

7. 12. 2011

Nicht deterministische Turingmaschinen

Def: " ist ein 7-Tupel  $\epsilon$

$M = (Q, \Sigma, \Gamma, b, q_0, S, \bar{F}, \delta)$

Stoppenstände  
← akz.

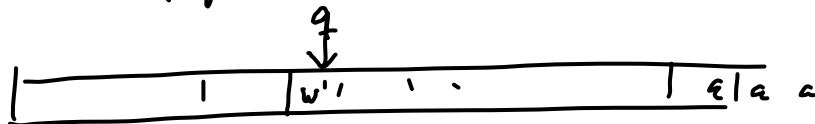
wie in der Def der TM, bis auf end. Mann

$$\delta: (Q \setminus S) \times \Gamma \rightarrow \frac{\mathcal{P}(Q \times \Gamma \times \{R, L\}) \setminus \{\emptyset\}}{Q \times \Gamma \times \{R, L\}}$$

Wir betrachten nun nicht det. TM, die langs jedes Berechnungspastes

stoppen.

Def: Konfiguration (wie vorher)



$(w, q, w)$

Def Eine Konfiguration  $C$  hat die Menge der (direkten) Nachfolgerkonfigurationen

$$\hat{\delta}(a_0, \dots, a_{i-1}, (q, a_i), \dots, a_{n-1})$$

$\updownarrow$   
 $\overline{a_{i-1} | a_i | \dots | a_n}$

$$= \left\{ (a_0, \dots, a_{i-2}, (q', a_{i-1}), a_i, \dots, a_{n-1}) \mid \delta(q, a_i) \ni (q', a_{i+1}, L) \right\} \\ \cup \left\{ (a_0, \dots, a_{i-1}, a'_i, (q', a_{i+1}), a_{i+2}, \dots, a_{n-1}) \mid (q', a'_i, R) \in \delta(q, a_i) \right\}$$

Wir schreiben  $C \vdash C'$  wenn  $C' \in \hat{\delta}^{(n)}(\{C\})$

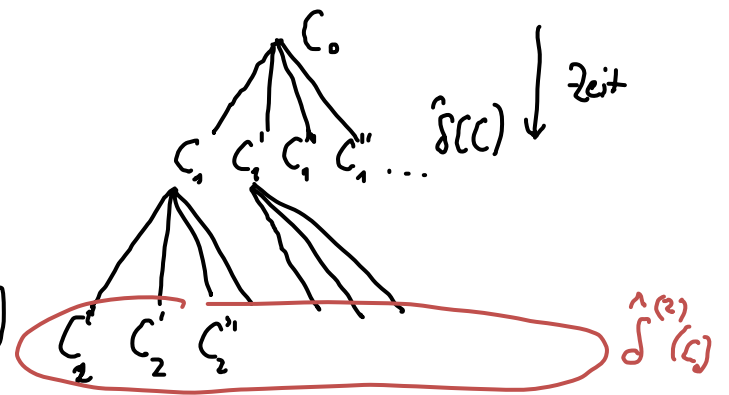
⋮  
Iteriert

$$\hat{\delta}^0(C) = C$$

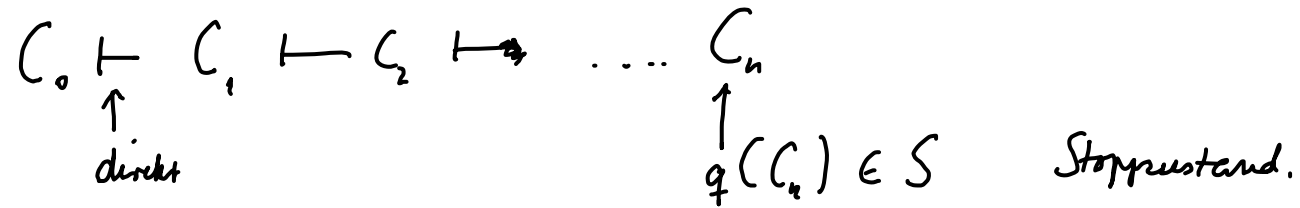
$$\hat{\delta}^n(C) = \hat{\delta}(C) \text{ wie oben definiert}$$

$$\hat{\delta}^{(n+1)}(C) = \bigcup \hat{\delta}[\hat{\delta}^{(n)}(C)] = \bigcup \hat{\delta}^{(n)} \hat{\delta}^{(n)}(C)$$

$$f'' X = \{f(x) \mid x \in X\}$$



Ein Berechnungspfad ist eine Folge



Def Akzeptierungsmenge

$$A(M) = \{ w \in \Sigma^* \mid \text{Startend von } C_0 = (\mathbb{Q}, q_0, w) \\ \text{(auch geschrieben als } (q_0, a_1, a_2, \dots, a_{n-1}) \text{)}$$

gibt es eine Konfigurationfolge  $C_0 \vdash C_1 \dots \vdash C_m$ , so dass  
 $q(C_m)$  akzeptierend }

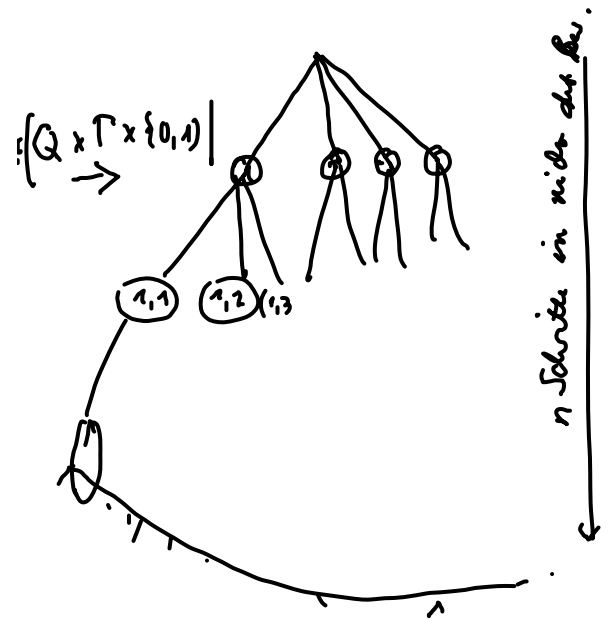
Satz Zu jeder nicht det. TM gibt es eine det. TM, die dieselbe Menge akzeptiert.

Beweis: Einfacher Fall: der nach der Definition von aus der Vorlesung,  
 dass beide Maschinentypen immer stoppen sollen.

Geg.  $M$  nicht det.

Gesucht  $M'$  det.  $A(M) = A(M')$ .

Die Tafel von  $M$  hat (mindestens)  $\left| \bigcup_{i \in \mathbb{N}} Q \times T \times \{L, R\} \right|$  viele Zustände.



Baum der Tiefe  $n$  mit höchstens  
 $k$  Kindern an jedem Knoten:



$\leq k^n$  viele Äste.  
 $\leq \sum_{i \leq n} k^i$  viele Knoten

Ein Zelle  $\delta(q, a)$  entspricht bei  $M$  dann eine Reihe  
 von  $|Q \times T \times \{0,1\}| \times 2$  viele Zellen, die besagen: Probiere jeden

## Nachfolge

Allgemeinere Auffassung von TM: müssen nicht immer halten.

Das obige Rezept der Übersetzung der Total der nicht det. Maschine in eine det. Total liefert: Wenn die nicht det. Maschine auf einem

Wort akzeptiert, dann akzeptiert die det. Maschine.

Die det. Maschine stoppt genau dann nicht, wenn es keine einzige akzeptierenden Wort gibt.

Korollar:  $A \subseteq \Sigma^*$ . Äquivalent sind

1. Es gibt ein TM  $M$ , s.d.  $A = A(M)$ .  
( $A$  ist Turing-berechenbar). rekursiv, effektiv, entscheidbar, berechenbar
2. Es gibt eine Mehrband-TM  $M'$ , s.d.  $A = A(M')$ .
3. Es gibt eine nicht-determ. TM  $M''$ , s.d.  $A = A(M'')$ .

# Zeitkomplexität

w Input.

Gesucht ist  $f(|w|)$ , s.d.  $T$  angewendet auf  $w$  in  $f(|w|)$  vielen  
Schritten stoppt.  
Länge von  $w$   
 $\in \mathbb{N}$

Schritte stoppt.

Def: die „Groß-O-Schreibweise“ und die klein-o-Schreibweise:

Seien  $f, g: \mathbb{N} \rightarrow \mathbb{N}$ . Wir schreiben  $f = O(g)$  : gdw

es ein  $c \in \mathbb{N} \setminus \{0\}$  s.d. für alle hinreichend großen  $n$   $f(n) \leq c \cdot g(n)$ .

$$\underbrace{\bigvee_n^\infty}_{\text{für alle bis auf endl. viele}} f(n) \leq c \cdot g(n)$$

für alle bis auf endl. viele

$f = o(g) : \Leftrightarrow$  f.a.  $\varepsilon > 0, \varepsilon \in \mathbb{R}$ , gibt es ein  $n_0$  s.d.  
f.a.  $n \geq n_0$   $f(n) \leq \varepsilon \cdot g(n)$

Beispiel: Die Zeitkomplexität folgender TM  $M$ , die

$$A(M) = \{0^k 1^k \mid k \geq 0\}.$$

Sei  $w$  geg.  $\Sigma = \{0, 1\}$ ,  $\Gamma = \{0, 1, x, \varepsilon\}$

1. Gehe das Band entlang, lehne  $w$  ab, falls eine 0 rechts von einer 1 steht.  $|w|$

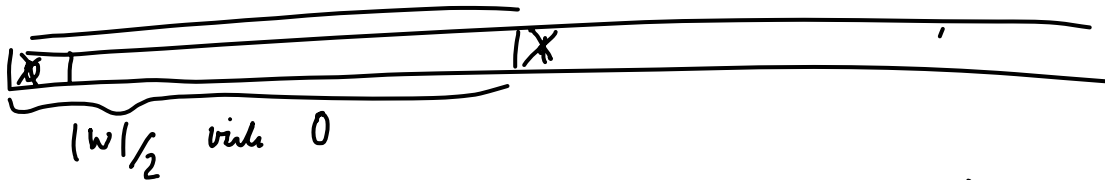
3. Wenn eine 0 aber keine 1 übrigbleibt, dann lehne ab. Sonst gehe zu 2.

Wenn kein Zeichen  $\neq x$  übrigbleibt, dann akzeptiere.

2. Wenn es sowohl eine 0 als auch eine 1 gibt, gehe das Band

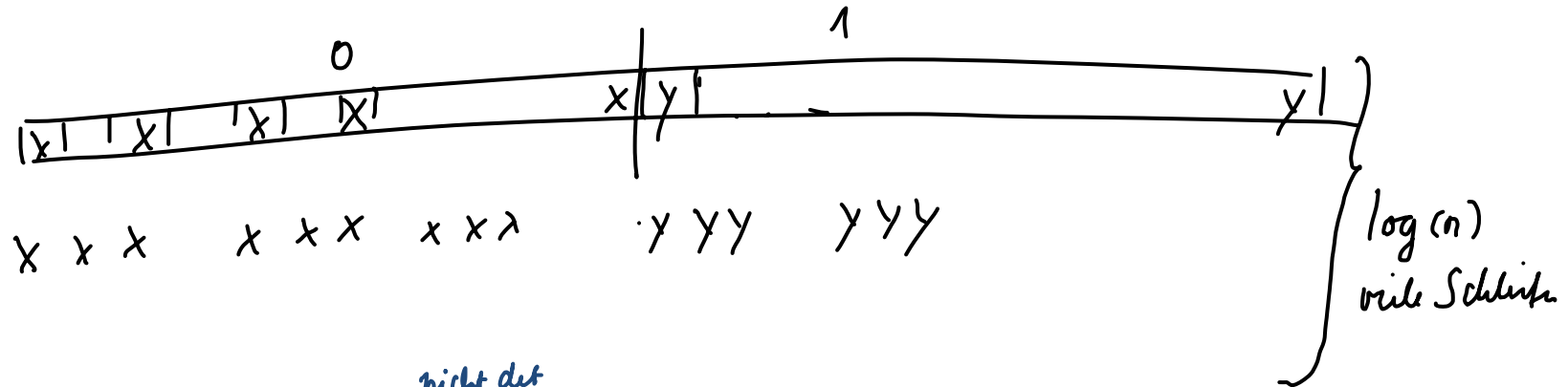
entlang und streiche eine 0 und eine 1 ab.

$2|w|$  Schritte für einen Schleifendurchlauf



Größe:  $\left(1 + \frac{|w|}{2}\right) 2|w|$  Schritte.  $\begin{matrix} O(|w|^2) \\ O(n^2) \end{matrix}$  viele Schritte.

Beh: Es gibt ein  $M'$  von Zeitkomplexität  $O(n \cdot \log(n))$   
 mit  $A(M') = A(M)$ .



Def:  $A$  ist von der <sup>nicht det</sup> Zeitkomplexität  $t$ .  $t: \mathbb{N} \rightarrow \mathbb{N}$  : gdw

es gibt eine <sup>nicht det</sup> TM  $M$  der Zeitkomplexität  $t$  s.d.  $A = A(M)$ .

$$[N]ZEIT(t) = \{A \subseteq \Sigma^* \mid A \text{ von } \text{von } \text{Zeitkomplex. } t \text{ } \}^{\text{nicht det.}}$$

$$P = \bigcup_{k \in \mathbb{N}} ZEIT(n^k) \quad \text{die polynomielle Zeitklasse}$$

$$NP = \bigcup_{k \in \mathbb{N}} NZEIT(n^k) \quad \text{die nicht det. polynomielle Zeitkl.}$$



Satz Sei  $t: \mathbb{N} \rightarrow \mathbb{N}$ , so dass f.a.  $n$   $t(n) \geq n$ .

1. Jede  $t$ -Zeit-Multiband TM  $M$  hat eine äquivalente  $O(t^2)$ -Einband-TM:  $M'$ .  $M$  ist äquivalent zu  $M' := A(M) = A(M')$ .

Beweisskizze: Die Bandbeschreibung braucht  $|w|$ -Schritte  
 $\leq t + \underline{\text{Länge des Eingabeworts}}$  viele Schritte.  
 $\leq 2t$

2. Jede nicht det  $t$ -Zeit-TM  $M$  hat eine äquivalente  $O(t) \cdot 2^{O(t)}$ -Zeit-TM.

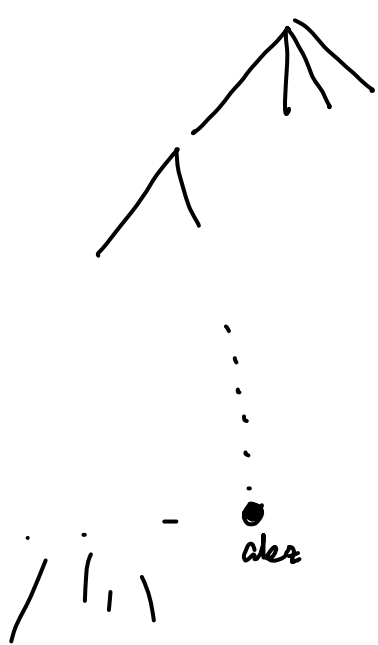
$$\left( \begin{array}{l} O(2^t) \\ c \cdot t \end{array} \right)$$

$$\left( \begin{array}{l} 2^{O(t)} \\ c \cdot t \end{array} \right)$$

$$c \cdot 2^t$$

$$2^c \cdot 2^t = 2^{c+t}$$

Beweisskizze: Kinderzahl im nichtdet. Baum  $\leq |\mathbb{Q} \times \Gamma \times \{L, R\}|$   
 $\uparrow$   
 von  $M$



Schrittzahl von  $M$   
 $t$

Schrittzahl beim  
 Abbruch des Baums

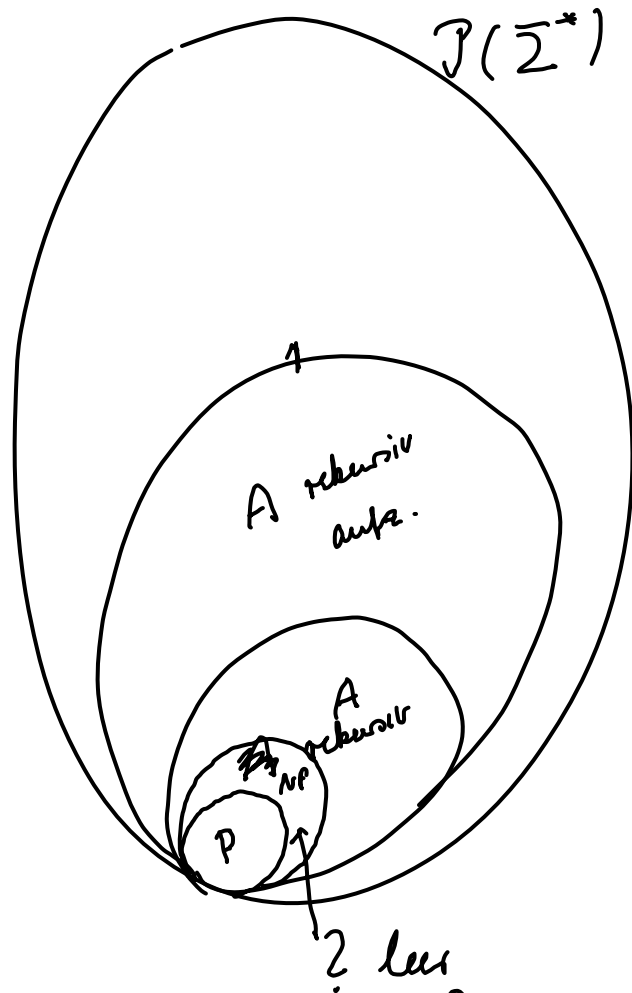
$$k^t \quad k = |Q \times \Gamma \times \{L, R\}|$$

$$k = 2^{k'} \quad (2^{k'})^t = 2^{k' \cdot t}$$

$NP = P$  Beweisversuch durch das Rezept des obigen Beweises:  
 $t = n^k$  für ein  $k \dots \dots \dots 2^{O(n^k)}$

Exponentieren wächst schneller als jedes Polynom:

f.a.  $k \in \mathbb{N}$   $\exists x_0 \in \mathbb{N}$   $\forall x \geq x_0$   $\left( e^x \right) \geq x^k$   $2^x \geq x^k$   
 $k^x \geq x^k$  für  $x \geq k$ .



$$Co(NP) = \{ \Sigma^* \setminus A \mid A \in NP \}$$

Beispiele für Problem in P:

Def: Ein gerichteter Graph ist eine  
 aus eine endl. Menge  $V$  und einer Menge

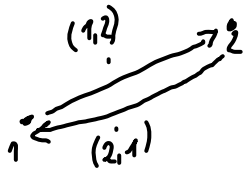
Vertex

$$Struktur (V, E)$$

$$E \subseteq V \times V \setminus \{ (v, v) \mid v \in V \}$$

~~$v_1, v_2 \in V$~~

$$V = (1, 2, 3, 4)$$



4

3