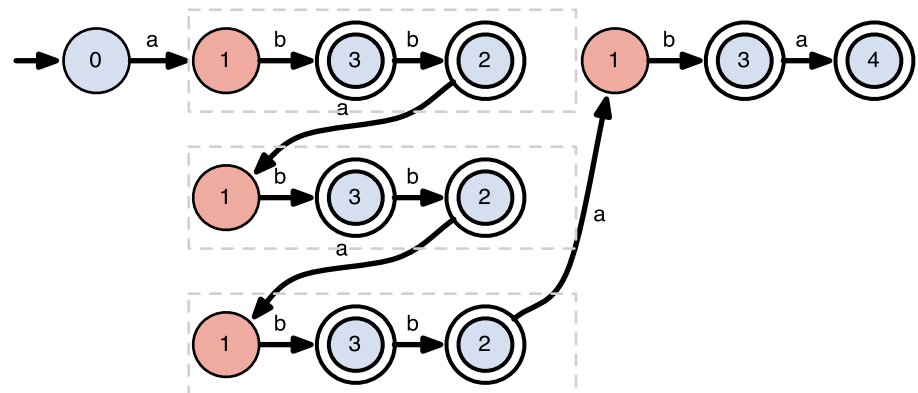


Berechenbarkeitstheorie

17. Vorlesung



Dr. Franziska Jahnke

Institut für Mathematische Logik und Grundlagenforschung

WWU Münster

Letztes Mal:

Es gibt eine Quine-Turingmaschine S :
 S gibt bei jeder Eingabe $\langle S \rangle$ aus.

Rekursionstheorem

Sei T eine TM, welche $t: \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ berechnet. Dann existiert eine durch die TM R beschriebene berechenbare Funktion $r: \Sigma^* \rightarrow \Sigma^*$, so dass für alle Eingaben $w \in \Sigma^*$ gilt

$$r(w) = t(\langle R \rangle, w).$$

Interpretation und Anwendung

- wir können für eine TM T annehmen, dass $\langle T \rangle$ Teil der Eingabe war und für uns verfügbar ist
- dann gibt es eine TM R , die genauso arbeitet, ohne dass $\langle R \rangle$ als Eingabe übergeben wurde
- wir können immer annehmen, dass eine TM über ein Unterprogramm `getYourOwnCode` verfügt

- (1) $\text{print}(w)$ TM-Programm, welches $\#w$ hinter die Eingabe druckt
- (2) $\text{seq}(\langle M_1, M_2, M_3 \rangle) := \langle M' \rangle$
 mit $M'(z)$ führt zuerst $M_1(z)$ aus und danach M_2 mit dem, was gerade auf dem Band steht, danach M_3

- R enthält 3 Teile: A, B, T – Teil T stimmt mit TM T überein

$R(y)$

1. Drucke $\#\langle B \rangle\#\langle T \rangle$ hinter Eingabe aufs Band
2. Sichere $y, \langle B \rangle$ und $\langle T \rangle$
3. Berechne $\text{print}(\#\langle B \rangle\#\langle T \rangle) = \langle A \rangle$
4. Berechne $\text{seq}(\langle A \rangle, \langle B \rangle, \langle T \rangle) = \langle R \rangle$
5. Drucke $\langle R, y \rangle$ aufs Band
6. führe $T(\langle R \rangle, y)$ aus

← Teil A

← Teil B

← Teil T

- $R = \text{seq}(A, B, T)$
- $R(y)$ arbeitet wie $T(\langle R \rangle, y)$

Alternativer Beweis zu $A_{\text{TM}} \notin \mathbb{E}$

- angenommen es gibt einen Entscheider H für A_{TM}
- wir konstruieren auf H basierend, die Anti-Simulationsmaschine B

$B(z)$

1. Sichere z
2. Bestimme $\langle B \rangle$
3. Simuliere $H(\langle B, z \rangle)$
4. Akzeptiere, wenn Simulation verwirft, ansonsten verwerfe

- $B(z)$ akzeptiert $\iff H(\langle B, z \rangle)$ verwirft $\iff B(z)$ verwirft
- Widerspruch zur Annahme \rightarrow Entscheider H für A_{TM} kann nicht existieren
- A_{TM} ist nicht entscheidbar

Def.: Eine TM M heißt **minimal**, gdw. es keine äquivalente TM M' gibt mit $|\langle M' \rangle| < |\langle M \rangle|$

Satz 26

$$\text{MIN}_{\text{TM}} = \{ \langle M \rangle \mid M \text{ ist minimal} \} \notin \mathbb{A}$$

Beweis

- Annahme: Es gibt Aufzähler E für MIN_{TM}
- Konstruiere TM C wie folgt

$C(z)$

1. Bestimme $\langle C \rangle$
2. Bestimme erste TM D in der Aufzählung von E mit $|\langle D \rangle| > |\langle C \rangle|$
3. Simuliere $D(z)$

- es gibt beliebig lange minimale TM \rightarrow Suche nach D erfolgreich
- C arbeitet wie D
- C hat aber kürzere Kodierung als minimale TM D
- Widerspruch zur Annahme $\rightarrow E$ kann nicht existieren □

PKP Definition

Eingabe: Folge von ℓ Wörterpaaren (x_i, y_i) .

Frage: Existiert eine nicht-leere Folge (i_1, i_2, \dots, i_k) mit
 $x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}$?

- die Wörterpaare (x_i, y_i) heißen auch Dominotypen

Darstellung der Eingabe:

$((ab, a), (ba, bb), (b, abb))$

ab	ba	b
a	bb	abb

- Lösung zur Frage heißt **PKP-Folge**. Das gebildete Wort **Lösungswort**.

Im Beispiel:

(Wiederholung möglich)

ab	ba	ab	b
a	bb	a	abb

- PKP Instanz ohne Lösung:
(Kein Abschluss möglich)

ab	ba	a	ab
a	bb	abb	aaa

- **Modifiziertes PKP (MPKP):** Wie PKP nur, dass man fordert, dass mit dem ersten Dominotyp begonnen werden muss!

$$\text{PKP} = \{ \langle \mathcal{S} \rangle \mid \exists \text{ PKP-Folge für } \mathcal{S} \}$$

$$\text{MPKP} = \{ \langle \mathcal{S} \rangle \mid \exists \text{ PKP-Folge für } \mathcal{S} \text{ mit } i_1 = 1 \text{ beginnend} \}$$

Satz 27

$$\text{MPKP} \leq_m \text{PKP}$$

Beweis

- **Idee :** modifiziere MPKP Instanz so, dass es nur PKP-Folgen mit i_1 beginnend geben kann
- **Plan :** Wenn (x_1, y_1) das einzige Paar mit gleichem Anfangszeichen, dann muss jede PKP-Folge mit i_1 beginnen
- Ersetze (x_1, y_1) durch $(\#x_1, \#y_1)$ ($\#$ neues Zeichen)
 1. **Problem:** i_1 kann in PKP-Folge mehrfach auftauchen. Nach Modifikation ist die PKP-Folge nicht mehr möglich.
 2. **Problem:** Auch andere Paare können gleiches Anfangszeichen haben.

(1.) Modifiziere jedes Paar (x_i, y_i) zu (x'_i, y'_i) mit

- $x_i = a_1 a_2 a_3 \cdots a_n \longrightarrow x'_i = a_1 \# a_2 \# \cdots \# a_n \# \quad (a_i \in \Sigma)$
- $y_i = b_1 b_2 b_3 \cdots b_m \longrightarrow y'_i = \# b_1 \# b_2 \# \cdots \# b_m \quad (b_i \in \Sigma)$

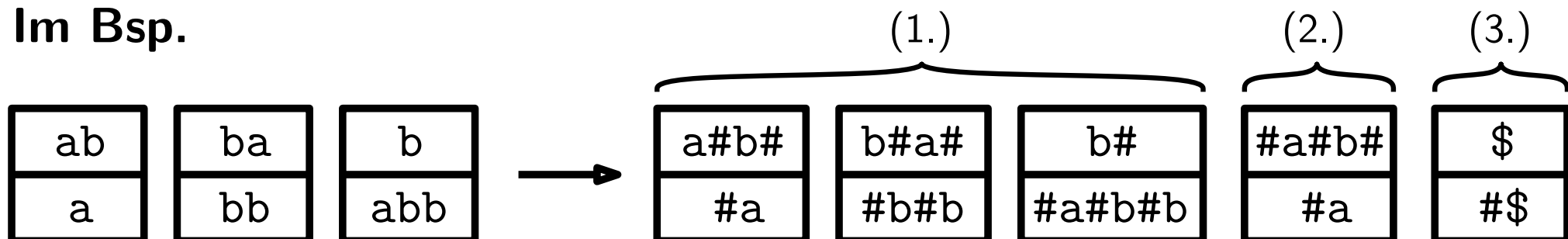
(2.) Füge als $(\ell + 1)$ tes Paar $(x_{\ell+1}, y_{\ell+1})$ hinzu mit

- $x_1 = a_1 a_2 a_3 \cdots a_n \longrightarrow x_{\ell+1} = \# a_1 \# a_2 \# \cdots \# a_n \# \quad (a_i \in \Sigma)$
- $y_1 = b_1 b_2 b_3 \cdots b_m \longrightarrow y_{\ell+1} = \# b_1 \# b_2 \# \cdots \# b_m \quad (b_i \in \Sigma)$

(3.) Füge als $(\ell + 2)$ tes Paar $(\$, \# \$)$ hinzu $(\$ \notin \Sigma)$

Nur das $(\ell + 1)$ te Paar beginnt mit gleichen Zeichen (es gibt aber auch eine Variante von (x_1, y_1) ohne gleiche 1. Zeichen)

Im Bsp.



Behauptung: Modifikation durch (1.) (2.) (3.) von \mathcal{S} nach $f(\mathcal{S})$ ist Reduktion von MPKP auf PKP

1. $\mathcal{S} \in \mathbf{MPKP} \Rightarrow f(\mathcal{S}) \in \mathbf{PKP}$

- Sei $(1, i_2, i_3, \dots, i_k)$ (M)PKP-Folge für \mathcal{S}
- $\rightarrow (\ell + 1, i_2, i_3, \dots, i_k, \ell + 2)$ ist PKP-Folge für $f(\mathcal{S})$

Im Bsp.

ab	ba	ab	b
a	bb	a	abb

$(1,2,1,3)$ (M)PKP-Folge für \mathcal{S}

#a#b#	b#a#	a#b#	b#	\$
#a	#b#b	#a	#a#b#b	#\$

$(4,2,1,3,5)$ PKP-Folge für \mathcal{S}

- Nach Konstruktion ist Lösungswort von \mathcal{S} , mit # durchsetzt und mit \$ abgeschlossen Lösungswort für $f(\mathcal{S})$.

2. $f(\mathcal{S}) \in \mathbf{PKP} \Rightarrow \mathcal{S} \in \mathbf{MPKP}$

Sei $(i_1, i_2, i_3, \dots, i_k)$ eine kürzeste PKP-Folge für $f(\mathcal{S})$

$f(\mathcal{S})$ Bsp.

#a#b#	a#b#	b#a#	b#	\$
#a	#a	#b#b	#a#b#b	#\$

1. Nur das erste Domino fängt mit den gleichen Zeichen an, also ist $i_1 = \ell + 1$
2. Nur das letzte Domino hört mit den gleichen Zeichen auf, also ist $i_k = \ell + 2$
3. Der $(\ell + 2)$ te Dominotyp tritt nur einmal auf, denn sonst gäbe es eine kürzere PKP-Folge.
4. Der $(\ell + 1)$ te Dominotyp tritt nur 1x auf, denn sonst gäbe es bei einmaliger Benutzung von Typ $\ell + 2$ zu viele # in der oberen Reihe.

Lösungswort beginnt mit #, endet auf \$ und jedes zweite Zeichen ist #

→ $(1, i_2, i_3, \dots, i_{k-1})$ ist (M)PKP-Folge für \mathcal{S}

→ f ist Reduktion für $\mathbf{MPKP} \leq_m \mathbf{PKP}$

Beweis

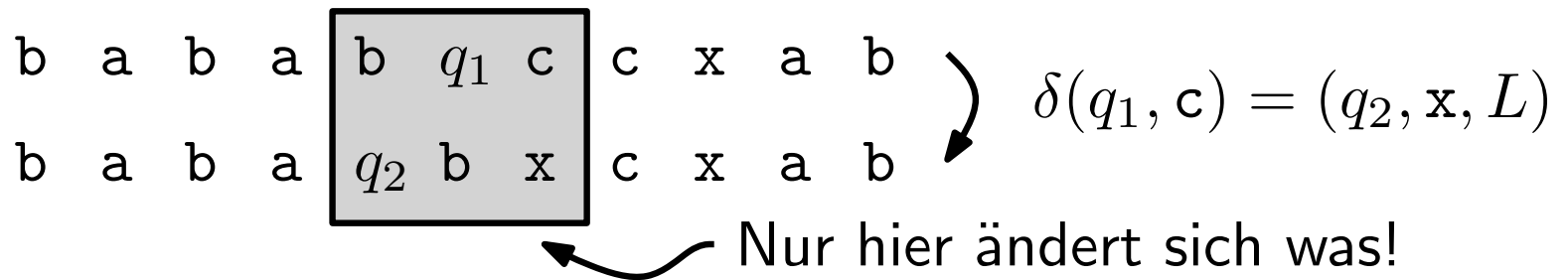
- **Wir zeigen:** $A_{\text{TM}} \leq_m \text{MPKP}$
- **Idee:** Lösungswort für MPKP Instanz ist akz. Berechnungspfad für $M(w)$

Kodierung Berechnungspfad:

Startkonf. # Folgekonf.1 # Folgekonf.2 # ... # akz. Konf.

Folgekonfiguration ist fast überall identisch

Bsp.



- Dominos "kopieren" Konfiguration, erlauben dabei Übergänge

* **Startdomino**

q_0w
#

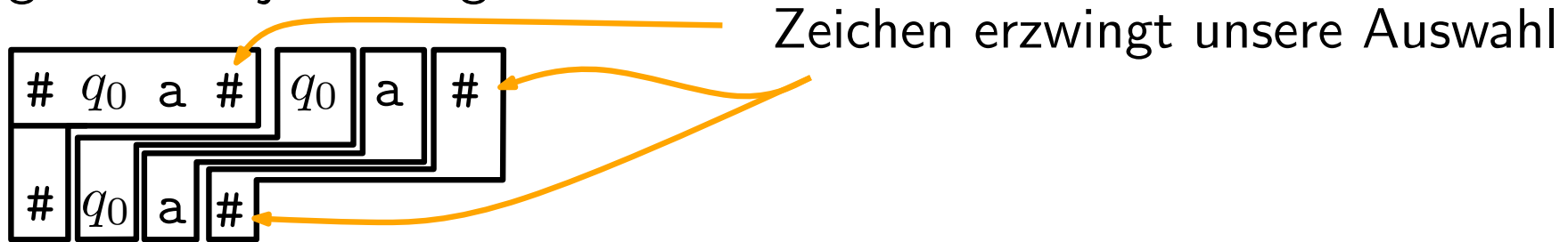
 obere Wort "läuft vor" ¹²

* **Kopierdominos**

<table border="1"><tr><td>q_0</td></tr><tr><td>q_0</td></tr></table>	q_0	q_0	<table border="1"><tr><td>q_1</td></tr><tr><td>q_1</td></tr></table>	q_1	q_1	...	<table border="1"><tr><td>q_z</td></tr><tr><td>q_z</td></tr></table>	q_z	q_z	<table border="1"><tr><td>#</td></tr><tr><td>#</td></tr></table>	#	#	<table border="1"><tr><td>a</td></tr><tr><td>a</td></tr></table>	a	a	<table border="1"><tr><td>b</td></tr><tr><td>b</td></tr></table>	b	b	...
q_0																			
q_0																			
q_1																			
q_1																			
q_z																			
q_z																			
#																			
#																			
a																			
a																			
b																			
b																			

 $\underbrace{\hspace{15em}}_{\forall q \in Q}$ $\underbrace{\hspace{15em}}_{\forall \gamma \in \Gamma}$

Folgendes ist jetzt möglich



Im Lösungswort würde eine wiederholte Kopie der Startkonfiguration stehen müssen. PKP-Folge kann aber nicht abgeschlossen werden.

* Übergangsdominos

c	p
q	a

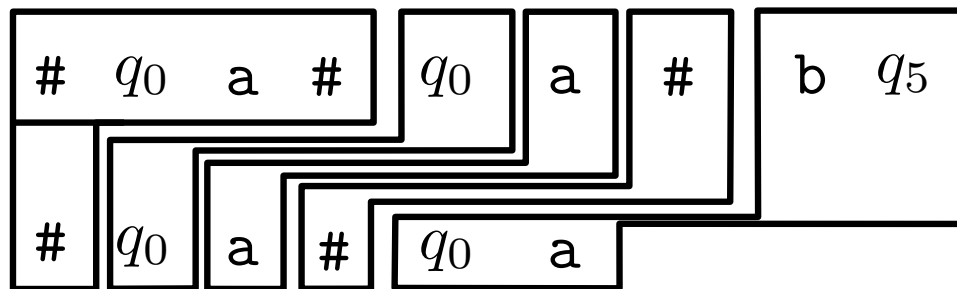
für alle Befehle
 $\delta(q, a) = (p, c, R)$

p	b	c
b	q	a

für alle Befehle
 $\delta(q, a) = (p, c, L), \forall b \in \Gamma$

Jetzt ist es möglich, entweder eine Konfiguration zu wiederholen, oder die Folgekonfiguration zu "schreiben".

Bsp.



für

$$\delta(q_0, a) = (q_5, b, R)$$

* Übergangsdominos für den Rand

Kopiere Konfiguration und füge vorne/hinten Blank an

q	□	#
q	#	

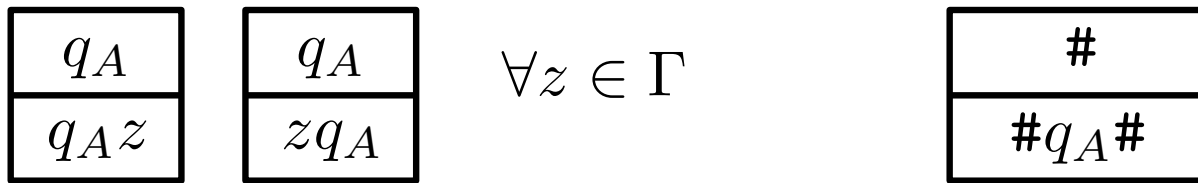
#	□	q
#	q	

für alle $q \in Q$

Jetzt ist zwar jeder Berechnungspfad darstellbar, ich kann die PKP-Folge aber immer noch nicht *beenden*. 14

Beenden soll nur möglich sein, wenn in meiner aktuell kopierten Konfiguration q_A enthalten ist.

* Pumpdominos



Entfernt Zeichen, vor
oder nach q_A

Entfernt q_A

- **Reduktion f :** Zu einer Turingmaschine $M(w)$ konstruiere die besprochenen Dominotypen $\mathcal{S} = f(\langle M, w \rangle)$
- **Noch zu zeigen:** M akzeptiert w genau dann, wenn es eine PKP-Folge für \mathcal{S} gibt

Nach Konstruktion kann man zu jedem akzept. Lauf eine PKP-Folge wie folgt ermitteln

- Lösungswort besteht zuerst aus Lauf (evtl. mit eingefügten Blanks)
- danach kommt eine Sequenz von Teilwörtern einer akzeptierenden Konfiguration, bei denen jeweils ein Zeichen entfernt wird
- zuletzt steht $q_A\#$

→ Wenn $M(w)$ akzeptierend, dann $S \in \text{MPKP}$

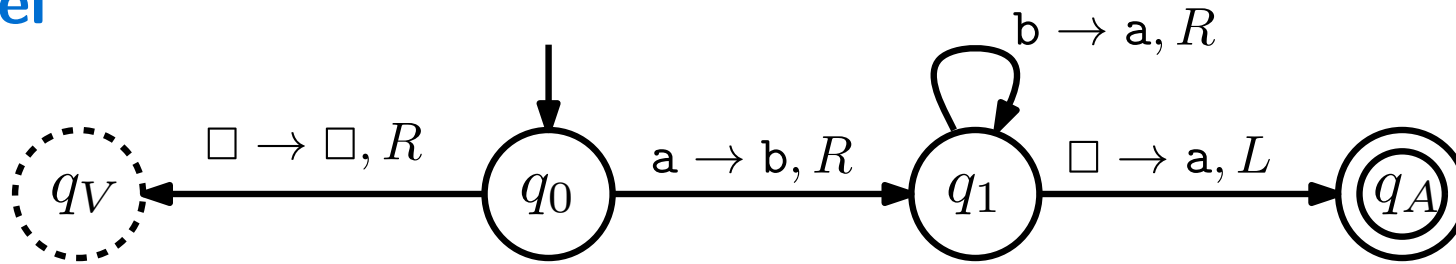
- Jedes Lösungswort beginnt mit der Startkonfiguration
- nach jedem $\#$ steht entweder die vorige Konfiguration, die Nachfolgekongfiguration, oder die vorige Konfiguration mit \square erweitert

→ Bei $M(w)$ nicht akz. erreicht man nie q_A , man kann kein Domino benutzen mit $|x_i| < |y_i| \rightarrow S \notin \text{MPKP}$

Es gilt also $A_{\text{TM}} \leq_m \text{MPKP} \leq_m \text{PKP}$

→ also: $A_{\text{TM}} \leq_m \text{PKP}$ und deshalb ist PKP **nicht entscheidbar**





Dominotypen (für Eingabe a)

#q ₀ a#	#	a	b	q ₀	q ₁	q ₂	q _A	□	bq ₁	□q _V	aq ₁	q _A aa	q _A ba	q _A □a
#	#	a	b	q ₀	q ₁	q ₂	q _A	□	q ₀ a	q ₀ □	q ₁ b	aq ₁ □	bq ₁ □	□q ₁ □

Startdomino

Kopierdominos

Übergangsdominos

#□q ₀	#□q ₁	q ₀ □#	q ₁ □#	q _A	q _A	q _A	q _A	q _A	q _A	q _A	#
#q ₀	#q ₁	q ₀ #	q ₁ #	q _A □	q _A a	q _A b	□q _A	aq _A	bq _A	#q _A #	

Übergangsdominos (Rand)

Pumpdominos

#q ₀ a#	bq ₁	#	b	q ₁ □#	q _A ba	#	q _A	a	#	q _A	#
#	q ₀ a	#	b	q ₁ #	bq ₁ □	#	q _A b	a	#	q _A a	#q _A #

Lösungswort: #q₀a#bq₁#bq₁□#q_Aba#q_Aa#q_A#