

(Cantorsches Diagonalargument:  $\text{Pot}(\mathbb{N}) = \mathcal{P}(\mathbb{N}) = 2^{\mathbb{N}}$ )

Def: unendliche Menge  $M$  heißt abzählbar, falls es eine Bijektion  $\beta: \mathbb{N} \rightarrow M$  gibt; andernfalls überabzählbar.

Satz (Cantor)  $\text{Pot}(\mathbb{N}), \text{Pot}(A^*)$  für endliches  $A$   $\left. \begin{matrix} \text{Abb}(\mathbb{N}, \{0,1\}) = \text{Menge der unendlichen } \{0,1\}-\text{Folgen} \\ \text{Sinn} \end{matrix} \right\} \text{überabzählbar}$

Beweis: es gilt Bijektion  $\mathbb{N} \rightarrow A^*$ , also auch Bijektion  $\text{Pot}(\mathbb{N}) \rightarrow \text{Pot}(A^*)$   
 $\mathbb{N} \rightarrow \text{Abb}(\mathbb{N}, \{0,1\})$ ,  $M \subseteq \mathbb{N} \mapsto \chi_M$

Angenommen  $\beta: \mathbb{N} \rightarrow \text{Abb}(\mathbb{N}, \{0,1\})$  ist Bijektion.

$$\beta(0) : 0 \ 1 \ 1 \ 0 \ 0 \ 0 \dots \xrightarrow{\quad} 1 \ 1 \ 0 \ \dots$$

$$\beta(1) : 1 \ 0 \ 1 \ 0 \ 1 \ 1 \dots$$

$$\beta(2) : 1 \ 1 \ 1 \ 1 \ 1 \ 1 \dots$$

$$1 - \beta(n)(n)$$

Die Folge  $\overline{(1 - \beta(n)(n))}_{n \in \mathbb{N}}$  kann kein  $\beta(n)$  sein.

$\text{Pot}(\mathbb{N})$  überabzählbar, aber  
nur abzählbar viele Teilmengen von  $\mathbb{N}$  sind (semi-)entscheidbar.

Satz (Unentscheidbarkeit der Prädikatenlogik - Gödel)

Wenn  $\mathcal{L}$  mindestens ein zweistelliges Relationszeichen enthält oder  
mindestens ein einstelliges Funktionszeichen, dann ist

$\{\varphi \mid \varphi \text{ allgemeingültige } \mathcal{L}\text{-Aussagen}\}$  nicht entscheidbar.

Bem: Wenn  $\mathcal{L}$  nur Konstanten und Prädikate enthält,  
dann entscheidbar.

Beweis: ①  $\varphi$  allgemeingültig ( $\Rightarrow \neg\varphi$  nicht wahrbar)

d.h. äquivalent zu  $\{\varphi \mid \varphi \text{ erfüllbar}\}$  ist nicht entscheidbar

② Zurückführung auf das Haltproblem:

Für T.M.  $\mathcal{L}$  und Eingabe  $w$  konstruiere  $\mathcal{L}$ -Aussage  $\sigma_{\mathcal{L},w}$  mit.

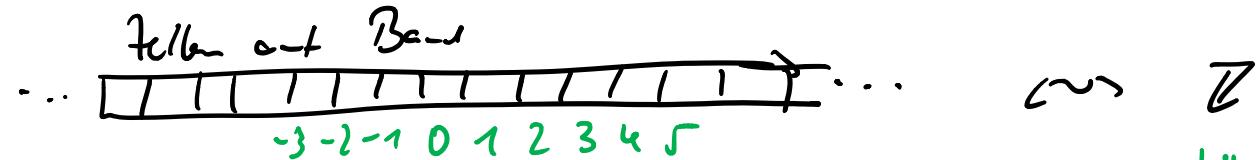
$\mathcal{L}$  stoppt bei Eingabe  $w$  nicht ( $\Rightarrow \sigma_{\mathcal{L},w}$  erfüllbar)

③ Wir nehmen an, dass  $\mathcal{L}$  mit  $A = \{0, 1\}$  arbeitet.

und arbeiten mit einer Sprache  $\mathcal{L}_{\mathcal{C}} = \mathcal{L}$ , die von  $\mathcal{L}$  abhängt

(Man muss sich überlegen, dass  $\mathcal{L}_{\mathcal{C}}$  in z.B. zweistelliger Relationsymbol Kodierbar ist)

④ T.M.  $\mathcal{L}$ .



$\mathbb{U}$

Berechnungsschritte / Zeitpunkte  $\rightsquigarrow \mathbb{N}$

0 1 2 3 4

$\Sigma$  besteht aus:

- zweistelliges Relationsymbol  $<$  für Anordnung der Zelle / Zeitpunkte
- zwei einstellige Flkt.-Symbol  $N, N^{-1}$  für Nachfolger / Vorgänger
- Konstante  $0$  für Startposition / Startzeitpunkt
- zweistelliges Rel.-Symbol  $K$  für:  $Kz_t$  bedeutet der Kopf steht  
zum Zeitpunkt  $t$  in der Zelle  $z$
- zwei zweistellige Relationssymbole  $A_0, A_i$ :  $A_i z_t$  zum Zeitpunkt  $t$   
steht in Zelle  $z$  das Symbol  $i$
- für jeden Testwert  $t_j$  ein Prädikat  $?_j$ :  $?_j t$  im Zeitpunkt  $t$  beinhaltet  
sich  $\Sigma$  im Test  $?_j$   
oder ein zweistelliges Relationssymbol  $\gamma$   
 $\text{Testwert } t_j \rightsquigarrow \gamma t N^0$

L-Aussage  $\sigma_{\Sigma, w}$  ist die Konjunktion von:

- $<$  ist eine diskrete Ordnung ohne Endpunkte,  
 $N \geq$  ist Nachfolger und  $N^{-1} \geq$  Vorgänger von  $\geq$
- in jeder Zelle steht zu jedem Zeitpunkt höchstens eins der Symbole 0, 1  
 $\forall z \forall t \rightarrow (A_0 \geq t \wedge A_1 \geq t)$
- die Maschine ist zu jedem Zeitpunkt in genau einem Zustand  
und im Startzeitpunkt 0 ist im Startzustand  $Z_0$   $Z_{0,0}$
- der Kopf steht zu jedem Zeitpunkt in genau einer Zelle  
und Startzeitpunkt in Zelle 0  $K_{0,0}$

Programm von  $\Sigma$

- Aussagen  $(0 \geq t \vee 0 < t)$   
 $\forall z \forall t \left( (t \geq 0 \wedge K \geq t \wedge Z_j \geq t \wedge A_i \geq t) \rightarrow (K \geq' N \wedge Z_j \geq' N \wedge A_i \geq N) \right)$

$t', j', i'$  hängen von Programm ab  
 $t$  oder  $N$  oder  $N^{-1}$   
← Übergangsfunction

- Eingabe  $w = (w_0, \dots, w_k) \quad w_i \in \{0,1\}$

wird beschrieben durch

$N \dots NO$

$$(A_{w_0}^{00} \wedge A_{w_1}^{NNO} \wedge \dots \wedge A_{w_k}^{N^k NO})$$

$$\wedge \forall z ((z \leq 0 \vee z > N^k 0) \rightarrow (\neg A_0 \geq 0 \wedge \neg A_1 \geq 0))$$

- $\Sigma$  stoppt nicht:  $\neg \exists t (t \geq 0 \wedge \exists, t)$   $t$ , Stopptestzeit

Von  $\Sigma$  mit Eingabe  $w$  nicht stoppt, wird der Lauf von  $\Sigma$  zu einem Modell von  $\sigma_{\Sigma, w}$

Umgekehrt: Wenn  $\sigma_{\Sigma, w}$  erfüllbar ist, dann hat sie ein Modell  $M$ .

$$M_0 := \{0^m, (NO)^m, (NNO)^m, \dots, (N^k 0)^m, \dots, (N^{-k} 0)^m, \dots\} \cong \Sigma$$

ist Unterstruktur von  $M$

$M_0$  beschreibt den Lauf von  $\Sigma$  bei Eingabe  $w$ , der nicht stoppt!



## Rekursive Funktionen

Def: Funktion  $f: \mathbb{N}^k \rightarrow \mathbb{N}$  ( $k \in \mathbb{N}$ ) heißt primativ rekursiv, falls  $f$  eine der folgenden Grundfunktionen ist:

- die konstante Nullfunktion  $0: \mathbb{N}^0 \rightarrow \mathbb{N}$
- die Nachfolgerfunktion  $S: \mathbb{N} \rightarrow \mathbb{N}$ ,  $n \mapsto n+1$
- die Projektionsfunktionen  $\pi_i^k: \mathbb{N}^k \rightarrow \mathbb{N}$ ,  $(n_1, \dots, n_k) \mapsto n_i$

Oder sich durch folgenden Regel ergibt:

(Komposition) Wenn  $f_1, \dots, f_e: \mathbb{N}^k \rightarrow \mathbb{N}$  prim. rekursiv sind und  $g: \mathbb{N}^e \rightarrow \mathbb{N}$  pr. rek., dann auch  $h: \mathbb{N}^k \rightarrow \mathbb{N}$ ,  $(n_1, \dots, n_k) \mapsto g(f_1(n_1, \dots, n_k), \dots, f_e(n_1, \dots, n_k))$

(Primative Rekursion) Wenn  $f: \mathbb{N}^k \rightarrow \mathbb{N}$  und  $g: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  pr. rek. sind, dann auch  $h: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  mit  $h(n_1, \dots, n_k, 0) = f(n_1, \dots, n_k)$

$$h(n_1, \dots, n_k, n+1) = g(h(n_1, \dots, n_k, n), n_1, \dots, n_k)$$

Eine (partielle) Funktion  $f: \mathbb{N}^k \rightarrow \mathbb{N}$  heißt rekursiv, falls zusätzlich die Regel erfüllt ist:

( $n$ -Rekursion): Wenn  $f: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$  rekursiv ist, dann auch

$$g: \mathbb{N}^k \rightarrow \mathbb{N} \text{ mit } g(n_1, \dots, n_k) := \begin{cases} \mu_n(f(n_1, \dots, n_k, n)) = 0 & \text{falls solch ein } n \text{ existiert} \\ \text{das kleinste } n \in \mathbb{N} \text{ mit} \\ f(n_1, \dots, n_k, n) = 0 & \\ \text{unbestimmt} & \text{andernfalls} \end{cases}$$

Eine Teilmenge  $M \subseteq \mathbb{N}$  heißt (primitiv) rekursiv, falls ob. def. Funktion es ist.

Satz: Die rekursiven Funktionen sind genau die (Turing-) berechenbaren Funktionen.  
(ohne Beweis)

Betrachte  $\mathcal{L} = \{\leq, +, \cdot, 0, 1\}$  und die  $\mathcal{L}$ -Struktur  $\mathbb{N}$

Bem: Jede rekursive Funktion ist durch  $\mathcal{L}$ -Formel definierbar!

Es gibt "berechenbare Übersetzung"  $T.M \subset \Sigma^*$  zu  $\mathcal{L}$ -Formel  $\varphi_{\mathcal{L}}$

Satz (Unvollständigkeitssatz von Gödel für  $\mathbb{N}$ )

$\text{Th}(\mathbb{N}) = \{\varphi \text{ } \mathcal{L}\text{-Aussage} \mid \mathbb{N} \models \varphi\}$  ist nicht entscheidbar.

Beweis: Sei  $\mathcal{L} \subseteq TM$ , d.h.  $f: \mathbb{N}^k \rightarrow \mathbb{N}$  berechnet

Dann gilt  $\mathbb{N} \models \exists v \varphi_{\mathcal{L}}(\underbrace{1 + \dots + 1}_{n \text{ mal}}) = v \iff \mathcal{L} \text{ stoppt bei Eingabe } n$   
(im wesentlichen)

D.h. Entscheidungsverfahren für  $\text{Th}(\mathbb{N})$  liefert Entscheidungsverfahren für Halteproblem  $\Sigma_1^0$

Cor: Wenn  $\widehat{T} \subseteq \text{Th}(\mathbb{N})$  semi-entscheidbar

(Idee:  $\widehat{T}$  ist Axiomatizierung von  $\mathbb{N}$ )

dann existiert  $\mathcal{L}$ -Formel  $\psi$ , d.h. von  $\widehat{T}$  nicht entschieden wird,  
d.h. beide  $\widehat{T} \vdash \psi$  und  $\widehat{T} \vdash \neg\psi$

⊓ Wenn  $T$  semi-entscheidbar, dann auch  $T^\vdash := \{\varphi \mid T \vdash \varphi\}$

Dann ist  $T^\vdash \neq \text{Th}(\mathbb{N})$

Dann  $\text{Th}(\mathbb{N})$  semi-entscheidbar, dann  $\text{Th}(\mathbb{N})$  entscheidbar,

denn das Komplement ist auch dann und kemi-entscheidbar

$\varphi \notin \text{Th}(\mathbb{N}) \Leftrightarrow \varphi$  ist keine  $\mathcal{L}$ -Aussage  
oder  $\neg\varphi \in \text{Th}(\mathbb{N})$

„Es gibt in  $\mathbb{N}$  wahr, nicht beweisbar Sätze“

Satz: ( Davis, Putnam, Robinson, Matiyasevich )

$M \subseteq \mathbb{N}^k$  ist genau dann rekursiv, wenn

$\exists \ell \in \mathbb{N}$  und Polynome  $P, Q \in \mathbb{N}[X_1, \dots, X_{k+\ell}]$

mit  $R = \{(n_1, \dots, n_k) \in \mathbb{N}^k \mid \exists m_1, \dots, m_\ell \in \mathbb{N} \text{ mit}$

$$P(n_1, \dots, n_k, m_1, \dots, m_\ell) = Q(n_1, \dots, n_k, m_1, \dots, m_\ell)\}$$

ist  $\mathbb{Z}: (P - Q)(n_1, \dots, n_k, m_1, \dots, m_\ell) = 0$

( schwerer Satz! )

Bsp:  $\{(n, 2^n) \mid n \in \mathbb{N}\}$  ist rekursiv

nicht offensichtlich, wie man P und Q findet!