Vorlesung Kap. 6

Automatentheorie und Formale Sprachen – LV 4110 –

Kapitel 6

Lernziele

- Verwendung von unterschiedlichen Rechnermodellen
- Kennenlernen der Begriffe: Berechenbarkeit und Entscheidbarkeit
- Definitionen für Entscheidungsverfahren und Aufzählverfahren
- Klärung, was man unter einer berechenbaren Funktion versteht
- Definitionen für abzählbare und überabzählbare Mengen
- Beispiele für Turing-berechenbare Funktionen
- Kennenlernen, was die Church-Turing'sche These ausdrückt
- Herausstellen von nicht entscheidbaren Problemen und Sprachen
- Erweiterungen der Turing-Maschine

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

Besitzt jedes Problem, das mathematisch exakt formulierbar ist, eine algorithmische Lösung oder

gibt es Grenzen der

Berechenbarkeit

?

Im Jahre **1900** präsentierte **David Hilbert** auf einem Mathematiker-Kongress eine Liste mit **23** ungelösten Problemen:

Problem Nr. 10:

Gebe einen Algorithmus an, der für jede diophantische Gleichung feststellt, ob sie eine ganzzahlige Lösung besitzt oder nicht!

Beispiele für diophantische Gleichungen:

$$x^2 + y^2 - z^2 = 0$$

Lösung:
$$x = 3$$
, $y = 4$, $z = 5$

$$6x^{18} - x + 3 = 0$$

hat keine ganzzahlige Lösung, da

$$\forall x \in \mathbf{Z} : 6x^{18} > x - 3$$

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

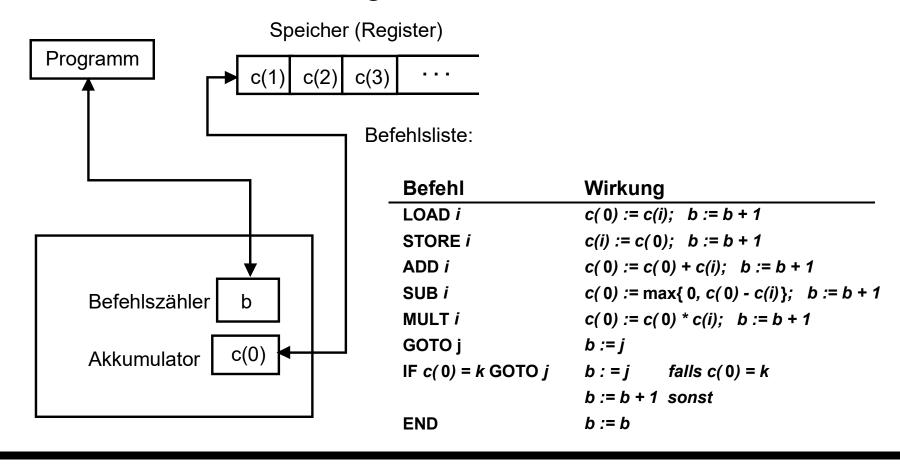
Modellbildung:

- Ein sehr realistisches Rechnermodell (nach der Vorstellung eines wirklichen Rechners) ist die **Registermaschine** (**R**andom **A**ccess **M**aschine, kurz **RAM**).
- Zwar scheint die **Turing-Maschine** (kurz **TM**) nicht besonders realistisch zu sein, dient sie jedoch als Rechnermodell, das sich für "allgemeine" theoretische Aussagen hervorragend eignet.
- Man kann zeigen (tun wir hier nicht!), dass die TM "gleichwertig" zur RAM ist, die – wie deren Arbeitsweise demonstrieren wird – wiederum einen wirklichen Rechner modelliert.

Arbeitsweise:

- Die RAM besteht aus einem Befehlszähler, einem Akkumulator, aus Registern und aus einem Programm.
- Die Inhalte von Befehlszähler, Akkumulator und Registern sind natürliche Zahlen. In den ersten Registern steht die Eingabe.
- Die Register bilden den (unendlichen) Speicher der RAM und haben alle eine eindeutige Adresse. Der Inhalt (content) des Registers i sei mit c(i) bezeichnet.
- Das Programm besteht aus einer Folge von Befehlen, wobei die Programmzeilen durchnummeriert (0, 1, 2, ...) sind.
- Der Befehlszähler startet bei Null, und enthält die Nummer des nächsten auszuführenden Befehls.

Schematische Darstellung der RAM:



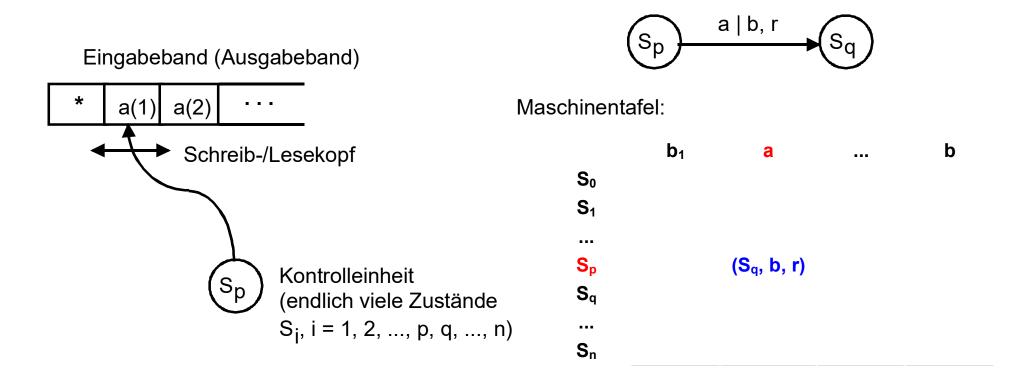
Beispiel: f(x) = 0, falls x gerade, sonst Endlosschleife

```
// Wert x in Reg. c(1) ablegen
     READ
                                  // c(1) = x in Akkumulator laden
     LOAD
  : DIV
                                  // dividiere Akku durch 2 (integer!)
3: MULT
                                  // multipliziere Akku mit 2 (integer!)
4 : STORE
                          2
                                  // Akkumulator in c(2) ablegen
5 : LOAD
                                  // c(1) in Akkumulator laden
6 : SUB
                                  // davon nun c(2) subtrahieren
                          10
  : IF c(0) = 0 GOTO
                                  // bedingter Sprung zu 10 (Ausgabe)
8 : SUB
                                  // Akkumulator wird bzw. bleibt 0
                         =1
                          8
  : IF c(0) = 0 GOTO
                                  // Rücksprung zu 8 (Endlosschleife)
10: WRITE
                                  // c(0) war 0 und somit 0 ausgeben
                          =0
                                  // Befehlszähler b bleibt 11
11: END
```

Arbeitsweise:

- Die TM besteht aus einem einseitig unendlichen Eingabe- und Ausgabeband mit einem freibeweglichen Schreib-/Lesekopf.
- Der Schreib-/Lesekopf wird von einer endlichen Kontrolleinheit (endlich viele Zustände) gesteuert.
- Das Eingabe- und Ausgabeband enthält eine Folge von Symbolen, welche zu Beginn der Berechnung die Eingabe darstellt.
- Die Kontrolleinheit entspricht dem Befehlszähler der RAM und die Zellen des Eingabe- und Ausgabebandes den Registern der RAM.
- Die Zustandsübergänge der TM werden anhand einer Maschinentafel vollzogen. Dabei bewegt sich der Schreib-/Lesekopf eine Stelle nach recht, nach links oder überhaupt nicht.

Schematische Darstellung der TM:



Beispiel: $L(TM) = \{ w \mid w = a^n b^n c^n \text{ für } n = 1, 2, ... \}$

 $\Sigma = \{a, b, c\}; \mathbf{B} = \{a, b, c, *, A, B, C\}; \mathbf{S} = \{S_0, S_1, ..., S_7\}; \mathbf{F} = \{S_7\}$

	а	b	С	Α	В	C	*
S_0	_	_	_	_	_	_	(S ₁ , *, r)
S ₁	(S ₂ , A, r)			_	(S ₅ , B, r)	1	_
S ₂	(S ₂ , a, r)	(S ₃ , B, r)	_	_	(S ₂ , B, r)	_	_
S ₃	_	(S ₃ , b, r)	(S ₄ , C, I)	_	_	(S ₃ , C, r)	_
S ₄	(S ₄ , a, I)	(S ₄ , b, I)	_	(S ₁ , A, r)	(S ₄ , B, I)	(S ₄ , C, I)	_
S ₅	_	_	_	_	(S ₅ , B, r)	(S ₅ , C, r)	(S ₆ , *, I)
S ₆	_	1		(S ₆ , A, I)	(S ₆ , B, I)	(S ₆ , C, I)	(S ₇ , *, h)

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

<u>Definition</u> (Algorithmus):

Es sei P eine Problemklasse und A die Menge der konkreten Problemausprägungen, d. h. die Menge derjenigen Daten, die ein Problem beschreiben.

Dann verstehen wir unter einem **Algorithmus A**_P zu der Klasse **P** ein allgemeines, deterministisches Verfahren, welches – auf richtige Anfangsdaten $a \in A$ angewendet – nach <u>endlich</u> vielen Schritten hält und die Lösung des Problems liefert (d. h. ein Element der Lösungsmenge **B**).

Wir schreiben: $A_P : A \rightarrow B$,

d. h. $\forall a \in \mathbf{A} : \exists b \in \mathbf{B} : \mathbf{A}_{\mathbf{P}}(a) = b$

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

<u>Definition</u> (Entscheidungs- und Aufzählverfahren):

Einen Algorithmus $A_P : A \rightarrow B$ nennen wir auch

- ein Entscheidungsverfahren, falls

- ein Aufzählverfahren, falls

$$A = IN$$

Beispiel 1 (Primzahlen):

geg: Zahl $Z \in IN$ ges: Algorithmus, der entscheiden kann, ob Z eine Primzahl ist oder nicht d. h. $\{2, 3, 5, 7, 11, 13, ...\}$?

⇒ Entscheidungsverfahren

Beispiel 2 (Primzahlen):

```
geg: A = \{ \forall Primzahlen \}
```

= { p | p ist nicht das Vielfache einer ganzen Zahl mit Ausnahme der 1 und p selbst)}

```
ges: A_P(1), A_P(2), A_P(3), ...
```

⇒ Aufzählverfahren

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

<u>Definition</u> (injektiv, surjektiv, bijektiv):

Injektion: f: A→B x₁ f: A→B yy₁ x₂ Definitionsbereich A Zielbereich B	\forall X ₁ , X ₂ ∈ A : X ₁ ≠ X ₂ \Rightarrow $f(x_1) ≠ f(x_2)$ A ≤ B (Kardinalität) auch linkseindeutig genannt Bsp.: R → R : $f(x)$ = arctan(x) N → N : $f(n)$ = n^2 ; aber: Z → Z : $f(n)$ = n^2 ist nicht injektiv	Zwei verschiedene Elemente von A werden auf verschiedene Elemente von B abgebildet – oder: Jedem y-Wert im Zielbereich besitz nur genau einen x-Wert im Definitionsbereich; daher wiederholt sich bei einer injektiven Funktion also nie ein Funktionswert.
Surjektion: f: A -> B x ₁ y ₂ y ₃ Definitionsbereich A Zielbereich B	$\forall y_i \in \mathbf{B} : \exists \frac{\text{mind. ein}}{f(x_i) = y_i} x_i \in \mathbf{A} :$ $ A \ge B $ auch rechtstotal genannt Bsp.: $\mathbf{Z} \to \mathbf{N} : f(x) = abs(x)$	Jedes Element der Zielmenge B ist ein Funktionswert, d. h. alle mög- lichen y-Werte im Zielbereich werden angenommen – oder: Bildbereich von f stimmt mit der Zielmenge von f überein.
Bijektion: f: A -> B Vy x V y Definitionsbereich A Zielbereich B	∀ $y_i \in \mathbf{B}$: ∃ genau ein $x_i \in \mathbf{A}$: $f(x_i) = y_i$ A = B Bsp.: {0 255} → {0, 1} ⁸ : $f(x) = 8\text{-stell. Binärzahl}$	f heißt bijektiv, falls es sowohl injektiv als auch surjektiv ist. Geanu dann existiert auch eine Umkehrfunktion x = f ⁻¹ (y)

<u>Definition</u> (berechenbare Funktion):

Eine Funktion f : $M_1 \rightarrow M_2$ heißt berechenbar, falls es einen Algorithmus

$$A_f: M_1 \rightarrow M_2$$

gibt mit

$$A_f(w) = f(w)$$
 für $\forall w \in M_1$

Interpretation:

Zu jedem Argument $w \in M_1$ kann man also den Funktionswert $f(w) \in M_2$ in endlich vielen Schritten berechnen.

Beispiel (berechenbare Funktion):

Für $M_1 = IN$ und $M_2 = IN$ ist

$$f: IN \rightarrow IN \text{ mit } f(n) = n \cdot (n + 1) / 2$$

eine <u>berechenbare</u> Funktion, da es für diese Funktion einen Algorithmus gibt (Aufgabe 1.3 – vgl. Übungsblatt 1).

Anmerkung:

Es ist keineswegs eine triviale Frage, ob <u>jede</u> gegebene Funktion berechenbar ist, also durch einen Algorithmus realisiert werden kann. Wir werden sehen, dass die Frage zu verneinen ist.

<u>Definition</u> (abzählbare Menge, überabzählbare Menge):

Es sei M eine Menge. Wir nennen M abzählbar, wenn sich M bijektiv auf die Menge IN (der natürlichen Zahlen) oder eine Teilmenge von **IN** abbilden lässt. Andernfalls nennen wir M überabzählbar.

Merke:

- Jede endliche Menge ist abzählbar.
- Ist A ein (endliches) Alphabet, so ist A* abzählbar (wegen lexikographischer Ordnung).

Satz:

Es sei Σ ein Alphabet und somit endlich. Dann gibt es überabzählbar viele Funktionen $f: \Sigma^* \to \Sigma^*$, von denen allerdings nur abzählbar viele berechenbar sind. (Beweis durch Wiederspruch! – vgl. Übungsblatt 12)

<u>Definition</u> (entscheidbare Menge):

a) Es seien $M_1 \subseteq M_2 \subseteq \Sigma^*$.

M₁ heißt entscheidbar relativ zu M₂, wenn es einen Algorithmus

```
A_{M1M2}: M_2 \rightarrow \{ \text{ True, False } \}
```

gibt, mit dessen Hilfe man **zu jedem** Element $w \in M_2$ feststellen kann, ob es zu M_1 gehört oder nicht.

```
kurz: \forall w \in M_2 : A_{M1M2}(w) = ", w \in M_1"
```

b) Es sei $M \subseteq \Sigma^*$.

M heißt absolut entscheidbar (oder kurz entscheidbar), wenn M relativ zu Σ^* entscheidbar ist. \rightarrow Entscheidbarkeit ist eine Mengeneigenschaft und nicht etwa die Eigenschaft eines einzelnen Objektes!

Beispiele:

a) Die Menge

```
M := \{ n \in IN \mid n \text{ ist eine Primzahl } \}
```

ist entscheidbar relativ zu IN, denn es muss zu einer vorgegebenen Zahl $n \in IN$ nur getestet werden, ob ein m < n mit $m \ne 1$ existiert, das $n \in IN$ muss $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ eine $m \ne 1$ eine $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ teilt $m \ne 1$ existiert, das $m \ne 1$ existiert existiert, das $m \ne 1$ existiert existiert, das $m \ne 1$ existiert existiert exi

<u>kurz:</u>

Für
$$n \in IN \exists m (m \neq 1 \land m < n) \mid (m, | "n) \Rightarrow n \notin IP$$

- b) Jede <u>endliche</u> Menge ist <u>entscheidbar</u>; ein entsprechender Algorithmus muss lediglich eine endliche Menge oder Liste durchsuchen, um die Entscheidung treffen zu können.
- c) Das allgemeine Wortproblem für **Typ-0-Grammatiken** ist <u>nicht</u> entscheidbar, d. h. es gibt <u>keinen</u> Algorithmus, der zu einer beliebig vorgegebenen Grammatik **G** und einem ebenfalls vorgegebenen Wort **w** entscheiden kann, ob **w** ∈ **L(G)** gilt oder nicht.

Mengen Aufzählbarkeit

<u>Definition</u> (aufzählbare Menge):

Eine Menge $M \subseteq \Sigma^*$ heißt aufzählbar, wenn es eine Funktion

 $f: IN_0 \rightarrow M$

gibt, die surjektiv <u>und</u> berechenbar ist. Wir sagen dann: "M wird durch f aufgezählt", d. h. $M = \{ f(0), f(1), f(2), f(1), ... \}$

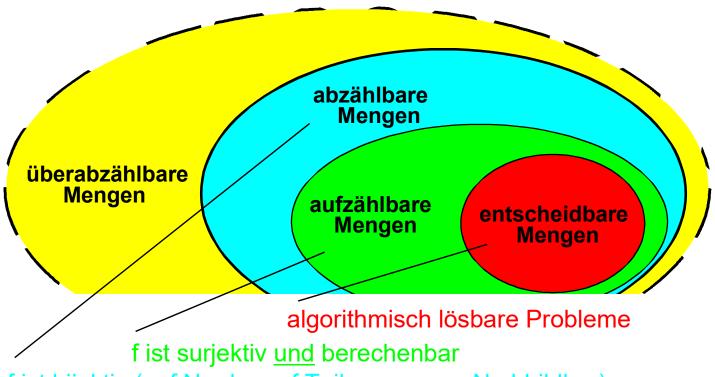
⇒ durch die Funktion f werden die Elemente von M in eine feste Reihenfolge gebracht, wobei nicht ausgeschlossen ist, dass ein Element von M mehrfach aufgezählt wird.

Satz:

Für eine Menge $M \subseteq \Sigma^*$ gilt:

- a) M ist **auf**zählbar \Rightarrow M ist **ab**zählbar; die Umkehrung gilt i.a. nicht!
- b) M ist **entscheid**bar ⇒ M ist **auf**zählbar

Veranschaulichung der Zusammenhänge:



f ist bijektiv (auf N oder auf Teilmenge von N abbildbar)

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

<u>Definition</u> (Turing-Berechenbarkeit):

Es sei **TM** = (S, So, F, Σ , B, δ) eine **Turing-Maschine** und M₁, M₂ $\subseteq \Sigma^*$.

- a) Wir sagen: Eine **TM** realisiert eine Funktion $f: M_1 \rightarrow M_2$, wenn folgendes gilt:
 - 1) Für \forall w \in M₁ gilt: (*, w, s₀) \Rightarrow (*, f(w), s_f), wobei (*, f(w), s_f) eine sog. Finalkonfiguration ist, d. h. die Maschine hält an, und s_f ist ein Endzustand.
 - 2) Andernfalls, d. h. für w ∉ M₁, geht die Maschine nie in eine Finalkonfiguration über, und das Verhalten der Maschine ist unbestimmt.
- b) Eine Funktion $f: M_1 \to M_2$ heißt Turing-berechenbar, wenn es eine **TM** gibt, die bei Eingabe von $w \in \Sigma^*$ den Funktionswert $f(w) \in \mathbf{B}^*$ berechnet.

Beispiele:

- a) Die Funktion $f: IN_0 \rightarrow IN$ mit f(n) = n + 1 ist Turing-berechenbar.
- b) Die Funktion $f: IN_0 \rightarrow IN_0$ mit $f(n_1, n_2) = n_1 + n_2$ ist ebenfalls Turingberechenbar.

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

Satz (Church-Turing'sche These):

Jede (im intuitiven Sinne) berechenbare Funktion ist auch Turingberechenbar und umgekehrt.

Dieser Satz ist <u>nicht</u> beweisbar; zur Aussage des Satzes hat aber noch niemand ein Gegenbeispiel angeben können.

Folgerung:

Aufgrund der vorgenommenen Definition und der Church-Turing'sche These gilt nun:

Jede aufzählbare bzw. entscheidbare Menge ist auch Turingaufzählbar bzw. Turing-entscheidbar und umgekehrt.

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

<u>Definition</u> (PKP):

Beim Post'schen Korrespondenzproblem (PKP) ist eine endliche Folge von Wortpaaren

$$K = ((x_1, y_1), (x_2, y_2), ..., (x_n, y_n))$$

über einem endlichen Alphabet Σ gegeben.

Es gilt weiter $x_i \notin \varepsilon$ und $y_i \notin \varepsilon$. Gefragt ist nun, ob es eine endliche Folge von Indizes $i_1, i_2, ..., i_k \in \{1, 2, ..., n\}$ gibt, so dass gilt:

$$x_{i1} x_{i2} ... x_{ik} = y_{i1} y_{i2} ... y_{ik}$$

Satz:

Das Post'schen Korrespondenzproblem (PKP) ist nicht entscheidbar.

Beispiel 1:

$$K = ((1, 111), (10111, 10), (10, 0))$$

hat die Lösung (2, 1, 1, 3), denn es gilt:

Beispiel 2:

$$K = ((10, 101), (011, 11), (101, 011))$$

hat keine Lösung.

Beispiel 3:

$$K = ((001, 0), (01, 011), (01, 101), (10, 011))$$

hat eine Lösung der Länge 66.

- 1. Hauptfrage in diesem Kapitel
- 2. Vergleich zwischen Register- und Turingmaschine
- 3. Definition für einen Algorithmus
- 4. Definitionen für Entscheidungs- und Aufzählverfahren
- 5. Berechenbare Funktionen und entscheidbare Mengen
- 6. Definition der Turing-Berechenbarkeit
- 7. Die Church-Turing'sche These
- 8. Das Post'sche Korrespondenzproblem
- 9. Erweiterungen der Turing-Maschine

Folgende Erweiterungsmöglichkeiten existieren bei einer TM:

- 1. Mehrere Schreib-/Leseköpfe
- 2. Mehrere Bänder
- 3. Mehrere Schreib-/Leseköpfe für mehrere Bänder
- 4. Mehrdimensionale Bänder

Satz:

Es hat sich gezeigt, dass <u>keine</u> dieser Erweiterungen mehr leistet, als eine "normale" Turing-Maschine. Man kann z. B. beweisen, dass jede **k**-Band Turing-Maschine durch eine **1**-Band Turing-Maschine simuliert werden kann. Das gleiche gilt auch für alle anderen angegebenen Modifikationen.