Modellierung von Problemen, Einführung der Turingmaschine

Prof. Dr. Berthold Vöcking
Lehrstuhl Informatik 1
Algorithmen und Komplexität
RWTH Aachen

Oktober 2011

Was ist ein *Problem*?

Informelle Umschreibung des Begriffes *Problem*:

Für gegebene Eingaben soll ein Algorithmus ...
... bestimmte Ausgaben produzieren.

Wir benötigen eine präzisere Definition ...

Alphabete und Wörter

- Ein- und Ausgaben sind Wörter über einem Alphabet Σ.
- Typischerweise $\Sigma = \{0, 1\}$.
- Σ^k ist die Menge aller Wörter der Länge k, z.B.

$$\{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

- Das *leere Wort*, also das Wort der Länge 0, bezeichnen wir mit ϵ, d.h. $\Sigma^0 = \{\epsilon\}$.
- $\Sigma^* = \bigcup_{k \in \mathbb{N}_0} \Sigma^k$ ist der *Kleenesche Abschluss* von Σ und enthält alle Wörter über Σ, die wir z.B. der Länge nach aufzählen können

$$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, \ldots$$

Problem als Relation

- Im Allgemeinen entspricht ein Problem einer *Relation* $R \subseteq \Sigma^* \times \Sigma^*$.
- Ein Paar (x, y) liegt in R, wenn y eine zulässige Ausgabe zur Eingabe x ist.

Beispiel: Primfaktorbestimmung

Zu einer natürlichen Zahl $q \geq 2$ suchen wir einen Primfaktor.

Wir einigen uns darauf Zahlen binär zu kodieren. Die Binärkodierung einer natürlichen Zahl i bezeichnen wir mit $bin(i)$.

Die entsprechende Relation ist

$$R = \{(x, y) \in \{0,1\}^* \times \{0,1\}^* \mid x = bin(q), y = bin(p), \\ p, q \in \mathbb{N}, q \geq 2, p \text{ prim}, p \text{ teilt } q\} \ .$$

Problem als Funktion

- Häufig gibt es zu jeder Eingabe eine eindeutige Ausgabe.
- Dann können wir das Problem als Funktion $f : \Sigma^* \to \Sigma^*$ beschreiben.
- Die zur Eingabe $x \in \Sigma^*$ gesuchte Ausgabe ist $f(x) \in \Sigma^*$.

Beispiel: Multiplikation

Zu zwei natürlichen Zahlen $i_1, i_2 \in \mathbb{N}$ suchen wir das Produkt.

Um die Zahlen i_1 und i_2 in der Eingabe voneinander trennen zu können, erweitern wir das Alphabet um ein Trennsymbol #, d.h. $\Sigma = \{0, 1, \#\}$.

Die entsprechende Funktion $f : \Sigma^* \to \Sigma^*$ ist

$$f(bin(i_1)\#bin(i_2)) \;=\; bin(i_1 \cdot i_2) \;.$$

Entscheidungsprobleme als Sprachen

- Viele Probleme lassen sich als Ja-Nein-Fragen formulieren.
- Derartige *Entscheidungsprobleme* sind von der Form $f : \Sigma^* \to \{0, 1\}$, wobei wir 0 als „Nein“ und 1 als „Ja“ interpretieren.
- Sei $L = f^{-1}(1) \subseteq \Sigma^*$ die Menge derjenigen Eingaben, die mit „Ja“ beantwortet werden.
- L ist eine Teilmenge der Wörter über dem Alphabet Σ. Eine solche Teilmenge wird allgemein als *Sprache* bezeichnet.

Entscheidungsprobleme als Sprachen

Beispiel: Graphzusammenhang

Problemstellung: Für einen gegebenen Graphen G soll bestimmt werden, ob G zusammenhängend ist.

Der Graph G liege dabei in einer geeigneten Kodierung $code(G) \in \Sigma^*$ vor, z.B. als binär kodierte Adjazenzmatrix.

Die zu diesem Entscheidungsproblem gehörende Sprache ist

$$L = \{ w \in \Sigma^* \mid \exists \text{ Graph } G\text{: } w = code(G) \text{ und } G \text{ ist zusammenhängend} \} .$$

Zentrale Fragestellung

Welche Funktionen sind durch einen Algorithmus berechenbar?

bzw.

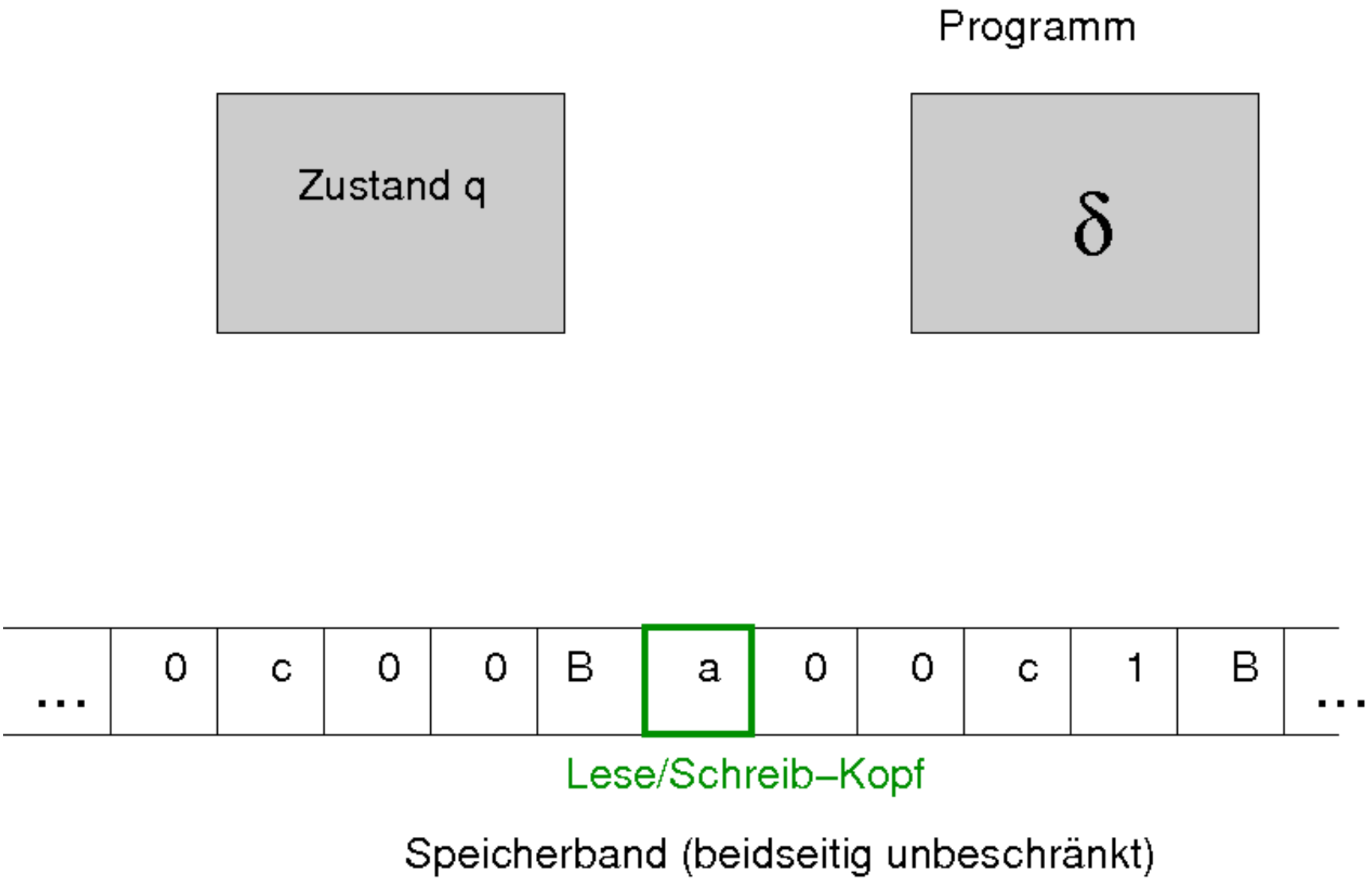
Welche Sprachen kann eine Algorithmus entscheiden?

Um diese Fragen in einem mathematisch exakten Sinne klären zu können, müssen wir festlegen, was eigentlich ein Algorithmus ist.

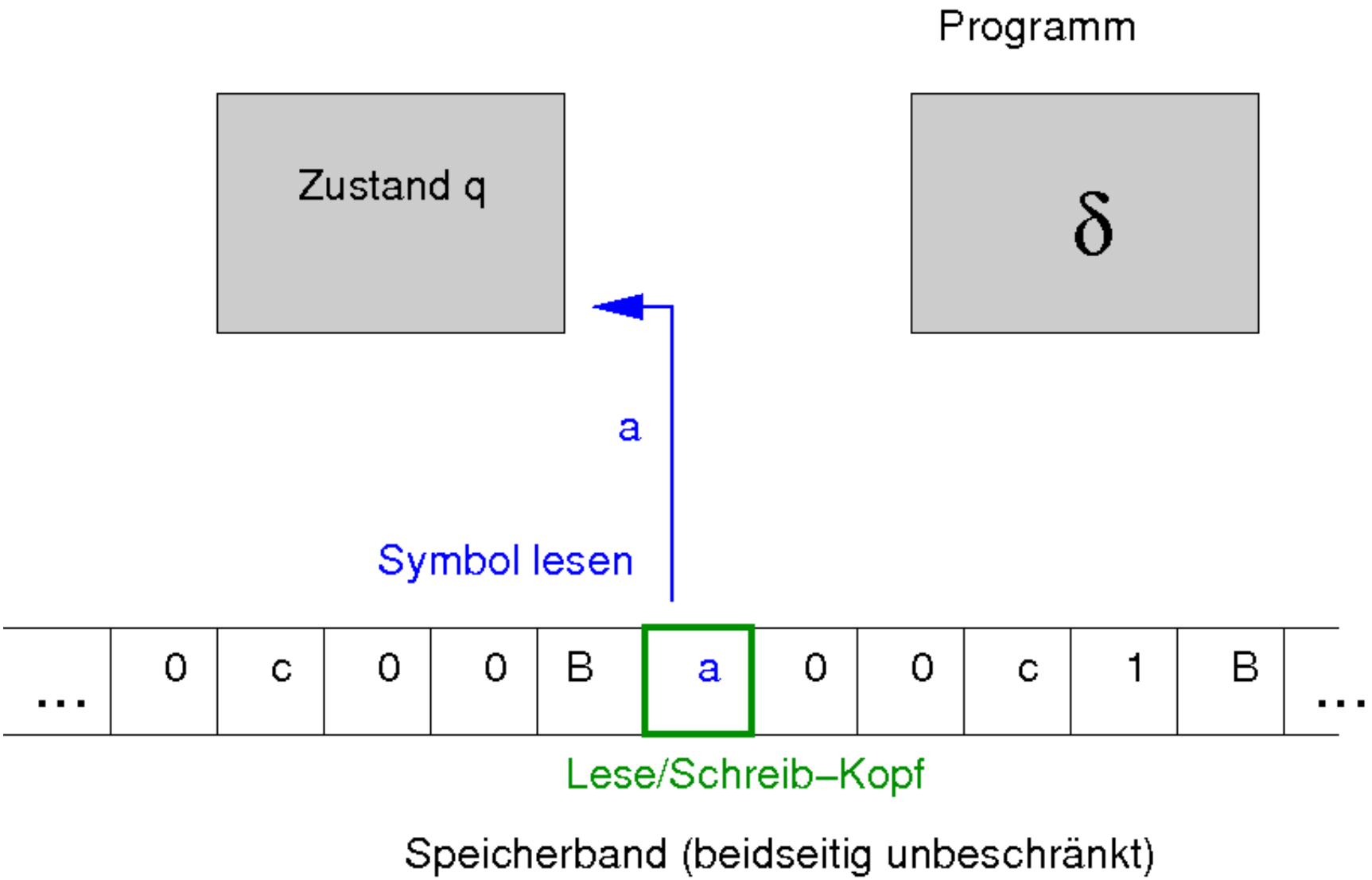
Zu diesem Zweck definieren wir ein einfaches „Computer“-Modell:

Die *Turingmaschine (TM)*.

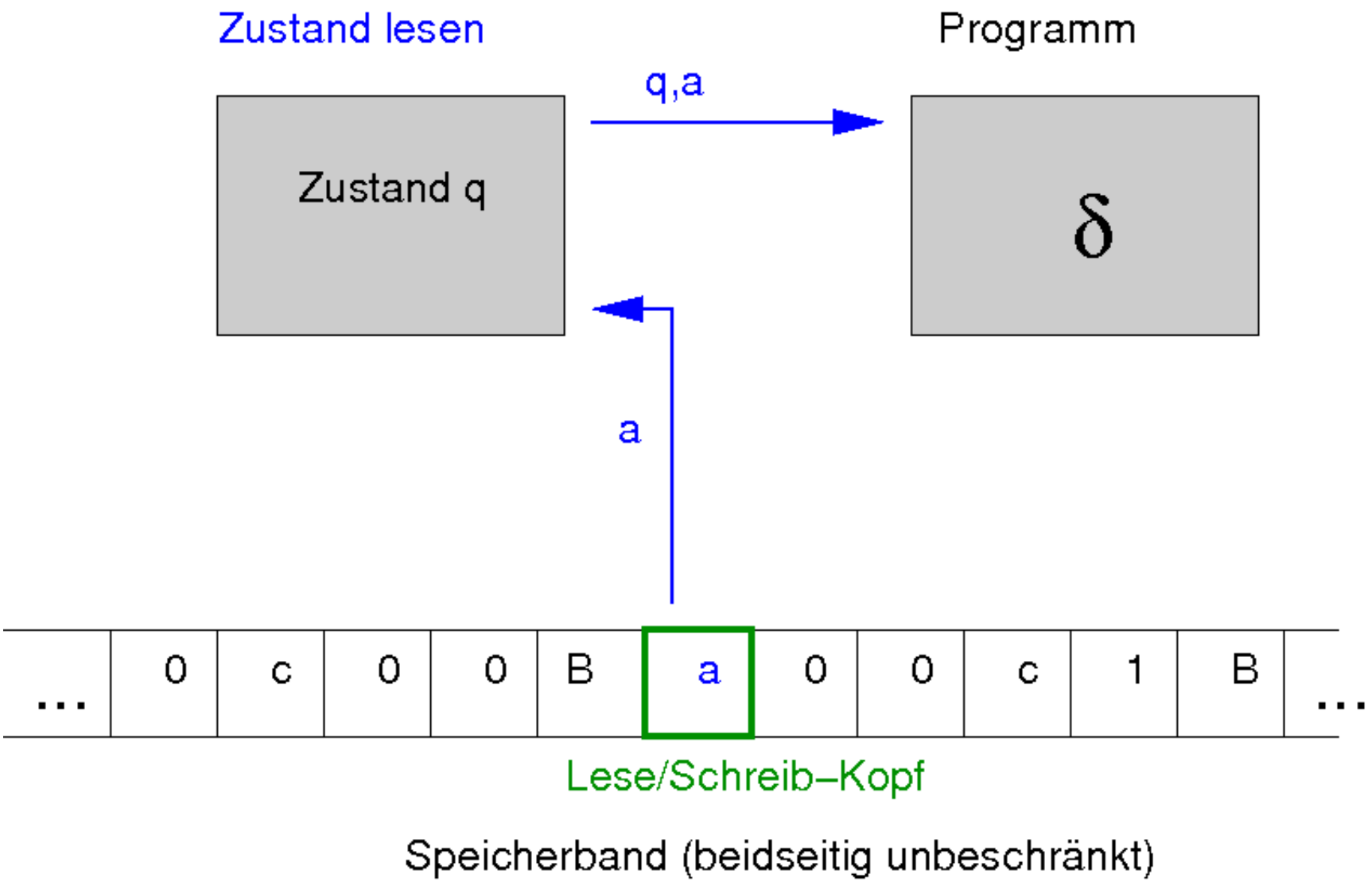
Deterministische Turingmaschine (TM bzw. DTM)



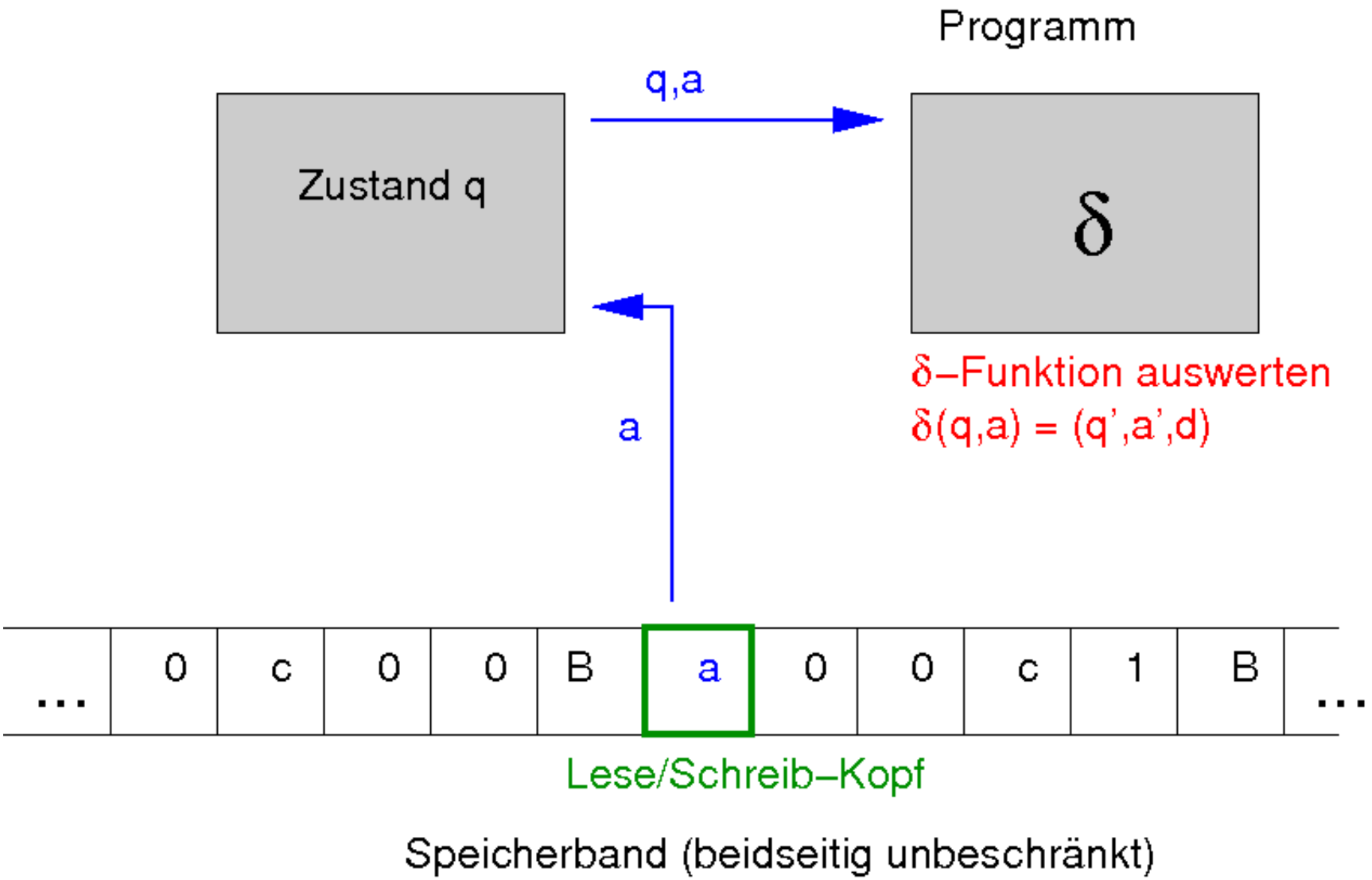
Deterministische Turingmaschine (TM bzw. DTM)



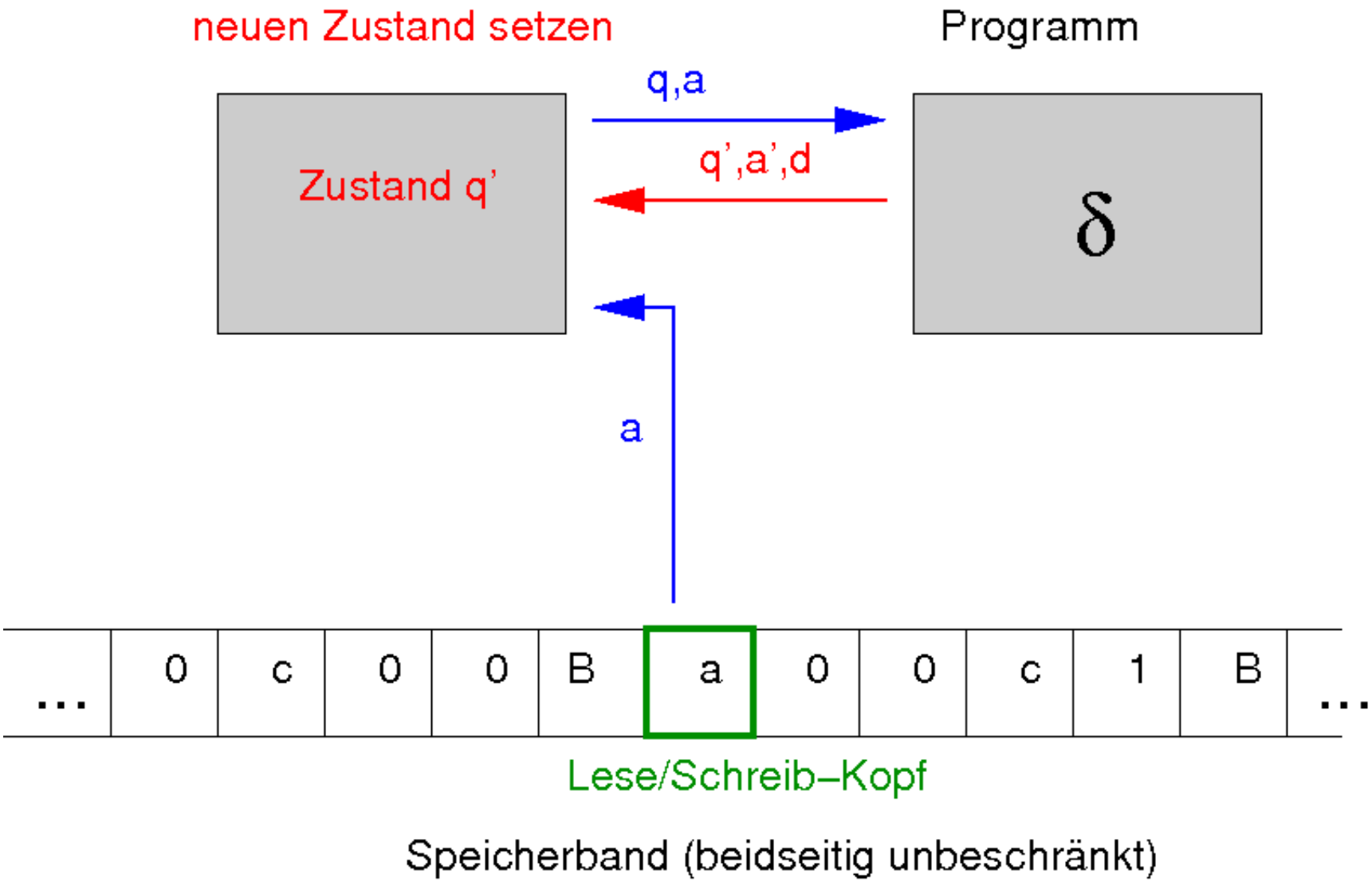
Deterministische Turingmaschine (TM bzw. DTM)



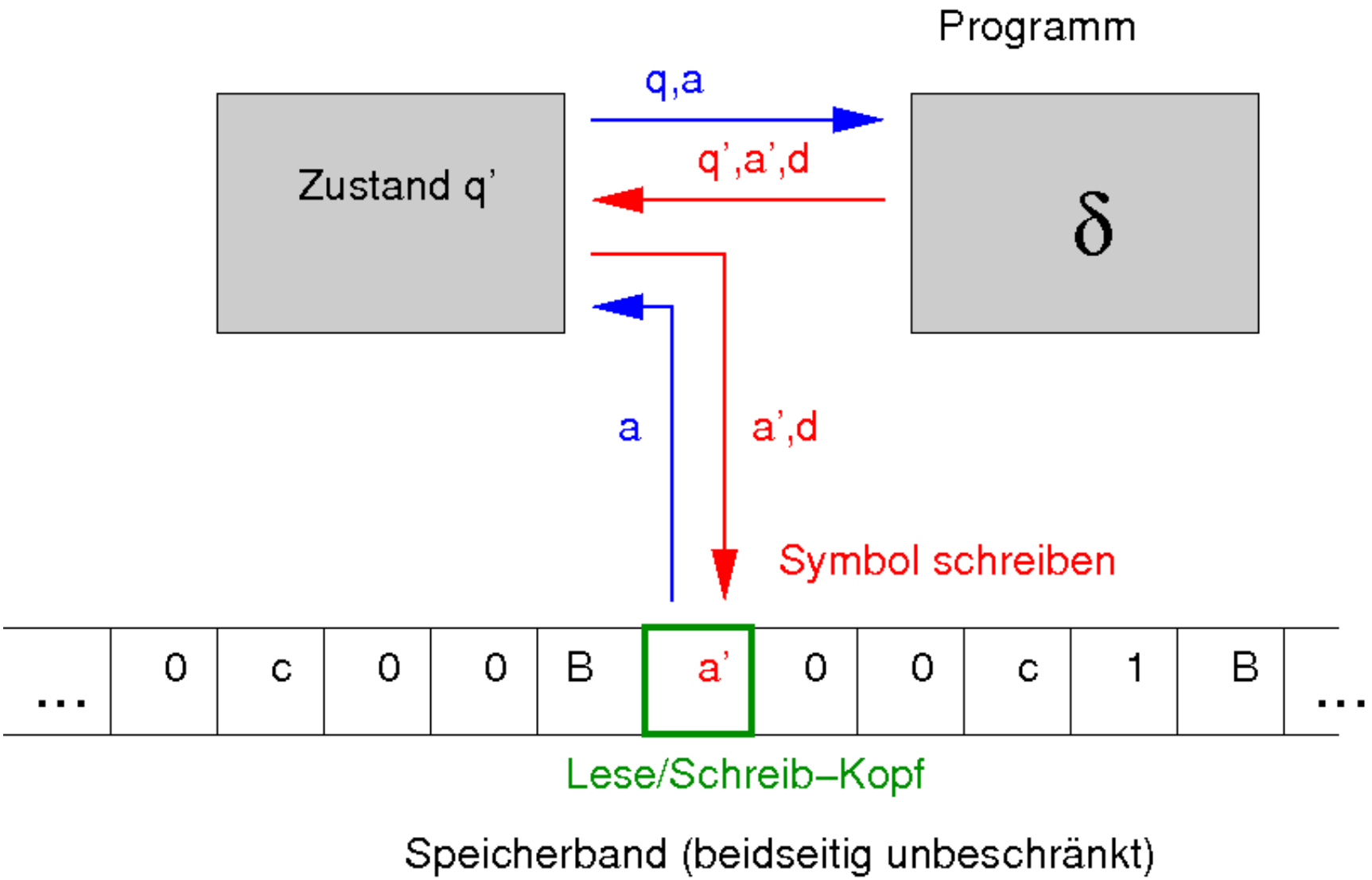
Deterministische Turingmaschine (TM bzw. DTM)



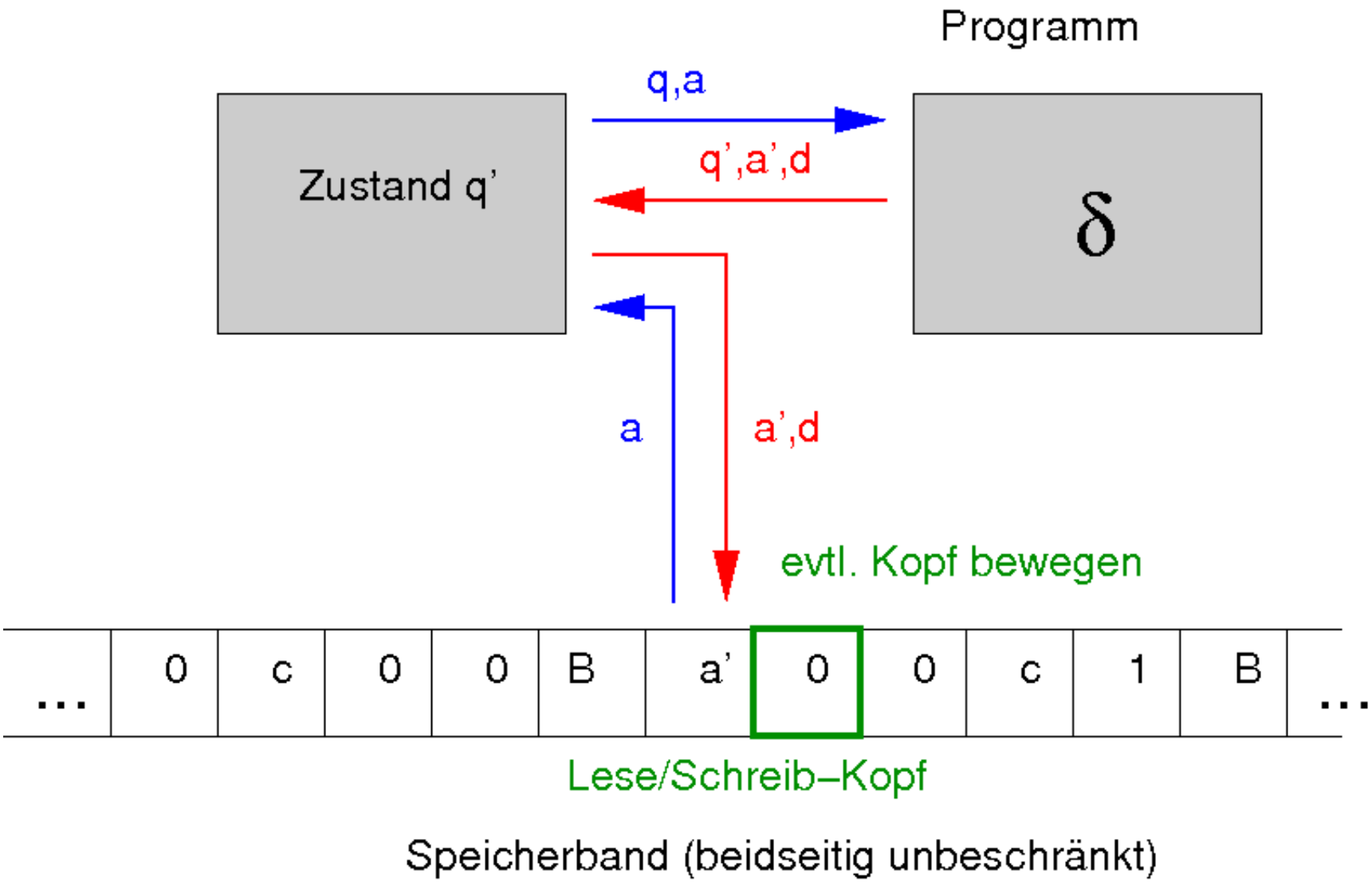
Deterministische Turingmaschine (TM bzw. DTM)



Deterministische Turingmaschine (TM bzw. DTM)



Deterministische Turingmaschine (TM bzw. DTM)



Komponenten der TM

- Q, die endliche Zustandsmenge
- Σ, das endliche Eingabealphabet
- $\Gamma \supset \Sigma$, das endliche Bandalphabet
- $B \in \Gamma \setminus \Sigma$, das Leerzeichen (Blank)
- $q_0 \in Q$, der Anfangszustand
- $\bar{q} \in Q$, der Endzustand
- $\delta : (Q \setminus \{\bar{q}\}) \times \Gamma \to Q \times \Gamma \times \{R, L, N\}$, die Zustandsüberführungsfunktion

Eine TM ist definiert durch das 7-Tupel $(Q, \Sigma, \Gamma, B, q_0, \bar{q}, \delta)$.

Funktionsweise der TM

Ausgangssituation

- auf dem Band steht die Eingabe $w \in \Sigma^*$ eingerahmt von Blanks
- der initiale Zustand ist q_0
- der Kopf steht über dem ersten Symbol von w

Nummerierung der Zellen des Bandes

- die initiale Kopfposition wird als Position 0 bezeichnet
- bewegt sich der Kopf einen Schritt „nach rechts“ erhöht sich die Position um 1
- bewegt sich der Kopf um einen Schritt „nach links“ erniedrigt sich die Position um 1

Funktionsweise der TM

Durchführung eines Rechenschrittes

- $a \in \Gamma$ bezeichne das gelesene Symbol
- $q \in Q \setminus \{\bar{q}\}$ bezeichne den aktuellen Zustand
- es sei $\delta(q, a) = (q', a', d)$, für $q' \in Q, a' \in \Gamma, d \in \{R, L, N\}$
- dann wird der Zustand auf q' gesetzt
- an der Kopfposition wird das Symbol a' geschrieben
- der Kopf

$$\text{bewegt sich} \begin{cases} \text{um eine Position nach rechts} & \text{falls } d = R \\ \text{um eine Position nach links} & \text{falls } d = L \\ \text{nicht} & \text{falls } d = N \end{cases}$$

Funktionsweise der TM

Ende der Rechnung

- die TM stoppt, wenn sie den Endzustand $\bar{q}$ erreicht
- das Ausgabewort $w' \in \Sigma^*$ kann dann vom Band abgelesen werden: w' beginnt an der Kopfposition und endet unmittelbar vor dem ersten Symbol aus $\Gamma \setminus \Sigma$
- *Spezialfall:* wenn wir es mit Entscheidungsproblemen zu tun haben, wird die Antwort wie folgt als JA oder NEIN interpretiert:
  - die TM *akzeptiert* das Eingabewort, wenn sie terminiert und das Ausgabewort mit einer 1 beginnt
  - die TM *verwirft* das Eingabewort, wenn sie terminiert und das Ausgabewort nicht mit einer 1 beginnt

Funktionsweise der TM

Bemerkungen

- Beachte, es gibt die Möglichkeit, dass die TM den Endzustand niemals erreicht. Wir sagen dann, die *Rechnung terminiert nicht*.
- Laufzeit = Anzahl der Zustandsübergänge bis zur Terminierung
- Speicherplatz = Anzahl der Bandzellen, die während der Rechnung besucht werden

Funktionsweise der TM am Beispiel

Sei $L = \{w1 | w \in \{0,1\}^*\}$.

L wird *entschieden* durch die TM $M = (Q, \Sigma, \Gamma, B, q_0, \bar{q}, \delta)$ mit

- $Q = \{q_0, q_1, \bar{q}\}$
- $\Sigma = \{0, 1\}$
- $\Gamma = \{0, 1, B\}$
- δ gemäß Tabelle

δ	0	1	B
q_0	(q_0, B, R)	(q_1, B, R)	reject
q_1	(q_0, B, R)	(q_1, B, R)	accept

„accept“ steht als Abkürzung für $(\bar{q}, 1, N)$.
„reject“ steht als Abkürzung für $(\bar{q}, 0, N)$.

Die TM ist ein formales Modell zur Beschreibung von Algorithmen.

Funktionsweise der TM am Beispiel

Die Übergangsfunktion ist zentraler Bestandteil des Algorithmus der TM.

Beschreibung der Übergangsfunktion als Tabelle:

δ	0	1	B
q_0	(q_0, B, R)	(q_1, B, R)	reject
q_1	(q_0, B, R)	(q_1, B, R)	accept

Verbale Beschreibung des Algorithmus der TM:

- Solange ein Symbol aus $\{0, 1\}$ gelesen wird
  - überschreibe das Symbol mit B,
  - bewege den Kopf nach rechts, und
  - gehe in den Zustand q_0, wenn das Symbol eine 0 war, sonst in den Zustand q_1
- Sobald ein Blank gelesen wird, so
  - akzeptiere die Eingabe, falls der aktuelle Zustand q_1 ist, und
  - verwirf die Eingabe ansonsten.

Zum Sinn und Zweck des TM-Modells

Die TM dient als formales bzw. mathematisches Modell zur Beschreibung von Algorithmen.

Die Frage, *ob es für ein Problem einen Algorithmus gibt*, setzen wir gleich mit der Frage, *ob es eine TM gibt, die dieses Problem löst*.

Natürlich stellt sich an dieser Stelle die Frage, ob dass TM-Modell allgemein genug ist, um alle denkbaren Algorithmen abzudecken bzw. um alle Fähigkeiten abzudecken, die ein moderner oder zukünftiger Computer hat bzw. haben könnte. Auf diese Problematik kommen wir später noch zurück.

Formale Definition des Begriffes *TM-berechenbar*

Bzgl. der Probleme beschränken wir uns in dieser Vorlesung auf Funktionen und Entscheidungsprobleme (Sprachen).

Definition

Eine Funktion $f : \Sigma^* \rightarrow \Sigma^*$ heißt *rekursiv (TM-berechenbar)*, wenn es eine TM gibt, die aus der Eingabe x den Funktionswert $f(x)$ berechnet.

Definition

Eine Sprache $L \subseteq \Sigma^*$ heißt *rekursiv (TM-entscheidbar)*, wenn es eine TM gibt, die für alle Eingaben terminiert und die Eingabe w genau dann akzeptiert, wenn $w \in L$ ist.

Programmierung der TM am Beispiel

Beispiel: Wir entwickeln eine TM für die Sprache

$$L = \{0^n 1^n | n \geq 1\} \ .$$

Sei $\Sigma = \{0, 1\}$, $\Gamma = \{0, 1, B\}$, $Q = \{q_0, \ldots, q_6, \bar{q}\}$.

Unsere TM arbeitet in zwei Phasen:

- **Phase 1:** Teste, ob das Eingabewort von der Form $0^i 1^j$ für $i \geq 0$ und $j \geq 1$ ist.
- **Phase 2:** Teste, ob $i = j$ gilt.

Phase 1 verwendet $\{q_0, q_1\}$ und wechselt bei Erfolg zu q_2.
Phase 2 verwendet $\{q_2, \ldots, q_6\}$ und akzeptiert bei Erfolg.

Programmierung der TM am Beispiel - Phase 1

δ	0	1	B
q_0	$(q_0, 0, R)$	$(q_1, 1, R)$	reject
q_1	reject	$(q_1, 1, R)$	(q_2, B, L)

q_0 : Laufe von links nach rechts über die Eingabe bis ein Zeichen ungleich 0 gefunden wird.

- Falls dieses Zeichen eine 1 ist, gehe über in Zustand q_1.
- Sonst ist dieses Zeichen ein Blank. Verwirf die Eingabe.

q_1 : Gehe weiter nach rechts bis zum ersten Zeichen ungleich 1.

- Falls dieses Zeichen eine 0 ist, verwirf die Eingabe.
- Sonst ist das gefundene Zeichen ein Blank. Bewege den Kopf um eine Position nach links auf die letzte gelesene 1. Wechsel in den Zustand q_2, Phase 2 beginnt.

Programmierung der TM am Beispiel - Phase 2

δ	0	1	B
q_2	reject	(q_3, B, L)	reject
q_3	$(q_3, 0, L)$	$(q_3, 1, L)$	(q_4, B, R)
q_4	(q_5, B, R)	reject	reject
q_5	$(q_6, 0, R)$	$(q_6, 1, R)$	accept
q_6	$(q_6, 0, R)$	$(q_6, 1, R)$	(q_2, B, L)

q_2 : Kopf steht auf dem letzten Nichtblank. Falls dieses Zeichen eine 1 ist, so lösche es, gehe nach links, und wechsel in den Zustand q_3. Sonst verwirf die Eingabe.

q_3 : Bewege den Kopf auf das erste Nichtblank. Dann q_4.

q_4 : Falls das gelesene Zeichen eine 0 ist, ersetze es durch ein Blank und gehe nach q_5, sonst verwirf die Eingabe.

q_5 : Wir haben jetzt die linkeste 0 und die rechteste 1 gelöscht. Falls Restwort leer, dann q_7 (akzeptiere), sonst q_6.

q_6 : Laufe wieder zum letzten Nichtblank und starte erneut in q_2.

Konfigurationen und (direkte) Nachfolgekonfigurationen

Definition

i) Eine *Konfiguration* einer TM ist ein String $\alpha q \beta$, für $q \in Q$ und $\alpha, \beta \in \Gamma^*$. Bedeutung: auf dem Band steht $\alpha\beta$ eingerahmt von Blanks, der Zustand ist q, und der Kopf steht unter dem ersten Zeichen von β.

ii) $\alpha' q' \beta'$ ist *direkte Nachfolgekonfiguration* von $\alpha q \beta$, falls $\alpha' q' \beta'$ in einem Rechenschritt aus $\alpha q \beta$ entsteht. Wir schreiben $\alpha q \beta \vdash \alpha' q' \beta'$.

iii) $\alpha'' q'' \beta''$ ist *Nachfolgekonfiguration* von $\alpha q \beta$, falls $\alpha'' q'' \beta''$ in endlich vielen Rechenschritten aus $\alpha q \beta$ entsteht. Wir schreiben $\alpha q \beta \vdash^* \alpha'' q'' \beta''$.

Bemerkung: insbesondere gilt $\alpha q \beta \vdash^* \alpha q \beta$.

Beispiel zum Umgang mit Konfigurationen

Die für die Sprache $L = \{0^n 1^n | n \geq 1\}$ beschriebene TM liefert in Phase 1 auf die Eingabe 0011 die folgende Konfigurationsfolge.

Phase 1:

$$q_0 0011 \vdash 0 q_0 011 \vdash 00 q_0 11 \vdash 001 q_1 1 \vdash 0011 q_1 B \vdash 001 q_2 1$$

Beobachtung: abgesehen von Blanks am Anfang und Ende des Strings sind die Konfigurationsbeschreibungen eindeutig.

Trick 1: Speicher im Zustandsraum

Für beliebiges festes $k \in \mathbb{N}$, können wir k Zeichen unseres Bandalphabets im Zustand abspeichern, indem wir den Zustandsraum um den Faktor $|\Gamma|^k$ vergrößern, d.h. wir setzen

$$Q_{neu} := Q \times \Gamma^k \quad .$$

Trick 2: Mehrspurmaschinen

Bei einer k-spurigen TM handelt es sich um eine TM, bei der das Band in k sogenannte Spuren eingeteilt ist, d.h. in jeder Bandzelle stehen k Zeichen, die der Kopf gleichzeitig einlesen kann. Das können wir erreichen, indem wir das Bandalphabet um k-dimensionale Vektoren erweitern, z.B.

$$\Gamma_{neu} := \Sigma \cup \Gamma^k \quad .$$

Beispiel: Addition mittels 3-spuriger TM

Die Verwendung einer mehrspurigen TM erlaubt es, Algorithmen einfacher zu beschreiben.

Wir verdeutlichen dies am Beispiel der Addition. Aus der Eingabe $bin(i_1)\#bin(i_2)$ für $i_1, i_2 \in \mathbb{N}$ soll $bin(i_1 + i_2)$ berechnet werden. Wir verwenden eine 3-spurige TM mit den Alphabeten $\Sigma = \{0, 1, \#\}$ und

$$\Gamma = \left\{ 0, 1, \#, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, B \right\} .$$

Beispiel: Addition mittels 3-spuriger TM

- *Schritt 1:* Transformation in Spurendarstellung: Schiebe die Eingabe so zusammen, dass die Binärkodierungen von i_1 und i_2 in der ersten und zweiten Spur rechtsbündig übereinander stehen. Aus der Eingabe 0011#0110 wird beispielsweise

$$B^* \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} B^* \quad .$$

- *Schritt 2:* Addition nach der Schulmethode indem der Kopf das Band von rechts nach links durchläuft. Überträge werden im Zustand gespeichert. Als Ergebnis auf Spur 3 ergibt sich

$$B^* \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} B^* \quad .$$

- *Schritt 3:* Rücktransformation von Spur 3 ins Einspur-Format: Ausgabe 1001.

Techniken zur Programmierung von TMen

Standardtechniken aus der Programmierung können auch auf TMen implementiert werden.

- *Schleifen* haben wir bereits im Beispiel gesehen.
- *Variablen* können realisiert werden, indem wir pro Variable eine Spur reservieren.
- *Felder (Arrays)* können ebenfalls auf einer Spur abgespeichert werden.
- *Unterprogramme* können implementiert werden indem wir eine Spur des Bandes als Prozedurstack verwenden.

Basierend auf diesen Techniken können wir uns klar machen, dass bekannte Algorithmen z.B. zum Sortieren von Daten ohne Weiteres auf der TM ausgeführt werden können.