine Teilmenge  $M \subseteq A^*$  A endliches Alphabet, z.B.  $\{0,1\}$

↳ Menge der Wörter über A

Genauer: das Entscheidungsproblem  
ist gegebenes  $w \in A^*$  in  $M$  oder nicht?

Ein Problem ist in  $\overset{\text{- polynomial}}{P}$  ( $= \text{PTIME}$ ), falls es ein Polynom  $t \in \mathbb{R}[x]$  und eine Maschine gibt, die in  $\leq t(\lg(w))$  Berechnungsschritten entscheidet, ob  $w \in M$ .

- Speicherplatz ist unbeschränkt

d.h. richtige Antwort wird ausgetragen

- in der Regul. (deterministische) Turing-Maschine

Ein Problem ist in NP (nicht-deterministisch polynomial) ...

nicht-deterministische Turing-Maschine

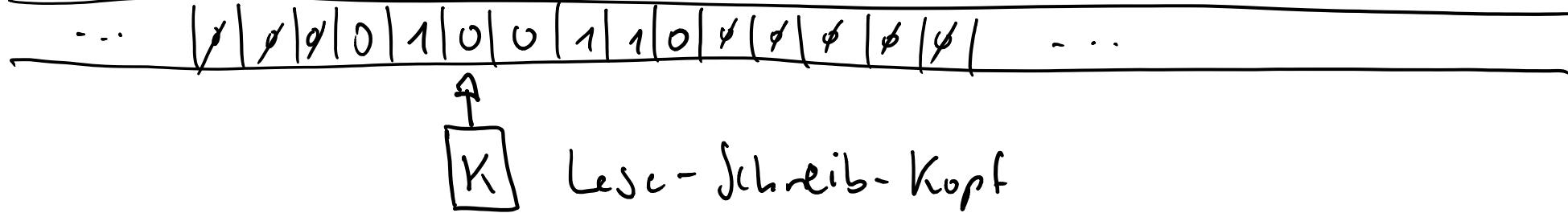
$$P \subseteq NP$$

$=, \neq ?$  großes offenes Problem

$$SAT \in NP$$

# Turing-Maschine (deterministisch)

beidseitig unendliches Speicherband



$A$  endliches Alphabet,  $A^+ = A \cup \{\phi\}$  Symbol dafür, dass  
die Zelle des Bandes leer ist  
(z.B.  $A = \{0, 1\}$ ) □

endliche Zustandsmenge  $Z$  mit Start-Zustand  $z_0 \in Z$   
und Stop-Zustände  $Z_{Stop} \subseteq Z$

Übergangsfunktion  $T: Z \setminus Z_{Stop} \times A^+ \rightarrow Z \times A^+ \times \{\leftarrow, ., \rightarrow\}$

aktueller Zustand    aktuelles Symbol    neuer Zustand    neues Symbol u. 1 Feld links    stechen über    1 Feld nach rechts

Anfangssituation:

$$\overbrace{\varnothing | \varnothing | w_1 | w_2 | \cdot | \dots | w_n | \varnothing | \varnothing | \dots}^{\uparrow \text{K}}$$

$w_i \in A$

Endzustand:

$$\overbrace{\varnothing | \varnothing | w'_1 | w'_2 | \dots | w'_n | \varnothing | \varnothing | \dots}^{\uparrow \text{K}} \quad w'_i \in A$$

$\boxed{K}$  ist irgendwo, Stop-Zustand ist erreicht

Bsp:  $A = \{0, \dots, 9, +\}$

Eingabe

$$\overbrace{\varnothing | \varnothing | 1 | 3 | 9 | 9 | + | 2 | 7 | 7 | 8 | 4 | \varnothing | \varnothing}^{\uparrow \text{K}}$$

# Modell der Berechenbarkeit

Church'sche These: alle ausdrucksstarken Berechenbarkeitsbegriffe sind äquivalent zur Berechenbarkeit durch Turing-Maschinen.

## nicht-deterministische Turing-Maschine

alles wie oben, aber Übergangsrelation statt -funktion:

$$T \subseteq \Sigma/\tau_S \times A^+ \times \Sigma \times A^+ \times \{\leftarrow, ., \rightarrow\}$$

mit: für alle  $\tau \in \Sigma/\tau_S$ ,  $a \in A^+$  gibt es  $\tau' \in \Sigma$ ,  $a' \in A'$ ,  $s \in \{\leftarrow, ., \rightarrow\}$  mit  $(\tau, a, \tau', a', s) \in T$

$M \subseteq A^*$

Problem ist in NP

$\Leftrightarrow$  eine nicht-deterministische Turing-Maschine entscheidet  $M$  in polynomieller Zeit:

wenn  $w \in M$ , dann gibt es einen "Lauf" der Maschine,  
der positive Antwort gibt und polynomial beschränkt ist  
(andernfalls nicht)

$\Leftrightarrow$  existiert endl. Alphabets  $B$ ,  $q \in \mathbb{N} \cup \{\infty\}$

und  $M' \subseteq A^* \times B^*$  mit  $M' \in P$

$w \in M \Leftrightarrow \exists c \in B^*$  mit  $(w, c) \in M'$   $lg(c) \leq q(lg(w))$   
"Zertifikat"

## NP-willständig

$M$  ist NP-willständig  $\Leftrightarrow M \in NP$  und  $M$  ist NP-schwer  
(NP-Hard)

$M$  NP-schwer: für jedes NP-Problem  $N \subseteq B^*$

gibt es eine polynomiale Reduktion von  $M$

d.h.  $r \in \mathbb{IR}[x]$ , berechenbar  $R: B^* \rightarrow A^*$  mit  $l_g(R(w)) \leq r(l_g(w))$   
und  $w \in N \Leftrightarrow R(w) \in M$

Bem: Wenn ein NP-schweres Problem in polynomialem Zeit  
lösbar ist, dann ist jedes NP-Problem in P.

Satz von Cook & Levin: SAT ist NP-vollständig

Beweisidee:  $N \subseteq B^*$  NP-Problem

wird durch nicht-deterministische Turing-Maschine  $TM$  beschrieben

Idee: beschreibe in einer aussagenlogischen Formel das Programm dieser TM  
braucht Aussagenvariablen Zeitpunkt  $t \in \mathbb{N}$ ,  $n \in \mathbb{Z}$ ,  $s \in A^+$ ,  $\tau \in \mathbb{Z}$   
 $Speicherfelder$

$A_{t,n,s}$ : zum Zeitpunkt  $t$  steht im Speicherfeld  $n$  das Symbol  $s$

$\exists_{t,\tau}$ : TM befindet sich zum Zeitpunkt  $t$  im Zustand  $\tau$

$K_{t,n}$ : Kopf befindet sich zum Zeitpunkt  $t$  an der Stelle  $n$

drücken z.B. aus, dass zu jedem Zeitpunkt in jedem Speicherfeld genau ein Symbol steht:

$$t \leq r$$

$$|n| \leq r$$

$$\bigvee_{S \subseteq A^+} (A_{t,n,s} \wedge \bigvee_{s' \neq s} A_{t,n,s'})$$

Schranke aus der polynomischen Beschränkung

$r = r(w)$ , wenn  $w$  entschieden werden soll

$\vdots$   
 $\vdots$   $c_r$

Achtung: Formel bleibt polynomial!

## ≈ 2.7? Semantik der intuitionistischen Aussagenlogik

Brouwer schreibt um 1910 das Prinzip des ausgeschlossenen  
Dritten an

Hilting gibt um 1930 Formalisierungen an

Curry - Howard - Korespondenz:

---

Programme entsprechen math. Beweisen

Syntax: gleiche wie in der klass. Aussagenlogik

hier: Beschränkung auf die Junktoren  $\perp, \top, \vee, \rightarrow$

denn intuitivisch gelten die folgenden Äquivalenzen:

$$\neg A \sim_{int} (A \rightarrow \perp)$$

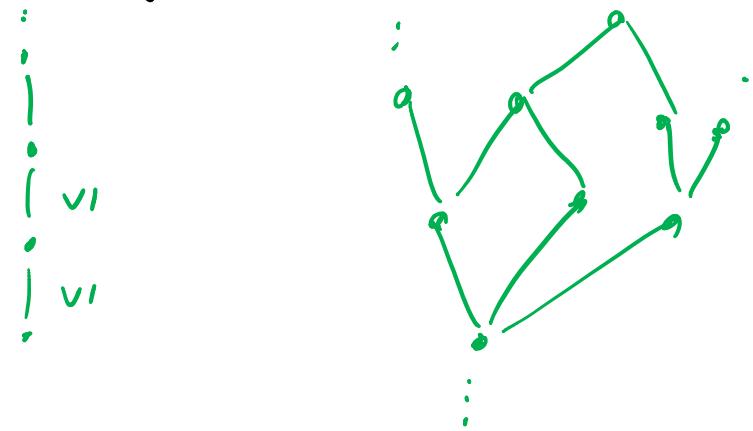
$$\top \sim \neg \perp \sim_{int} (\perp \rightarrow \perp)$$

$$(A \leftrightarrow B) \sim_{int} ((A \rightarrow B) \wedge (B \rightarrow A))$$

Modelle des Intuitionismus"

"

partiell geordnete Menge  $(W, \leq)$  d.h.  $\leq$  ist reflexiv und transiti-



$w \in W$  heißen „feststehend“  
oder „mögliche Welten“

Abbildung  $\beta: W \times \{A_i : i \in I\} \rightarrow \{0, 1\}$

mit  $\beta(w, A_i) = 1 , w \leq w' \Rightarrow \beta(w', A_i) = 1$

satz  $\beta$  für zu  $W \times \{F \mid F \text{ Formel}\} \rightarrow \{0, 1\}$

folge-durmaßen:

$$\beta(w, \perp) = 0 \quad \text{für alle } w$$

$$\beta(w, (F \wedge G)) = \min \{ \beta(w, F), \beta(w, G) \}$$

$$\beta(w, (F \vee G)) = \max \{ \beta(w, F), \beta(w, G) \}$$

$$\beta(w, (F \rightarrow G)) = \begin{cases} 1 & \text{für alle } w' \geq w \text{ gilt } \beta(w, F) \leq \beta(w, G) \\ 0 & \text{sonst} \end{cases}$$

Def: Ein Formal  $F$  ist eine intuitionistische Tautologie,  $\vdash_{\text{int}} F$ ,

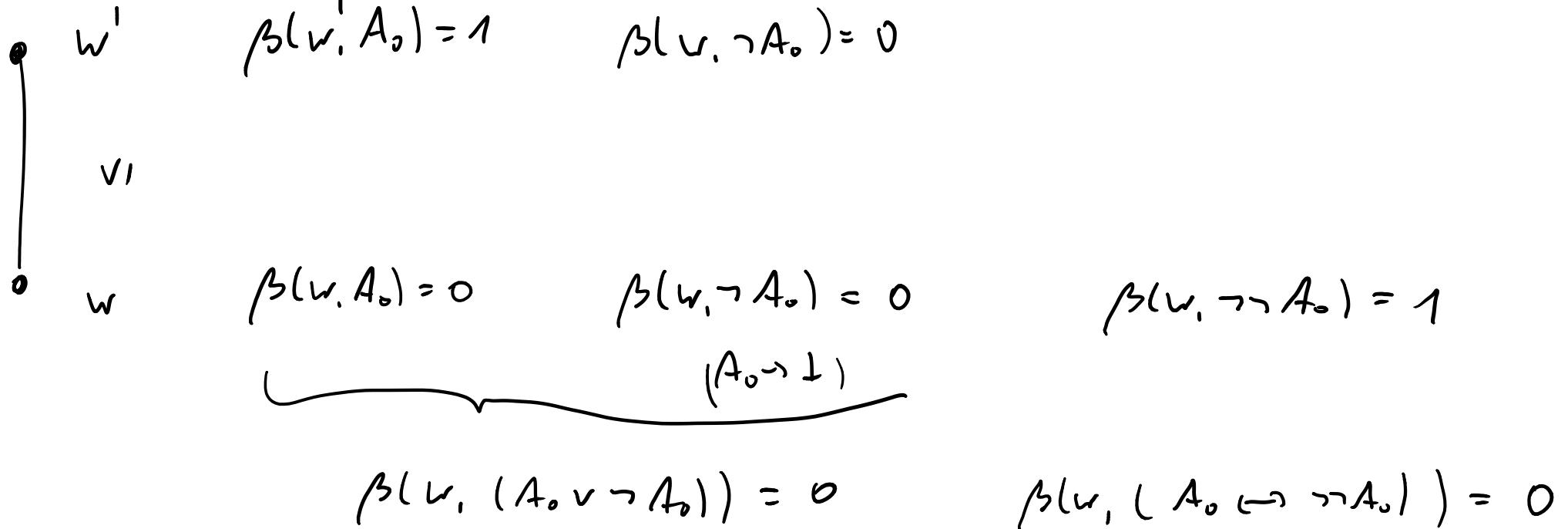
Wenn für alle  $(W, \leq)$  und  $\beta$  gilt:  $\beta(w, F) = 1$  für alle  $w \in W$

$F \sim_{\text{int}} G \Leftrightarrow \vdash_{\text{int}} (F \leftrightarrow G) \Leftrightarrow \vdash_{(W, \leq)} \beta \quad \forall w \in W$   
 $\beta(w, F) = \beta(w, G)$

Lemma : Wenn  $\vdash_{\text{inf}} F$ , dann  $\vdash F$  (klassisch)

Lemma: Wenn  $(U, \leq)$  :  $\beta(w, F) = 1$ ,  $v \leq w' \Rightarrow \beta(v', F) = 1$   
und  $\beta$  gegeben

Bsp:



In der intuitionistischen Logik:

$$\vdash_{\text{int}} (A_0 \vee \neg A_0)$$

$$A_0 \vdash_{\text{int}} \neg\neg A_0$$

$$\neg\neg A_0 \vdash_{\text{int}} A_0$$

$$\neg A_0 \vdash_{\text{int}} \neg\neg\neg A_0$$

intuitionistisch

T  
!

