Komplexitätstheorie

(3 V + 2 Ü)

Nicole Schweikardt
Goethe-Universität Frankfurt am Main

Webseite:

www.tks.informatik.uni-frankfurt.de/teaching/komp

Literatur:

[AB] Sanjeev Arora, Boaz Barak:
Computational Complexity: A Modern Approach.
Cambridge University Press, 2009

Kapitel 0: Einleitung und grundlegende Notationen

0.0 Einleitung

Ziel: Charakterisierung des Schwierigkeitsgrads bestimmter Probleme.

Insbes: Berechnungskomplexität — d.h.: Wie schwer ist es, die Lösung eines vorgegebenen Problems zu berechnen?

Beispiele für Berechnungsprobleme:

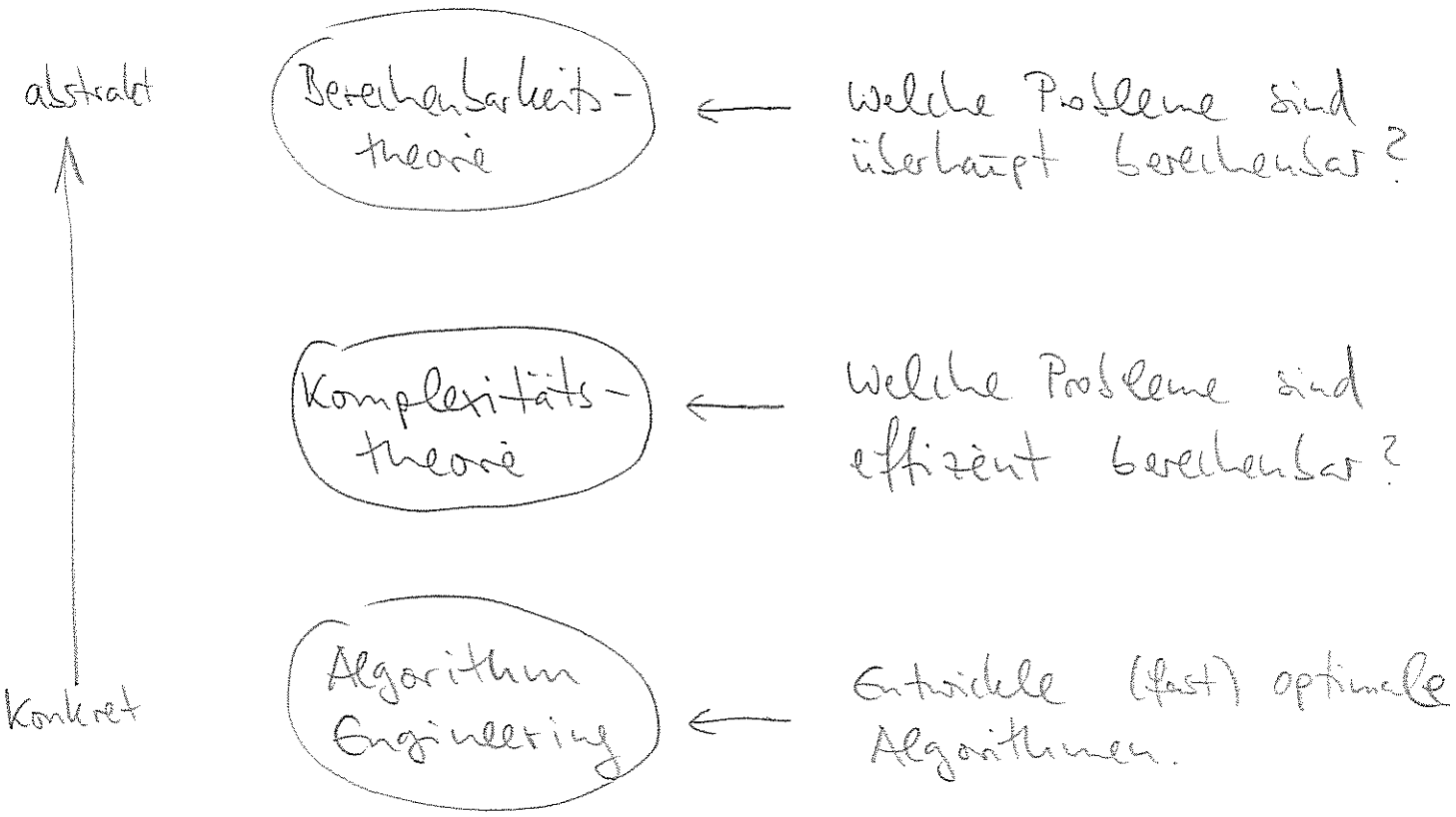
(i) Gegeben zwei natürliche Zahlen, berechne deren Produkt.

(ii) Gegeben ein lineares Gleichungssystem bestehend aus n linearen Gleichungen über n Variablen, finde eine Lösung des linearen Gleichungssystems (falls es eine gibt).

(iii) Gegeben eine Liste von Personen und eine Liste von Paaren $\{x,y\}$ von Personen, die nicht miteinander auskommen, finde eine möglichst große Menge der Personen, die Du zu einer Feier einladen kannst, so dass alle geladenen Gäste miteinander auskommen.

Forschungsgebiete:

Fragestellung / Ziel:



Beispiele für effiziente Berechnungen.

(i) Multiplikation zweier natürlicher Zahlen a und b:

Algorithmus 1: "Wiederholtes Addieren":

```
p := 0
for i := 1 to b do
    p := p + a
end
```

Algorithmus 2: "Grundschul-Multiplikation"

Bsp: $577 \cdot 423$

$$
\begin{array}{r}
1731 \\
1154 \\
2308 \\
\hline
244071
\end{array}
$$

Frage: Was ist effizienter?

Idee:
- Algo 1 benötigt 423 Additionsschritte für Berechnung von $577 \cdot 423$,
- Algo 2 benötigt 3 Multiplikationen der Zahl 577 mit einer Ziffer und zusätzlich die Addition von 3 Zahlen

Allgemein: Für Multiplikation zweier n-stelliger Zahlen (d.h. Zahlen zwischen 10^{n-1} und 10^n) benötigt
- Algo 1 mindestens 10^{n-1} Additionsschritte
- Algo 2 höchstens n Multiplikationsschritte und n Additionsschritte.

Jeder Additions- und Multiplikationsschritt benötigt $O(n)$ Elementarschritte

$\Rightarrow$ Bereits für 20-stellige Zahlen liefert Algo 2, ausgeführt von einem Viertklässler, schneller ein Ergebnis als Algo 1, ausgeführt auf einem Supercomputer.

Bemerkung: Es ist ein noch schnellerer Algorithmus zur Multiplikation bekannt, der auf der schnellen Fouriertransformation beruht und in $O(n \cdot \log n \cdot \log\log n)$ Elementarschritten zum Ziel führt; siehe Kapitel 16 von [AB].

(ii): Lösung eines linearen Gleichungssystems aus n Gleichungen über n Variablen:

Algo 1: Gauß-Elimination

$\rightsquigarrow$ $O(n^3)$ arithmetische Operationen

Algo 2: Strassens Algorithmus (1960er Jahre)

$\rightsquigarrow$ $O(n^{2,81})$ Operationen

... Noch effizientere Algorithmen bekannt.

(iii): "konfliktfreie Gästeliste":

Naiver Algorithmus:

~~For~~ $i := n$ to 1:

Betrachte jede i-elementige Teilmenge der gegebenen n-elementigen Liste von Personen und teste, ob diese Teilmenge ein Paar $\{x, y\}$ enthält, das nicht miteinander auskommt.

Falls nein: STOP; die gerade betrachtete Teilmenge ist eine größtmögliche konfliktfreie Gästeliste.

Anzahl Schritte im Worst-Case: mehr als 2^n.

Bemerkung: Bis heute ist kein wesentlich effizienteres Algorithmus für Lösung dieses Problems bekannt. Mehr dazu in Kapitel 2 bzgl des "Independent Set" - Problems, das NP-vollständig ist

Eins der Ziele der Komplexitätstheorie:

Nachweis unterer Schranken für die Ressourcen, die für Lösung eines Problems prinzipiell benötigt werden.

Schön wäre z.B., wenn wir beweisen könnten, dass es keinen Algorithmus geben kann, der das "Konfliktfreie Gästeliste" - Problem löst und dabei weniger als $2^{n/10}$ Schritte durchführt.

0.1 Grundlegende Notationen und Konventionen

- $\mathbb{N} := \{0, 1, 2, \dots\}$ Menge der natürlichen Zahlen
- Zahlen, die durch Buchstaben i, j, k, ℓ, m, n bezeichnet werden, sind stets ganze Zahlen
- Für $n \geq 1$ ist $[n] := \{1, \dots, n\}$
- Für $x \in \mathbb{R}$ ist
  - $\lceil x \rceil$ das kleinste $z \in \mathbb{Z}$ mit $x \leq z$
  - $\lfloor x \rfloor$ das größte $z \in \mathbb{Z}$ mit $z \leq x$
- Wann immer wir eine reelle Zahl x in einem Kontext benutzen, in dem eigentlich eine ganze Zahl erwartet wird, ist $\lceil x \rceil$ gemeint.
- $\log x := \log_2 x$
- Wir sagen
  "eine Bedingung $P(n)$ gilt für hinreichend große n",
  falls es eine Zahl N gibt, so dass $P(n)$ für alle $n > N$ gilt
  (Bsp: $2^n > 100n^2$ gilt für hinreichend große n)
- Falls u ein Wort (oder Vektor) ist, so bezeichnet u_i das i-te Symbol von u (oder die i-te Koordinate von u)
  (Bsp: Für $u = aabab$ gilt $u_3 = b$, $u_4 = a$)

- Ist S ein Alphabet (d.h. eine Menge), so bezeichnet S^n die Menge aller Worte der Länge n über S (für $n \in \mathbb{N}$).
- $S^* = \bigcup_{n \in \mathbb{N}} S^n$
- $x \in S^*$, $k \in \mathbb{N}$ $\Rightarrow$ $x^k := \underbrace{x \circ \dots \circ x}_{k\text{-mal } x \text{ hintereinander-geschrieben}}$
- $x \in S^*$ $\Rightarrow$ $|x|$ bezeichnet die Länge von x

  Für $a \in S$ bezeichnet $|x|_a$ die Anzahl der Vorkommen des Buchstabens a in x

  (Bsp: Für $x = aabab$ ist $|x|_a = 3$).

Repräsentation von Objekten durch Worte

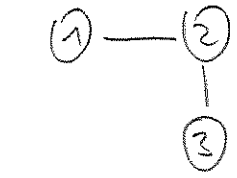
Die Berechnungsaufgaben, die wir in der Veranstaltung "Komplexitätstheorie" betrachten, betreffen zumeist Funktionen, deren Ein- und Ausgabe Bitstrings sind, d.h. Funktionen $f: \{0,1\}^* \to \{0,1\}^*$.

Dies ist keine wirkliche Einschränkung, da wir allgemeine Objekte leicht durch Bitstrings repräsentieren können:

z.B. repräsentieren wir natürliche Zahlen durch deren Binärdarstellung (z.B. 18 durch 10010).

Einen Graph G auf der Knotenmenge $[n] = \{1,\dots,n\}$ repräsentieren wir durch seine Adjazenzmatrix A mit $A_{i,j} = 1 \iff \{i,j\} \in E(G)$ (f.a. $i,j \in [n]$), deren Zeilen wir hintereinander schreiben

Bsp: G:



A

	1	2	3
1	0	1	0
2	1	0	1
3	0	1	0

Bitstring: 010 101 010

Meistens werden wir es vermeiden, uns um die "Low-Level"-Details der Repräsentation zu kümmern und schreiben kurz $\langle x \rangle$, um eine kanonische (und nicht näher spezifizierte) Binärrepräsentation eines Objekts x zu bezeichnen. Oft schreiben wir auch einfach x an Stelle des formal korrekten $\langle x \rangle$.

Beachte: Die Binärrepräsentation $\langle x \rangle$ hat nichts mit dem Symbol $\lfloor x \rfloor$ zum Abrunden einer reellen Zahl zu tun. — Wir verwenden hier die Notation aus [AB].

Repräsentation von Paaren und Tupeln

Wir schreiben $\langle x, y \rangle$, um das geordnete Paar bestehend aus x und y zu bezeichnen.

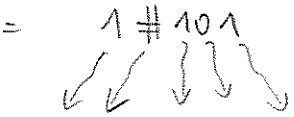
Eine kanonische Repräsentation von $\langle x, y \rangle$ durch einen Bitstring erhalten wir wie folgt:

Repräsentiere $\langle x, y \rangle$ durch das Wort $\lfloor x \rfloor \# \lfloor y \rfloor$ über dem Alphabet $\{0, 1, \#\}$

und ersetze dann jedes Symbol

0 durch 00
1 durch 11
durch 01

Bsp: $\langle 1, 5 \rangle \rightsquigarrow \lfloor 1 \rfloor \# \lfloor 5 \rfloor = 1\#101$



$11\,01\,11\,00\,11 = \lfloor \langle 1, 5 \rangle \rfloor$

Meistens schreiben wir einfach $\langle x, y \rangle$ an Stelle von $\lfloor \langle x, y \rangle \rfloor$

Auf die gleiche Weise können wir auch 3-Tupel $\langle x, y, z \rangle$ oder allgemein k-Tupel $\langle x_1, \ldots, x_k \rangle$ durch Bitstrings repräsentieren.

Berechnung von Funktionen, die nicht auf Bitstrings operieren

Funktionen f, deren Definitions- oder Wertebereich nicht $\{0,1\}^*$ ist, werden wir stillschweigend mit einer entsprechenden Funktion $g: \{0,1\}^* \to \{0,1\}^*$ identifizieren, so dass $f.a.$ x im Definitionsbereich von f gilt: $g(x) = f(x)$.

0.2 Entscheidungsprobleme und Sprachen

Wichtiger Spezialfall von Funktionen, die Bitstrings auf Bitstrings abbilden:

Boolesche Funktionen, d.h. $f: \{0,1\}^* \to \{0,1\}$.

Wir identifizieren eine Boolesche Funktion f mit der Menge

$$L_f := \{ x \in \{0,1\}^* : f(x) = 1 \}.$$

L_f wird auch Sprache (als Teilmenge von $\{0,1\}^*$) oder Entscheidungsproblem (gegeben $x \in \{0,1\}^*$, entscheide, ob $x \in L_f$ ist) genannt.

Wir identifizieren das Problem, $f: \{0,1\}^* \to \{0,1\}$ zu berechnen (d.h. bei Eingabe x den Wert $f(x)$ zu berechnen) mit dem Problem, die Sprache L_f zu entscheiden (d.h. bei Eingabe x zu entscheiden, ob $x \in L_f$ ist).

Beispiel 0.1:

Das "Konfliktfreie Gästeliste"-Problem können wir durch einen Graphen mit Knotenmenge $[n]$ repräsentieren, bei dem eine Kante zwischen zwei Personen i und j anzeigt, dass i und j nicht miteinander auskommen.
Ziel ist, eine möglichst große Menge unabhängiger Knoten zu finden, d.h. Knoten, zwischen denen keine Kante verläuft — ein sog. "independent set".

Das zugehörige Entscheidungsproblem ist

$$\text{INDSET} := \{ \langle G,k \rangle : \exists\, S \subseteq V(G) \text{ s.d. } |S| \geq k \text{ und } \forall u,v \in S \text{ ist } \{u,v\} \notin E(G) \}$$

Ein Algorithmus, der INDSET löst, sagt uns für gegebenes G und k, ob eine konfliktfreie Gästeliste der Größe $\geq k$ existiert. In Kapitel 2 werden wir sehen, dass man daraus auch tatsächlich eine entsprechende Gästeliste berechnen kann

0.3 Die $\mathcal{O}$-Notation

Definition 0.2:

Falls $f, g : \mathbb{N} \to \mathbb{N}$, so sagen wir

(1) $f = \mathcal{O}(g)$, falls es $c \in \mathbb{N}$ s.d.
$f(n) \leq c \cdot g(n)$ für hinreichend große n

(2) $f = \Omega(g)$, falls $g = \mathcal{O}(f)$

(3) $f = \Theta(g)$, falls $f = \mathcal{O}(g)$ und $f = \Omega(g)$

(4) $f = o(g)$, falls f.a. $\varepsilon > 0$ gilt.
$f(n) \leq \varepsilon \cdot g(n)$ für hinreichend große n
(d.h.: $\frac{f(n)}{g(n)} \xrightarrow{n \to \infty} 0$)

(5) $f = \omega(g)$, falls $g = o(f)$

Oft schreiben wir $f(n) = \mathcal{O}(g(n))$ an Stelle von $f = \mathcal{O}(g)$.

Beispiele 0.3:

(1) Für $f(n) = 100n \cdot \log n$ und $g(n) = n^2$ gilt:
$f = \mathcal{O}(g)$, $g = \Omega(f)$, $f = o(g)$, $g = \omega(f)$

(2) Für $f(n) = 100n^2 + 24n + 2\log_2 n$ gilt:

$f(n) = \Theta(n^2)$

(3) Für $f(n) = \min\{n, 10^6\}$ und $g(n) = 1$ $(\forall\, n \in \mathbb{N})$ gilt: $f = \Theta(g)$.

kurz: $f = \Theta(1)$.

(4) Für jedes $c \in \mathbb{N}$ gilt: $n^c = o(2^n)$.

Schreibweise: Wir schreiben $h(n) = n^{O(1)}$ (oder $h(n) = \text{poly}(n)$), um auszusagen, dass es ein $c \in \mathbb{N}$ gibt, so dass $h(n) \leq n^c$ für hinreichend große n gilt.

Übungsaufgaben:

A0.1

(a) Teile (a), (b), (e), (f) von [AB], Exercise 0.1

(b) Teile (a), (c), (d), (g) ------ 0.2

↑

u.a. $f: \mathbb{N} \to \mathbb{N}$ mit $f(0) = 10$ und, $\forall\, n \geq 1$:

(a) $f(n) = f(n-1) + 10$
$\rightsquigarrow f = \Theta(n)$

(b) $f(n) = f(n-1) + n$
$\rightsquigarrow f = \Theta(n^2)$

(c) $f(n) = f(\frac{n}{2}) + 10$
$\rightsquigarrow f = \Theta(\log n)$

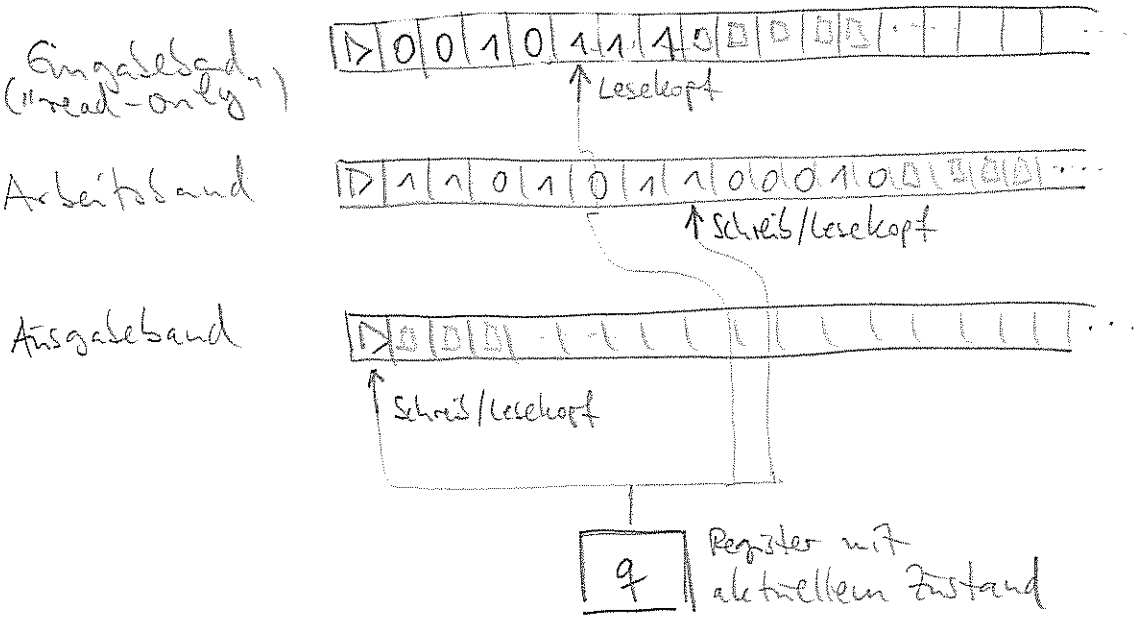
A0.2

[AB], Exercise 0.3.

Kapitel 1:
Das Berechnungsmodell – und warum Details der Definition nicht wichtig sind

1.1 Turingmaschinen

k-Band-TM: (hier für $k=3$)



Definition 1.1

Sei $k \geq 2$. Eine (deterministische) (k-Band) Turingmaschine M (kurz: TM) wird durch ein Tupel (Γ, Q, δ) beschrieben, wobei

- Γ eine endliche Menge von Symbolen ist, die in den Zellen der k Bänder von M stehen können. Dabei gilt $\Gamma \supseteq \{0, 1, \triangleright, \square\}$, wobei $\square$ das Blank-Symbol ist und $\triangleright$ ein besonderes Start-Symbol, das in der linkesten Zelle jedes Bandes steht. Γ heißt das Alphabet von M

- Q eine endliche Menge von Zuständen ist, die sich im Register von M befinden können.

  Dabei gilt $Q \supseteq \{q_{start}, q_{halt}\}$, wobei q_{start} der Startzustand und q_{halt} der Haltezustand ist.

- Einer Funktion $\delta: Q \times \Gamma^k \to Q \times \Gamma^{k-1} \times \{L, S, R\}^k$

  (L: left, S: stay, R: right)

  der sog. Transitionsfunktion von M.

Ist M in Zustand $q \in Q$ und liest die Symbole $(\sigma_1, \dots, \sigma_k)$ an den Schreib/Leseköpfen der Bänder $1, \dots, k$ und ist $\delta(q, \sigma_1, \dots, \sigma_k) = (q', \sigma_2', \dots, \sigma_k', B)$ mit $B \in \{L, S, R\}^k$, so werden im nächsten Berechnungsschritt die an den Schreib-/Leseköpfen der Bänder $2, \dots, k$ stehenden Symbole $\sigma_2, \dots, \sigma_k$ durch die Symbole $\sigma_2', \dots, \sigma_k'$ ersetzt, der Zustand q im Register wird durch den Zustand q' ersetzt, und die Schreib-/Leseköpfe der Bänder $1, \dots, k$ bewegen sich um einen Schritt in die durch B angegebene Richtung (d.h.: der Kopf auf Band i bewegt sich nach links / nach rechts / gar nicht, falls $B_i = L$, $B_i = R$, $B_i = S$).

Falls ein Schreib/Lesekopf, der auf dem linksten Band-symbol steht, um einen Schritt nach links bewegt werden soll, dann bleibt er stattdessen einfach auf der

linkesten Bandposition.

Startkonfiguration bei Eingabe $x \in \{0,1\}^*$:

- Zustand q_{start}
- Die Schreib/Leseköpfe der k Bänder stehen jeweils auf der linkesten Bandposition
- Auf dem Eingabeband befindet sich ganz links das Startsymbol $\triangleright$, auf den nächsten $|x|$ Bandpositionen steht das Wort x, und alle anderen Bandpositionen sind mit dem Blanksymbol $\square$ beschriftet
- Auf jedem der Bänder $2, \dots, k$ befindet sich ganz links das Startsymbol $\triangleright$; alle anderen Bandpositionen sind mit dem Blanksymbol $\square$ beschriftet.

Berechnungsschritte:

Jeder Berechnungsschritt erfolgt durch Anwenden der Transitionsfunktion δ, wie oben beschrieben

Ende der Berechnung:

δ muss die folgende Eigenschaft haben: Ist M in Haltezustand q_{halt}, so wird weder die Bandbeschriftung noch der aktuelle Zustand geändert

Die Beschriftung des k-ten Bandes zwischen dem Start-symbol $\triangleright$ und dem ersten Symbol aus $\Gamma \setminus \{0,1\}$ ist dann die Ausgabe von M bei Eingabe x, kurz: $M(x)$.

Beispiel 1.2 (Palindrome)

Sei $PAL : \{0,1\}^* \to \{0,1\}$ wie folgt definiert:

F.a. $x \in \{0,1\}^*$ ist $PAL(x) := \begin{cases} 1 & \text{falls } x \text{ ein Palindrom ist} \\ 0 & \text{sonst} \end{cases}$

(Zur Erinnerung: $x = x_1 \cdots x_n$ ist ein Palindrom, falls $x_1 \cdots x_n = x_n \cdots x_1$).

Eine 3-Band TM M, die PAL berechnet, kann wie folgt vorgehen:

(1) Kopiere die Eingabe auf das Arbeitsband (Band 2)

(2) Bewege den Lesekopf des Eingabebandes wieder ganz nach links zum Startsymbol

(3) Lies parallel das Eingabeband von links nach rechts und das Arbeitsband von rechts nach links. Falls dabei auf den beiden Bändern irgendwann verschiedene Symbole gelesen werden, so schreibe "0" auf Ausgabeband und gehe in Zustand q_{halt}

(4) Falls der Kopf des Eingabebandes am ersten Blanksymbol $\square$ und der Kopf des Arbeitsbandes am Startsymbol $\triangleright$ angekommen ist, so schreibe "1" auf Ausgabeband und gehe in Zustand q_{halt}

Details: $M = (\Gamma, Q, \delta)$ mit

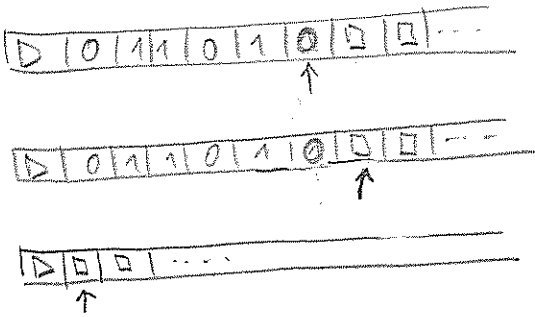
- $\Gamma = \{0, 1, \triangleright, \square\}$,
- $Q = \{q_{start}, q_{copy}, q_{left}, q_{test}, q_{halt}\}$
- δ wie folgt:

(1) $\delta(q_{start}, \triangleright, \triangleright, \triangleright) = (q_{copy}, \triangleright, \triangleright, R, R, R)$

$\delta(q_{copy}, a, \square, \square) = (q_{copy}, a, \square, R, R, S)$ für $a \in \{0,1\}$

$\delta(q_{copy}, \square, \square, \square) = (q_{left}, \square, \square, L, S, S)$

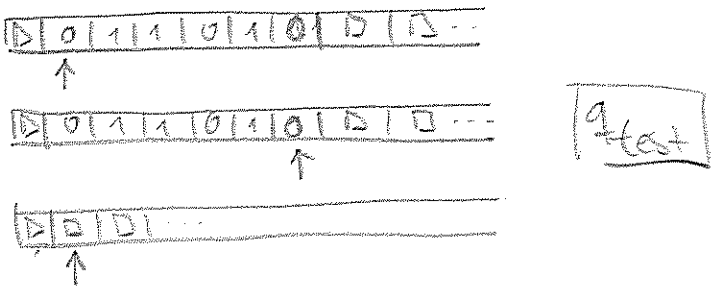
Situation: wenn erstmals in q_{left}



(2): $\delta(q_{left}, a, \square, \square) = (q_{left}, \square, \square, L, S, S)$ für $a \in \{0,1\}$

$\delta(q_{left}, \triangleright, \square, \square) = (q_{test}, \square, \square, R, L, S)$

Situation wenn erstmals in q_{test}:



(3) $\delta(q_{test}, a, a, \square) = (q_{test}, a, \triangleright, R, L, S)$ für $a \in \{0,1\}$

$\delta(q_{test}, a, b, \triangleright) = (q_{halt}, b, 0, S, S, S)$ für $a, b \in \{0,1\}$ mit $a \neq b$

(4) $\delta(q_{test}, \square, \triangleright, \square) = (q_{halt}, \triangleright, 1, S, S, S)$

und $\delta(q, a, b, c) = (q, b, c, S, S, S)$ für alle noch nicht genannte weite $(q, a, b, c) \in Q \times \Gamma^3$.

1.2 Effizienz und Laufzeit

Ansatz: Zähle die Anzahl der Berechnungsschritte einer TM in Bezug auf die Länge n des Eingabewortes.

Definition 1.3 (Berechnung einer Funktion, Laufzeit)

Sei $f: \{0,1\}^* \to \{0,1\}^*$ und sei $T: \mathbb{N} \to \mathbb{N}$.

Sei M eine TM.

(a) Wir sagen: M berechnet f, falls $\forall x \in \{0,1\}^*$ gilt: Wird M in der Startkonfiguration bei Eingabe x gestartet, so gelangt M nach endlich vielen Berechnungsschritten in den Haltezustand q_{halt} und steht dann das Wort $f(x)$ auf dem Band.

(b) Wir sagen: M berechnet f in $T(n)$ Schritten, falls M f berechnet und für jede Eingabe $x \in \{0,1\}^*$ gilt: M gelangt nach höchstens $T(|x|+1)$ Berechnungsschritten in den Endzustand q_{end}.

Beispiel 1.4

Die TM aus Bsp 1.2 berechnet PAL in $3n$ Schritten.

Definition 1.5 (zeitkonstruierbarkeit)

Eine Funktion $T: \mathbb{N} \to \mathbb{N}$ heißt zeitkonstruierbar, falls gilt:

(1) $T(n) \geq n$ und

(2) Es gibt eine TM M, die die Funktion $f: \{0,1\}^* \to \{0,1\}^*$ mit $f(x) = \underline{T(|x|)}$ (f.a. $x \in \{0,1\}^*$) in Zeit $O(T(n))$ berechnet.

(Beachte: Wie in Kapitel 0 vereinbart ist $\underline{T(|x|)}$ die Binärdarstellung der Zahl $T(|x|)$

Fakt 1.6

z.B. die folgenden Funktionen sind zeitkonstruierbar:

(a) 2^n (genauer: $T: \mathbb{N} \to \mathbb{N}$ mit $T(n) = 2^n$ f.a. $n \in \mathbb{N}$)

(b) n^2

(c) n^c, für jedes $c \in \mathbb{N}$ mit $c \geq 2$

(d) $n \cdot \log n$

Beweis:

(a) Bei Eingabe der Länge n muss in $O(2^n)$ Schritten die Binärdarstellung der Zahl 2^n, d.h. der Bitstring 10^n berechnet werden. Das geht ganz leicht, sogar in $O(n)$ Schritten.

(b), (c), (d): Übung!

Frage: Ist $\underline{n}$ zeitkonstruierbar?
(d.h. die Funktion $T: \mathbb{N} \to \mathbb{N}$ mit $T(n) = n$ f.a. $n \in \mathbb{N}$)