

Skript zur Vorlesung

Algorithmen und Berechnungskomplexität II

Prof. Dr. Heiko Röglin

Institut für Informatik



Sommersemester 2014

23. Juni 2014

Inhaltsverzeichnis

1	Einleitung	1
1.1	Probleme und Funktionen	2
1.2	Rechnermodelle	5
1.2.1	Turingmaschinen	5
1.2.2	Registermaschinen	14
1.2.3	Die Church-Turing-These	17
2	Berechenbarkeitstheorie	18
2.1	Entwurf einer universellen Turingmaschine	19
2.2	Die Unentscheidbarkeit des Halteproblems	22
2.3	Turing- und Many-One-Reduktionen	25
2.4	Der Satz von Rice	29
2.5	Rekursiv aufzählbare Sprachen	31
2.6	Weitere nicht entscheidbare Probleme	36
3	Komplexitätstheorie	37
3.1	Die Klassen P und NP	38
3.1.1	Die Klasse P	38
3.1.2	Die Klasse NP	43
3.1.3	P versus NP	47
3.2	NP-Vollständigkeit	48
3.3	Weitere NP-vollständige Probleme	57

Bitte senden Sie Hinweise auf Fehler im Skript und Verbesserungsvorschläge an die E-Mail-Adresse `roeglin@cs.uni-bonn.de`.

Einleitung

Wir haben im vergangenen Semester effiziente Algorithmen zur Lösung einer Vielzahl von Problemen entworfen. In dieser Vorlesung werden wir die Grenzen der Algorithmik kennenlernen und uns damit beschäftigen, für welche Probleme es keine effizienten Algorithmen gibt und welche überhaupt nicht algorithmisch gelöst werden können.

Wir starten mit einer Einführung in die *Berechenbarkeitstheorie*. Dieses Teilgebiet der theoretischen Informatik ist der Frage gewidmet, welche Probleme nicht durch Algorithmen in endlicher Zeit gelöst werden können und zwar unabhängig davon, wie leistungsfähig unsere Rechner in der Zukunft auch sein mögen. Die Existenz solcher *unberechenbaren* Probleme ist uns bereits aus der Vorlesung „Logik und diskrete Strukturen“ bekannt. Wir haben dort jedoch kein konkretes nicht berechenbares Problem angegeben, sondern nur ausgenutzt, dass die Menge der Funktionen überabzählbar ist, während es nur abzählbar unendlich viele Programme gibt. Dieses Ergebnis lässt die Möglichkeit offen, dass alle in der Praxis relevanten Probleme algorithmisch gelöst werden können und nicht berechenbare Probleme im Informatik-Alltag keine Rolle spielen.

Wir werden jedoch am Beispiel des *Halteproblems* demonstrieren, dass es auch ausgesprochen wichtige Probleme gibt, die nicht berechenbar sind. Bei diesem Problem soll für ein gegebenes Programm entschieden werden, ob es nach endlich vielen Schritten terminiert. Zur Verifikation der Korrektheit von Programmen wäre es hilfreich, einen Compiler zu haben, der bei nicht terminierenden Programmen eine Warnung ausgibt. Wir werden beweisen, dass es einen solchen Compiler nicht geben kann, da das Halteproblem nicht berechenbar ist. Anschließend werden wir Techniken kennenlernen, mit deren Hilfe man auch für viele weitere Probleme nachweisen kann, dass sie nicht berechenbar sind.

Im zweiten Teil der Vorlesung werden wir uns mit *Komplexitätstheorie* beschäftigen. In diesem Teilgebiet der theoretischen Informatik geht es um die Frage, welche Ressourcen notwendig sind, um bestimmte Probleme zu lösen. Wir konzentrieren uns insbesondere auf die Ressource Rechenzeit, denn für praktische Anwendungen ist die Laufzeit eines Algorithmus oft von entscheidender Bedeutung. Wer möchte schon einen Tag oder gar mehrere Jahre auf die Ausgabe seines Navigationsgerätes warten? Leider gibt es eine

ganze Reihe von Problemen, die zwar berechenbar sind, für die es aber vermutlich keine effizienten Algorithmen gibt. Ein solches Problem, das in vielen logistischen Anwendungen eine Rolle spielt, ist das *Problem des Handlungsreisenden*, bei dem eine Landkarte mit mehreren Städten gegeben ist und die kürzeste Rundreise durch diese Städte gesucht wird.

Das Problem des Handlungsreisenden gehört wie viele andere natürliche Probleme zu der Klasse der *NP-schweren* Probleme. Man vermutet, dass es für diese Probleme keine effizienten Algorithmen gibt. Diese sogenannte *$P \neq NP$ -Vermutung* ist bis heute unbewiesen und eines der größten ungelösten Probleme der Mathematik und der theoretischen Informatik. Wir werden besprechen, was diese Vermutung genau besagt, und zahlreiche NP-schwere Probleme kennenlernen.

Zwar werden in dieser Vorlesung hauptsächlich negative Ergebnisse gezeigt, diese haben aber wichtige Auswirkungen auf die Praxis. Hat man beispielsweise bewiesen, dass ein Problem nicht effizient gelöst werden kann, so ist klar, dass die Suche nach einem effizienten Algorithmus eingestellt werden kann und dass man stattdessen über Alternativen (Abwandlung des Problems etc.) nachdenken sollte. Außerdem beruhen Kryptosysteme auf der Annahme, dass gewisse Probleme nicht effizient gelöst werden können. Wäre es beispielsweise möglich, große Zahlen effizient zu faktorisieren, so wäre RSA kein sicheres Kryptosystem. In diesem Sinne können also auch negative Ergebnisse gute Nachrichten sein.

Zum Abschluss der Vorlesung werden wir uns mit *Approximationsalgorithmen* beschäftigen. Trifft die $P \neq NP$ -Vermutung zu, so können NP-schwere Probleme nicht effizient gelöst werden. Für solche Probleme ist es deshalb oft sinnvoll, die Anforderungen zu reduzieren und statt nach einer optimalen nur noch nach einer möglichst guten Lösung zu suchen. Ein *r -Approximationsalgorithmus* ist ein effizienter Algorithmus, der für jede Eingabe eine Lösung berechnet, die höchstens um den Faktor r schlechter ist als die optimale Lösung. Ein 2-Approximationsalgorithmus für das Problem des Handlungsreisenden ist also beispielsweise ein Algorithmus, der stets eine Rundreise berechnet, die höchstens doppelt so lang ist wie die kürzeste Rundreise. Wir werden für einige NP-schwere Probleme Approximationsalgorithmen entwerfen und die Grenzen dieses Ansatzes diskutieren.

Es gibt zahlreiche Bücher und Skripte, in denen die Inhalte dieser Vorlesung nachgelesen werden können (z. B. [1, 2, 3]). Diese Vorlesung orientiert sich insbesondere an dem Buch von Ingo Wegener [6] und dem Skript von Berthold Vöcking [5].

1.1 Probleme und Funktionen

Wir haben bereits im letzten Semester diskutiert, dass ein *Algorithmus* eine Handlungsvorschrift ist, mit der Eingaben in Ausgaben transformiert werden können. Diese Handlungsvorschrift muss so präzise formuliert sein, dass sie von einem Computer ausgeführt werden kann. Unter einem *Problem* verstehen wir informell den gewünschten Zusammenhang zwischen der Eingabe und der Ausgabe. Beim Sortierproblem besteht

die Eingabe beispielsweise aus einer Menge von Zahlen und die gewünschte Ausgabe ist eine aufsteigend sortierte Permutation dieser Zahlen.

Um den Begriff „Problem“ zu formalisieren, gehen wir davon aus, dass (wie bei der Betrachtung von formalen Sprachen) eine beliebige endliche Menge Σ gegeben ist, die wir *Alphabet* nennen. Die Eingaben und Ausgaben sind als Zeichenketten über diesem Alphabet codiert. Denkt man an reale Rechner, so ergibt die Wahl $\Sigma = \{0, 1\}$ natürlich Sinn. Für theoretische Betrachtungen ist es aber manchmal hilfreich (wenngleich nicht notwendig) Alphabete mit mehr als zwei Zeichen zu betrachten. Wenn nicht explizit anders erwähnt, so gehen wir in dieser Vorlesung stets davon aus, dass $\{0, 1\} \subseteq \Sigma$ gilt. Wie üblich bezeichnen wir mit Σ^* die Menge aller Zeichenketten endlicher Länge, die sich über dem Alphabet Σ bilden lassen. Dazu gehört insbesondere das leere Wort ε der Länge 0. Für ein Wort $w \in \Sigma^*$ bezeichnen wir mit $|w|$ seine Länge. Außerdem bezeichnet w^R das gespiegelte Wort, das heißt für $w = w_1 \dots w_n$ ist $w^R = w_n \dots w_1$.

Unter einem *Problem* verstehen wir eine Relation $R \subseteq \Sigma^* \times \Sigma^*$ mit der Eigenschaft, dass es für jede Eingabe $x \in \Sigma^*$ mindestens eine Ausgabe $y \in \Sigma^*$ mit $(x, y) \in R$ gibt. Gibt es zu jeder Eingabe eine eindeutige Ausgabe, so können wir das Problem auch als Funktion $f: \Sigma^* \rightarrow \Sigma^*$ beschreiben, die jeder Eingabe $x \in \Sigma^*$ ihre Ausgabe $f(x) \in \Sigma^*$ zuweist. Ein Algorithmus *löst* ein Problem, das durch eine Relation R beschrieben wird, wenn er zu jeder Eingabe $x \in \Sigma^*$ eine Ausgabe $y \in \Sigma^*$ mit $(x, y) \in R$ produziert. Ein Algorithmus *löst* ein Problem, das durch eine Funktion f beschrieben wird, wenn er zu jeder Eingabe $x \in \Sigma^*$ die Ausgabe $f(x)$ produziert. Wir sagen dann auch, dass der Algorithmus die Funktion f *berechnet*.

Wir legen ein besonderes Augenmerk auf Funktionen der Form $f: \Sigma^* \rightarrow \{0, 1\}$. Eine solche Funktion beschreibt ein sogenanntes *Entscheidungsproblem*, da für eine Eingabe $x \in \Sigma^*$ nur entschieden werden muss, ob $f(x) = 0$ oder $f(x) = 1$ gilt. Eine *Sprache* über dem Alphabet Σ ist eine Teilmenge von Σ^* . Zwischen Entscheidungsproblemen und *Sprachen* existiert eine eineindeutige Beziehung. Jedes Entscheidungsproblem $f: \Sigma^* \rightarrow \{0, 1\}$ kann als Sprache $L_f = \{x \in \Sigma^* \mid f(x) = 1\}$ aufgefasst werden. Ebenso kann jede Sprache $L \subseteq \Sigma^*$ als Funktion $f_L: \Sigma^* \rightarrow \{0, 1\}$ mit

$$f_L(x) = \begin{cases} 1 & \text{falls } x \in L \\ 0 & \text{falls } x \notin L \end{cases}$$

aufgefasst werden. Die Funktion f_L heißt die *charakteristische Funktion* der Sprache L .

Wir betrachten nun einige Beispiele für Probleme. In diesen Beispielen und im weiteren Verlauf der Vorlesung bezeichnen wir die Binärdarstellung einer Zahl $n \in \mathbb{N}_0$ ohne führende Nullen mit $\text{bin}(n)$ und wir bezeichnen mit $\text{val}(x) \in \mathbb{N}_0$ die Zahl, die durch $x \in \{0, 1\}^*$ binär codiert wird. Erlauben wir in der Binärdarstellung führende Nullen, so ist $\text{val}(x)$ für jede Zeichenkette $x \in \{0, 1\}^*$ eindeutig bestimmt.

- Das Problem, eine natürliche Zahl in Binärdarstellung zu quadrieren, lässt sich sowohl durch die Funktion $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ mit $f(x) = \text{bin}(\text{val}(x)^2)$ als auch durch die Relation

$$R = \{(x, y) \mid \text{val}(y) = \text{val}(x)^2\} \subseteq \Sigma^* \times \Sigma^*$$

beschreiben. Obwohl beides sinnvolle Modellierungen desselben Problems sind, sind sie formal nicht ganz identisch. Um dies einzusehen, betrachten wir einen Algorithmus, der das Quadrat der Eingabe korrekt berechnet, binär codiert ausgibt und an die Ausgabe zusätzlich noch eine führende Null anfügt. Dieser Algorithmus löst das Problem, das durch die Relation R beschrieben wird, er berechnet aber nicht die Funktion f .

- Das Problem, einen Primfaktor einer natürlichen Zahl zu bestimmen, lässt sich nicht als Funktion beschreiben, da es zu manchen Eingaben mehrere mögliche Ausgaben gibt. Stattdessen kann es aber durch die Relation

$$R = \{(x, y) \mid \text{val}(y) \text{ ist eine Primzahl, die } \text{val}(x) \text{ teilt}\} \subseteq \Sigma^* \times \Sigma^*$$

beschrieben werden.

- Wir betrachten als nächstes das Problem, für einen ungerichteten Graphen $G = (V, E)$ zu entscheiden, ob er zusammenhängend ist oder nicht. Um dieses Problem formal beschreiben zu können, müssen wir zunächst festlegen, wie der Graph G codiert wird. Dazu gibt es zahlreiche Möglichkeiten. Wir entscheiden uns dafür, ihn als Adjazenzmatrix darzustellen, wobei wir die Zeilen dieser Matrix nacheinander schreiben. Für einen Graphen mit n Knoten besitzt diese Darstellung eine Länge von n^2 . Somit codieren genau solche Eingaben $x \in \{0, 1\}^*$ einen Graphen, deren Länge $|x|$ eine Quadratzahl ist. Ist $|x|$ eine Quadratzahl, so bezeichnen wir mit $G(x)$ den durch x codierten Graphen. Wir können das Zusammenhangsproblem als Funktion $f: \{0, 1\}^* \rightarrow \{0, 1\}$ mit

$$f(x) = \begin{cases} 1 & \text{falls } |x| = n^2 \text{ für ein } n \in \mathbb{N} \text{ und } G(x) \text{ ist zusammenhängend} \\ 0 & \text{sonst} \end{cases}$$

modellieren. Diese Funktion gibt den Wert 1 aus, wenn die Eingabe einen zusammenhängenden Graphen codiert, und den Wert 0, wenn die Eingabe entweder syntaktisch nicht korrekt ist oder einen nicht zusammenhängenden Graphen codiert. Dies können wir auch als Sprache

$$L = \{x \in \{0, 1\}^* \mid |x| = n^2 \text{ für ein } n \in \mathbb{N} \text{ und } G(x) \text{ ist zusammenhängend}\}$$

ausdrücken.

Der Leser möge sich als Übung für einige weitere Probleme aus dem letzten Semester überlegen, wie sie formal als Funktion oder Relation beschrieben werden können. Außerdem sollte er sich überlegen, warum es keine echte Einschränkung ist, nur das Alphabet $\Sigma = \{0, 1\}$ zu betrachten.

1.2 Rechnermodelle

Bereits im vergangenen Semester haben wir gesehen, dass zum Entwurf und zur Analyse von Algorithmen ein *Rechnermodell* benötigt wird. Dabei handelt es sich um ein formales Modell, das festlegt, welche Operationen ein Algorithmus ausführen darf und welche Ressourcen (insbesondere welche Rechenzeit) er für diese Operationen benötigt. Wir haben das Modell der *Registermaschine* kennengelernt, das in etwa dieselben Operationen bietet wie eine rudimentäre Assemblersprache. Wir haben uns dann davon überzeugt, dass Registermaschinen das Verhalten realer Rechner gut abbilden, und deshalb für die allermeisten Anwendungen ein vernünftiges Rechnermodell darstellen.

In dieser Vorlesung werden wir jedoch stattdessen das Modell der *Turingmaschine* zugrunde legen. Dieses hat auf den ersten Blick deutlich weniger mit realen Rechnern gemein als Registermaschinen, es ist dafür aber strukturell einfacher und erleichtert deshalb die theoretischen Betrachtungen. Wir werden sehen, dass Turingmaschinen trotz ihrer Einfachheit genauso mächtig sind wie Registermaschinen. Damit sind auch Turingmaschinen ein gutes Modell für reale Rechner, auch wenn man das anhand ihrer Definition nicht direkt erkennen kann.

Nachdem wir das Modell der Turingmaschine eingeführt haben, werden wir die *Church-Turing-These* diskutieren. Diese These besagt, dass eine Turingmaschine alle Funktionen berechnen kann, die „intuitiv berechenbar“ sind. Diese These kann prinzipiell nicht bewiesen werden, da der Begriff „intuitiv berechenbar“ nicht formal definiert ist. Eine formalere Variante dieser These, die zwar prinzipiell beweisbar, aber noch unbewiesen ist, lautet wie folgt: Die Gesetze der Physik erlauben es nicht, eine Maschine zu konstruieren, die eine Funktion berechnet, die nicht auch von einer Turingmaschine berechnet werden kann.

1.2.1 Turingmaschinen

Informell kann man eine Turingmaschine als einen endlichen Automaten beschreiben, der mit einem Band mit unendlich vielen Speicherzellen ausgestattet ist. In jeder Zelle des Bandes steht eins von endlich vielen Zeichen. Dabei bezeichne Γ die endliche Menge von möglichen Zeichen und $\square \in \Gamma$ sei das Leerzeichen. Wie ein endlicher Automat befindet sich auch eine Turingmaschine zu jedem Zeitpunkt in einem von endlich vielen Zuständen, wobei wir die endliche Zustandsmenge wieder mit Q bezeichnen.

Darüber hinaus besitzt eine Turingmaschine einen Lese-/Schreibkopf, der zu jedem Zeitpunkt auf einer Zelle des Bandes steht und das dort gespeicherte Zeichen liest. Basierend auf dem gelesenen Zeichen und ihrem aktuellen Zustand kann die Turingmaschine in einem Rechenschritt das Zeichen an der aktuellen Kopfposition ändern, in einen anderen Zustand wechseln und den Kopf um eine Position nach links oder rechts verschieben. Zu Beginn befindet sich die Eingabe auf dem Band, der Kopf steht auf dem ersten Zeichen der Eingabe (oder auf einem Leerzeichen, wenn die Eingabe das leere Wort ε ist), alle Zellen links und rechts von der Eingabe enthalten das Leerzeichen \square und die Turingmaschine befindet sich im Startzustand $q_0 \in Q$. Die Eingabe

ist dabei keine Zeichenkette aus Γ^* , sondern aus Σ^* für ein Eingabealphabet $\Sigma \subseteq \Gamma$ mit $\square \notin \Sigma$.

Die Turingmaschine führt solange Rechenschritte der oben beschriebenen Form durch, bis sie einen bestimmten Endzustand $\bar{q} \in Q$ erreicht hat. Bezeichne $w_i \in \Gamma$ beim Erreichen des Endzustandes \bar{q} den Inhalt von Zelle i und sei $j \in \mathbb{Z}$ die Kopfposition zu diesem Zeitpunkt. Dann ist die Zeichenkette $w_j \dots w_{k-1} \in \Sigma^*$ die Ausgabe, wobei $k \geq j$ den eindeutigen Index bezeichne, für den $w_j, \dots, w_{k-1} \in \Sigma$ und $w_k \in \Gamma \setminus \Sigma$ gilt. Die Ausgabe ist also die Zeichenkette aus Σ^* , die an der aktuellen Kopfposition beginnt und nach rechts durch das erste Zeichen aus $\Gamma \setminus \Sigma$ beschränkt ist.

Genauso wie bei endlichen Automaten sind die Rechenschritte einer Turingmaschine durch eine Zustandsüberföhrungsfunktion δ bestimmt. Diese erhalt als Eingaben den aktuellen Zustand und das Zeichen an der aktuellen Kopfposition und liefert als Ausgaben den neuen Zustand, das Zeichen, durch das das Zeichen an der Kopfposition ersetzt werden soll, und ein Element aus der Menge $\{L, N, R\}$, das angibt, ob der Kopf an der aktuellen Position stehen bleiben soll (N), eine Position nach links (L) oder eine Position nach rechts (R) verschoben werden soll. Formal handelt es sich dabei um eine Funktion $\delta: (Q \setminus \{\bar{q}\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, N, R\}$.

Definition 1.1. *Eine Turingmaschine (TM) M ist ein 7-Tupel $(Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$, das aus den folgenden Komponenten besteht.*

- Q , die Zustandsmenge, ist eine endliche Menge von Zustanden.
- $\Sigma \supseteq \{0, 1\}$, das Eingabealphabet, ist eine endliche Menge von Zeichen.
- $\Gamma \supseteq \Sigma$, das Bandalphabet, ist eine endliche Menge von Zeichen.
- $\square \in \Gamma \setminus \Sigma$ ist das Leerzeichen.
- $q_0 \in Q$ ist der Startzustand.
- \bar{q} ist der Endzustand.
- $\delta: (Q \setminus \{\bar{q}\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, N, R\}$ ist die Zustandsüberföhrungsfunktion.

Abbildung 1.1 zeigt exemplarisch die Rechenschritte einer Turingmaschine. Die Eingabe ist das Wort $1001 \in \Sigma^*$, welches links und rechts von Leerzeichen umschlossen ist. Der Kopf steht zu Beginn auf dem ersten Zeichen der Eingabe und die Turingmaschine befindet sich im Startzustand q_0 . Die Zustandsüberföhrungsfunktion δ gibt vor, dass im Zustand q_0 beim Lesen des Zeichens 1 in den Zustand q gewechselt wird, das Zeichen 1 geschrieben wird und der Kopf um eine Position nach rechts bewegt wird. Im zweiten Schritt wird in Zustand q das Zeichen 0 gelesen, was gemaß δ dazu föhrt, dass in den Zustand q' gewechselt, das Zeichen 1 geschrieben und der Kopf um eine Position nach rechts bewegt wird. Im dritten und letzten Schritt wird das Zeichen 0 im Zustand q' gelesen, was gemaß δ dazu föhrt, dass in den Endzustand \bar{q} gewechselt, das Zeichen 0 geschrieben und der Kopf nicht bewegt wird. Die Ausgabe der Turingmaschine ist in diesem Beispiel das Wort $01 \in \Sigma^*$.

Mit jeder Turingmaschine M kann man eine Funktion $f_M: \Sigma^* \rightarrow \Sigma^* \cup \{\perp\}$ assoziieren, die für jede Eingabe $w \in \Sigma^*$ angibt, welche Ausgabe $f_M(w)$ die Turingmaschine bei dieser Eingabe produziert. In dem gerade besprochenen Beispiel gilt folglich $f_M(1001) = 01$. Erreicht die Turingmaschine M bei einer Eingabe w den Endzustand \bar{q} nicht nach endlich vielen Schritten, so sagen wir, dass sie bei Eingabe w nicht hält (oder nicht terminiert), und wir definieren $f_M(w) = \perp$. Wir sagen, dass die Turingmaschine M die Funktion f_M berechnet.

Definition 1.2. Eine Funktion $f: \Sigma^* \rightarrow \Sigma^*$ heißt berechenbar (oder rekursiv¹), wenn es eine Turingmaschine M mit $f_M = f$ gibt. Eine solche Turingmaschine terminiert insbesondere auf jeder Eingabe.

Wenn wir das Verhalten einer Turingmaschine beschreiben oder analysieren, so sprechen wir im Folgenden oft von der Konfiguration einer Turingmaschine. Darunter verstehen wir zu einem Zeitpunkt die aktuelle Kombination aus Bandinhalt, Kopfposition und Zustand.

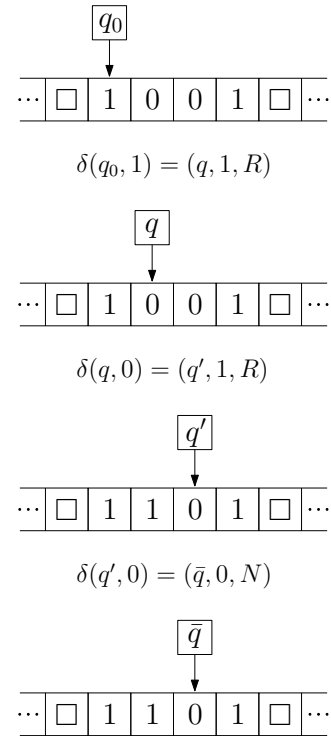


Abbildung 1.1: Beispiel für eine Turingmaschine

Wir betrachten ein Beispiel für eine Turingmaschine $M = (Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$. Es sei $Q = \{q_0, q_1, \dots, q_5, \bar{q}\}$, $\Sigma = \{0, 1\}$ und $\Gamma = \{0, 1, \#, \square\}$. Die Zustandsübergangsfunktion δ ist in der folgenden Tabelle dargestellt. Diese enthält an zwei Stellen das Symbol —, da die entsprechenden Kombinationen von Zustand und Zeichen nicht auftreten können (wie wir weiter unten argumentieren werden). Formal könnte man dort ein beliebiges Tripel aus $Q \times \Gamma \times \{L, N, R\}$ einsetzen, um die Tabelle zu vervollständigen.

	q_0	q_1	q_2	q_3	q_4	q_5
0	$(q_0, 0, R)$	$(q_2, \#, N)$	$(q_2, 0, R)$	$(q_3, 0, R)$	$(q_4, 0, L)$	$(\bar{q}, 0, N)$
1	$(q_0, 1, R)$	$(q_3, \#, N)$	$(q_2, 1, R)$	$(q_3, 1, R)$	$(q_4, 1, L)$	$(\bar{q}, 1, N)$
#	—	$(q_1, \#, L)$	$(q_2, \#, R)$	$(q_3, \#, R)$	$(q_1, \#, N)$	(q_5, \square, R)
\square	$(q_1, \#, N)$	(q_5, \square, R)	$(q_4, 0, N)$	$(q_4, 1, N)$	—	(\bar{q}, \square, N)

Um zu verstehen, welche Funktion diese Turingmaschine berechnet, kann man sich zunächst ihr Verhalten auf einigen Beispielen anschauen. Diese kann man entweder von Hand durchgehen oder man schreibt ein Programm, mit dem man Turingmaschinen simulieren kann. Insbesondere Letzteres sei dem Leser als Übung empfohlen. Wir können aber auch versuchen, direkt zu verstehen, was die Turingmaschine

¹Auf den ersten Blick hat das Wort „rekursiv“ in diesem Kontext nichts mit dem normalen Gebrauch dieses Wortes in der Informatik zu tun. Die Bezeichnung stammt von einer alternativen Charakterisierung berechenbarer Funktionen, die wir in dieser Vorlesung nicht besprechen werden.

in den einzelnen Zuständen macht. Die folgenden Eigenschaften können wir direkt aus der Zustandsüberföhrungsfunktion ablesen.

q_0 : M schiebt den Kopf rechts bis zum Ende der Eingabe (ohne den Bandinhalt dabei zu verändern) und schreibt anschließend rechts neben die Eingabe das Zeichen $\#$. Danach wird in den Zustand q_1 gewechselt und Zustand q_0 wird nie wieder erreicht.

q_1 : M schiebt den Kopf nach links, solange an der aktuellen Position das Zeichen $\#$ steht. Das weitere Vorgehen ist abhängig vom ersten Zeichen ungleich $\#$, das erreicht wird. Ist es 0 oder 1, so wird es durch $\#$ ersetzt und in den Zustand q_2 bzw. q_3 gewechselt. Ist es ein Leerzeichen, so wird in den Zustand q_5 gewechselt.

q_2 : M schiebt den Kopf nach rechts bis zum ersten Leerzeichen, welches sie durch 0 ersetzt. Anschließend wechselt sie in den Zustand q_4 .

q_3 : M schiebt den Kopf nach rechts bis zum ersten Leerzeichen, welches sie durch 1 ersetzt. Anschließend wechselt sie in den Zustand q_4 .

q_4 : M schiebt den Kopf nach links bis sie das erste Mal das Zeichen $\#$ erreicht. Dann wechselt sie in den Zustand q_1 .

q_5 : M schiebt den Kopf nach rechts, bis sie das erste Zeichen ungleich $\#$ erreicht. Alle Rauten, die sie dabei sieht, werden durch Leerzeichen ersetzt. Danach terminiert M .

Nun können wir einen Schritt weitergehen und uns überlegen, was aus diesen Eigenschaften folgt. Dazu betrachten wir das Verhalten der Turingmaschine M , wenn ihr Bandinhalt von der Form $xa\#\dots\#y$ für $x, y \in \{0, 1\}^*$ und $a \in \{0, 1\}$ ist, der Kopf auf der Raute am weitesten rechts steht und die TM sich im Zustand q_1 befindet. Diese Konfiguration erreicht M wenn sie von q_0 in den Zustand q_1 wechselt (zu diesem Zeitpunkt entspricht xa noch der Eingabe, y ist das leere Wort und genau eine Raute steht auf dem Band). In den folgenden Abbildungen ist das Verhalten der Turingmaschine M in dieser Konfiguration dargestellt (links für $a = 0$ und rechts für $a = 1$). Dabei ist nicht jeder einzelne Schritt eingezeichnet, sondern nur diejenigen, in denen Zustandswechsel erfolgen.

q_1	q_1
$x_1 \cdots x_n 0 \# \cdots \# \# y_1 \cdots y_m \square$	$x_1 \cdots x_n 1 \# \cdots \# \# y_1 \cdots y_m \square$
q_1	q_1
$x_1 \cdots x_n 0 \# \cdots \# \# y_1 \cdots y_m \square$	$x_1 \cdots x_n 1 \# \cdots \# \# y_1 \cdots y_m \square$
q_2	q_3
$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m \square$	$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m \square$
q_2	q_3
$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m \square$	$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m \square$
q_4	q_4
$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m 0$	$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m 1$
q_4	q_4
$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m 0$	$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m 1$
q_1	q_1
$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m 0$	$x_1 \cdots x_n \# \# \cdots \# \# y_1 \cdots y_m 1$

Nach den dargestellten Schritten befindet sich die Turingmaschine wieder in fast derselben Konfiguration wie zu Beginn. Der einzige Unterschied ist, dass der Bandinhalt nun von der Form $x\#\dots\#ya$ ist. Das heißt, der letzte Buchstabe auf der linken Seite wurde an die rechte Seite angehängt. Dies wird solange wiederholt, bis die linke Seite leer ist. Anschließend werden die Rauten im Zustand q_5 gelöscht. Danach steht der Kopf auf dem ersten Zeichen der rechten Seite und die Turingmaschine terminiert. Aus diesen Überlegungen folgt, dass M die Funktion $f(w) = w^R$ berechnet. Sie dreht also die Eingabe um.

Der Leser sollte als Übung Turingmaschinen für andere einfache Probleme entwerfen. Natürlich ist es nicht Sinn und Zweck dieser Vorlesung, zu lernen, wie man Turingmaschinen konstruiert. Es wird vermutlich nur sehr wenigen Spaß machen, eine Turingmaschine für das Zusammenhangsproblem oder andere nicht triviale Probleme zu konstruieren (auch wenn dies möglich wäre). Das Spielen mit dem Modell der Turingmaschine dient an dieser Stelle dazu, ein Gefühl dafür zu entwickeln, wie mächtig Turingmaschinen sind und wie man prinzipiell damit Probleme lösen und Funktionen berechnen kann.

Wir passen Definition 1.2 nun noch an Entscheidungsprobleme und Sprachen an. Bei einem solchen Problem besteht die Ausgabe immer aus genau einem Zeichen (0 oder 1), weshalb uns nur das Zeichen interessiert, das am Ende der Berechnung an der Kopfposition steht. Dies ist in folgender Definition formalisiert.

Definition 1.3. Eine Turingmaschine M akzeptiert (oder verwirft) eine Eingabe $w \in \Sigma^*$, wenn sie bei Eingabe w terminiert und ein Wort ausgibt, das mit 1 (bzw. 0) beginnt.

Eine Turingmaschine M entscheidet eine Sprache $L \subseteq \Sigma^*$, wenn sie jedes Wort $w \in L$ akzeptiert und jedes Wort $w \in \Sigma^* \setminus L$ verwirft.

Eine Sprache $L \subseteq \{0,1\}^*$ heißt entscheidbar oder rekursiv, wenn es eine Turingmaschine M gibt, die L entscheidet. Wir sagen dann, dass M eine Turingmaschine für die Sprache L ist. Eine solche Turingmaschine terminiert insbesondere auf jeder Eingabe.

Wir betrachten als Beispiel eine Turingmaschine $M = (Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$ mit $Q = \{q_0, q_1, q_2, \bar{q}\}$, $\Sigma = \{0, 1\}$ und $\Gamma = \{0, 1, \square\}$. Die Zustandsübergangsfunktion δ ist in der folgenden Tabelle dargestellt.

	q_0	q_1	q_2
0	$(q_1, 0, R)$	$(q_1, 0, R)$	$(q_1, 0, R)$
1	$(q_0, 1, R)$	$(q_2, 1, R)$	$(q_0, 1, R)$
\square	$(\bar{q}, 0, N)$	$(\bar{q}, 0, N)$	$(\bar{q}, 1, N)$

Man beobachtet zunächst leicht, dass die Turingmaschine in jedem Schritt, in dem sie nicht in den Endzustand wechselt, den Kopf nach rechts bewegt und den Bandinhalt nicht ändert. Die Turingmaschine terminiert, sobald sie das erste Leerzeichen (also das Ende der Eingabe) erreicht hat. Die Turingmaschine verhält sich also wie ein endlicher Automat, der die Eingabe Zeichen für Zeichen von links nach rechts liest und dabei Zustandsübergänge durchführt. Sie akzeptiert die Eingabe genau dann, wenn sie das erste Leerzeichen im Zustand q_2 erreicht. Ansonsten verwirft sie die Eingabe. Betrachtet man die Zustandsübergänge, so sieht man, dass Zustand q_2 genau dann erreicht wird, wenn der bisher gelesene Teil der Eingabe mit 01 endet. Daraus folgt insgesamt, dass die Turingmaschine M genau die Wörter akzeptiert, die mit 01 enden. Alle anderen Wörter verwirft sie.

Das Modell der Turingmaschine wurde bereits 1937 von dem britischen Mathematiker Alan Turing eingeführt [4]. Turing geht in dieser wegweisenden Arbeit der Frage nach, welche Funktionen $f: \mathbb{N} \rightarrow \{0, 1\}$ von Computern berechnet werden können. Allerdings hatte der Begriff „Computer“ damals eine andere Bedeutung als heute. Man verstand darunter einen Menschen, der mathematische Berechnungen gemäß fester Regeln durchführt, also gewissermaßen einen Menschen, der einen Algorithmus von Hand durchführt. Solche menschlichen Computer wurden einige Jahrhunderte lang für aufwendige Berechnungen in Wissenschaften wie beispielsweise der Astronomie eingesetzt. Letztlich spielt es bei der Frage, welche Funktionen durch Algorithmen berechnet werden können, aber keine Rolle, ob die Algorithmen von einem Menschen oder einem elektronischen Computer ausgeführt werden.

Techniken zum Entwurf von Turingmaschinen

Um ein besseres Gefühl dafür zu bekommen, wie man prinzipiell Turingmaschinen für nicht triviale Probleme entwerfen kann, ist es hilfreich, sich zu überlegen, wie man grundlegende Programmier Techniken auf Turingmaschinen anwenden kann.

1. Eine Variable, die Werte aus einer endlichen Menge annehmen kann, kann in der Zustandsmenge einer Turingmaschine gespeichert werden. Möchte man beispielsweise eine Variable realisieren, die für ein festes $k \in \mathbb{N}$ Werte aus der Menge $\{0, \dots, k\}$ annehmen kann, so kann man die Zustandsmenge Q zu der Menge $Q' = Q \times \{0, \dots, k\}$ erweitern. Ein Zustand aus Q' ist dann ein Paar (q, a) ,

wobei $q \in Q$ den eigentlichen Zustand der Turingmaschine beschreibt und $a \in \{0, \dots, k\}$ den Wert der Variablen. Die Zustandsüberföhrungsfunktion kann diesen Wert berücksichtigen und ihn gegebenenfalls ändern. Es ist allerdings wichtig, dass k konstant ist, da die erweiterte Zustandsmenge Q' endlich sein muss. Das bedeutet insbesondere, dass wir die Variable nicht dazu einsetzen können, um zum Beispiel die Länge der Eingabe zu speichern. Analog können auch endlich viele Variablen mit endlichen Wertebereichen realisiert werden.

2. Oft ist es hilfreich, wenn das Band der Turingmaschine aus verschiedenen Spuren besteht. Das bedeutet, in jeder Zelle stehen k Zeichen aus Γ , die alle gleichzeitig in einem Schritt gelesen und geschrieben werden. Ist $k \in \mathbb{N}$ eine Konstante, so kann dies dadurch realisiert werden, dass das Bandalphabet Γ zu $\Gamma' = \Sigma \cup \Gamma^k$ erweitert wird. Dies ist für endliches Γ und endliches k eine endliche Menge. Die Zustandsüberföhrungsfunktion kann dann entsprechend angepasst werden und in jedem Schritt die k Zeichen verarbeiten, die sich an der aktuellen Kopfposition befinden. Wir werden im Folgenden ein Zeichen $a \in \Sigma$ mit dem Element $(a, \square, \square, \dots, \square) \in \Gamma^k$ identifizieren.

Um den Sinn von mehreren Spuren und das Abstraktionsniveau, auf dem wir zukünftig Turingmaschinen beschreiben wollen, zu verdeutlichen, betrachten wir das Problem, zwei gegebene Zahlen in Binärdarstellung zu addieren. Sei $\Sigma = \{0, 1, \#\}$ das Eingabealphabet und sei $\text{bin}(x)\#\text{bin}(y)$ für $x \in \mathbb{N}$ und $y \in \mathbb{N}$ eine Eingabe. Die Aufgabe ist es, $\text{bin}(x+y)$ zu berechnen. Dazu konstruieren wir eine Turingmaschine mit drei Spuren und dem Bandalphabet

$$\Gamma' = \left\{ 0, 1, \#, \square, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}.$$

Die Turingmaschine arbeitet in mehreren Phasen. In der ersten Phase verschiebt sie die Binärdarstellungen $\text{bin}(x)$ und $\text{bin}(y)$ so, dass sie auf den ersten beiden Spuren rechtsbündig untereinander stehen (ggf. mit führenden Nullen, wenn die Darstellungen nicht dieselbe Länge haben). Die Eingabe $101\#1100$ wird in dieser Phase beispielsweise in den Bandinhalt

$$\dots \square \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \square \dots$$

überföhrt. In der zweiten Phase geht die Turingmaschine die Bits von rechts nach links durch und führt die Addition bitweise nach der Schulmethode durch. Das Ergebnis wird dabei auf die dritte Spur geschrieben. Tritt in einem Schritt ein Übertrag auf, so merkt die Turingmaschine sich dies im Zustand. In dem obigen Beispiel ergibt sich nach dieser Phase der Bandinhalt

$$\dots \square \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \square \dots$$

In der dritten Phase wird das Ergebnis zurück in das (einspurige) Eingabealphabet Σ übersetzt. Dabei werden die Inhalte der ersten beiden Spuren gelöscht und nur der Inhalt der dritten Spur bleibt erhalten.

3. Mithilfe mehrerer Spuren können auch Variablen realisiert werden, die beliebig viele Zustände annehmen können. Diese können nicht mehr in den Zustand codiert werden, sondern sie müssen auf dem Band gespeichert werden. Man könnte zum Beispiel für jede Variable eine Spur benutzen oder mehrere durch Trennzeichen getrennte Variablen auf derselben Spur abspeichern.
4. Mit etwas Aufwand kann man beim Entwurf von Turingmaschinen auch Unterprogramme einsetzen. Dazu kann man beispielsweise für jedes Unterprogramm eine Teilmenge von Zuständen auszeichnen, die ausschließlich in diesem Unterprogramm angenommen werden. Ebenso kann man beim Aufruf eines Unterprogramms einen separaten (beispielsweise weit rechts liegenden) Speicherbereich auf dem Band reservieren, in dem die Berechnungen des Unterprogramms erfolgen. Es können dabei einige technische Probleme auftreten. Genügt der reservierte Speicherbereich beispielsweise nicht, so muss er gegebenenfalls verschoben werden. Ebenso muss ein Aufrufstack verwaltet werden. All dies ist möglich, aber relativ komplex und wenig elegant. Wir wollen die Diskussion hier nicht weiter vertiefen. Für die weiteren Betrachtungen ist lediglich wichtig zu wissen, dass Unterprogramme prinzipiell realisiert werden können.
5. Auch können for- und while-Schleifen in Turingmaschinen realisiert werden. Eine solche Schleife haben wir bereits implizit in der obigen Turingmaschine gesehen, die bei Eingabe w das gespiegelte Wort w^R berechnet. Letztendlich kann man Schleifen aber auch als eine spezielle Art von Unterprogramm auffassen, sodass sie genauso wie andere Unterprogramme realisiert werden können.

Turingmaschinen mit mehreren Bändern

Wir haben oben bereits diskutiert, dass Turingmaschinen mit mehreren Spuren durch eine einfache Anpassung des Bandalphabets simuliert werden können. Diese Maschinen besitzen aber weiterhin nur einen Lese-/Schreibkopf, der die k Zeichen unter der aktuellen Kopfposition gleichzeitig verarbeiten kann. Nun gehen wir einen Schritt weiter und betrachten Turingmaschinen mit einer konstanten Anzahl an Bändern. Bei diesen Maschinen besitzt jedes Band seinen eigenen Lese-/Schreibkopf, der unabhängig von den anderen Köpfen bewegt werden kann.

Eine k -Band-Turingmaschine M ist ein 7-Tupel $(Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$, bei dem die ersten sechs Komponenten die gleiche Bedeutung haben wie in Definition 1.1. Die Zustandsüberföhrungsfunktion δ ist von der Form

$$\delta: (Q \setminus \{\bar{q}\}) \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, N, R\}^k.$$

Sie erhält als Eingabe den aktuellen Zustand und die k Zeichen, die sich an den aktuellen Kopfpositionen befinden. Als Ausgabe liefert sie den Nachfolgezustand, die k

Zeichen, durch die die alten ersetzt werden sollen, und die Bewegungen der k Köpfe. Das erste Band fungiert dabei wie bei einer normalen Turingmaschine als Ein-/Ausgabeband. Die anderen Bändern sind initial leer. Eine 1-Band-Turingmaschine ist somit identisch zu einer normalen Turingmaschine gemäß Definition 1.1.

Da sich die Köpfe unabhängig bewegen können, erscheint eine einfache Simulation durch eine 1-Band-Turingmaschine nicht ohne Weiteres möglich zu sein. Wir werden nun aber beweisen, dass k -Band-Turingmaschinen stets durch normale Turingmaschinen simuliert werden können, wobei allerdings ein gewisser Zeitverlust auftritt. Um dies quantifizieren zu können, definieren wir die Begriffe Rechenzeit und Platzbedarf zunächst formal.

Definition 1.4. *Es sei M eine k -Band-Turingmaschine. Die Rechenzeit $t_M(w)$ von M auf Eingabe w ist die Anzahl an Zustandsübergängen, die M bei Eingabe w bis zur Terminierung durchführt. Terminiert M nicht auf w , so ist die Rechenzeit unendlich. Der Platzbedarf $s_M(w)$ von M auf Eingabe w ist die Anzahl (summiert über alle Bänder) an verschiedenen Zellen, auf denen sich im Laufe der Rechnung mindestens einmal ein Lese-/Schreibkopf befunden hat. Terminiert M nicht, so kann der Platzbedarf unendlich sein.*

Die Rechenzeit $t_M(n)$ von M auf Eingaben der Länge $n \in \mathbb{N}$ ist die maximale Rechenzeit, die bei Eingaben der Länge n auftritt, also $t_M(n) = \max_{w \in \Sigma^n} t_M(w)$. Analog ist der Platzbedarf $s_M(n)$ von M auf Eingaben der Länge n als $s_M(n) = \max_{w \in \Sigma^n} s_M(w)$ definiert.

Nun werden wir sehen, wie man k -Band-Turingmaschinen durch 1-Band-Turingmaschinen simulieren kann.

Theorem 1.5. *Eine k -Band Turingmaschine M mit Rechenzeit $t(n)$ und Platzbedarf $s(n)$ kann durch eine 1-Band-Turingmaschine M' mit Rechenzeit $O(t(n)^2)$ und Platzbedarf $O(s(n))$ simuliert werden.*

Beweis. Die Turingmaschine M' simuliert die Turingmaschine M Schritt für Schritt und verwendet dafür $2k$ Spuren. Nach der Simulation des t -ten Rechenschrittes von M durch M' mit $t \in \mathbb{N}_0$ sind die folgenden Invarianten erfüllt.

1. Die ungeraden Spuren $1, 3, \dots, 2k - 1$ enthalten den Inhalt der k Bänder von M .
2. Auf den geraden Spuren $2, 4, \dots, 2k$ sind die Kopfpositionen von M mit dem Zeichen $\#$ markiert (Spur $2i$ enthält die Markierung für die Kopfposition auf Band i von M). Alle anderen Zellen auf diesen Bändern enthalten das Leerzeichen.
3. Der Kopf von M' steht an der linkensten Position, die auf einem der geraden Bänder mit $\#$ markiert ist.

Die Spuren können in konstanter Zeit initialisiert werden. Dazu muss lediglich das Zeichen $\#$ an der aktuellen Position (die zu Beginn dem ersten Zeichen der Eingabe entspricht) auf alle geraden Spuren geschrieben werden. Um nun einen Rechenschritt

von M zu simulieren, geht M' wie folgt vor. Sie schiebt den Kopf solange nach rechts, bis sie alle k Markierungen $\#$ gesehen hat. Dabei merkt sie sich im Zustand, welche k Zeichen sich an den aktuellen Kopfpositionen befinden. Nachdem sie die letzte Markierung erreicht und alle k Zeichen gelesen hat, wertet sie die Zustandsüberföhrungsfunktion von M aus und merkt sich im Zustand den neuen Zustand von M , durch welche Zeichen die k Zeichen an den Kopfpositionen ersetzt werden sollen und wie die Köpfe sich bewegen sollen. Anschließend schiebt sie den Kopf wieder nach links zurück und ändert dabei den Bandinhalt an den markierten Positionen und verschiebt die Markierungen entsprechend den Bewegungen von M . Sie stoppt, sobald sie alle k Markierungen gesehen und den Rechenschritt von M komplett simuliert hat. Danach ist die Invariante wieder hergestellt. Der Leser mache sich noch einmal klar, dass M' sich bei dieser Konstruktion nur konstante viele Informationen im Zustand merken muss.

Die Anzahl Schritte, die M' benötigt, um einen Schritt von M zu simulieren, ist proportional zu dem Abstand, den die beiden Markierungen am weitesten links und am weitesten rechts voneinander haben, da M' diese Entfernung zweimal zurücklegen muss. Da die Laufzeit von M durch $t(n)$ beschränkt ist, können diese beiden Markierungen zu jedem Zeitpunkt um maximal $2t(n)$ viele Positionen auseinander liegen (schlimmstenfalls geht ein Kopf von M in jedem Schritt nach links und ein anderer geht in jedem Schritt nach rechts). Jeder einzelne der $t(n)$ vielen Schritte kann somit in Zeit $O(t(n))$ simuliert werden, woraus direkt die behauptete Rechenzeit von $O(t(n)^2)$ folgt. Dass der Platzbedarf von M' in derselben Größenordnung wie der von M liegt, folgt direkt daraus, dass M' nur dann eine Zelle besucht, wenn M auf einem seiner Bänder ebenfalls diese Zelle besucht. \square

1.2.2 Registermaschinen

Wir haben uns bereits im letzten Semester mit dem Modell der *Registermaschine* beschäftigt, das an eine rudimentäre Assemblersprache erinnert, die auf die wesentlichen Befehle reduziert wurde. In diesem Modell steht als Speicher eine unbegrenzte Anzahl an Registern zur Verfügung, die jeweils eine natürliche Zahl enthalten und auf denen grundlegende arithmetische Operationen durchgeführt werden können. Die Inhalte zweier Register können addiert, subtrahiert, multipliziert und dividiert werden. Ebenso können Registerinhalte kopiert werden und Register können mit Konstanten belegt werden. Darüber hinaus unterstützen Registermaschinen unbedingte Sprungoperationen (GOTO) und bedingte Sprungoperationen (IF), wobei als Bedingung nur getestet werden darf, ob ein Register kleiner, gleich oder größer als ein anderes Register ist.

Formal besteht ein Registermaschinenprogramm aus einer endlichen durchnummerierten Folge von Befehlen, deren Syntax in Tabelle 1.1 zusammengefasst ist. Wird ein solches Programm ausgeführt, so wird ein Befehlszähler b verwaltet, der angibt, welcher Befehl als nächstes ausgeführt werden soll. Zu Beginn wird $b = 1$ gesetzt. Jeder Befehl ändert den Befehlszähler (ist es kein Sprungbefehl, so wird b lediglich um eins erhöht) und gegebenenfalls den Inhalt der Register. Wir bezeichnen mit $c(0), c(1), c(2), \dots$ die Inhalte der Register. Dabei gilt stets $c(i) \in \mathbb{N}_0$. Zu Beginn steht in dem Register $c(0)$

Syntax	Zustandsänderung	Änderung von b
LOAD i	$c(0) := c(i)$	$b := b + 1$
CLOAD i	$c(0) := i$	$b := b + 1$
INDLOAD i	$c(0) := c(c(i))$	$b := b + 1$
STORE i	$c(i) := c(0)$	$b := b + 1$
INDSTORE i	$c(c(i)) := c(0)$	$b := b + 1$
ADD i	$c(0) := c(0) + c(i)$	$b := b + 1$
CADD i	$c(0) := c(0) + i$	$b := b + 1$
INDADD i	$c(0) := c(0) + c(c(i))$	$b := b + 1$
SUB i	$c(0) := c(0) - c(i)$	$b := b + 1$
CSUB i	$c(0) := c(0) - i$	$b := b + 1$
INDSUB i	$c(0) := c(0) - c(c(i))$	$b := b + 1$
MULT i	$c(0) := c(0) \cdot c(i)$	$b := b + 1$
CMULT i	$c(0) := c(0) \cdot i$	$b := b + 1$
INDMULT i	$c(0) := c(0) \cdot c(c(i))$	$b := b + 1$
DIV i	$c(0) := \lfloor c(0)/c(i) \rfloor$	$b := b + 1$
CDIV i	$c(0) := \lfloor c(0)/i \rfloor$	$b := b + 1$
INDDIV i	$c(0) := \lfloor c(0)/c(c(i)) \rfloor$	$b := b + 1$
GOTO j	-	$b := j$
IF $c(0) = x$ GOTO j	-	$b := \begin{cases} j & \text{falls } c(0) = x \\ b + 1 & \text{sonst} \end{cases}$
IF $c(0) < x$ GOTO j	-	$b := \begin{cases} j & \text{falls } c(0) < x \\ b + 1 & \text{sonst} \end{cases}$
IF $c(0) \leq x$ GOTO j	-	$b := \begin{cases} j & \text{falls } c(0) \leq x \\ b + 1 & \text{sonst} \end{cases}$
END	Ende der Rechnung	-

Tabelle 1.1: Syntax und Semantik der Befehle einer Registermaschine

die Eingabe und für alle anderen Register gilt $c(i) = 0$. Die Ausgabe findet sich am Ende der Rechnung ebenfalls in Register $c(0)$. In Tabelle 1.1 ist auch die Semantik der einzelnen Befehle aufgeführt.

In einer Registermaschine kann jedes Register eine beliebig große natürliche Zahl enthalten. Im letzten Semester haben wir das *uniforme Kostenmaß* zugrunde gelegt, bei dem die Ausführung jedes Befehls unabhängig von der Größe der Zahlen eine Zeiteinheit benötigt. Werden in den Registern große Zahlen gespeichert, so ist es realistischer das *logarithmische Kostenmaß* einzusetzen. Bei diesem ist die Laufzeit eines Befehls proportional zu der Länge der Zahlen in den angesprochenen Registern in Binärdarstellung. Die Laufzeit eines Befehl ist also proportional zum Logarithmus der beteiligten Zahlen.

Analog zu Definition 1.4 interessiert uns auch bei Registermaschinen die Laufzeit in Abhängigkeit von der Eingabegröße. Diese messen wir im logarithmischen Kostenmaß durch die Länge der Binärdarstellung der Eingabe in Register $c(0)$. Wir nennen eine Registermaschine im logarithmischen Kostenmaß *t(n)-zeitbeschränkt*, wenn die Lauf-

zeit im logarithmischen Kostenmaß für jedes $n \in \mathbb{N}$ und jede Eingabe mit n Bits durch $t(n)$ beschränkt ist.

Um die Mächtigkeit des Modells der Turingmaschine zu verdeutlichen, zeigen wir nun, dass Registermaschinen durch Turingmaschinen simuliert werden können und andersherum. Da wir Registermaschinen bereits im letzten Semester als realistisches Modell realer Rechner akzeptiert haben, bedeutet dies, dass auch Turingmaschinen ein realistisches Modell darstellen.

Theorem 1.6. *Jede im logarithmischen Kostenmaß $t(n)$ -zeitbeschränkte Registermaschine kann durch eine Turingmaschine simuliert werden, deren Rechenzeit $O(q(n + t(n)))$ für ein Polynom q beträgt.*

Wir werden das Theorem nicht beweisen. Der Beweis ist zwar nicht schwer, aber wenig erhellend. Man kann dazu eine Turingmaschine mit 2-Bändern konstruieren, die für jede Zeile des Registermaschinenprogramms ein Unterprogramm enthält. Die Unterprogramme werden dabei auf dem ersten Band ausgeführt, während das zweite Band die Inhalte der Register in Binärdarstellung enthält. Die Turingmaschine simuliert dann Schritt für Schritt das Verhalten der Registermaschine. Die genaue Konstruktion dieser Turingmaschine ist allerdings sehr technisch.

Theorem 1.6 sagt nicht nur, dass jede Registermaschine durch eine Turingmaschine simuliert werden kann, sondern auch, dass die Laufzeit der entsprechenden Turingmaschine nur polynomiell größer ist als die der Registermaschine. Insbesondere ist die Laufzeit der Turingmaschine polynomiell, wenn die Laufzeit der Registermaschine polynomiell ist. Um dies einzusehen, nehmen wir an, dass die Laufzeit $t(n)$ der Registermaschine ein Polynom vom Grad $d \geq 1$ ist. Laut dem Theorem existiert ein Polynom q , dessen Grad wir mit d^* bezeichnen, für das die Rechenzeit der Turingmaschine durch $O(q(n + t(n))) = O(q(t(n))) = O(q(n^d)) = O(n^{dd^*})$ beschränkt ist. Damit ist auch die Laufzeit der Turingmaschine durch ein Polynom beschränkt.

Wir werden später in dieser Vorlesung noch ausführlich über die Bedeutung polynomieller Laufzeit sprechen. An dieser Stelle sollte der Leser die Erkenntnis mitnehmen, dass jedes Problem, das von einer Registermaschine im logarithmischen Kostenmaß in polynomieller Zeit gelöst werden kann, auch von einer Turingmaschine in polynomieller Zeit gelöst werden.

Auch umgekehrt kann jede Turingmaschine mit polynomiell Zeitverlust durch eine Registermaschine im logarithmischen Kostenmaß simuliert werden kann.

Theorem 1.7. *Jede Turingmaschine, deren Rechenzeit durch $t(n)$ beschränkt ist, kann durch eine im logarithmischen Kostenmaß $O((t(n) + n) \log(t(n) + n))$ -zeitbeschränkte Registermaschine simuliert werden.*

Zusammen implizieren die Theoreme 1.6 und 1.7, dass die Klasse der von Turingmaschinen berechenbaren Funktionen und die Klasse der von Registermaschinen berechenbaren Funktionen übereinstimmen. Darüber hinaus sind sogar die Rechenzeiten bis auf polynomielle Faktoren vergleichbar. Etwas präziser formuliert besagen die Theoreme, dass die Klasse der von Turingmaschinen in polynomieller Zeit berechenbaren Funktionen und die Klasse der von Registermaschinen in polynomieller Zeit berechenbaren Funktionen übereinstimmen.

1.2.3 Die Church-Turing-These

In Definition 1.2 haben wir festgelegt, dass eine Funktion berechenbar ist, wenn es eine Turingmaschine gibt, die zu jeder Eingabe in endlich vielen Schritten die durch die Funktion beschriebene Ausgabe liefert. Der Begriff der Berechenbarkeit ist demnach zunächst an das Modell der Turingmaschine gekoppelt. Dies ist uns aber nicht allgemein genug, denn haben wir für eine Funktion nachgewiesen, dass sie nicht berechenbar ist, so wäre es zunächst ja durchaus denkbar, dass sie zwar nicht von einer Turingmaschine, aber von einem Java- oder C++-Programm berechnet werden kann. Geht auch dies nicht, so kann man die Funktion vielleicht mithilfe anderer Hardware (Quantencomputer, Analogrechner, etc.) berechnen. Falls dies wirklich der Fall wäre, so wäre ein Begriff der Berechenbarkeit, der sich wie Definition 1.2 nur auf Turingmaschinen stützt, nicht besonders interessant.

Tatsächlich haben wir aber bereits in Theorem 1.6 gesehen, dass Registermaschinen nicht mächtiger sind als Turingmaschinen. Registermaschinen wiederum sind ein realistisches Modell für heutige reale Rechner (unabhängig von der benutzten Programmiersprache). Ist eine Funktion also auf einem realen Rechner berechenbar, so ist sie auch auf einer Registermaschine und damit auch auf einer Turingmaschine berechenbar. Andersherum formuliert, kann eine Funktion, die nicht von einer Turingmaschine berechnet werden kann, auch von keinem heutigen realen Rechner berechnet werden.

Darüber hinaus gibt es neben Turingmaschinen und Registermaschinen eine ganze Reihe von weiteren theoretischen Modellen, mit denen man versucht hat, den Begriff der Berechenbarkeit zu formalisieren (WHILE-Programme, μ -rekursive Funktionen, etc.). Diese Modelle wurden unabhängig voneinander entworfen, es hat sich aber im Nachhinein herausgestellt, dass sie alle zur selben Klasse von berechenbaren Funktionen führen. Dies sind starke Indizien für die Vermutung, dass alle Funktionen, die man auf irgendeine algorithmische Art berechnen kann, auch von Turingmaschinen berechnet werden können. Dies ist die sogenannte *Church-Turing-These*.

These 1.8 (Church-Turing-These). *Alle „intuitiv berechenbaren“ Funktionen können von Turingmaschinen berechnet werden.*

Diese These ist prinzipiell nicht beweisbar, da der Begriff „intuitiv berechenbar“ nicht formal definiert ist. Eine formalere Variante dieser These, die zwar prinzipiell beweisbar, aber noch unbewiesen ist, lautet wie folgt.

These 1.9 (Physikalische Church-Turing-These). *Die Gesetze der Physik erlauben es nicht, eine Maschine zu konstruieren, die eine Funktion berechnet, die nicht auch von einer Turingmaschine berechnet werden kann.*

Auch für diese These gibt es eine ganze Reihe von Indizien. Beispielsweise weiß man, dass weder mit Quantencomputern noch mit Analogrechnern Funktionen berechnet werden können, die man nicht auch mit einer Turingmaschine berechnen kann. Tatsächlich gibt es mittlerweile unter dem Stichwort „unconventional computing“ ein ganzes Kuriositätenkabinett an physikalischen, biologischen und chemischen Modellen, mit denen Berechnungen durchgeführt werden können. Keines der bekannten Modelle widerspricht jedoch der oben formulierten physikalischen Church-Turing-These.

Berechenbarkeitstheorie

In diesem Kapitel weisen wir für das Halteproblem nach, dass es nicht entscheidbar ist. Der Beweis beruht auf der Existenz einer sogenannten *universellen Turingmaschine*. Dabei handelt es sich um eine Turingmaschine, die beliebige andere Turingmaschinen simulieren kann. Sie erhält als Eingabe die Codierung einer Turingmaschine M und ein Wort w und simuliert das Verhalten von M auf w .

Die Existenz einer solchen universellen Turingmaschine ist bei genauer Betrachtung nicht besonders schwierig nachzuweisen. Sie ist aber von zentraler Bedeutung, denn sie besagt, dass man bei Turingmaschinen genauso wie bei realen Rechnern die Hardware vom auszuführenden Programmcode trennen kann. Bei der universellen Turingmaschine handelt es sich um einen programmierbaren Rechner, der mit derselben Hardware beliebige Programme ausführen kann. Denkt man an heutige Rechner, so ist diese Eigenschaft natürlich eine Selbstverständlichkeit. Im Jahre 1936 als Alan Turing seine revolutionäre Arbeit schrieb und das Modell der Turingmaschine eingeführt hat, gab es allerdings nur festverdrahtete Rechner für bestimmte Aufgaben und die Von-Neumann-Architektur war noch unbekannt.

Ist erstmal für eine Sprache $A \subseteq \Sigma^*$ nachgewiesen, dass sie nicht entscheidbar ist, so kann die Unentscheidbarkeit weiterer Sprachen durch *Reduktionen* gezeigt werden. Sei beispielsweise $B \subseteq \Sigma^*$ eine Sprache, deren Unentscheidbarkeit wir nachweisen wollen. Unter einer Reduktion von A auf B verstehen wir eine Turingmaschine zur Lösung von A , die eine (hypothetische) Turingmaschine zur Lösung von B als Unterprogramm einsetzt. Existiert eine solche Reduktion und eine Turingmaschine, die B entscheidet, so kann folglich auch A entschieden werden. Da A aber laut Voraussetzung nicht entscheidbar ist, folgt aus der Reduktion mit einem Widerspruchsbeweis, dass auch B nicht entscheidbar sein kann. Wir nutzen dies aus, indem wir zunächst die Unentscheidbarkeit einer speziell für diesen Zweck konstruierten künstlichen Sprache nachweisen und anschließend mithilfe von Reduktionen nachweisen, dass das Halteproblem und andere interessante Probleme nicht entscheidbar sind.

Zum Schluss dieses Kapitels lernen wir noch eine Abstufung innerhalb der Klasse der nicht entscheidbaren Sprachen kennen. Wir nennen eine Sprache L *rekursiv aufzählbar* oder *semi-entscheidbar*, wenn es eine Turingmaschine gibt, die alle Eingaben $x \in L$

akzeptiert und Eingaben $x \notin L$ entweder verwirft oder nicht auf ihnen terminiert. Wir werden kurz diskutieren, warum diese Klasse interessant ist und welcher Zusammenhang zu den entscheidbaren Sprachen besteht.

Bevor wir uns formal mit der Berechenbarkeitstheorie beschäftigen, zeigen wir, dass es nicht nur für die Informatik sondern auch für die Mathematik weitreichende und unglaubliche Konsequenzen hätte, wenn das Halteproblem entscheidbar wäre. Dazu betrachten wir den folgenden an Java angelehnten Pseudocode.

```
void main() {
    int n = 4;
    while (true) {
        boolean foundPrimes = false;
        for (int p = 2; p < n; p++) {
            if (prime(p) && prime(n-p)) foundPrimes = true;
        }
        if (!foundPrimes) return;
        n = n + 2;
    }
}
```

Wir gehen davon aus, dass die Methode `prime` für eine gegebene Zahl entscheidet, ob sie eine Primzahl ist oder nicht. Weiterhin gehen wir davon aus, dass n und p beliebig große Werte annehmen können, ohne dass Überläufe auftreten. Dies kann in Java beispielsweise durch die Verwendung der Klasse `java.math.BigInteger` erreicht werden. Aus Gründen der Übersichtlichkeit haben wir aber auf die Verwendung dieser Klasse verzichtet. In der `while`-Schleife wird über alle geraden Zahlen $n = 4, 6, 8, \dots$ größer als zwei iteriert, solange bis in einer Iteration die Abbruchbedingung greift. Man sieht leicht, dass das Programm genau dann terminiert, wenn eine Zahl n erreicht wird, die sich nicht als Summe zweier Primzahlen schreiben lässt. Zusammengefasst lässt sich also Folgendes sagen.

Beobachtung 2.1. *Das obige Programm terminiert genau dann, wenn es eine gerade Zahl größer als zwei gibt, die sich nicht als Summe zweier Primzahlen schreiben lässt.*

In der Vorlesung „Logik und diskrete Strukturen“ haben wir bereits die *Goldbachsche Vermutung* kennengelernt, die besagt, dass sich jede gerade Zahl größer als zwei als Summe zweier Primzahlen schreiben lässt. Diese Vermutung ist trotz intensiver Bemühungen zahlreicher Mathematiker bis heute unbewiesen. Hätten wir einen Compiler zur Hand, der uns sagen könnte, ob das obige Programm terminiert, so könnten wir damit einfach die Goldbachsche Vermutung entscheiden: Terminiert das Programm, so ist die Goldbachsche Vermutung falsch, ansonsten ist sie korrekt.

2.1 Entwurf einer universellen Turingmaschine

In diesem Abschnitt entwerfen wir eine universelle Turingmaschine. Wir betrachten der Einfachheit halber nur Turingmaschinen mit dem Eingabealphabet $\Sigma = \{0, 1\}$ und dem Bandalphabet $\Gamma = \{0, 1, \square\}$, was (wie oben bereits erwähnt) keine echte Einschränkung ist. Eine universelle Turingmaschine erhält als Eingabe eine Zeichenkette der Form $\langle M \rangle w$, wobei $\langle M \rangle \in \{0, 1\}^*$ die Codierung einer Turingmaschine M

und $w \in \{0, 1\}^*$ eine beliebige Zeichenkette ist. Die universelle Turingmaschine simuliert bei dieser Eingabe das Verhalten der Turingmaschine M auf der Eingabe w . Das heißt, sie terminiert auf der Eingabe $\langle M \rangle w$ genau dann, wenn die Turingmaschine M auf der Eingabe w terminiert, und sie akzeptiert (verwirft) die Eingabe $\langle M \rangle w$ genau dann, wenn M die Eingabe w akzeptiert (verwirft).

Wir müssen zunächst festlegen, wie die Codierung $\langle M \rangle$ einer Turingmaschine M aussehen soll. Eine solche Codierung nennen wir auch Gödelnummerierung (nach dem Mathematiker Kurt Gödel) und es gibt eine Vielzahl an Möglichkeiten, wie sie realisiert werden kann.

Definition 2.2. *Eine injektive Abbildung der Menge aller Turingmaschinen in die Menge $\{0, 1\}^*$ heißt Gödelnummerierung. Für eine feste Gödelnummerierung bezeichnen wir mit $\langle M \rangle \in \{0, 1\}^*$ die Gödelnummer der Turingmaschine M , also die Zeichenkette, auf die M gemäß der Gödelnummerierung abgebildet wird.*

Eine Gödelnummerierung heißt präfixfrei, wenn kein echtes Präfix (Anfangsstück) einer Gödelnummer $\langle M \rangle$ selbst eine gültige Gödelnummer ist.

Die Präfixfreiheit garantiert, dass wir bei einer Zeichenkette der Form $\langle M \rangle w$ stets eindeutig entscheiden können, an welcher Stelle die Gödelnummer aufhört und das Wort w beginnt. Wir geben nun noch eine konkrete präfixfreie Gödelnummerierung an und bezeichnen mit \mathcal{G} die Menge aller gültigen Gödelnummern in dieser Nummerierung. Sprechen wir im Folgenden von *der* Gödelnummer einer Turingmaschine, so bezieht sich das immer auf diese konkrete Gödelnummerierung. Die Präfixfreiheit folgt direkt aus der Tatsache, dass jede gültige Gödelnummer in unserer Nummerierung mit der Zeichenkette 111 endet und die Zeichenkette 111 an keiner anderen Stelle in einer Gödelnummer vorkommt.

Es sei eine Turingmaschine $M = (Q, \Sigma, \Gamma, \square, q_1, q_2, \delta)$ gegeben, deren Komponenten die folgende Form haben.

- Es sei $Q = \{q_1, q_2, \dots, q_t\}$ für ein $t \geq 2$.
- Es sei $\Sigma = \{X_1, X_2\}$ und $\Gamma = \Sigma \cup \{X_3\}$ für $X_1 = 0$, $X_2 = 1$ und $X_3 = \square$.
- Es sei q_1 der Startzustand und q_2 der Endzustand.

Wir nummerieren die drei möglichen Kopfbewegungen und setzen $D_1 = L$, $D_2 = N$ und $D_3 = R$. Einen Übergang $\delta(q_i, X_j) = (q_k, X_\ell, D_m)$ codieren wir mit der Zeichenkette $0^i 10^j 10^k 10^\ell 10^m$. Die Zustandsüberföhrungsfunktion besteht aus $3(t - 1)$ vielen solchen Übergängen (jeweils drei für jeden Zustand ungleich q_2), deren Codierungen wir mit $\text{code}(1), \dots, \text{code}(3(t - 1))$ bezeichnen. Die Gödelnummer von M ist dann

$$\langle M \rangle = 11 \text{code}(1) 11 \text{code}(2) 11 \dots 11 \text{code}(3(t - 1)) 111.$$

Theorem 2.3. *Es existiert eine universelle Turingmaschine U , die auf jeder Eingabe der Form $\langle M \rangle w \in \{0, 1\}^*$ das Verhalten der Turingmaschine M auf der Eingabe $w \in \{0, 1\}^*$ simuliert. Die Rechenzeit von U auf der Eingabe $\langle M \rangle w$ ist nur um einen konstanten Faktor (das heißt in diesem Kontext, dass der Faktor nur von M , nicht aber von w abhängt) größer als die Rechenzeit von M auf der Eingabe w .*

Beweis. Wir konstruieren die universelle Turingmaschine U als 3-Band-Turingmaschine. Dies genügt zum Beweis des Theorems, da wir gemäß Theorem 1.5 jede 3-Band-Turingmaschine durch eine normale 1-Band-Turingmaschine simulieren können. Zu Beginn steht die Eingabe $\langle M \rangle w$ auf dem ersten Band. Zunächst schreibt U die Gödelnummer $\langle M \rangle$ auf das zweite Band und löscht sie vom ersten. Auf dem ersten Band steht dann nur noch das Wort w und der Kopf befindet sich auf dem ersten Zeichen von w . Auf das dritte Band schreibt U eine Codierung des Startzustandes. Wir codieren dabei den Zustand q_i als 0^i . Das bedeutet, zu Beginn befindet sich auf Band 3 die Zeichenkette 0 , da q_1 der Startzustand ist. Für jede gegebene Turingmaschine M kann diese Initialisierung in konstanter Zeit (d. h. unabhängig von w) durchgeführt werden.

Die universelle Turingmaschine U simuliert nun Schritt für Schritt die Berechnung von M auf w . Dabei werden die drei Bänder stets die folgenden Inhalte enthalten.

- Band 1 enthält den Bandinhalt von M nach den bereits simulierten Schritten. Die Kopfposition auf Band 1 stimmt ebenfalls mit der von M überein.
- Band 2 enthält die Gödelnummer $\langle M \rangle$.
- Band 3 codiert den Zustand von M nach den bereits simulierten Schritten. Ist dies q_i , so enthält Band 3 die Zeichenkette 0^i , die links und rechts von Leerzeichen eingeschlossen ist.

Zur Simulation eines Schrittes von M sucht U auf Band 2 nach einem passenden Übergang. Das bedeutet, U sucht nach der Zeichenkette 110^i10^j , wobei q_i der aktuell auf Band 3 codierte Zustand sei und X_j das Zeichen, das sich auf Band 1 an der Kopfposition befindet. Findet die universelle Turingmaschine eine entsprechende Zeichenfolge auf Band 2, so kann sie entsprechend der oben beschriebenen Codierung den Übergang $\delta(q_i, X_j) = (q_k, X_\ell, D_m)$ rekonstruieren. Sie kann dann dementsprechend das Zeichen an der Kopfposition auf Band 1 durch X_ℓ ersetzen, den Kopf von Band 1 gemäß D_m bewegen und den Inhalt von Band 3 durch 0^k ersetzen.

Die universelle Turingmaschine simuliert auf die oben beschriebene Art und Weise Schritt für Schritt das Verhalten der Turingmaschine M , solange bis der Endzustand q_2 erreicht wird. Da die Ausgabe bei einer Mehrbandmaschine auf dem ersten Band zu finden ist, stimmen die Ausgaben von U auf $\langle M \rangle w$ und von M auf w überein.

Die beschriebene universelle Turingmaschine benötigt für die Simulation eines Schrittes von M nur eine konstante Anzahl an Schritten (also eine Anzahl, die zwar abhängig von M nicht jedoch von w ist). Bei der Simulation der beschriebenen 3-Band-Turingmaschine durch eine normale 1-Band-Turingmaschine gemäß Theorem 1.5 handeln wir uns einen quadratischen Zeitverlust ein. Dieser kann vermieden werden, indem die universelle Turingmaschine von vornherein als 3-Spur-Turingmaschine konstruiert wird, bei der die Spuren dieselben Aufgaben erfüllen wie die Bänder in der oben beschriebenen Konstruktion. Bei dieser Konstruktion muss darauf geachtet werden, dass die Inhalte der Spuren 2 und 3, die zu jedem Zeitpunkt nur eine konstante Länge haben, mit dem Kopf der Turingmaschine mitverschoben werden. Auf die Details dieser Konstruktion werden wir hier allerdings nicht eingehen. \square

2.2 Die Unentscheidbarkeit des Halteproblems

Wir werden in diesem Abschnitt das *Halteproblem* formal definieren und nachweisen, dass es nicht entscheidbar ist. Dazu werden wir die Technik der *Diagonalisierung* einsetzen, mit der wir bereits in der Vorlesung „Logik und diskrete Strukturen“ gezeigt haben, dass die Menge der reellen Zahlen überabzählbar ist. Anstatt diese Technik direkt auf das Halteproblem anzuwenden, werden wir zunächst eine Hilfssprache (die *Diagonalsprache*) definieren, für die mithilfe von Diagonalisierung leicht nachgewiesen werden kann, dass sie nicht entscheidbar ist. Dann werden wir durch eine *Reduktion* zeigen, dass aus der Unentscheidbarkeit der Diagonalsprache auch die des Halteproblems folgt.

Für die folgenden Betrachtungen ist es nützlich, eine Ordnung auf den Wörtern aus der Menge $\{0, 1\}^*$ zu definieren. Für zwei Wörter $x = x_1 \dots x_\ell \in \{0, 1\}^\ell$ und $y = y_1 \dots y_\ell \in \{0, 1\}^\ell$ derselben Länge ℓ heißt x *lexikographisch kleiner* als y , wenn für das erste Zeichen x_i bzw. y_i , in dem sich die beiden Wörter unterscheiden, $x_i = 0$ und $y_i = 1$ gilt. Etwas formaler ausgedrückt, ist x lexikographisch kleiner als y , wenn ein Index i existiert, für den $x_1 \dots x_{i-1} = y_1 \dots y_{i-1}$ sowie $x_i = 0$ und $y_i = 1$ gilt. Nun können wir die *kanonische Ordnung* auf der Menge $\{0, 1\}^*$ definieren. In dieser Ordnung kommt ein Wort $x \in \{0, 1\}^*$ vor einem Wort $y \in \{0, 1\}^*$, wenn $|x| < |y|$ gilt oder wenn $|x| = |y|$ gilt und x lexikographisch kleiner als y ist. Die ersten Wörter in der kanonischen Ordnung von $\{0, 1\}^*$ sehen demnach wie folgt aus:

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, \dots$$

Wir bezeichnen im Rest dieses Abschnittes für $i \in \mathbb{N}$ mit w_i das Wort aus $\{0, 1\}^*$, das in der kanonischen Ordnung an der i -ten Stelle steht. Es gilt also beispielsweise $w_1 = \varepsilon$ und $w_5 = 01$.

Die kanonische Ordnung überträgt sich auf natürliche Art und Weise auf Teilmengen von $\{0, 1\}^*$. Insbesondere können die Gödelnummern aus \mathcal{G} gemäß der kanonischen Ordnung sortiert werden. Im Rest dieses Abschnittes bezeichne M_i für $i \in \mathbb{N}$ die Turingmaschine, deren Gödelnummer $\langle M \rangle$ in der kanonischen Ordnung der Menge \mathcal{G} an der i -ten Stelle steht.

Für das weitere Vorgehen ist die genaue Definition der kanonischen Ordnung nicht von Bedeutung. Letztlich ist nur wichtig, dass wir mithilfe dieser Ordnung sowohl die Menge aller Wörter aus $\{0, 1\}^*$ als auch die Menge aller Turingmaschinen in einer festen Reihenfolge nummeriert haben (formal haben wir diese Mengen bijektiv auf die Menge der natürlichen Zahlen abgebildet). Ferner sollte sich der Leser als Übung überlegen, dass es möglich ist, für ein gegebenes $i \in \mathbb{N}$ das Wort w_i und die Gödelnummer der Turingmaschine M_i zu berechnen. Außerdem ist es möglich für ein gegebenes Wort $w \in \{0, 1\}^*$ den Index i mit $w_i = w$ zu berechnen und für eine gegebene Gödelnummer $\langle M \rangle \in \mathcal{G}$ den Index $i \in \mathbb{N}$ mit $M_i = M$.

Definition 2.4. *Die Sprache*

$$D = \{w_i \in \{0, 1\}^* \mid M_i \text{ akzeptiert } w_i \text{ nicht}\}$$

heißt Diagonalsprache. Die Diagonalsprache D enthält das Wort w_i , das in der kanonischen Ordnung von $\{0,1\}^*$ an der i -ten Stelle steht, also genau dann, wenn es von der Turingmaschine M_i , deren Gödelnummer in der kanonischen Ordnung von \mathcal{G} an der i -ten Stelle steht, nicht akzeptiert wird.

Die folgende Tabelle zeigt, warum die Diagonalsprache ihren Namen trägt. Jede Spalte entspricht einem Wort aus $\{0,1\}^*$ und jede Zeile entspricht einer Turingmaschine. Dabei sind sowohl die Wörter aus $\{0,1\}^*$ als auch die Turingmaschinen gemäß der kanonischen Ordnung sortiert. In einer Zelle, die zu einer Turingmaschine M_j und einem Wort w_i gehört, steht genau dann eine Eins, wenn M_j das Wort w_i akzeptiert, und ansonsten eine Null. Die konkreten Werte in der Tabelle sind fiktiv gewählt. Ein Wort w_i gehört genau dann zur Diagonalsprache D , wenn auf der Diagonalen in der Zelle, die zu der Turingmaschine M_i und dem Wort w_i gehört, eine Null steht. In dem Beispiel gilt also $w_1, w_3 \in D$ aber $w_2, w_4, w_5 \notin D$.

	w_1	w_2	w_3	w_4	w_5	...
M_1	0	1	1	0	1	...
M_2	1	1	0	0	0	...
M_3	1	0	0	1	1	...
M_4	1	0	0	1	0	...
M_5	0	1	1	1	1	...
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\ddots

Theorem 2.5. Die Diagonalsprache D ist nicht entscheidbar.

Beweis. Wir führen einen Widerspruchsbeweis und gehen davon aus, dass D entscheidbar ist. Dann gibt es per Definition eine Turingmaschine M , die D entscheidet. Für alle $x \in \{0,1\}^*$ gilt also $f_M(x) = 1$ genau dann, wenn $x \in D$ ist. Da die Gödelnummer $\langle M \rangle$ von M zu der Menge \mathcal{G} gehört, gibt es einen Index $i \in \mathbb{N}$ mit $M = M_i$. Das bedeutet, die Turingmaschine, die die Diagonalsprache D entscheidet, kommt in der Aufzählung aller Turingmaschinen gemäß der kanonischen Ordnung an der i -ten Stelle.

Uns interessiert nun, wie sich die Turingmaschine $M = M_i$ auf dem Wort w_i verhält, das in der Aufzählung aller Wörter aus $\{0,1\}^*$ gemäß der kanonischen Ordnung an der i -ten Stelle kommt. Dazu unterscheiden wir zwei Fälle.

- Gilt $w_i \in D$, so akzeptiert M_i das Wort w_i , da M_i die Diagonalsprache D entscheidet. Aus der Definition von D folgt dann aber direkt, dass $w_i \notin D$ gilt.
- Gilt $w_i \notin D$, so akzeptiert M_i das Wort w_i nicht, da M_i die Diagonalsprache D entscheidet. Aus der Definition von D folgt dann aber direkt, dass $w_i \in D$ gilt.

Da wir in beiden Fällen einen Widerspruch erhalten, kann es im Widerspruch zu der Annahme keine Turingmaschine geben, die die Diagonalsprache entscheidet. \square

Für den Beweis von Theorem 2.5 war die spezielle Konstruktion der Diagonalsprache entscheidend. Deshalb ist ein solcher direkter Beweis der Unentscheidbarkeit einer Sprache für andere (weniger künstliche) Sprachen schwierig. Aus diesem Grunde werden wir alle weiteren Unentscheidbarkeitsresultate mithilfe von Reduktionen zeigen.

Definition 2.6. *Die Sprache*

$$H = \{ \langle M \rangle w \mid M \text{ hält auf } w \} \subseteq \{0, 1\}^*$$

nennen wir Halteproblem¹.

Theorem 2.7. *Das Halteproblem H ist nicht entscheidbar.*

Beweis. Wir reduzieren die Diagonalsprache auf das Halteproblem. Das bedeutet, wir führen einen Widerspruchsbeweis und gehen davon aus, dass das Halteproblem H entscheidbar ist. Dann gibt es eine Turingmaschine M_H , die das Halteproblem entscheidet. Mithilfe dieser Turingmaschine M_H konstruieren wir eine Turingmaschine M_D , die die Diagonalsprache entscheidet. Da es eine solche Turingmaschine laut Theorem 2.5 nicht geben kann, haben wir damit die Annahme, dass M_H existiert, zum Widerspruch geführt.

Die Turingmaschine M_D führt auf einer beliebigen Eingabe $w \in \{0, 1\}^*$ die folgenden Schritte aus. Wir gehen davon aus, dass die Gödelnummer $\langle M_H \rangle$ der Turingmaschine M_H bekannt ist.

$M_D(w)$

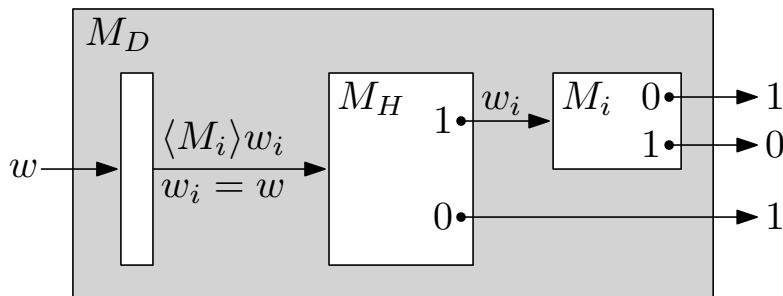
- 1 Berechne, welchen Index $i \in \mathbb{N}$ das Wort w in der kanonischen Ordnung von $\{0, 1\}^*$ besitzt. Für diesen Index gilt per Definition $w_i = w$. Berechne die Gödelnummer $\langle M_i \rangle$, die in der kanonischen Ordnung von \mathcal{G} an der i -ten Stelle steht.
- 2 Simuliere das Verhalten von M_H auf der Eingabe $\langle M_i \rangle w_i$.
- 3 **if** (M_H akzeptiert $\langle M_i \rangle w_i$ nicht)
- 4 akzeptiere w ;
- 5 **else**
- 6 Simuliere das Verhalten von M_i auf der Eingabe w_i .
- 7 **if** (M_i akzeptiert w_i)
- 8 verwirf w ;
- 9 **else**
- 10 akzeptiere w ;

Wir haben bereits bei der Definition der kanonischen Ordnung diskutiert, dass die Berechnung des Index i und der Gödelnummer $\langle M_i \rangle$ in Schritt 1 möglich ist. Auch das Simulieren der Turingmaschine M_H in Schritt 2 ist kein Problem, da wir bereits in Abschnitt 2.1 bei der Diskussion der universellen Turingmaschine beschrieben haben,

¹Es wäre sprachlich präziser, H als die Haltesprache zu bezeichnen. Der Name Halteproblem ist aber geläufiger, weshalb wir ihn auch in dieser Vorlesung verwenden.

wie eine Turingmaschine eine andere simulieren kann. Da M_H das Halteproblem entscheidet, terminiert M_H insbesondere auf jeder Eingabe. Das bedeutet, dass auch die Simulation in Schritt 2 terminiert. Auch die Simulation von M_i auf der Eingabe w_i in Schritt 6 terminiert, da Schritt 6 nur dann erreicht wird, wenn M_H die Eingabe $\langle M_i \rangle w_i$ akzeptiert, d. h. wenn $\langle M_i \rangle w_i \in H$ gilt, was per Definition bedeutet, dass M_i auf der Eingabe w_i terminiert.

Die folgende Abbildung illustriert noch einmal das Verhalten der Turingmaschine M_D .



Wir haben oben bereits argumentiert, dass die Turingmaschine M_D auf jeder Eingabe terminiert. Es bleibt zu zeigen, dass sie die Eingabe w genau dann akzeptiert, wenn $w \in D$ gilt. Sei $i \in \mathbb{N}$ der Index, der in Schritt 1 berechnet wird. Dann gilt $w_i = w$.

- Gilt $w_i \in D$, so akzeptiert die Turingmaschine M_i die Eingabe w_i nicht (per Definition von D). In diesem Fall gerät M_i auf der Eingabe w_i entweder in eine Endlosschleife oder M_i terminiert und verwirft w_i .
 - Gerät M_i in eine Endlosschleife, so gilt $\langle M_i \rangle w_i \notin H$ (per Definition von H) und damit akzeptiert M_H die Eingabe $\langle M_i \rangle w_i$ nicht. Dann wird $w = w_i$ in Zeile 4 von M_D akzeptiert.
 - Terminiert M_i und verwirft w_i , so gilt $\langle M_i \rangle w_i \in H$ und damit wird Zeile 6 erreicht. Da M_i die Eingabe w_i verwirft, wird $w = w_i$ in Zeile 10 akzeptiert.
- Gilt $w_i \notin D$, so akzeptiert die Turingmaschine M_i die Eingabe w_i (per Definition von D). Das bedeutet insbesondere, dass M_i auf der Eingabe w_i terminiert. Es wird also Zeile 6 erreicht. Da M_i die Eingabe w_i akzeptiert, wird $w = w_i$ in Zeile 8 verworfen.

Damit ist der Beweis abgeschlossen, denn wir haben gezeigt, dass M_D jedes Wort $w \in D$ akzeptiert und jedes Wort $w \notin D$ verwirft. Da es gemäß Theorem 2.5 die Turingmaschine M_D nicht geben kann, kann die Annahme, dass eine Turingmaschine M_H für das Halteproblem H existiert, nicht gelten. \square

2.3 Turing- und Many-One-Reduktionen

Wir haben in der Einleitung dieses Kapitels definiert, dass eine Reduktion einer Sprache A auf eine Sprache B eine Turingmaschine ist, die die Sprache A mithilfe eines (hypothetischen) Unterprogramms für die Sprache B löst. Diese Art der Reduktion wird in

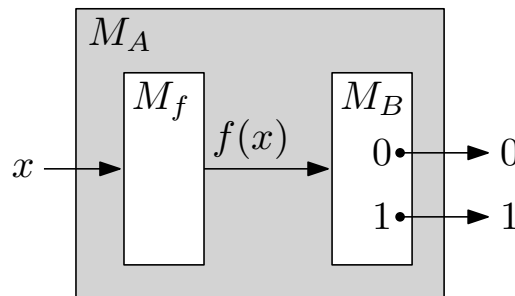
der Literatur auch als *Turing-Reduktion* oder *Unterprogrammtechnik* bezeichnet. Wir beschäftigen uns nun noch mit einer eingeschränkten Klasse von Turing-Reduktionen, den sogenannten *Many-One-Reduktionen*.

Definition 2.8. Eine Many-One-Reduktion² einer Sprache $A \subseteq \Sigma_1^*$ auf eine Sprache $B \subseteq \Sigma_2^*$ ist eine berechenbare Funktion $f: \Sigma_1^* \rightarrow \Sigma_2^*$ mit der Eigenschaft, dass

$$x \in A \iff f(x) \in B$$

für alle $x \in \Sigma_1^*$ gilt. Existiert eine solche Reduktion, so heißt A auf B *reduzierbar* und wir schreiben $A \leq B$.

Eine Many-One-Reduktion f kann als Spezialfall einer Turing-Reduktion angesehen werden. Um die Sprache A mithilfe einer hypothetischen Turingmaschine M_B für die Sprache B zu entscheiden, genügt es, für eine gegebene Eingabe $x \in \Sigma_1^*$ den Funktionswert $f(x) \in \Sigma_2^*$ zu berechnen und dann die Turingmaschine M_B auf der Eingabe $f(x)$ zu simulieren. Es gilt $x \in A$ genau dann, wenn M_B die Eingabe $f(x)$ akzeptiert. Sei M_A die so konstruierte Turingmaschine für A und sei M_f eine Turingmaschine, die die Funktion f berechnet. Dann kann die Many-One-Reduktion schematisch wie folgt dargestellt werden.



Im folgenden Theorem halten wir noch einmal die wesentlichen Konsequenzen einer Reduktion fest.

Theorem 2.9. Es seien $A \subseteq \Sigma_1^*$ und $B \subseteq \Sigma_2^*$ zwei Sprachen, für die $A \leq B$ gilt. Ist B entscheidbar, so ist auch A entscheidbar. Ist A nicht entscheidbar, so ist auch B nicht entscheidbar.

Beweis. Wir haben oben bereits beschrieben, dass man eine Turingmaschine M_A für die Sprache A konstruieren kann, wenn $A \leq B$ gilt und eine Turingmaschine M_B für B existiert. Damit ist der erste Teil des Theorems bewiesen.

Der zweite Teil folgt mit einem Widerspruchsbeweis direkt aus dem ersten, denn aus der Annahme, dass B entscheidbar ist, folgt mit $A \leq B$ direkt, dass auch A entscheidbar ist. \square

Intuitiv besagt die Existenz einer Reduktion $A \leq B$ also, dass die Sprache A höchstens so schwer zu entscheiden ist wie die Sprache B . Wir definieren nun noch einige Abwandlungen des Halteproblems, deren Unentscheidbarkeit wir durch Reduktionen nachweisen werden.

²Wir werden den Begriff „Reduktion“ im Folgenden stets im Sinne von Many-One-Reduktion benutzen. Sprechen wir über Turing-Reduktionen, so werden wir dies explizit erwähnen.

Definition 2.10. Das spezielle Halteproblem H_ε sei definiert durch

$$H_\varepsilon = \{ \langle M \rangle \mid M \text{ hält auf } \varepsilon \} \subseteq \{0, 1\}^*.$$

Das vollständige Halteproblem H_{all} sei definiert durch

$$H_{\text{all}} = \{ \langle M \rangle \mid M \text{ hält auf jeder Eingabe aus } \{0, 1\}^* \} \subseteq \{0, 1\}^*.$$

Die universelle Sprache U sei definiert durch

$$U = \{ \langle M \rangle w \mid M \text{ akzeptiert } w \} \subseteq \{0, 1\}^*.$$

Wir beschäftigen uns zunächst nur mit dem speziellen Halteproblem und der universellen Sprache. Auf das vollständige Halteproblem kommen wir später im Abschnitt über rekursiv aufzählbare Sprachen noch einmal zurück.

Theorem 2.11. Die universelle Sprache U ist nicht entscheidbar.

Beweis. Wir reduzieren das Halteproblem H auf die universelle Sprache. Dazu konstruieren wir eine Funktion $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$, die Eingaben für das Halteproblem H auf Eingaben für die universelle Sprache U abbildet. Ist $x \in \{0, 1\}^*$ nicht von der Form $\langle M \rangle w$ für eine Turingmaschine M (das heißt, x beginnt nicht mit einer gültigen Gödelnummer), so sei $f(x) = x$.

Gilt $x = \langle M \rangle w$ für eine Turingmaschine M und ein $w \in \{0, 1\}^*$, so berechnen wir die Gödelnummer einer Turingmaschine M^* mit dem folgenden Verhalten. Die Turingmaschine M^* simuliert das Verhalten von M auf der gegebenen Eingabe Schritt für Schritt, solange bis M terminiert. Anschließend akzeptiert M^* die Eingabe unabhängig von der Ausgabe von M . Es sei dann $f(\langle M \rangle w) = \langle M^* \rangle w$. Die Funktion f ist berechenbar, da die Turingmaschine M^* für gegebenes M leicht konstruiert werden kann.

Wir müssen nun noch zeigen, dass die oben definierte Funktion f tatsächlich eine Reduktion von H auf U darstellt. Wir zeigen die beiden zu der Äquivalenz $x \in H \iff f(x) \in U$ gehörenden Implikationen getrennt.

„ \Rightarrow “ Sei $x \in H$. Dann muss $x = \langle M \rangle w$ für eine Turingmaschine M und ein Wort $w \in \{0, 1\}^*$ gelten. Ferner folgt aus $x = \langle M \rangle w \in H$, dass die Turingmaschine M auf der Eingabe w hält. Da die Turingmaschine M^* das Verhalten von M simuliert, hält sie ebenfalls auf der Eingabe w . Per Definition akzeptiert M^* jede Eingabe, auf der sie hält. Dies bedeutet, dass $f(x) = \langle M^* \rangle w \in U$ gilt.

„ \Leftarrow “ Sei $x \notin H$. Dann ist x entweder nicht von der Form $\langle M \rangle w$ oder es gilt $x = \langle M \rangle w$, aber die Turingmaschine M hält nicht auf der Eingabe w . Ist x nicht von der Form $\langle M \rangle w$, so gilt $f(x) = x \notin U$. Gilt $x = \langle M \rangle w$ für eine Turingmaschine M , die auf der Eingabe w nicht hält, so hält die Turingmaschine M^* ebenfalls nicht auf der Eingabe w . Das bedeutet, dass sie die Eingabe w nicht akzeptiert, woraus $f(x) = \langle M^* \rangle w \notin U$ folgt.

Damit haben wir gezeigt, dass $H \leq U$ gilt. Aus den Theoremen 2.7 und 2.9 folgt somit, dass U nicht entscheidbar ist. \square

Der Beweis des nächsten Theorems ist sehr ähnlich zu dem gerade geführten Beweis für die Aussage, dass die universelle Sprache U nicht entscheidbar ist. Da Reduktionen aber ein sehr wichtiges Konzept in der theoretischen Informatik sind, kann es nicht schaden, ein weiteres Beispiel dafür zu sehen.

Theorem 2.12. *Das spezielle Halteproblem H_ε ist nicht entscheidbar.*

Beweis. Wir reduzieren das Halteproblem H auf das spezielle Halteproblem H_ε . Dazu konstruieren wir eine Funktion $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$, die Eingaben für das Halteproblem H auf Eingaben für das spezielle Halteproblem H_ε abbildet. Ist $x \in \{0, 1\}^*$ nicht von der Form $\langle M \rangle w$ für eine Turingmaschine M (das heißt, x beginnt nicht mit einer gültigen Gödelnummer), so sei $f(x) = x$.

Gilt $x = \langle M \rangle w$ für eine Turingmaschine M und ein $w \in \{0, 1\}^*$, so berechnen wir die Gödelnummer einer Turingmaschine M_w^* mit dem folgenden Verhalten. Die Turingmaschine M_w^* löscht zunächst die Eingabe und ersetzt diese durch w . Anschließend simuliert sie das Verhalten von M auf der Eingabe w Schritt für Schritt. Es sei dann $f(\langle M \rangle w) = \langle M_w^* \rangle$. Die Funktion f ist berechenbar, da die Turingmaschine M_w^* für gegebenes M und w leicht konstruiert werden kann.

Wir müssen nun noch zeigen, dass die oben definierte Funktion f tatsächlich eine Reduktion von H auf H_ε darstellt. Wir zeigen die beiden zu der Äquivalenz $x \in H \iff f(x) \in H_\varepsilon$ gehörenden Implikationen getrennt.

„ \Rightarrow “ Sei $x \in H$. Dann muss $x = \langle M \rangle w$ für eine Turingmaschine M und ein Wort $w \in \{0, 1\}^*$ gelten. Ferner folgt aus $x = \langle M \rangle w \in H$, dass die Turingmaschine M auf der Eingabe w hält. Da die Turingmaschine M_w^* bei jeder Eingabe das Verhalten von M auf w simuliert, hält sie bei jeder Eingabe (insbesondere bei der leeren Eingabe). Dies bedeutet, dass $f(x) = \langle M_w^* \rangle \in H_\varepsilon$ gilt.

„ \Leftarrow “ Sei $x \notin H$. Dann ist x entweder nicht von der Form $\langle M \rangle w$ oder es gilt $x = \langle M \rangle w$, aber die Turingmaschine M hält nicht auf der Eingabe w . Ist x nicht von der Form $\langle M \rangle w$, so beginnt x nicht mit der Gödelnummer einer Turingmaschine. Insbesondere ist x dann auch nicht von der Form $\langle M \rangle$ für eine Turingmaschine M . In diesem Fall gilt $f(x) = x \notin H_\varepsilon$. Gilt $x = \langle M \rangle w$ für eine Turingmaschine M , die auf der Eingabe w nicht hält, so hält die Turingmaschine M_w^* auf keiner Eingabe (insbesondere nicht auf der leeren Eingabe). Dies bedeutet, dass $f(x) = \langle M_w^* \rangle \notin H_\varepsilon$ gilt.

Damit haben wir gezeigt, dass $H \leq H_\varepsilon$ gilt. Aus den Theoremen 2.7 und 2.9 folgt somit, dass H_ε nicht entscheidbar ist. \square

Der Leser sollte sich als Übung überlegen, dass die Reduktion von H auf H_ε im letzten Beweis auch eine Reduktion von H auf H_{all} ist und somit auch die Unentscheidbarkeit von H_{all} beweist.

2.4 Der Satz von Rice

Die Tatsache, dass das Halteproblem nicht entscheidbar ist, zeigt bereits, dass eine automatische Programmverifikation im Allgemeinen nicht möglich ist. In diesem Abschnitt zeigen wir sogar noch ein verschärftes Ergebnis: Für keine nicht triviale Menge von Funktionen kann entschieden werden, ob eine gegebene Turingmaschine eine Funktion aus dieser Menge berechnet. Dieses als *Satz von Rice* bekannte Resultat werden wir nun formalisieren und beweisen.

Im Folgenden betrachten wir der Einfachheit halber wieder das Eingabealphabet $\Sigma = \{0, 1\}$. Es bezeichne

$$\mathcal{R} = \{f: \Sigma^* \rightarrow \Sigma^* \cup \{\perp\} \mid \exists \text{ Turingmaschine } M \text{ mit } f_M = f\}$$

die Menge aller von Turingmaschinen berechenbaren Funktionen. Für eine Teilmenge $S \subseteq \mathcal{R}$ der berechenbaren Funktionen bezeichnen wir mit

$$L(S) = \{\langle M \rangle \mid f_M \in S\}$$

die Menge der Gödelnummern der Turingmaschinen, die eine Funktion aus der Menge S berechnen.

Theorem 2.13 (Satz von Rice). *Es sei $S \subseteq \mathcal{R}$ mit $S \neq \emptyset$ und $S \neq \mathcal{R}$ eine Teilmenge der berechenbaren Funktionen. Dann ist die Sprache $L(S)$ nicht entscheidbar.*

Beweis. Sei $S \subseteq \mathcal{R}$ mit $S \neq \emptyset$ und $S \neq \mathcal{R}$ beliebig. Wir zeigen das Theorem mittels einer Turing-Reduktion des speziellen Halteproblems H_ε auf die Sprache $L(S)$. Dazu konstruieren wir eine Turingmaschine M_{H_ε} , die das spezielle Halteproblem H_ε mithilfe einer hypothetischen Turingmaschine $M_{L(S)}$ für die Sprache $L(S)$ als Unterprogramm entscheidet.

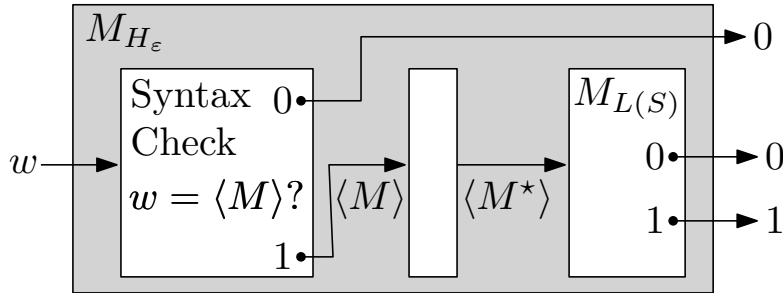
Es sei $u: \Sigma^* \rightarrow \Sigma^* \cup \{\perp\}$ die überall undefinierte Funktion mit $u(x) = \perp$ für alle $x \in \Sigma^*$. Die Funktion u gehört zu der Menge \mathcal{R} der berechenbaren Funktionen, da sie von jeder Turingmaschine, die auf keiner Eingabe hält, berechnet wird. Wir unterscheiden nun die beiden Fälle $u \in S$ und $u \notin S$.

Zunächst betrachten wir den Fall $u \notin S$. In diesem Fall sei $f \neq u$ eine beliebige Funktion aus S . Eine solche Funktion existiert, da S nicht leer ist. Sei M_f eine Turingmaschine, die f berechnet. Die Turingmaschine M_{H_ε} führt zunächst eine Überprüfung der Syntax der Eingabe w durch. Ist w keine gültige Gödelnummer, so gilt $w \notin H_\varepsilon$ und M_{H_ε} verwirft w direkt. Ansonsten sei $w = \langle M \rangle$ für eine Turingmaschine M . In diesem Fall konstruiert M_{H_ε} die Gödelnummer $\langle M^* \rangle$ einer Turingmaschine M^* mit dem folgenden Verhalten.

Erhält die Turingmaschine M^* eine Eingabe x , so simuliert sie in Phase 1 das Verhalten von M auf der leeren Eingabe ε . Anschließend simuliert M^* in Phase 2 die Turingmaschine M_f auf der Eingabe x und gibt $f(x)$ aus.

Die so konstruierte Turingmaschine M^* besitzt die folgende Eigenschaft: Hält M nicht auf der leeren Eingabe, so hält M^* auf keiner Eingabe und berechnet dementsprechend die überall undefinierte Funktion u . Hält M auf der leeren Eingabe, so erreicht M^* Phase 2 und berechnet die Funktion f .

Nachdem M_{H_ε} die Gödelnummer $\langle M^* \rangle$ berechnet hat, simuliert sie das Verhalten von $M_{L(S)}$ auf der Eingabe $\langle M^* \rangle$ und übernimmt die Ausgabe. Das Verhalten von M_{H_ε} ist schematisch in der folgenden Abbildung dargestellt.



Wir zeigen nun, dass die Turingmaschine M_{H_ε} das spezielle Halteproblem H_ε löst.

- Sei $w \in H_\varepsilon$. Dann muss $w = \langle M \rangle$ für eine Turingmaschine M gelten. Ferner folgt aus $w = \langle M \rangle \in H_\varepsilon$, dass die Turingmaschine M auf der leeren Eingabe ε hält. Dies bedeutet gemäß der obigen Beobachtung, dass die Turingmaschine M^* die Funktion f berechnet. Wegen $f \in S$ bedeutet dies, dass $\langle M^* \rangle \in L(S)$ gilt. Dementsprechend akzeptiert die Turingmaschine $M_{L(S)}$ die Eingabe $\langle M^* \rangle$. Damit akzeptiert M_{H_ε} die Eingabe w .
- Sei $w \notin H_\varepsilon$. Dann ist w entweder keine gültige Gödelnummer und wird direkt von M_{H_ε} verworfen oder es gilt $w = \langle M \rangle$ für eine Turingmaschine M , die nicht auf der leeren Eingabe ε hält. Letzteres bedeutet gemäß der obigen Beobachtung, dass die Turingmaschine M^* die Funktion u berechnet. Wegen $u \notin S$ bedeutet dies, dass $\langle M^* \rangle \notin L(S)$ gilt. Dementsprechend verwirft die Turingmaschine $M_{L(S)}$ die Eingabe $\langle M^* \rangle$. Damit verwirft M_{H_ε} die Eingabe w .

Damit haben wir für den Fall $u \notin S$ gezeigt, dass aus der Entscheidbarkeit von $L(S)$ die Entscheidbarkeit des speziellen Halteproblems H_ε im Widerspruch zu Theorem 2.12 folgt. Der Fall $u \in S$ kann ähnlich behandelt werden. In diesem Fall wählt man $f \in \mathcal{R} \setminus S$ beliebig und ändert lediglich im letzten Schritt das Akzeptanzverhalten von M_{H_ε} dahingehend, dass M_{H_ε} die Eingabe w genau dann akzeptiert, wenn $M_{L(S)}$ die Eingabe $\langle M^* \rangle$ verwirft. Es ist eine gute Übung für den Leser, die Details dieses Falles noch einmal nachzuvollziehen. \square

Der Satz von Rice _{ε} hat weitreichende Konsequenzen für die Verifikation von Programmen. Er besagt, dass es unmöglich ist, automatisch zu verifizieren, dass ein gegebenes Programm ein bestimmtes Problem löst. Betrachten wir als Beispiel das Problem, zu testen, ob eine gegebene Zahl eine Primzahl ist oder nicht. Dies können wir durch die Funktion $f: \{0, 1\}^* \rightarrow \{0, 1\}$ mit

$$f(x) = \begin{cases} 1 & \text{val}(x) \text{ ist eine Primzahl} \\ 0 & \text{sonst} \end{cases}$$

beschreiben. Wählen wir $S = \{f\}$, so besagt der Satz von Rice, dass nicht entschieden werden kann, ob eine gegebene Turingmaschine M die Funktion f berechnet. Bei Problemen, die durch Relationen beschrieben sind, müssen wir die Menge S anders definieren. Betrachten wir dazu noch einmal das Problem, eine gegebene Zahl in Binärdarstellung zu quadrieren. Dieses haben wir in der Einleitung durch die Relation

$$R = \{(x, y) \mid \text{val}(y) = \text{val}(x)^2\} \subseteq \{0, 1\}^* \times \{0, 1\}^*$$

modelliert. Wir definieren dann S als die Menge aller berechenbaren Funktionen, die bei jeder Eingabe $x \in \{0, 1\}^*$ eine Ausgabe $y \in \{0, 1\}^*$ mit $(x, y) \in R$ produzieren:

$$S = \{f \in \mathcal{R} \mid \forall x \in \{0, 1\}^* : (x, f(x)) \in R\}.$$

Eine Turingmaschine löst das durch R beschriebene Problem genau dann, wenn sie eine Funktion aus S berechnet. Außerdem gilt $S \neq \emptyset$ und $S \neq \mathcal{R}$. Wieder besagt der Satz von Rice also, dass nicht entschieden werden kann, ob eine gegebene Turingmaschine dieses Problem löst.

2.5 Rekursiv aufzählbare Sprachen

Eine Sprache L heißt gemäß Definition 1.3 entscheidbar oder rekursiv, wenn es eine Turingmaschine gibt, die auf jeder Eingabe hält und genau die Wörter aus der Sprache L akzeptiert. Bei vielen nicht entscheidbaren Problemen, die wir kennengelernt haben, besteht eine Asymmetrie zwischen Wörtern aus der Sprache und Wörtern, die nicht zu der Sprache gehören.

Um dies zu erläutern, konstruieren wir eine Turingmaschine M_H , die das Halteproblem zwar nicht löst, aber zumindest nie ein falsches Ergebnis ausgibt. Erhält M_H eine Eingabe $\langle M \rangle w$, so simuliert sie das Verhalten von M auf w . Terminiert diese Simulation nach endlich vielen Schritten, so akzeptiert M_H anschließend die Eingabe $\langle M \rangle w$. Erhält M_H eine syntaktisch nicht korrekte Eingabe, so verwirft sie diese direkt. Die so definierte Turingmaschine M_H akzeptiert jede Eingabe $x \in H$. Jede Eingabe $x \notin H$ wird entweder verworfen (wenn sie syntaktisch nicht korrekt ist) oder M_H hält nicht auf x . Somit gibt M_H niemals ein falsches Ergebnis aus. Auf Eingaben, die zu H gehören, gibt sie sogar stets das richtige Ergebnis aus. Nur auf Eingaben, die nicht zu H gehören, terminiert sie nicht notwendigerweise.

Definition 2.14. *Eine Turingmaschine M erkennt eine Sprache $L \subseteq \Sigma^*$, wenn sie jedes Wort $w \in L$ akzeptiert und jedes Wort $w \in \Sigma^* \setminus L$ entweder verwirft oder darauf nicht terminiert. Eine Sprache $L \subseteq \Sigma^*$ heißt semi-entscheidbar oder rekursiv aufzählbar, wenn es eine Turingmaschine M gibt, die L erkennt.*

Aus der Definition folgt direkt, dass rekursive Sprachen auch rekursiv aufzählbar sind. Aber auch viele nicht rekursive Sprachen, die wir in dieser Vorlesung kennengelernt haben, sind rekursiv aufzählbar. Der Leser überlege sich, dass dies insbesondere auf das Halteproblem H , das spezielle Halteproblem H_ε und die universelle Sprache U

zutritt. Wir haben allerdings auch Sprachen kennengelernt, bei denen auf den ersten Blick nicht klar ist, ob sie rekursiv aufzählbar sind. Ein Beispiel ist das vollständige Halteproblem H_{all} . Erhält man die Gödelnummer $\langle M \rangle$ einer Turingmaschine M , die auf jeder Eingabe hält, so existiert (anders als beim Halteproblem H , bei dem man eine gegebene Turingmaschine nur auf einer gegebenen Eingabe simulieren muss) kein offensichtliches Verfahren, um dies in endlicher Zeit festzustellen. Im Folgenden werden wir nachweisen, dass das vollständige Halteproblem H_{all} tatsächlich nicht rekursiv aufzählbar ist.

Zunächst werden wir uns aber noch mit den sogenannten *Abschlusseigenschaften* von rekursiv aufzählbaren Sprachen beschäftigen. Das heißt, wir werden untersuchen, bezüglich welcher Operationen (Schnitt, Vereinigung, Komplementbildung) die Menge der rekursiv aufzählbaren Sprachen abgeschlossen sind.

Theorem 2.15. *Es seien $L_1 \subseteq \Sigma^*$ und $L_2 \subseteq \Sigma^*$ zwei rekursiv aufzählbare Sprachen. Dann sind auch die Sprachen $L_1 \cup L_2$ und $L_1 \cap L_2$ rekursiv aufzählbar.*

Beweis. Es seien M_1 und M_2 Turingmaschinen, die die Sprachen L_1 bzw. L_2 erkennen. Gemäß Definition 2.14 bedeutet dies, dass die Turingmaschine M_i jedes Wort $x \in M_i$ akzeptiert und kein Wort $x \notin M_i$ akzeptiert.

Wir konstruieren zunächst eine Turingmaschine M_{\cap} für den Schnitt $L_1 \cap L_2$. Die Turingmaschine M_{\cap} simuliert bei einer Eingabe $x \in \Sigma^*$ zunächst die Turingmaschine M_1 auf x und anschließend (sofern die Simulation von M_1 auf x terminiert) die Turingmaschine M_2 auf x . Sie akzeptiert die Eingabe x genau dann, wenn sowohl M_1 als auch M_2 die Eingabe x akzeptiert haben.

Man überlegt sich leicht, dass die so konstruierte Turingmaschine M_{\cap} den Schnitt $L_1 \cap L_2$ erkennt. Sie akzeptiert jedes Wort $x \in L_1 \cap L_2$, da jedes solche Wort auch von M_1 und M_2 akzeptiert wird. Sie akzeptiert kein Wort $x \notin L_1 \cap L_2$, da jedes solche Wort von mindestens einer der Turingmaschinen M_1 oder M_2 nicht akzeptiert wird.

Auf den ersten Blick erscheint es so, als könne man analog eine Turingmaschine M_{\cup} konstruieren, die die Vereinigung $L_1 \cup L_2$ erkennt. Würde man allerdings erst M_1 und anschließend M_2 auf der Eingabe x simulieren und x akzeptieren, wenn mindestens eine der beiden Turingmaschinen x akzeptiert hat, so gibt es im Allgemeinen Wörter $x \in L_1 \cup L_2$, die nicht akzeptiert werden. Für Wörter $x \in L_1 \cup L_2$ mit $x \in L_2$ und $x \notin L_1$ kann es nämlich passieren, dass die Simulation von M_1 auf x nicht terminiert und die Simulation von M_2 gar nicht erreicht wird.

Die Lösung besteht darin, die Turingmaschinen M_1 und M_2 parallel zu simulieren. Konkret kann man M_{\cup} als eine 2-Band-Turingmaschine konstruieren, die auf einem Band das Verhalten von M_1 und auf dem anderen das Verhalten von M_2 simuliert. Die Turingmaschine M_{\cup} simuliert in jedem Rechenschritt parallel einen Schritt von M_1 und einen von M_2 auf dem entsprechenden Band. Sie akzeptiert die Eingabe, sobald eine von den beiden Simulationen terminiert und die Eingabe akzeptiert. Da jedes Wort $x \in L_1 \cup L_2$ nach endlich vielen Schritten von M_1 oder M_2 akzeptiert wird und kein Wort $x \notin L_1 \cup L_2$ von M_1 oder M_2 akzeptiert wird, erkennt die so konstruierte Turingmaschine die Vereinigung $L_1 \cup L_2$. \square

Der Leser möge sich als kurze Übung überlegen, dass das obige Theorem auch analog für rekursive Sprachen gilt, dass also die Vereinigung und der Schnitt zweier rekursiver Sprachen wieder rekursiv sind. Das *Komplement* einer Sprache $L \subseteq \Sigma^*$ ist definiert als $\bar{L} = \Sigma^* \setminus L$. Der Leser sollte sich ebenfalls als Übung überlegen, dass das Komplement jeder rekursiven Sprache ebenfalls rekursiv ist. Rekursiv aufzählbare Sprachen sind hingegen nicht abgeschlossen unter Komplementbildung, was aus dem folgenden Theorem folgt.

Theorem 2.16. *Sind eine Sprache $L \subseteq \Sigma^*$ und ihr Komplement \bar{L} rekursiv aufzählbar, so ist L rekursiv.*

Beweis. Es seien M_L und $M_{\bar{L}}$ Turingmaschinen, die L bzw. \bar{L} erkennen. Wir konstruieren nun eine Turingmaschine M , die L entscheidet. Die Turingmaschine M simuliert auf einer Eingabe x die Turingmaschinen M_L und $M_{\bar{L}}$ parallel (analog zu der Turingmaschine M_{\cup} aus dem Beweis von Theorem 2.15). Sie stoppt, sobald eine der beiden Turingmaschinen M_L oder $M_{\bar{L}}$ die Eingabe x akzeptiert. Akzeptiert M_L die Eingabe x , so akzeptiert auch M die Eingabe x . Akzeptiert hingegen $M_{\bar{L}}$ die Eingabe x , so verwirft M die Eingabe x .

Um zu zeigen, dass M die Sprache L entscheidet, halten wir zunächst fest, dass jedes $x \in \Sigma^*$ entweder zu L oder zu \bar{L} gehört und demnach von genau einer der beiden Turingmaschinen M_L oder $M_{\bar{L}}$ akzeptiert wird. Damit ist sichergestellt, dass die Turingmaschine M auf jeder Eingabe x terminiert. Da jede Eingabe $x \in L$ von M_L akzeptiert wird, akzeptiert M ebenfalls jede Eingabe aus L . Da jede Eingabe $x \notin L$ von $M_{\bar{L}}$ akzeptiert wird, verwirft M jede Eingabe, die nicht zu L gehört. Daraus folgt, dass M die Sprache L entscheidet. \square

Das vorangegangene Theorem impliziert gemeinsam mit unserem Wissen über das Halteproblem, dass das Komplement einer rekursiv aufzählbaren Sprache im Allgemeinen nicht rekursiv aufzählbar ist. Wir haben oben diskutiert, dass H rekursiv aufzählbar ist. Wäre das Komplement \bar{H} ebenfalls rekursiv aufzählbar, so würde aus Theorem 2.16 folgen, dass H rekursiv ist, was im Widerspruch zu der Nichtentscheidbarkeit des Halteproblems (Theorem 2.7) steht.

Hat man bewiesen, dass eine Sprache nicht rekursiv aufzählbar ist, so kann man für weitere Sprachen wieder mittels Reduktionen nachweisen, dass sie ebenfalls nicht rekursiv aufzählbar sind. Das folgende Theorem lässt sich analog zu Theorem 2.9 beweisen.

Theorem 2.17. *Es seien $A \subseteq \Sigma_1^*$ und $B \subseteq \Sigma_2^*$ zwei Sprachen, für die $A \leq B$ gilt. Ist B rekursiv aufzählbar, so ist auch A rekursiv aufzählbar. Ist A nicht rekursiv aufzählbar, so ist auch B nicht rekursiv aufzählbar.*

Für die meisten Sprachen L , die wir in dieser Vorlesung kennengelernt haben, kann man relativ einfach zeigen, dass entweder L oder \bar{L} rekursiv aufzählbar ist. Mithilfe von zwei Reduktionen zeigen wir nun, dass H_{all} nicht in diese Kategorie fällt.

Theorem 2.18. *Weder das vollständige Halteproblem H_{all} noch sein Komplement \bar{H}_{all} sind rekursiv aufzählbar.*

Beweis. Wir haben nach dem Beweis von Theorem 2.12 angemerkt, dass die in diesem Beweis konstruierte Funktion auch eine Reduktion von H auf H_{all} darstellt. Der Leser überlege sich, dass eine Reduktion einer Sprache A auf eine Sprache B auch stets eine Reduktion von \overline{A} auf \overline{B} ist. Dies folgt direkt aus Definition 2.8. Somit liefert der Beweis von Theorem 2.12 eine Reduktion von \overline{H} auf $\overline{H_{\text{all}}}$. Da \overline{H} , wie oben diskutiert, nicht rekursiv aufzählbar ist, impliziert dies, dass auch $\overline{H_{\text{all}}}$ nicht rekursiv aufzählbar ist.

Zu zeigen ist also nur noch, dass auch H_{all} nicht rekursiv aufzählbar ist. Dazu geben wir eine Reduktion $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$ von $\overline{H_\varepsilon}$ auf H_{all} an. Die Sprache $\overline{H_\varepsilon}$ ist nicht rekursiv aufzählbar, da ihr Komplement H_ε rekursiv aufzählbar aber nicht rekursiv ist. Eingaben x für $\overline{H_\varepsilon}$, die keine Gödelnummern sind, werden durch f auf eine beliebige Gödelnummer $f(x) = \langle M_1 \rangle \in H_{\text{all}}$ abgebildet. Gilt $x = \langle M \rangle$ für eine Turingmaschine M , so sei $f(x) = \langle M^* \rangle$ für eine Turingmaschine M^* mit dem folgenden Verhalten.

Erhält die Turingmaschine M^* eine Eingabe w , so simuliert sie die Turingmaschine M auf der leeren Eingabe solange bis sie entweder hält oder $|w|$ viele Schritte gemacht hat. Falls M innerhalb dieser $|w|$ vielen simulierten Schritte hält, so geht M^* in eine Endlosschleife. Ansonsten terminiert M^* .

Wir zeigen nun, dass $x \in \overline{H_\varepsilon} \iff f(x) \in H_{\text{all}}$ für alle $x \in \{0, 1\}^*$ gilt.

- Sei $x \in \overline{H_\varepsilon}$. Dann ist x entweder keine gültige Gödelnummer oder es gilt $x = \langle M \rangle$ für eine Turingmaschine, die nicht auf der leeren Eingabe hält. Ist x keine gültige Gödelnummer, so gilt per Definition $f(x) = \langle M_1 \rangle \in H_{\text{all}}$. Ist $x = \langle M \rangle \in \overline{H_\varepsilon}$, so folgt aus der obigen Konstruktion, dass die Turingmaschine M^* auf jeder Eingabe w terminiert. Damit gilt $f(x) = \langle M^* \rangle \in H_{\text{all}}$.
- Sei $x \notin \overline{H_\varepsilon}$, also $x \in H_\varepsilon$. Dann gilt $x = \langle M \rangle$ für eine Turingmaschine M , die auf der leeren Eingabe hält. Es sei $t \in \mathbb{N}$ die Anzahl an Schritten, die M auf der leeren Eingabe benötigt. Aus der obigen Konstruktion folgt, dass die Turingmaschine M^* für jede Eingabe w mit $|w| > t$ in eine Endlosschleife gerät. Somit terminiert M^* nicht auf jeder Eingabe und es gilt $f(x) = \langle M^* \rangle \notin H_{\text{all}}$.

Zusammengefasst haben wir in diesem Beweis die beiden Reduktionen $\overline{H} \leq \overline{H_{\text{all}}}$ und $\overline{H_\varepsilon} \leq H_{\text{all}}$ gezeigt. Da \overline{H} und $\overline{H_\varepsilon}$ nicht rekursiv aufzählbar sind, ist somit weder H_{all} noch $\overline{H_{\text{all}}}$ rekursiv aufzählbar. \square

Wir lernen nun noch eine alternative Charakterisierung von rekursiv aufzählbaren Sprachen kennen, die insbesondere die Namensgebung erklärt.

Definition 2.19. *Ein Aufzähler für eine Sprache $L \subseteq \Sigma^*$ ist eine Turingmaschine mit einem zusätzlichen Ausgabeband, das zu Beginn leer ist. Ein Aufzähler erhält keine Eingabe und er schreibt nach und nach Wörter aus L (durch Leerzeichen getrennt) auf das Ausgabeband. Er schreibt keine Wörter auf das Ausgabeband, die nicht zu L gehören, und zu jedem Wort $w \in L$ existiert ein Index $i_w \in \mathbb{N}$, sodass das Wort w nach i_w Schritten des Aufzählers auf dem Ausgabeband steht.*

Wir haben in der obigen Definition keinerlei Aussage darüber getroffen, in welcher Reihenfolge die Wörter aus L auf das Band geschrieben werden, und wir erlauben insbesondere, dass ein Wort aus L mehrfach auf das Ausgabeband geschrieben wird.

Theorem 2.20. *Eine Sprache L ist genau dann rekursiv aufzählbar, wenn ein Aufzähler für L existiert.*

Beweis. Mithilfe eines Aufzählers A für eine Sprache L kann leicht eine Turingmaschine M konstruiert werden, die L erkennt. Erhält diese Turingmaschine eine Eingabe w , so simuliert sie den Aufzähler A . Sie terminiert und akzeptiert die Eingabe w , sobald der Aufzähler das Wort w auf das Ausgabeband schreibt. Da jedes Wort $w \in L$ nach endlich vielen Schritten vom Aufzähler auf das Ausgabeband geschrieben wird, akzeptiert M jedes Wort aus L . Auf Wörtern $w \notin L$ terminiert M nicht, da diese vom Aufzähler nicht auf das Ausgabeband geschrieben werden. Somit erkennt M die Sprache L .

Sei nun andersherum eine Turingmaschine M gegeben, die die Sprache L akzeptiert. Mithilfe dieser Turingmaschine möchten wir nun einen Aufzähler A für die Sprache L konstruieren. Würde M die Sprache L entscheiden (also insbesondere auf jeder Eingabe terminieren), so könnte M einfach in einen Aufzähler umgebaut werden. Wir müssten dazu lediglich M nacheinander auf allen Wörtern aus Σ^* (zum Beispiel in kanonischer Reihenfolge) simulieren und genau die Wörter auf das Ausgabeband schreiben, die M akzeptiert. Da M die Sprache L aber nur erkennt (und somit auf Wörtern, die nicht zur Sprache gehören, im Allgemeinen nicht hält), schlägt dieser Ansatz fehl.

Stattdessen simulieren wir die Turingmaschine M in gewisser Weise für alle Wörter aus Σ^* parallel. Um dies zu präzisieren, sei wieder w_1, w_2, w_3, \dots die Aufzählung aller Wörter aus Σ^* in kanonischer Reihenfolge. Der Aufzähler A arbeitet wie folgt.

Aufzähler A für L

- 1 **for** $i = 1, 2, 3, \dots$
- 2 Simuliere jeweils i Schritte von M auf den Eingaben w_1, \dots, w_i .
- 3 Wird bei einer dieser Simulationen ein Wort w akzeptiert,
 so schreibe es auf das Ausgabeband.

Die so definierte Turingmaschine A ist ein Aufzähler für L . Sie schreibt nur Wörter auf das Ausgabeband, die von M akzeptiert werden. Somit schreibt sie keine Wörter, die nicht zu L gehören, auf das Ausgabeband. Für jedes Wort $w \in L$ gibt es ein t_w , sodass M die Eingabe w nach t_w vielen Schritten akzeptiert. Somit gibt A jedes Wort $w \in L$ für $i = t_w$ (also nach endlich vielen Schritten) aus. \square

Es ist essentiell, dass wir die Reihenfolge, in der die Wörter durch einen Aufzähler auf das Band geschrieben werden, nicht vorgeschrieben haben. Der Leser überlege sich als Übung, dass die Existenz eines *kanonischen Aufzählers*, der die Wörter einer Sprache L in kanonischer Reihenfolge auf das Band schreibt, äquivalent zu der Entscheidbarkeit von L ist.

2.6 Weitere nicht entscheidbare Probleme

Bei allen nicht entscheidbaren Probleme, die wir in dieser Vorlesung bislang kennengelernt haben, tauchten Turingmaschinen und Gödelnummern explizit in der Definition auf. Zum Abschluss dieses Kapitels wollen wir noch kurz zwei weitere nicht entscheidbare Probleme vorstellen, die auf den ersten Blick nichts mit Turingmaschinen zu tun haben.

Der Mathematiker David Hilbert hat im Jahre 1900 eine Liste von 23 zentralen offenen Problemen der Mathematik präsentiert. Eines davon (*Hilberts zehntes Problem*) war die Frage, mit welchem Algorithmus man feststellen kann, ob ein gegebenes Polynom eine ganzzahlige Nullstelle besitzt. Die Frage bezieht sich insbesondere auf multivariate Polynome, also Polynome mit mehreren Variablen. Ein solches Polynom ist die Summe von Monomen, wobei ein Monom das Produkt eines Koeffizienten mit Potenzen der Variablen ist. Sind also beispielsweise x , y und z die Variablen, so sind die Terme xy , x^2 , $10xy^2$, $-2x^2y^3z$ sowie -7 Monome und $xy + x^2 + 10xy^2 - 2x^2y^3z - 7$ ist ein Polynom.

Hilbert interessierte sich für einen Algorithmus, der entscheidet, ob es ganzzahlige Werte für die Variablen gibt, für die das Polynom den Wert 0 annimmt. 1970 hat Yuri Matiyasevich dieses Problem gelöst, allerdings anders als von Hilbert erwartet.

Theorem 2.21. *Hilberts zehntes Problem ist nicht entscheidbar.*

Den recht komplexen Beweis dieses Theorems werden wir in dieser Vorlesung nicht besprechen.

Ein anderes klassisches nicht entscheidbares Problem ist das *Postsche Korrespondenzproblem (PKP)*, das auf den ersten Blick an ein einfaches Puzzle erinnert. Eine Eingabe für dieses Problem besteht aus einer endlichen Menge K von Paaren $K = \{(x_1, y_1), \dots, (x_k, y_k)\}$ mit $x_i, y_i \in \Sigma^*$ für ein endliches Alphabet Σ . Anschaulich kann man sich ein Element (x_i, y_i) aus K als Dominostein vorstellen, der in der oberen Hälfte mit x_i und in der unteren Hälfte mit y_i beschriftet ist. Jedes Element aus K repräsentiert eine Klasse von Dominosteinen und wir gehen davon aus, dass von jeder Klasse beliebig viele Steine verfügbar sind.

Die Frage lautet nun, ob es möglich ist, Dominosteine auszuwählen und hintereinander zu legen, sodass oben und unten dieselbe Zeichenkette steht. Formaler ausgedrückt, soll entschieden werden, ob ein $n \geq 1$ und Indizes $i_1, \dots, i_n \in \{1, \dots, k\}$ existieren, sodass $x_{i_1} \dots x_{i_n} = y_{i_1} \dots y_{i_n}$ gilt.

Theorem 2.22. *Das Postsche Korrespondenzproblem ist nicht entscheidbar.*

Auch diese Theorem werden wir aus Zeitgründen nicht in dieser Vorlesung beweisen. Sein Beweis ist allerdings deutlich einfacher als der von Theorem 2.21 und wir werden in den Übungen näher darauf eingehen. Die wesentliche Idee besteht darin, dass man die Berechnung einer gegebenen Turingmaschine mithilfe geeigneter gewählter Dominosteine simulieren kann. Insbesondere kann man die Dominosteine so wählen, dass es genau dann eine Lösung für das PKP gibt, wenn die entsprechende Turingmaschine auf einer gegebenen Eingabe hält.

Komplexitätstheorie

In diesem Kapitel beschäftigen wir uns hauptsächlich mit Problemen, bei denen einfach zu sehen ist, dass sie berechenbar sind. Für praktische Anwendungen ist es aber wichtig, Probleme nicht nur in endlicher Zeit, sondern auch möglichst effizient zu lösen, da man nicht beliebig lange auf die Ausgabe eines Algorithmus warten kann. Welche Laufzeit akzeptabel ist, hängt von der Anwendung ab. Während man die Ausgabe eines Navigationsgerätes innerhalb weniger Sekunden erwartet, akzeptiert man bei manchen großen Optimierungsproblemen in der Logistik vielleicht auch eine Laufzeit von mehreren Tagen.

Wir werden zunächst formal definieren, wann wir einen Algorithmus als *effizient* betrachten. Dabei interessiert uns in erster Linie, wie seine Laufzeit von der Eingabelänge abhängt. Es hat sich bewährt, Algorithmen als effizient zu betrachten, wenn ihre Laufzeit nur höchstens polynomiell mit der Eingabelänge wächst. Probleme, für die es solche Algorithmen gibt, gehören der *Komplexitätsklasse* P an.

Anschließend beschäftigen wir uns mit *nichtdeterministischen Turingmaschinen*. Dabei handelt es sich um Turingmaschinen, die nichtdeterministische Schritte machen dürfen (analog zu nichtdeterministischen endlichen Automaten, die der Leser sich noch einmal ins Gedächtnis rufen sollte). Wir definieren dann die Komplexitätsklasse NP als die Menge der Probleme, die von solchen nichtdeterministischen Turingmaschinen in polynomieller Zeit gelöst werden können. Genauso wie nichtdeterministische endliche Automaten sind nichtdeterministische Turingmaschinen nur ein Hilfsmittel für unsere theoretischen Betrachtungen und sie entsprechen (vermutlich) keinem physikalisch realisierbaren Rechner.

Aus der Definition folgt direkt, dass $P \subseteq NP$ gilt, es ist aber bis heute unklar, ob alle Probleme aus NP auf einer (deterministischen) Turingmaschine in polynomieller Zeit gelöst werden können, ob also $P = NP$ gilt. Man vermutet, dass dies nicht der Fall ist. Wir lernen insbesondere die Klasse der *NP-schweren* Probleme kennen. Ein NP-schweres Problem hat die Eigenschaft, dass die Existenz eines effizienten Algorithmus für dieses Problem implizieren würde, dass $P = NP$ gilt. Zeigt man für ein Problem also, dass es NP-schwer ist, so kann man dies als starkes Indiz dafür werten, dass es keinen effizienten Algorithmus für dieses Problem gibt.

3.1 Die Klassen P und NP

3.1.1 Die Klasse P

Um die Klasse P formal zu definieren, erinnern wir den Leser noch einmal an Definition 1.4. Dort wird die Laufzeit $t_M(n)$ einer Turingmaschine M auf Eingaben der Länge n als $t_M(n) = \max_{w \in \Sigma^n} t_M(w)$ definiert. Somit ist $t_M(n)$ die *Worst-Case-Laufzeit* von M auf Eingaben der Länge n .

Definition 3.1. *Ein Entscheidungsproblem L gehört genau dann zu der Komplexitätsklasse P, wenn es eine Turingmaschine M gibt, die L entscheidet, und eine Konstante $k \in \mathbb{N}$, für die $t_M(n) = O(n^k)$ gilt.*

Ein Entscheidungsproblem gehört also genau dann zu der Klasse P, wenn es einen Algorithmus für das Problem gibt, dessen Worst-Case-Laufzeit sich auf einer Turingmaschine polynomiell in der Eingabelänge beschränken lässt. Wir haben bereits in Abschnitt 1.2.2 diskutiert, dass die Klassen derjenigen Probleme, die von Turingmaschinen bzw. Registermaschinen im logarithmischen Kostenmaß in polynomieller Zeit gelöst werden können, übereinstimmen. Dementsprechend hätten wir in Definition 3.1 anstatt über Turingmaschinen auch über Registermaschinen im logarithmischen Kostenmaß sprechen können.

Die Klasse P wird gemeinhin als die Klasse der effizient lösbaren Probleme angesehen, und sprechen wir im Folgenden von einem *effizienten Algorithmus*, so meinen wir damit stets einen Algorithmus, dessen Laufzeit nur höchstens polynomiell mit der Eingabelänge wächst. Solche Algorithmen nennen wir auch *polynomielle Algorithmen*. Es bedarf sicherlich einer Diskussion, ob diese Festlegung des Effizienzbegriffes sinnvoll ist. Im Allgemeinen scheint sie zumindest fragwürdig, denn selbst ein Algorithmus mit einer linearen Laufzeit von $O(n)$ für Eingaben der Länge n kann in der Praxis zu langsam sein, wenn in der O-Notation sehr große Konstanten versteckt sind. Ebenso ist ein Algorithmus mit Laufzeit $\Theta(n^{100})$ für praktische Zwecke nicht zu gebrauchen, selbst wenn in der O-Notation keine großen Konstanten verborgen sind. Auf der anderen Seite ist ein Algorithmus mit einer exponentiellen Laufzeit von $O(1,00000001^n)$ gemäß der obigen Definition nicht effizient, obwohl er in der Praxis durchaus schnell sein kann. Ebenso gibt es Algorithmen mit einer exponentiellen Laufzeit von beispielsweise $\Omega(2^n)$, die in der Praxis dennoch auch für große Eingaben schnell sind, da es zu pessimistisch ist, nur den Worst Case zu betrachten. Ein aus dem letzten Semester bekanntes Beispiel ist der Simplex-Algorithmus, der auf Worst-Case-Eingaben zwar eine exponentielle Laufzeit besitzt, aber auf typischen Eingaben, die in Anwendungen auftreten, sehr schnell ist.

Wie bei der Diskussion, die wir im letzten Semester nach der Einführung der O-Notation geführt haben, müssen wir also auch hier zugeben, dass es Fälle geben kann, in denen wir nicht das richtige Abstraktionsniveau getroffen haben. Dennoch hat es sich bewährt, Effizienz mit polynomieller Laufzeit gleichzusetzen, denn für fast alle interessanten Probleme, die in polynomieller Zeit gelöst werden können, gibt es effiziente Algorithmen, bei denen der Grad der polynomiellen Laufzeit klein ist. Das heißt, fast

alle interessanten Probleme aus der Klasse P können auch tatsächlich in praktischen Anwendungen schnell gelöst werden. Man sollte aber in Erinnerung behalten, dass es Fälle gibt, in denen es eine zu starke Vereinfachung ist, die effiziente Lösbarkeit eines Problems mit der Existenz eines polynomiellen Algorithmus gleichzusetzen.

Wir sollten ebenfalls die Einschränkung auf Entscheidungsprobleme in Definition 3.1 diskutieren. Zunächst besteht kein Grund für diese Einschränkung und man hätte P auch genauso gut als die Menge aller Probleme oder Funktionen definieren können, die in polynomieller Zeit gelöst bzw. berechnet werden können. Tatsächlich findet man solche abweichenden Definitionen auch in der Literatur. Die Einschränkung auf Entscheidungsprobleme bereitet schon auf die Definition der Klasse NP vor und sie ist nicht so gravierend, wie sie auf den ersten Blick erscheinen mag. Um dies zu illustrieren betrachten wir drei Varianten des *Cliquenproblems*, das in dieser Vorlesung später noch mehrfach auftreten wird. Bei diesem Problem ist ein ungerichteter Graph $G = (V, E)$ gegeben. Eine *Clique* in einem solchen Graphen ist eine Teilmenge $V' \subseteq V$ der Knoten, für die es zwischen jedem Paar von verschiedenen Knoten $u \in V'$ und $v \in V'$ eine Kante in E gibt. Eine Clique V' mit $k = |V'|$ nennen wir auch *k-Clique von G*.

- *Optimierungsvariante*
Eingabe: Graph $G = (V, E)$
Aufgabe: Berechne eine Clique von G mit maximaler Kardinalität.
- *Wertvariante*
Eingabe: Graph $G = (V, E)$
Aufgabe: Berechne das größte $k^* \in \mathbb{N}$, für das es eine k^* -Clique in G gibt.
- *Entscheidungsvariante*
Eingabe: Graph $G = (V, E)$ und ein Wert $k \in \mathbb{N}$
Aufgabe: Entscheide, ob es in G eine Clique der Größe mindestens k gibt.

In den meisten Anwendungen, in denen das Cliquenproblem auftritt, sind wir an der Optimierungsvariante interessiert und wollen eine größtmögliche Clique finden. Wir zeigen nun aber, dass entweder alle drei Varianten in polynomieller Zeit gelöst werden können oder gar keine. Das bedeutet, es genügt, nur die Komplexität der Entscheidungsvariante zu untersuchen.

Theorem 3.2. *Entweder gibt es für alle drei Varianten des Cliquenproblems polynomielle Algorithmen oder für gar keine.*

Beweis. Mit einem polynomiellen Algorithmus für die Optimierungsvariante des Cliquenproblems können wir offensichtlich auch die Wertvariante in polynomieller Zeit lösen. Dazu müssen wir nur die Kardinalität der gefundenen größtmöglichen Clique ausgeben. Ebenso können wir einfach mit einem polynomiellen Algorithmus für die Wertvariante auch die Entscheidungsvariante in polynomieller Zeit lösen, indem wir einfach die berechnete maximale Cliquengröße k^* mit der übergebenen Zahl k vergleichen. Nicht trivial sind lediglich die Rückrichtungen.

Zunächst zeigen wir, wie wir aus einem polynomiellen Algorithmus A für die Entscheidungsvariante des Cliquesproblems einen polynomiellen Algorithmus für die Wertvariante konstruieren können. Sei dazu G ein Graph mit N Knoten, für den wir die Größe k^* der maximalen Clique bestimmen wollen. Die genaue Eingabegröße hängt von der Codierung von G ab. Wir gehen der Einfachheit halber davon aus, dass G als Adjazenzmatrix gegeben ist und für die Eingabelänge dementsprechend $n = N^2$ gilt. Sei $A(G, k) \in \{0, 1\}$ die Ausgabe von Algorithmus A bei Eingabe (G, k) . Dabei bedeute $A(G, k) = 1$, dass es in dem Graphen G eine Clique der Größe mindestens k gibt. Um die Wertvariante des Cliquesproblems für den gegebenen Graphen G zu lösen, berechnen wir $k^* = \max\{k \in \{1, \dots, N\} \mid A(G, k) = 1\}$ mithilfe von maximal N Aufrufen des Algorithmus A . Das Maximum k^* ist per Definition der Wert, den wir suchen. Da A ein polynomieller Algorithmus ist, gibt es eine Konstante $\alpha \in \mathbb{N}$, für die wir die Laufzeit zur Berechnung von k^* mit $O(N \cdot (n')^\alpha)$ abschätzen können, wobei n' die Eingabegröße von (G, k) ist. Es gilt $n' \leq N^2 + \lceil \log_2(N) \rceil = O(N^2)$, da G mit N^2 Bits und $k \in \{1, \dots, N\}$ mit $\lceil \log_2(N) \rceil$ Bits codiert werden kann. Dementsprechend beträgt die Laufzeit, die wir zur Berechnung von k^* benötigen, $O(N \cdot (N^2)^\alpha) = O(n^{\alpha+1})$. Diese Laufzeit ist, wie gewünscht, polynomiell in der Eingabelänge n .

Nun fehlt nur noch die Umwandlung eines polynomiellen Algorithmus für die Wertvariante in einen polynomiellen Algorithmus für die Optimierungsvariante. Sei dazu G ein Graph mit N Knoten, für den wir eine Clique mit maximaler Kardinalität bestimmen wollen. Sei nun A ein Algorithmus, der die Wertvariante des Cliquesproblems in polynomieller Zeit löst. Wir bezeichnen mit $A(G)$ die Ausgabe von Algorithmus A bei Eingabe G und konstruieren einen Algorithmus A_{opt} , der mithilfe von A die Optimierungsvariante löst. Dieser Algorithmus ist im folgenden Pseudocode dargestellt und er benutzt das Konzept eines *induzierten Teilgraphen*. Für einen Graphen $G = (V, E)$ ist der durch $V' \subseteq V$ induzierte Teilgraph der Graph $G' = (V', E')$ mit $E' = \{(u, v) \in E \mid u, v \in V'\}$. Es ist also der Teilgraph von G mit Knotenmenge V' , der genau die Kanten aus E enthält, die innerhalb der Menge V' verlaufen.

```

Aopt(G)
1   $k^* = A(G)$ ;
2   $V' := V = \{v_1, \dots, v_N\}$ ;
3  for ( $i = 1$ ;  $i \leq N$ ;  $i++$ )
4       $G'$  sei induzierter Teilgraph von  $G$  mit Knotenmenge  $V' \setminus \{v_i\}$ .
5      if ( $A(G') == k^*$ )  $V' := V' \setminus \{v_i\}$ ;
6  return  $V'$ ;

```

Man beweist leicht per Induktion die Invariante, dass es zu jedem Zeitpunkt eine k^* -Clique gibt, die komplett in der aktuellen Knotenmenge V' enthalten ist. Ferner kann man leicht argumentieren, dass ein Knoten, der in Zeile 5 nicht aus der Menge V' entfernt wird, in jeder k^* -Clique $V^* \subseteq V'$ enthalten sein muss. Daraus folgt mit kurzer Argumentation, dass die Menge V' am Ende genau aus einer k^* -Clique besteht. Die Details dieser Argumentation überlassen wir dem Leser als Übung.

Die Laufzeit von A_{opt} ist durch $O(N \cdot (N^2)^\alpha)$ nach oben beschränkt, wenn die Laufzeit von A auf Graphen mit N Knoten durch $O((N^2)^\alpha)$ nach oben beschränkt ist. Somit

ist die Laufzeit von A_{opt} polynomiell in der Eingabelänge $n = N^2$ beschränkt. \square

Wir haben in dem obigen Beweis relativ genau die Anzahl an Bits angegeben, die benötigt werden, um eine Eingabe zu codieren. Der Leser sollte sich aber klar machen, dass das vorangegangene Theorem robust gegenüber Änderungen der Codierung ist. Es gilt also beispielsweise auch, wenn die Graphen als Adjazenzlisten codiert sind oder wenn die Zahlen nicht binär sondern dezimal codiert sind. Für die allermeisten Optimierungsprobleme, die wir bislang kennengelernt haben, kann man analog drei verschiedene Varianten definieren (man denke zum Beispiel an das Kürzeste-Wege-Problem, an Flussprobleme oder an das Rucksackproblem). Genauso wie beim Cliquesproblem kann man für all diese Probleme nachweisen, dass die drei Varianten im Sinne polynomieller Berechenbarkeit äquivalent sind.

Nebenbei sei angemerkt, dass wir Theorem 3.2 mittels zweier spezieller Turing-Reduktionen bewiesen haben. Wir haben erst gezeigt, wie die Wertvariante auf die Entscheidungsvariante reduziert werden kann und anschließend wie die Optimierungsvariante auf die Wertvariante reduziert werden kann. Die wesentliche Eigenschaft dieser Reduktionen ist, dass sie nicht nur berechenbar sind, sondern auch in polynomieller Zeit berechnet werden können. Solche sogenannten *polynomiellen Reduktionen* werden wir später noch ausführlich besprechen.

Aus den oben diskutierten Gründen konzentrieren wir uns im Folgenden nur noch auf Entscheidungsprobleme und wir betrachten zum Abschluss dieses Abschnittes noch ein paar Beispiele.

- Wir haben uns im letzten Semester mit dem Problem beschäftigt, für einen Graphen zu testen, ob er zusammenhängend ist oder nicht. Mithilfe einer Tiefensuche kann man dies für Graphen mit n Knoten in Zeit $O(n^2)$ entscheiden, wenn der Graph als Adjazenzmatrix gegeben ist. Diese Laufzeit bezieht sich allerdings auf das uniforme Kostenmaß. Im logarithmischen Kostenmaß beträgt die Laufzeit $O(n^2 \log n)$, da wir $O(\log n)$ Bits benötigen, um den Index eines Knotens zu codieren. Diese Laufzeit ist polynomiell in der Eingabelänge n^2 beschränkt und damit gehört das Zusammenhangsproblem zu P. Generell trifft dies auf alle Graphenprobleme zu, die mit Algorithmen gelöst werden können, deren Laufzeit polynomiell in der Anzahl der Knoten und Kanten beschränkt ist.
- Ein weiteres Problem aus dem letzten Semester ist das Problem, einen minimalen Spannbaum zu berechnen. Bei diesem Problem besteht die Eingabe aus einem ungerichteten Graphen $G = (V, E)$ mit Kantengewichten $w: E \rightarrow \mathbb{N}$. Um dieses Problem in ein Entscheidungsproblem zu transformieren, erweitern wir die Eingabe um einen Wert $z \in \mathbb{N}$ und stellen die Frage, ob G einen Spannbaum mit Gewicht höchstens z besitzt. Der Leser sollte sich überlegen, dass die Optimierungsvariante des Spannbaumproblems genau dann in polynomieller Zeit gelöst werden kann, wenn dies für die Entscheidungsvariante der Fall ist.

Für zusammenhängende Graphen mit n Knoten und $m \geq n - 1$ Kanten löst der Algorithmus von Kruskal das Spannbaumproblem in Zeit $O(m \log m)$ im

uniformen Kostenmaß, wenn der Graph als Adjazenzliste gegeben ist. Im logarithmischen Kostenmaß ist die Abschätzung der Laufzeit aufwendiger. Zunächst müssen die Kanten gemäß ihrem Gewicht sortiert werden. Benutzt man dazu Mergesort, so beträgt die Laufzeit für das Sortieren $O(m \log(m) \log(W))$ für $W = \max_{e \in E} w(e)$, da die Laufzeit durch die $O(m \log m)$ wesentlichen Vergleiche dominiert wird, die im logarithmischen Kostenmaß jeweils eine Laufzeit von $O(\log W)$ benötigen. Die Kosten für die restlichen Schritte des Algorithmus von Kruskal können wir im uniformen Kostenmaß durch $O(m \log m)$ und im logarithmischen Kostenmaß durch $O(m \log(m) \log(n))$ beschränken. Der zusätzliche Faktor resultiert wieder aus der Tatsache, dass wir $O(\log n)$ Bits benötigen, um den Index eines Knotens zu speichern. Insgesamt ergibt sich damit eine Laufzeit von $O(m \log m \cdot \max\{\log(W), \log(n)\})$. Die Eingabelänge beträgt $\Omega(m \log(n) + \log(W))$, da wir zur Codierung einer Kante $\Omega(\log(n))$ viele Bits benötigen und $\Omega(\log(W))$ Bits zur Codierung des maximalen Gewichtes W . Es gilt

$$m \log m \cdot \max\{\log(W), \log(n)\} = O((m \log(n) + \log(W))^2)$$

und somit ist die Laufzeit des Algorithmus von Kruskal polynomiell in der Eingabelänge beschränkt.

- Man kann die Entscheidungsvariante des Cliquesproblems lösen, indem man für einen gegebenen Graphen $G = (V, E)$ und eine gegebene Zahl $k \in \mathbb{N}$ alle Teilmengen von V der Größe k daraufhin testet, ob sie eine Clique bilden. Da es $\binom{n}{k} \geq (n/k)^k$ solcher Teilmengen gibt, besitzt dieser Algorithmus eine Laufzeit von $\Omega((n/k)^k)$, was sich nicht polynomiell in der Eingabelänge $O(n^2 + \log k)$ beschränken lässt. Damit ist natürlich nicht bewiesen, dass die Entscheidungsvariante des Cliquesproblems nicht zu der Klasse P gehört, sondern nur, dass der obige einfache Algorithmus keine polynomielle Laufzeit besitzt. Tatsächlich werden wir sehen, dass das Cliquesproblem NP-schwer ist. Es ist demnach bis heute unklar, ob das Cliquesproblem in polynomieller Zeit gelöst werden kann.
- Wir betrachten als letztes Beispiel die Entscheidungsvariante des Rucksackproblems. Sei eine Eingabe für das Rucksackproblem mit Nutzenwerten $p_1, \dots, p_N \in \mathbb{N}$, Gewichten $w_1, \dots, w_N \in \mathbb{N}$ und einer Kapazität $t \in \mathbb{N}$ gegeben. Um ein Entscheidungsproblem zu erhalten, erweitern wir diese Eingabe um einen Wert $z \in \mathbb{N}$ und fragen, ob es eine Teilmenge $I \subseteq \{1, \dots, N\}$ der Objekte mit $\sum_{i \in I} w_i \leq t$ und $\sum_{i \in I} p_i \geq z$ gibt. Wieder sollte der Leser sich als Übung überlegen, dass die Optimierungsvariante des Rucksackproblems genau dann in polynomieller Zeit gelöst werden kann, wenn dies für die Entscheidungsvariante der Fall ist. Im vergangenen Semester haben wir die Optimierungsvariante des Rucksackproblems mithilfe dynamischer Programmierung in Zeit $O(N^2W)$ für $W = \max_i w_i$ gelöst. Dementsprechend kann auch die Entscheidungsvariante in dieser Zeit gelöst werden. Auch diese Laufzeit bezog sich auf das uniforme Kostenmaß. Im logarithmischen Kostenmaß ergibt sich eine Laufzeit von $O(N^2W \log P)$ für $P = \sum_i p_i$. Ist dies eine polynomielle Laufzeit? Um diese Frage zu beantworten, müssen wir uns zunächst überlegen, wie die Größen N , W und P mit der Eingabelänge in

Beziehung stehen. Typischerweise werden Zahlen in der Eingabe binär codiert. Betrachten wir den Spezialfall, dass alle Nutzenwerte p_i , alle Gewichte w_i und die Kapazität t Zahlen sind, die binär mit jeweils $N \in \mathbb{N}$ Bits codiert werden können. Dann kann W Werte bis $2^N - 1$ annehmen, P kann Werte bis $N(2^N - 1)$ annehmen und die Eingabelänge beträgt $n = (2N + 1)N$. Dieser Spezialfall zeigt bereits, dass die Laufzeitschranke $O(N^2W \log P) = O(N^3(2^N - 1))$ im Allgemeinen nicht polynomiell in der Eingabelänge beschränkt ist. Wir werden sehen, dass auch das Rucksackproblem NP-schwer ist.

3.1.2 Die Klasse NP

Um die Komplexitätsklasse NP zu definieren, formalisieren wir zunächst den Begriff einer nichtdeterministischen Turingmaschine.

Definition 3.3. *Bei einer nichtdeterministischen Turingmaschine (NTM) handelt es sich um ein 7-Tupel $(Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$, bei dem alle Komponenten bis auf δ identisch mit denen einer (deterministischen) Turingmaschine aus Definition 1.1 sind. Bei δ handelt es sich nun nicht mehr um eine Zustandsüberföhrungsfunktion, sondern um eine Zustandsüberföhrungsrelation*

$$\delta \subseteq ((Q \setminus \{\bar{q}\}) \times \Gamma) \times (Q \times \Gamma \times \{L, N, R\}).$$

Das Verhalten einer deterministischen Turingmaschine gemäß Definition 1.1 ist durch die Funktion δ eindeutig bestimmt. Liest die Turingmaschine in einem Zustand $q \in Q \setminus \{\bar{q}\}$ ein Zeichen $a \in \Gamma$, so gibt $\delta(q, a) = (q', a', D)$ mit $q' \in Q$, $a' \in \Gamma$ und $D \in \{L, N, R\}$ das Verhalten vor: die Turingmaschine ersetzt das Zeichen an der aktuellen Kopfposition durch a' , wechselt in den Zustand q' und bewegt den Kopf gemäß D .

Das Verhalten einer nichtdeterministischen Turingmaschine M ist im Allgemeinen nicht eindeutig bestimmt. Für einen Zustand $q \in Q \setminus \{\bar{q}\}$ und ein Zeichen $a \in \Gamma$ kann es mehrere Tripel $(q', a', D) \in Q \times \Gamma \times \{L, N, R\}$ geben, für die $((q, a), (q', a', D)) \in \delta$ gilt. Die nichtdeterministische Turingmaschine kann dann eines davon wählen und den entsprechenden Schritt ausführen. Für eine gegebene Konfiguration gibt es bei einer nichtdeterministischen Turingmaschine also im Allgemeinen mehrere erlaubte Nachfolgekonfigurationen.

Es kann auch passieren, dass es für ein Paar (q, a) gar kein Tripel (q', a', D) gibt, für das $((q, a), (q', a', D)) \in \delta$ gilt. Dann gibt es für die aktuelle Konfiguration keine gültige Nachfolgekonfiguration. Dies definieren wir als gleichbedeutend damit, dass die Turingmaschine die Eingabe verwirft. Alternativ könnten wir auch für jedes solche Paar (q, a) das Tupel $((q, a), (\bar{q}, 0, N))$ zur Relation δ hinzufügen.

Da die Rechenschritte einer nichtdeterministischen Turingmaschine nicht eindeutig sind, kann es bei derselben Eingabe im Allgemeinen verschiedene mögliche Ausgaben geben. Insbesondere kann es bei einem Entscheidungsproblem Eingaben geben, für die es sowohl einen Rechenweg zu einer akzeptierenden Endkonfiguration (d. h. zu einer Konfiguration, bei der unter dem Kopf das Zeichen 1 steht) als auch einen Rechenweg

zu einer verwerfenden Endkonfiguration gibt. Dabei ist ein *Rechenweg* eine Folge von gültigen Rechenschritten der Turingmaschine ausgehend von der Startkonfiguration. Wir erinnern uns daran, dass dieselbe Problematik schon bei nichtdeterministischen Automaten aufgetreten ist. Dort haben wir gesagt, dass ein nichtdeterministischer Automat ein Wort akzeptiert, wenn es mindestens einen Rechenweg gibt, der zu einem akzeptierenden Endzustand führt. Genau diese Definition übernehmen wir auch für Turingmaschinen.

Definition 3.4. *Eine nichtdeterministische Turingmaschine M akzeptiert eine Eingabe $w \in \Sigma^*$, wenn es einen mindestens einen Rechenweg von M gibt, der bei Eingabe w zu einer akzeptierenden Endkonfiguration (d. h. zu einer Konfiguration, bei der unter dem Kopf das Zeichen 1 steht) führt. Wieder definieren wir $L(M) \subseteq \Sigma^*$ als die Menge der von M akzeptierten Eingaben und wir sagen, dass M die Sprache $L(M)$ entscheidet.*

Genauso wie die Ausgabe von den nichtdeterministischen Entscheidungen der Turingmaschine abhängen kann, kann auch die Laufzeit stark davon abhängen. Wir interessieren uns bei einer nichtdeterministischen Turingmaschine grundsätzlich nur für die Laufzeit auf Eingaben, die sie akzeptiert, und definieren die Laufzeit über den kürzesten Rechenweg zu einer akzeptierenden Endkonfiguration.

Definition 3.5. *Die Laufzeit $t_M(w)$ einer nichtdeterministischen Turingmaschine M auf einer Eingabe $w \in L(M)$ ist definiert als die Länge des kürzesten Rechenweges, der bei Eingabe w zu einer akzeptierenden Endkonfiguration führt. Für Eingaben $w \notin L(M)$ sei $t_M(w) = 0$. Wieder sei $t_M(n) = \max_{w \in \Sigma^n} t_M(w)$ die Worst-Case-Laufzeit für Eingaben der Länge $n \in \mathbb{N}$.*

Der Leser wird sich an dieser Stelle vermutlich fragen, warum nichtdeterministische Turingmaschinen interessant sind und warum wir ihre Laufzeit auf die obige unnatürliche Art definiert haben. Wir erinnern noch einmal daran, dass das Modell der nichtdeterministischen Turingmaschine nur ein Hilfsmittel für die Analyse der Komplexität von Problemen ist und nicht mit dem Ziel definiert wurde, reale Rechner zu modellieren. Wir definieren nun die Klasse NP als das Äquivalent zu der Klasse P für nichtdeterministische Turingmaschinen.

Definition 3.6. *Ein Entscheidungsproblem L gehört genau dann zu der Komplexitätsklasse NP, wenn es eine nichtdeterministische Turingmaschine M gibt, die L entscheidet, und eine Konstante $k \in \mathbb{N}$, für die $t_M(n) = O(n^k)$ gilt.*

Zur Veranschaulichung betrachten wir zwei Beispiele für Probleme aus der Klasse NP.

Theorem 3.7. *Die Entscheidungsvarianten des Cliquenproblems und des Rucksackproblems liegen in NP.*

Beweis. Bei der Entscheidungsvariante des Cliquenproblems besteht die Eingabe aus einem ungerichteten Graphen $G = (V, E)$ mit n Knoten sowie einer Zahl $k \in \mathbb{N}$ und es soll entschieden werden, ob es in G eine Clique der Größe mindestens k gibt.

Wir konstruieren eine nichtdeterministische Turingmaschine M für dieses Problem, die in zwei Phasen arbeitet. In der ersten Phase nutzt sie den Nichtdeterminismus und wählt eine beliebige Teilmenge der Knoten aus. In der zweiten Phase arbeitet sie deterministisch und überprüft, ob mindestens k Knoten ausgewählt wurden und diese eine Clique bilden. Ist dies der Fall, so akzeptiert sie, ansonsten verwirft sie die Eingabe.

Die erste Phase kann beispielsweise dadurch realisiert werden, dass die Turingmaschine zunächst deterministisch n Rauten auf das Band schreibt, den Kopf auf die erste Raute verschiebt und in einen speziellen Zustand q wechselt, in dem die Übergänge $((q, \#), (q, 0, R)) \in \delta$ und $((q, \#), (q, 1, R)) \in \delta$ erlaubt sind. Dies führt dazu, dass in den nächsten n Schritten eine beliebige Zeichenkette $x \in \{0, 1\}^n$ auf das Band geschrieben werden kann. Diese kann als Auswahl der Knoten interpretiert werden. Abgesehen von diesen Übergängen sind alle anderen Schritte der Turingmaschine deterministisch, d. h. der komplette Nichtdeterminismus ist in der Zeichenkette x enthalten.

Die soeben beschriebene Turingmaschine akzeptiert eine Eingabe genau dann, wenn es in dem Graphen $G = (V, E)$ eine Clique der Größe mindestens k gibt. Um dies zu sehen, betrachten wir zunächst eine Eingabe, für die dies der Fall ist. Sei $V' \subseteq V$ eine Clique der Größe mindestens k . Wählt die Turingmaschine diese Teilmenge in Phase 1 nichtdeterministisch aus, so akzeptiert sie die Eingabe in Phase 2. Enthält auf der anderen Seite der Graph G keine Clique der Größe mindestens k , so führt jede in Phase 1 ausgewählte Teilmenge dazu, dass die Eingabe verworfen wird, da sie entweder zu klein ist oder keine Clique bildet.

Die Laufzeit interessiert uns gemäß Definition 3.5 nur für Eingabe (G, k) , für die G eine Clique der Größe mindestens k enthält, da sie ansonsten als 0 definiert ist. Sei also (G, k) eine solche Eingabe. Phase 1 kann in polynomieller Zeit durchgeführt werden, da nur die Zeichenkette $\#^n$ auf das Band geschrieben wird und anschließend genau n nichtdeterministische Schritte erfolgen. Zu Beginn von Phase 2 ist bereits eine Teilmenge der Knoten ausgewählt. Es muss nur getestet werden, ob sie mindestens k Elemente enthält und zwischen jedem Paar von ausgewählten Knoten eine Kante verläuft. Auch dies geht in polynomieller Zeit. Damit ist insgesamt gezeigt, dass die Entscheidungsvariante des Cliquesproblems in NP liegt.

Der Beweis, dass die Entscheidungsvariante des Rucksackproblems in NP liegt, kann vollkommen analog geführt werden. Auch für dieses Problem kann eine nichtdeterministische Turingmaschine konstruiert werden, die in zwei Phasen arbeitet. In der ersten Phase wählt sie eine beliebige Teilmenge der Objekte nichtdeterministisch aus und in der zweiten Phase überprüft sie, ob das Gewicht dieser Teilmenge die Kapazität nicht überschreitet und ob die Teilmenge den vorgegebenen Nutzen erreicht. \square

Sei $\text{CLIQUE} \subseteq \{0, 1\}^*$ die Sprache aller Paare (G, k) , wobei G ein Graph ist, der eine Clique der Größe mindestens k enthält. Wir gehen davon aus, dass das Paar (G, k) auf eine naheliegende Art über dem Alphabet $\{0, 1\}$ codiert ist. Den ersten Teil des vorangegangenen Theorems können wir dann auch kurz als $\text{CLIQUE} \in NP$ schreiben. Im Beweis haben wir den Nichtdeterminismus nur dazu genutzt, eine Zeichenkette $x \in \{0, 1\}^n$ zu erzeugen, die eine Teilmenge der Knoten beschreibt. Für einen

gegebenen Graphen G , der eine Clique der Größe mindestens k enthält, kann man diese Zeichenkette als ein *Zertifikat* für $(G, k) \in \text{CLIQUE}$ auffassen. Die zweite Phase kann man dann als Verifikation des Zertifikat betrachten. Die wesentlichen Eigenschaften sind, dass diese Verifikation in polynomieller Zeit durchgeführt werden kann, dass es für jede Eingabe $(G, k) \in \text{CLIQUE}$ mindestens ein gültiges Zertifikat gibt und dass es für keine Eingabe $(G, k) \notin \text{CLIQUE}$ ein gültiges Zertifikat gibt. Diese Einsicht kann man auf beliebige Sprachen aus NP übertragen und erhält eine Charakterisierung der Klasse NP, in der nichtdeterministische Turingmaschinen nicht vorkommen.

Theorem 3.8. *Eine Sprache $L \subseteq \Sigma^*$ ist genau dann in der Klasse NP enthalten, wenn es eine deterministische Turingmaschine V (einen Verifizierer), deren Worst-Case-Laufzeit polynomiell beschränkt ist, und ein Polynom p gibt, sodass für jede Eingabe $x \in \Sigma^*$ gilt*

$$x \in L \iff \exists y \in \{0, 1\}^* : |y| \leq p(|x|) \text{ und } V \text{ akzeptiert } x\#y.$$

Dabei sei $\#$ ein beliebiges Zeichen, das zum Eingabealphabet des Verifizierers, aber nicht zu Σ gehört.

Beweis. Sei $L \in \text{NP}$. Dann gibt es eine nichtdeterministische Turingmaschine $M = (Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$, die L entscheidet, und ein Polynom r , für das $t_M(n) \leq r(n)$ gilt. Wir konstruieren nun einen deterministischen Verifizierer V für L , der die nichtdeterministische Turingmaschine M simuliert. Dabei gibt das Zertifikat y die nichtdeterministischen Entscheidungen vor.

In jeder Konfiguration kann die Turingmaschine M zwischen maximal $\ell := 3|Q||\Gamma|$ möglichen Rechenschritten wählen, da es für jedes Paar $(q, a) \in Q \setminus \{\bar{q}\} \cup \Gamma$ maximal ℓ viele Tripel $(q', a', D) \in Q \times \Gamma \times \{L, N, R\}$ mit $((q, a), (q', a', D)) \in \delta$ gibt. Wir gehen davon aus, dass die Tripel aus $Q \times \Gamma \times \{L, N, R\}$ beliebig nummeriert sind. Dann kann jeder Rechenschritt durch eine Zahl aus der Menge $\{1, \dots, \ell\}$ beschrieben werden. Eine solche Zahl kann mit $\ell^* := \lceil \log_2 \ell \rceil$ Bits codiert werden, was für eine gegebene Turingmaschine M eine Konstante ist. Der Verifizierer V erhalte die Eingabe $x\#y$ für ein Zertifikat $y \in \{0, 1\}^m$. Ist die Länge m des Zertifikates nicht durch ℓ^* teilbar oder echt größer als $\ell^*r(|x|)$, so verwirft der Verifizierer die Eingabe $x\#y$. Ansonsten zerlegt er das Zertifikat y in eine Folge von Zeichenketten der Länge jeweils ℓ^* und interpretiert diese als Folge $\alpha_1, \dots, \alpha_{m'}$ von Zahlen aus der Menge $\{1, \dots, \ell\}$, die jeweils einen Rechenschritt von M beschreiben. Beschreibt eine der Zeichenketten eine Zahl größer als ℓ , so verwirft der Verifizierer die Eingabe $x\#y$.

Der Verifizierer V simuliert das Verhalten von M auf der Eingabe x . In Schritt i versucht er den durch α_i beschriebenen Rechenschritt auszuführen. Ist dieser gemäß δ nicht erlaubt, so verwirft er die Eingabe $x\#y$. Sind alle durch $\alpha_1, \dots, \alpha_{m'}$ beschriebenen Schritte erlaubt, so testet der Verifizierer V , ob nach diesen m' Schritten eine akzeptierende Endkonfiguration erreicht wird (d. h. die Turingmaschine M befindet sich im Zustand \bar{q} und unter dem Kopf steht das Zeichen 1). Er akzeptiert die Eingabe $x\#y$, wenn dies der Fall ist, und verwirft sie ansonsten.

Wählen wir $p(n) = \ell^*r(n) = O(r(n))$, so erfüllt dieser Verifizierer die gewünschten Eigenschaften. Zu einer Eingabe $x \in \Sigma^*$ existiert genau dann ein Zertifikat $y \in \{0, 1\}^*$ mit $|y| \leq p(|x|)$, für das V die Eingabe $x\#y$ akzeptiert, wenn es einen Rechenweg

der nichtdeterministischen Turingmaschine M der Länge höchstens $r(|x|)$ gibt, der bei Eingabe w zu einer akzeptierenden Endkonfiguration führt. Dies ist genau dann der Fall, wenn M die Eingabe x akzeptiert, was gleichbedeutend mit $x \in L$ ist.

Sei nun eine Sprache L gegeben, für die es ein Polynom p und einen Verifizierer V mit den geforderten Eigenschaften gibt. Wir konstruieren daraus eine nichtdeterministische Turingmaschine M für die Sprache L , die auf einer Eingabe x wie folgt arbeitet. In der ersten Phase erzeugt sie nichtdeterministisch ein beliebiges Zertifikat $y \in \{0, 1\}^*$ mit $|y| \leq p(|x|)$. In der zweiten Phase simuliert sie den Verifizierer V auf der Eingabe $x\#y$ und akzeptiert genau dann die Eingabe x , wenn V die Eingabe $x\#y$ akzeptiert. Die Laufzeit der Turingmaschine M ist polynomiell beschränkt, da das Erzeugen von y in Zeit $O(p(|x|))$ erfolgt und der Verifizierer ebenfalls eine polynomielle Laufzeit besitzt.

Die Turingmaschine M akzeptiert ein Wort x genau dann, wenn es zu L gehört. Denn für jedes Wort $x \in L$ gibt es mindestens ein Zertifikat y (d. h. mindestens einen Rechenweg von M), der zu einer akzeptierenden Endkonfiguration führt. Andererseits gibt es für kein $x \notin L$ ein solches Zertifikat, das heißt, jedes solche Wort wird von M unabhängig von der nichtdeterministischen Wahl von y verworfen. Damit ist insgesamt gezeigt, dass M die Sprache L in polynomieller Zeit entscheidet. Somit gehört L zu NP. \square

3.1.3 P versus NP

Wir haben die Klassen P und NP kennengelernt, aber bislang noch nichts über ihren Zusammenhang ausgesagt. Direkt aus den Definitionen folgt, dass $P \subseteq NP$ gilt, denn gibt es für eine Sprache eine polynomielle deterministische Turingmaschine M , so kann man diese auch als nichtdeterministische Turingmaschine auffassen, die vom Nichtdeterminismus keinen Gebrauch macht.

Es stellt sich nun die Frage, wie groß die Klasse NP ist. Da wir sie über nichtdeterministische Turingmaschinen definiert haben, die (vermutlich) kein physikalisch realisierbares Rechnermodell darstellen, wäre es prinzipiell sogar möglich, dass selbst nicht entscheidbare Sprachen zu NP gehören. Wir werden als erstes beweisen, dass dies nicht der Fall ist, da jede Sprache aus NP in exponentieller Zeit von einer deterministischen Turingmaschine entschieden werden kann.

Theorem 3.9. *Für jede Sprache $L \in NP$ gibt es eine deterministische Turingmaschine M , die L entscheidet, und ein Polynom r , für das $t_M(n) \leq 2^{r(n)}$ gilt.*

Beweis. Es sei $L \in NP$ beliebig. Dann gibt es gemäß Theorem 3.8 ein Polynom p und einen polynomiellen Verifizierer V , sodass für jede Eingabe $x \in \Sigma^*$

$$x \in L \iff \exists y \in \{0, 1\}^* : |y| \leq p(|x|) \text{ und } V \text{ akzeptiert } x\#y$$

gilt. Wir konstruieren nun eine deterministische Turingmaschine M für die Sprache L , die bei einer Eingabe x den Verifizierer V für alle möglichen Zertifikate $y \in \{0, 1\}^*$ mit $|y| \leq p(|x|)$ auf der Eingabe $x\#y$ simuliert. Sie akzeptiert die Eingabe x genau

dann, wenn der Verifizierer in mindestens einer dieser Simulation akzeptiert hat. Aus der Eigenschaft des Verifizierers folgt direkt, dass die so konstruierte Turingmaschine M die Sprache L entscheidet. Sie akzeptiert eine Eingabe x nämlich genau dann, wenn ein gültiges Zertifikat y existiert.

Da es sich bei V um eine polynomielle deterministische Turingmaschine handelt, kann sie für eine gegebene Eingabe $x\#y$ mit $|y| \leq p(|x|)$ in Zeit $r'(|x|)$ für ein Polynom r' simuliert werden. Die Gesamtlaufzeit der Turingmaschine M ist dann durch $O(r'(|x|) \cdot 2^{p(|x|)})$ nach oben beschränkt, da es $\sum_{i=0}^{p(|x|)} 2^i = 2^{p(|x|)+1} - 1 = O(2^{p(|x|)})$ viele Zertifikate y gibt, die getestet werden. Für ein geeignetes Polynom r gilt $O(r'(|x|) \cdot 2^{p(|x|)}) = 2^{r(|x|)}$. \square

Das vorangegangene Theorem zeigt, dass nichtdeterministische Turingmaschinen durch deterministische Turingmaschinen und damit auch durch reale Rechner simuliert werden können. Dabei kann sich die Laufzeit aber drastisch vergrößern und aus polynomiellen nichtdeterministischen Turingmaschinen können exponentielle deterministische Turingmaschinen werden. Es stellt sich nun die Frage, ob dies so sein muss, oder ob es eine bessere Möglichkeit gibt, nichtdeterministische Turingmaschinen durch deterministische zu simulieren, bei der kein so großer Zeitverlust auftritt.

Formaler formuliert ist dies die Frage, ob $P = NP$ gilt oder ob es Sprachen aus NP gibt, die nicht in P enthalten sind. Dies ist die größte offene Frage der theoretischen Informatik. Auf ihre Lösung wurde vom Clay Mathematics Institute sogar ein Preisgeld in Höhe von einer Million US-Dollar ausgelobt. Wenn man die alternative Charakterisierung von NP in Theorem 3.8 betrachtet, scheint die Hypothese $P \neq NP$ naheliegend, da es intuitiv einfacher erscheint, ein Zertifikat auf Korrektheit zu prüfen als ein Zertifikat aus einer exponentiell großen Menge zu finden. Ein Beweis ist das aber natürlich nicht, obwohl auch die Mehrheit der Forscher im Bereich der theoretischen Informatik glaubt, dass $P \neq NP$ gilt.

3.2 NP-Vollständigkeit

Aus unserer bisherigen Diskussion geht noch nicht hervor, warum es überhaupt interessant ist, sich mit der Klasse NP zu beschäftigen. Wir wissen beispielsweise, dass die Entscheidungsvariante des Cliquesproblems zu NP gehört. Die einzige Konsequenz für die Komplexität des Cliquesproblems, die wir bislang daraus ziehen können, ist, dass es gemäß Theorem 3.9 in exponentieller Zeit gelöst werden kann. Dies sieht man aber auch leicht direkt ein, ohne den Umweg über NP gehen zu müssen.

Die Bedeutung der Klasse NP entsteht erst dadurch, dass es Probleme aus NP gibt (die Entscheidungsvariante des Cliquesproblems ist ein Beispiel), auf die sich alle anderen Probleme aus NP in polynomieller Zeit reduzieren lassen. Diese Probleme nennt man NP -vollständige Probleme. Das bedeutet, dass ein polynomieller Algorithmus für ein solches Problem implizieren würde, dass man alle Probleme aus NP in polynomieller Zeit lösen kann. Geht man also von der Hypothese $P \neq NP$ aus und zeigt, dass ein gegebenes Problem NP -vollständig ist, so bedeutet das, dass man dieses Problem nicht effizient lösen kann. Dies werden wir im Folgenden präzisieren.

Definition 3.10. Eine polynomielle Reduktion einer Sprache $A \subseteq \Sigma_1^*$ auf eine Sprache $B \subseteq \Sigma_2^*$ ist eine Many-One-Reduktion $f: \Sigma_1^* \rightarrow \Sigma_2^*$, die in polynomieller Zeit berechnet werden kann. Existiert eine solche Reduktion, so heißt A auf B polynomiell reduzierbar und wir schreiben $A \leq_p B$.

Wir erinnern noch einmal daran, dass bei einer Many-One-Reduktion f

$$x \in A \iff f(x) \in B$$

für alle $x \in \Sigma_1^*$ gilt. Dass die Many-One-Reduktion $f: \Sigma_1^* \rightarrow \Sigma_2^*$ in polynomieller Zeit berechnet werden kann, bedeutet formal, dass es eine Turingmaschine M und ein $k \in \mathbb{N}$ gibt, sodass M zu jedem $x \in \Sigma_1^*$ die Ausgabe $f(x)$ in Zeit $t_M(|x|) = O(|x|^k)$ berechnet.

Analog zu Theorem 2.9 können wir das folgende Resultat für polynomielle Reduktionen festhalten.

Theorem 3.11. Es seien $A \subseteq \Sigma_1^*$ und $B \subseteq \Sigma_2^*$ zwei Sprachen, für die $A \leq_p B$ gilt. Ist $B \in \mathcal{P}$, so ist auch $A \in \mathcal{P}$. Ist $A \notin \mathcal{P}$, so ist auch $B \notin \mathcal{P}$.

Beweis. Es genügt, den ersten Teil zu zeigen, da der zweite Teil direkt daraus folgt. Sei also $A \leq_p B$ mit der zugehörigen polynomiellen Reduktion $f: \Sigma_1^* \rightarrow \Sigma_2^*$ und sei $B \in \mathcal{P}$. Ferner sei M_B eine Turingmaschine, die die Sprache B in polynomieller Zeit entscheidet und es sei M_f eine Turingmaschine, die die Reduktion f in polynomieller Zeit berechnet. Wir konstruieren eine Turingmaschine M_A für A , die bei einer Eingabe x zunächst M_f simuliert und $f(x)$ berechnet und dann anschließend M_B auf $f(x)$ simuliert.

Wie schon im Beweis von Theorem 2.9 diskutiert, entscheidet die so konstruierte Turingmaschine M_B die Sprache B . Wir müssen lediglich noch zeigen, dass ihre Laufzeit polynomiell ist. Seien p und q Polynome, für die $t_{M_B}(n) \leq p(n)$ und $t_{M_f}(n) \leq q(n)$ gilt. Die Laufzeit von M_A bei einer Eingabe x der Länge n beträgt dann $O(q(n) + p(q(n) + n))$, da zunächst $f(x)$ in Zeit $O(q(n))$ berechnet wird und anschließend die Turingmaschine M_B in Zeit $O(p(q(n) + n))$ auf der Eingabe $f(x)$ mit Länge höchstens $q(n) + n$ simuliert wird. Wir haben bereits nach Theorem 1.6 diskutiert, dass die Verschachtelung zweier Polynome wieder ein Polynom ist. Damit ist das Theorem bewiesen. \square

Wir betrachten ein Beispiel für eine polynomielle Reduktion und führen dazu zunächst eine Variante des Kürzeste-Wege-Problems ein, die wir *beschränktes Kürzeste-Wege-Problem* nennen. Genauso wie beim normalen Kürzeste-Wege-Problem enthält eine Eingabe für dieses Problem einen gerichteten Graphen $G = (V, E)$ mit Kantengewichten $w: E \rightarrow \mathbb{N}_0$ sowie einen Startknoten $s \in V$ und einen Zielknoten $t \in V$. Um aus dem Kürzeste-Wege-Problem ein Entscheidungsproblem zu machen, fügen wir der Eingabe zusätzlich eine Zahl $W \in \mathbb{N}_0$ hinzu, und fragen, ob es einen Weg P von s nach t gibt, dessen Gewicht/Länge $\sum_{e \in P} w(e)$ höchstens W beträgt. Beim beschränkten Kürzeste-Wege-Problem wird die Situation dadurch komplizierter, dass es zusätzlich noch Kantenkosten $c: E \rightarrow \mathbb{N}_0$ und ein Budget $C \in \mathbb{N}_0$ gibt. Die Frage ist

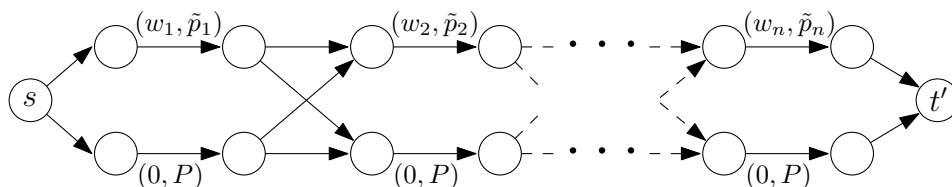
dann, ob es einen Weg P von s nach t gibt, dessen Länge $\sum_{e \in P} w(e)$ höchstens W beträgt und der das Budget einhält, d. h. für den $\sum_{e \in P} c(e) \leq C$ gilt. Dieses Problem tritt in vielen Anwendungen auf. Denkt man beispielsweise an Routenplanung, so könnte das Gewicht einer Kante angeben, wie lange es dauert, die entsprechende Strecke zurückzulegen, und die Kosten könnten der Maut entsprechen.

Wir bezeichnen im Folgenden mit KP die Entscheidungsvariante des Rucksackproblems und mit BKWP die soeben definierte Entscheidungsvariante des beschränkten Kürzeste-Wege-Problems. Sowohl bei KP als auch bei BKWP handelt es sich um Sprachen über geeignet gewählten endlichen Alphabeten. Wir können ohne Beschränkung der Allgemeinheit davon ausgehen, dass beides Sprachen über dem Alphabet $\{0, 1\}$ sind.

Theorem 3.12. *Es gilt $KP \leq_p BKWP$.*

Beweis. Sei $\mathcal{I} = (p_1, \dots, p_n, w_1, \dots, w_n, t, z)$ eine Eingabe für das Rucksackproblem, wobei wir davon ausgehen, dass alle Komponenten aus \mathbb{N}_0 sind. Diese Eingabe (bzw. eine geeignete Codierung $\text{code}(\mathcal{I}) \in \{0, 1\}^*$ von \mathcal{I}) gehört genau dann zu KP , wenn es eine Menge $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} w_i \leq t$ und $\sum_{i \in I} p_i \geq z$ gibt. Der Einfachheit halber werden wir im Folgenden stets $\mathcal{I} \in KP$ statt $\text{code}(\mathcal{I}) \in KP$ schreiben. Dabei setzen wir eine beliebige „sinnvolle“ Codierung voraus, deren Länge polynomiell in n und dem Logarithmus der größten Zahl in \mathcal{I} beschränkt ist.

Wir transformieren nun die gegebene Eingabe für das Rucksackproblem in eine Eingabe für das beschränkte Kürzeste-Wege-Problem. Dazu konstruieren wir den Graphen G mit $4n + 2$ Knoten, der in der folgenden Abbildung dargestellt ist.



In diesem Graphen sei s der Startknoten und t' der Zielknoten. An einigen Kanten finden sich Beschriftungen der Form (a, b) . Damit ist gemeint, dass die entsprechende Kante ein Gewicht von a und Kosten in Höhe von b besitzt. Es sei $P = \max_i p_i$ und $\tilde{p}_i = P - p_i$. Für Kanten, die nicht beschriftet sind, sind sowohl das Gewicht als auch die Kosten Null. Man kann sich bei diesen Kanten also die Beschriftung $(0, 0)$ dazu denken. Schließlich setzen wir noch W auf die gegebene Kapazität t des Rucksacks und $C = nP - z$.

Wir haben somit aus der Instanz \mathcal{I} für das Rucksackproblem eine Instanz \mathcal{I}' des BKWP erzeugt, in der die Frage darin besteht, ob in dem obigen Graphen ein Weg von der Quelle s zur Senke t' existiert, dessen Gesamtgewicht höchstens $W = t$ beträgt und dessen Gesamtkosten höchstens $C = nP - z$ betragen. Ist dies der Fall, so schreiben wir $\mathcal{I}' \in BKWP$. Genau wie beim Rucksackproblem müssten wir formal korrekt eigentlich $\text{code}(\mathcal{I}') \in BKWP$ für eine geeignete Codierung von \mathcal{I}' schreiben.

Die Instanz \mathcal{I}' für das beschränkte Kürzeste-Wege-Problem können wir für eine gegebene Instanz \mathcal{I} des Rucksackproblems in polynomieller Zeit erzeugen. Es bleibt zu

zeigen, dass es sich um eine Reduktion handelt, dass also $\mathcal{I} \in \text{KP} \iff \mathcal{I}' \in \text{BKWP}$ gilt.

- Wir zeigen zunächst $\mathcal{I} \in \text{KP} \Rightarrow \mathcal{I}' \in \text{BKWP}$. Wegen $\mathcal{I} \in \text{KP}$ gibt es eine Menge $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} w_i \leq t$ und $\sum_{i \in I} p_i \geq z$. Aus dieser Menge konstruieren wir einen Weg T von s nach t' in dem Graphen G . Dieser benutzt für jedes $i \in I$ die Kante mit Gewicht/Kostenkombination (w_i, \tilde{p}_i) und für jedes $i \notin I$ die darunterliegende Kante mit Gewicht/Kostenkombination $(0, P)$. Ansonsten benutzt der Weg nur Kanten, die sowohl Gewicht als auch Kosten Null haben. Ein solcher Weg kann in dem gegebenen Graphen einfach konstruiert werden.

Der Weg T besitzt ein Gesamtgewicht von

$$\sum_{i \in I} w_i + \sum_{i \notin I} 0 = \sum_{i \in I} w_i \leq t = W$$

und Gesamtkosten von

$$\sum_{i \in I} \tilde{p}_i + \sum_{i \notin I} P = \sum_{i \in I} (P - p_i) + \sum_{i \notin I} P = nP - \sum_{i \in I} p_i \leq nP - z = C.$$

Der Weg T beweist, dass $\mathcal{I}' \in \text{BKWP}$ gilt.

- Nun zeigen wir noch $\mathcal{I}' \in \text{BKWP} \Rightarrow \mathcal{I} \in \text{KP}$. Wegen $\mathcal{I}' \in \text{BKWP}$ existiert in G ein Weg T von s nach t' mit Gesamtgewicht höchstens $W = t$ und Gesamtkosten von höchstens $C = nP - z$. Wir konstruieren aus diesem Weg T eine Lösung $I \subseteq \{1, \dots, n\}$ für das Rucksackproblem. Zunächst beobachten wir, dass aus der Struktur des Graphen G direkt folgt, dass für jedes $i \in \{1, \dots, n\}$ entweder die Kante mit Gewicht/Kostenkombination (w_i, \tilde{p}_i) oder die darunterliegende Kante mit Gewicht/Kostenkombination $(0, P)$ enthalten ist. Die Menge I enthält ein Objekt i genau dann, wenn der Weg T die Kante mit Gewicht/Kostenkombination (w_i, \tilde{p}_i) enthält.

Die Menge I besitzt ein Gesamtgewicht von

$$\sum_{i \in I} w_i = \sum_{e \in T} w(e) \leq W = t.$$

Da T Gesamtkosten höchstens $C = nP - z$ besitzt und sich die Kosten von T als

$$\sum_{i \in I} \tilde{p}_i + \sum_{i \notin I} P = \sum_{i \in I} (P - p_i) + \sum_{i \notin I} P = nP - \sum_{i \in I} p_i$$

schreiben lassen, folgt

$$nP - \sum_{i \in I} p_i \leq C = nP - z,$$

was äquivalent zu

$$\sum_{i \in I} p_i \geq z$$

ist. Damit ist I , wie gewünscht, eine Auswahl der Objekte mit Gesamtgewicht höchstens t und Gesamtnutzen mindestens z .

Insgesamt folgt nun $KP \leq_p BKWP$. □

Eine wesentliche Implikation von Theorem 3.12 ist, dass jeder effiziente Algorithmus für das beschränkte Kürzeste-Wege-Problem mithilfe der Reduktion in einen effizienten Algorithmus für das Rucksackproblem umgebaut werden kann. Könnten wir also beispielsweise den Algorithmus von Dijkstra so anpassen, dass er effizient das beschränkte Kürzeste-Wege-Problem löst, so hätten wir damit auch direkt einen effizienten Algorithmus für das Rucksackproblem gefunden. Könnte man andersherum zeigen, dass es für das Rucksackproblem keinen effizienten Algorithmus gibt, so folgt aus der Reduktion, dass es auch keinen effizienten Algorithmus für das beschränkte Kürzeste-Wege-Problem geben kann.

Polynomielle Reduktionen setzen also die Komplexität von Problemen in einem gewissen Sinne zueinander in Beziehung. Es gibt mittlerweile in der Literatur Tausende Beispiele für polynomielle Reduktionen. Weitere polynomielle Reduktionen ergeben sich aus den bekannten, wenn man die Transitivität ausnutzt. Das bedeutet, wenn $A \leq_p B$ und $B \leq_p C$ für drei Sprachen A , B und C gilt, so gilt auch $A \leq_p C$. Der Leser überlege sich dies als Übung.

Die große Bedeutung von polynomiellen Reduktionen ergibt sich daraus, dass es damit auch möglich ist, die Komplexität eines Problem zu der Komplexität aller Probleme aus NP in Beziehung zu setzen. Um dies zu erläutern, benötigen wir zunächst die folgende Definition.

Definition 3.13. *Eine Sprache L heißt NP-schwer, wenn $L' \leq_p L$ für jede Sprache $L' \in NP$ gilt. Ist eine Sprache L NP-schwer und gilt zusätzlich $L \in NP$, so heißt L NP-vollständig.*

NP-vollständige Sprachen sind informell gesprochen, die schwierigsten Sprachen aus NP. Das folgende Theorem zeigt, dass sie genau dann effizient gelöst werden können, wenn $P = NP$ gilt.

Theorem 3.14. *Gibt es eine NP-schwere Sprache $L \in P$, so gilt $P = NP$.*

Beweis. Sei $L' \in NP$ beliebig. Aus Definition 3.13 folgt, dass $L' \leq_p L$ gilt. Wegen $L \in P$ und Theorem 3.11 folgt damit $L' \in P$. Da dieses Argument für jede Sprache $L' \in NP$ gilt, folgt $NP \subseteq P$. Wir haben bereits oben diskutiert, dass $P \subseteq NP$ gilt. Damit ist das Theorem bewiesen. □

Korollar 3.15. *Es sei L eine NP-vollständige Sprache. Dann gilt $L \in P$ genau dann, wenn $P = NP$ gilt.*

Können wir für ein Problem beweisen, dass es NP-vollständig ist, so ist dies also ein starkes Indiz dafür, dass das Problem nicht effizient gelöst werden kann. Auf den ersten Blick ist es allerdings vollkommen unklar, ob es überhaupt NP-vollständige Probleme gibt. Es wäre gut möglich, dass es gar kein Problem aus NP gibt, auf das alle anderen Probleme aus dieser Klasse reduziert werden können.

Unabhängig voneinander haben Stephen Cook und Leonid Levin 1971 bzw. 1973 auf den beiden Seiten des eisernen Vorhangs bewiesen, dass das Erfüllbarkeitsproblem der Aussagenlogik NP-vollständig ist. Dieses Problem ist uns bereits im ersten Semester begegnet und wir werden es im Folgenden mit SAT (engl. satisfiability) bezeichnen. Eine Eingabe für SAT besteht aus einer aussagenlogischen Formel und es soll entschieden werden, ob es eine Belegung der Variablen gibt, die diese Formel erfüllt.

Wir betrachten nur Formeln in konjunktiver Normalform als Eingaben und erinnern den Leser an die folgende Definition aus der Vorlesung „Logik und diskrete Strukturen“.

Definition 3.16. Eine Formel der Form x oder $\neg x$ für eine Variable x nennen wir ein Literal. Ein Literal der Form x nennen wir positives Literal und ein Literal der Form $\neg x$ nennen wir negatives Literal.

Eine aussagenlogische Formel φ ist in konjunktiver Normalform (KNF), wenn sie eine Konjunktion von Disjunktionen von Literalen ist, d. h. wenn sie die Gestalt

$$\varphi = \bigwedge_{i=1}^n \left(\bigvee_{j=1}^{m_i} \ell_{i,j} \right)$$

hat, wobei $n, m_1, \dots, m_n \in \mathbb{N}$ gilt und $\ell_{i,j}$ für jedes i und j ein Literal ist.

Die Teilformeln $\bigvee_{j=1}^{m_i} \ell_{i,j}$ nennen wir die Klauseln von φ .

Wieder gehen wir auf die Codierung von Formeln als Zeichenketten nicht näher ein und gehen nur davon aus, dass eine sinnvolle binäre Codierung gewählt wurde, dass also $\text{SAT} \subseteq \{0, 1\}^*$ gilt.

Theorem 3.17 (Satz von Cook und Levin). SAT ist NP-vollständig.

Beweis. Der Beweis besteht aus zwei Teilen. Wir müssen zeigen, dass $\text{SAT} \in \text{NP}$ gilt und dass sich jedes Problem aus NP polynomiell auf SAT reduzieren lässt. Eine polynomielle nichtdeterministische Turingmaschine für SAT kann einfach konstruiert werden. Für eine gegebene aussagenlogische Formel erzeugt diese analog zum Beweis von Theorem 3.7 zunächst nichtdeterministisch eine beliebige Belegung der Variablen (d. h. jede Variable wird nichtdeterministisch auf 0 oder 1 gesetzt). Anschließend überprüft die Turingmaschine deterministisch, ob die erzeugte Belegung die Formel erfüllt, und akzeptiert genau dann, wenn dies der Fall ist. Diese Überprüfung kann für eine gegebene Belegung und eine gegebene Formel leicht in polynomieller Zeit durchgeführt werden. Genau dann, wenn die Formel erfüllbar ist, gibt es einen Rechenweg der nichtdeterministischen Turingmaschine, der zu einer akzeptierenden Endkonfiguration führt.

Der zweite Teil ist deutlich schwieriger zu beweisen. Wir müssen nachweisen, dass jede Sprache aus NP polynomiell auf SAT reduziert werden kann. Sei $L \in \text{NP}$ beliebig. Das einzige, was wir über L wissen, ist, dass es eine nichtdeterministische Turingmaschine $M = (Q, \Sigma, \Gamma, \square, q_0, \bar{q}, \delta)$ gibt, die L in polynomieller Zeit entscheidet. Sei p ein Polynom, für das $t_M(n) \leq p(n)$ für alle $n \in \mathbb{N}_0$ gilt.

Unser Ziel ist es, eine polynomiell berechenbare Funktion $f: \Sigma^* \rightarrow \{0, 1\}^*$ zu finden, die jede Eingabe $x \in \Sigma^*$ für L in eine aussagenlogische Formel $f(x)$ in konjunktiver Normalform übersetzt, sodass gilt:

$$x \in L \iff f(x) \text{ ist erfüllbar.}$$

Sei im Folgenden $x \in \Sigma^*$ mit $n := |x|$ beliebig. Wir beschreiben nun, wie die Formel $\varphi := f(x)$ erzeugt wird. Da wir über L nichts weiter wissen, als dass es die nichtdeterministische Turingmaschine M gibt, die L entscheidet, müssen wir genau an dieser Stelle ansetzen. Die grobe Idee des Beweises besteht darin, dass wir mithilfe der Formel φ die Berechnung der Turingmaschine M simulieren wollen.

Um dies zu präzisieren, erinnern wir den Leser noch einmal daran, dass wir unter der *Konfiguration* einer Turingmaschine zu einem Zeitpunkt die aktuelle Kombination aus Bandinhalt, Kopfposition und Zustand verstehen. Sind K und K' Konfigurationen von M , so sagen wir, dass K' eine *direkte Nachfolgekonfiguration* von K ist, wenn es in Konfiguration K einen erlaubten Rechenschritt der Turingmaschine M gibt, der zu Konfiguration K' führt. Wir schreiben dann $K \vdash K'$. Bezeichnen wir mit K_0 die initiale Konfiguration der Turingmaschine M bei Eingabe x , so soll die Formel φ genau dann erfüllbar sein, wenn es eine Folge von Konfigurationen K_1, K_2, \dots, K_ℓ mit $\ell \leq p(n)$ und $K_0 \vdash K_1 \vdash K_2 \vdash \dots \vdash K_\ell$ gibt, wobei K_ℓ eine akzeptierende Endkonfiguration ist. Da die Turingmaschine M die Sprache L entscheidet und $t_M(n) \leq p(n)$ gilt, gibt es genau dann eine solche Folge von Konfigurationen, wenn $x \in L$ gilt.

Um die Konstruktion der Formel φ zu vereinfachen, bauen wir die Turingmaschine M ein wenig um. Eine akzeptierende Endkonfiguration ist dadurch gekennzeichnet, dass der Endzustand \bar{q} erreicht ist und direkt unter dem Kopf das Zeichen 1 steht. Wir fügen der Turingmaschine M nun einen neuen Zustand q_{akz} hinzu und ändern die Zustandsüberführungsrelation δ so ab, dass in einer akzeptierenden Endkonfiguration der neue Zustand q_{akz} statt \bar{q} erreicht wird. Jeder mögliche Übergang in den Zustand \bar{q} wird also darauf überprüft, ob er zu einer akzeptierenden oder verwerfenden Endkonfiguration führt. Führt er zu einer verwerfenden Endkonfiguration, so wird er nicht verändert. Führt er jedoch zu einer akzeptierenden Endkonfiguration, so wird statt in \bar{q} in den Zustand q_{akz} gewechselt. Ist dieser Zustand einmal erreicht, so terminiert die Turingmaschine nicht, sondern sie gerät in eine Endlosschleife, in der sie den Zustand q_{akz} nicht mehr verlässt, den Kopf nicht mehr bewegt und keine Veränderungen am Band mehr vornimmt.

Durch die Einführung des Zustandes q_{akz} haben wir erreicht, dass wir uns nur noch Rechenwege der Länge genau $p(n)$ anschauen müssen. Unser Ziel ist es nun also, die Formel φ so zu generieren, dass die folgende Eigenschaft gilt.

Die Formel φ ist genau dann erfüllbar, wenn es eine Folge von Konfigurationen $K_1, K_2, \dots, K_{p(n)}$ der Turingmaschine M mit $K_0 \vdash K_1 \vdash K_2 \vdash \dots \vdash K_{p(n)}$ gibt, wobei in $K_{p(n)}$ der Zustand q_{akz} angenommen wird und K_0 die initiale Konfiguration der Turingmaschine M bei Eingabe x ist.

Definition der Variablen: Die Variablen der Formel φ werden die Konfigurationen $K_0, \dots, K_{p(n)}$ codieren. Sie enthalten also für jeden Zeitpunkt $t \in \{0, 1, \dots, p(n)\}$ Informationen über den Bandinhalt, die Kopfposition und den Zustand. Nummerieren wir die Zellen des Bandes mit ganzen Zahlen und treffen die Konvention, dass die initiale Kopfposition den Index 0 hat, so kann die Turingmaschine in $p(n)$ Schritten nur die Zellen mit den Indizes $-p(n), -p(n) + 1, \dots, p(n) - 1, p(n)$ erreichen. Alle anderen Zellen enthalten stets das Leerzeichen und sind deshalb nicht von Interesse. Wir können demnach die Konfigurationen $K_0, K_1, \dots, K_{p(n)}$ mithilfe der folgenden (binären) Variablen vollständig beschreiben.

- $Q(t, q)$ für $t \in \{0, \dots, p(n)\}$ und $q \in Q$

$$Q(t, q) = \begin{cases} 1 & \text{falls in } K_t \text{ Zustand } q \text{ angenommen wird} \\ 0 & \text{sonst} \end{cases}$$

- $H(t, j)$ für $t \in \{0, \dots, p(n)\}$ und $j \in \{-p(n), \dots, p(n)\}$

$$H(t, j) = \begin{cases} 1 & \text{falls Kopf in } K_t \text{ auf Zelle } j \text{ steht} \\ 0 & \text{sonst} \end{cases}$$

- $S(t, j, a)$ für $t \in \{0, \dots, p(n)\}$, $j \in \{-p(n), \dots, p(n)\}$ und $a \in \Gamma$

$$S(t, j, a) = \begin{cases} 1 & \text{falls Zelle } j \text{ in } K_t \text{ das Zeichen } a \text{ enthält} \\ 0 & \text{sonst} \end{cases}$$

Die Anzahl der Variablen ist polynomiell in n beschränkt, da p ein Polynom ist und Q und Γ endliche Mengen konstanter Größe sind.

Codierung einzelner Konfigurationen: Als erstes geben wir Klauseln an, die sicherstellen, dass die Variablen für jedes feste t eine Konfiguration von M codieren. Sei also $t \in \{0, \dots, p(n)\}$ beliebig. Dann muss jede erfüllende Belegung von φ dergestalt sein,

- dass es genau ein $q \in Q$ mit $Q(t, q) = 1$ gibt,
- dass es genau ein $j \in \{-p(n), \dots, p(n)\}$ mit $H(t, j) = 1$ gibt und
- dass es für jedes $j \in \{-p(n), \dots, p(n)\}$ genau ein $a \in \Gamma$ mit $S(t, j, a) = 1$ gibt.

Diese drei Bedingungen haben gemeinsam, dass für eine bestimmte Variablenmenge codiert werden muss, dass genau eine der Variablen auf 1 und alle anderen auf 0 gesetzt sind. Für eine Variablenmenge $\{y_1, \dots, y_m\}$ kann dies durch die Formel

$$(y_1 \vee \dots \vee y_m) \wedge \bigwedge_{i \neq j} (\neg y_i \vee \neg y_j)$$

in konjunktiver Normalform erreicht werden. Diese Formel besitzt eine Länge von $O(m^2)$, wobei wir unter der Länge die Anzahl der auftretenden Literale verstehen. Wir können auf diese Weise also die obigen drei Bedingungen mit einer Formel φ_t der Länge $O(p(n)^2)$ in konjunktiver Normalform codieren.

Codierung von Konfigurationsübergängen: Mithilfe der Formeln φ_t können wir für jedes einzelne t erreichen, dass jede gültige Variablenbelegung eine Konfigurationsfolge $K_0, \dots, K_{p(n)}$ beschreibt. Diese Konfigurationen haben aber im Allgemeinen nichts miteinander zu tun. Deshalb müssen wir als nächstes codieren, dass K_t für jedes $t \in \{1, \dots, p(n)\}$ eine direkte Nachfolgekongfiguration von K_{t-1} ist. Sei im Folgenden $t \in \{1, \dots, p(n)\}$ beliebig.

Zunächst erzwingen wir, dass sich der Bandinhalt nur in der Zelle ändern kann, an der sich der Kopf befindet. Dies erreichen wir durch die Formel

$$\bigwedge_{j=-p(n)}^{p(n)} \bigwedge_{a \in \Gamma} \left((S(t-1, j, a) \wedge \neg H(t-1, j)) \Rightarrow S(t, j, a) \right).$$

Diese besagt, dass für jede Position $j \in \{-p(n), \dots, p(n)\}$ und jedes Zeichen $a \in \Gamma$ gilt: Wenn zum Zeitpunkt $t-1$ an Position j das Zeichen a steht ($S(t-1, j, a)$) und der Kopf sich zum Zeitpunkt $t-1$ nicht an Position j befindet ($\neg H(t-1, j)$), so muss auch zum Zeitpunkt t an der Position j das Zeichen a stehen ($S(t, j, a)$). Den Implikationspfeil haben wir der besseren Lesbarkeit halber verwendet. Man kann $A \Rightarrow B$ durch den äquivalenten Ausdruck $\neg A \vee B$ ersetzen. Wendet man dann noch das De Morgansche Gesetz an, dass $\neg(A \wedge B)$ äquivalent zu $\neg A \vee \neg B$ ist, so erhält man die folgende Formel in konjunktiver Normalform:

$$\bigwedge_{j=-p(n)}^{p(n)} \bigwedge_{a \in \Gamma} \left(\neg S(t-1, j, a) \vee H(t-1, j) \vee S(t, j, a) \right). \quad (3.1)$$

Diese Formel besitzt eine Länge von $O(p(n))$.

Nun müssen wir noch erreichen, dass im Schritt von K_{t-1} zu K_t ein durch δ beschriebener Rechenschritt ausgeführt wird. Dazu erzeugen wir für jedes $q \in Q$, jedes $j \in \{-p(n), \dots, p(n)\}$ und jedes $a \in \Gamma$ die Formel

$$\begin{aligned} & \left(Q(t-1, q) \wedge H(t-1, j) \wedge S(t-1, j, a) \right) \\ \Rightarrow & \bigvee_{((q,a),(q',a',D)) \in \delta} \left(Q(t, q') \wedge H(t, j+D) \wedge S(t, j, a') \right), \end{aligned}$$

wobei wir der Einfachheit halber davon ausgehen, dass $D \in \{-1, 0, +1\}$ statt $D \in \{L, N, R\}$ die Bewegung des Kopfes angibt. Diese Formel besagt: Wenn sich die Turingmaschine zum Zeitpunkt $t-1$ in Zustand q befindet ($Q(t-1, q)$), der Kopf sich an Position j befindet ($H(t-1, j)$) und an Position j das Zeichen a steht ($S(t-1, j, a)$), so gilt für einen Übergang $((q, a), (q', a', D)) \in \delta$, dass sich die Turingmaschine zum Zeitpunkt t in Zustand q' befindet ($Q(t, q')$), der Kopf sich an Position $j+D$ befindet ($H(t, j+D)$) und an Position j das Zeichen a' steht ($S(t, j, a')$).

Wir haben bereits in der Vorlesung „Logik und diskrete Strukturen“ gesehen, dass es zu jeder Formel eine äquivalente Formel in konjunktiver Normalform gibt. Im Allgemeinen kann diese Formel um einen Faktor länger sein, der exponentiell in der Zahl der Variablen ist. Da die obige Formel für festes t sowie feste q , j und a konstante Länge besitzt (es gibt nur konstant viele Tripel (q', a', D) mit $((q, a), (q', a', D)) \in \delta$),

gibt es eine äquivalente Formel in konjunktiver Normalform, die ebenfalls konstante Länge besitzt. Konjugieren wir die Formeln für jede Wahl von q , j und a , so erhalten wir insgesamt eine Formel der Länge $O(p(n))$.

Zusammen mit (3.1) erhalten wir somit für jedes $t \in \{1, \dots, p(n)\}$ eine Formel $\varphi_{\rightarrow t}$ in konjunktiver Normalform, die codiert, dass K_t eine direkte Nachfolgekonfiguration von K_{t-1} ist.

Codierung der initialen Konfiguration: Um zu codieren, dass K_0 die initiale Konfiguration der Turingmaschine M bei Eingabe x ist, müssen wir erreichen, dass sich M in K_0 im Startzustand q_0 befindet, der Bandinhalt x ist und der Kopf auf dem ersten Zeichen von x steht. Sei $x = x_1 \dots x_n$. Dann kann dies durch die Formel

$$\varphi_{\text{init}} = Q(0, q_0) \wedge H(0, 0) \wedge \bigwedge_{i=1}^n S(0, i-1, x_i) \wedge \bigwedge_{j=-p(n)}^{-1} S(0, j, \square) \wedge \bigwedge_{j=n+1}^{p(n)} S(0, j, \square)$$

in konjunktiver Normalform erreicht werden.

Zusammensetzen der Formel: Nun können wir alle Teilformeln zusammensetzen und zusätzlich noch codieren, dass nach $p(n)$ Schritten der Zustand q_{akz} erreicht werden soll. Es ergibt sich die Formel

$$\varphi = \varphi_{\text{init}} \wedge \bigwedge_{t=0}^{p(n)} \varphi_t \wedge \bigwedge_{t=1}^{p(n)} \varphi_{\rightarrow t} \wedge Q(p(n), q_{\text{akz}}).$$

Diese Formel in konjunktiver Normalform besitzt eine Länge von $O(p(n)^3)$ und sie kann für ein gegebenes $x \in \Sigma^*$ in polynomieller Zeit konstruiert werden.

Aus unseren Vorüberlegungen ergibt sich direkt, dass es genau dann eine erfüllende Belegung für die Formel φ gibt, wenn es eine Folge von Konfigurationen $K_1, K_2, \dots, K_{p(n)}$ der Turingmaschine M mit $K_0 \vdash K_1 \vdash K_2 \vdash \dots \vdash K_{p(n)}$ gibt, wobei in $K_{p(n)}$ der Zustand q_{akz} angenommen wird und K_0 die initiale Konfiguration bei Eingabe x ist. Dies ist genau dann der Fall, wenn $x \in L$ gilt. Somit gilt $L \leq_p \text{SAT}$. \square

3.3 Weitere NP-vollständige Probleme

Der Beweis, dass SAT NP-vollständig ist, war relativ lang. Müsste man für jedes Problem einen ähnlichen Beweis führen, so wären sicherlich weit weniger NP-vollständige Probleme bekannt als das heutzutage der Fall ist. Hat man erst einmal ein erstes NP-schweres Problem L gefunden, so kann man die NP-Schwere eines anderen Problems L' aber auch einfach dadurch nachweisen, dass man L polynomiell auf L' reduziert. Da sich jedes Problem aus NP auf L polynomiell reduzieren lässt, folgt dann aus der Transitivität des Reduktionskonzeptes, dass sich auch jedes Problem aus NP polynomiell auf L' reduzieren lässt. Dies halten wir noch einmal im folgenden Lemma fest.

Lemma 3.18. *Sei L' eine beliebige Sprache und sei L eine beliebige NP-schwere Sprache. Gilt $L \leq_p L'$, so ist auch L' NP-schwer.*

Aus den polynomiellen Reduktionen, die wir bisher in den Übungen gesehen haben, folgt gemeinsam mit Theorem 3.17 also bereits, dass zahlreiche Probleme NP-vollständig sind. Wir fassen kurz zusammen, was aus den Übungen bekannt ist.

- $\text{SAT} \leq_p \text{3-SAT}$, wobei 3-SAT die eingeschränkte Variante von SAT bezeichnet, in der jede Klausel genau drei Literale enthält.
- $\text{3-SAT} \leq_p \text{CLIQUE}$
- $\text{CLIQUE} \leq_p \text{VC}$, wobei VC das *Vertex-Cover-Problem* bezeichnet, bei dem für einen ungerichteten Graphen $G = (V, E)$ und eine Zahl $k \in \mathbb{N}$ entschieden werden soll, ob es eine Teilmenge $V' \subseteq V$ der Knoten mit $|V'| \leq k$ gibt, sodass jede Kante aus E zu mindestens einem Knoten aus V' inzident ist.
- $\text{3-SAT} \leq_p \text{DOMSET}$, wobei DOMSET das *Dominating-Set-Problem* bezeichnet, bei dem für einen ungerichteten Graphen $G = (V, E)$ und eine Zahl $k \in \mathbb{N}$ entschieden werden soll, ob es eine Teilmenge $V' \subseteq V$ der Knoten mit $|V'| \leq k$ gibt, sodass jeder Knoten aus V entweder zu V' gehört oder adjazent zu einem Knoten aus V' ist.
- $\text{3-SAT} \leq_p \text{HC}$, wobei HC das *Hamiltonkreis-Problem* bezeichnet, bei dem für einen ungerichteten Graphen $G = (V, E)$ entschieden werden soll, ob er einen Kreis enthält, der jeden Knoten genau einmal besucht (einen sogenannten Hamiltonkreis).
- $\text{HC} \leq_p \text{TSP}$, wobei TSP das *Problem des Handlungsreisenden* bezeichnet, bei dem für einen vollständigen ungerichteten Graphen $G = (V, E)$ mit Kantengewichten $w: E \rightarrow \mathbb{N}_0$ und eine Zahl $t \in \mathbb{N}_0$ entschieden werden soll, ob ein Hamiltonkreis mit Gewicht höchstens t existiert.

Hieraus folgt direkt, dass die Probleme 3-SAT, CLIQUE, VC, DOMSET, HC und TSP NP-schwer sind. Man sieht leicht, dass diese Probleme alle zu NP gehören. Somit sind sie sogar NP-vollständig.

Ein Problem, mit dem wir uns in dieser Vorlesung schon beschäftigt haben, das aber in der obigen Liste noch fehlt, ist das Rucksackproblem. Wir werden nun zeigen, dass dieses Problem und einige verwandte Probleme ebenfalls NP-schwer sind. Als erstes betrachten wir das Problem SUBSETSUM. Die Eingabe bei diesem Problem besteht aus Zahlen $a_1, \dots, a_n \in \mathbb{N}$ sowie einer Zahl $b \in \mathbb{N}$ und es soll entschieden werden, ob es eine Teilmenge $I \subseteq \{1, \dots, n\}$ gibt, für die $\sum_{i \in I} a_i = b$ gilt. Wieder geben wir keine konkrete Codierung von Eingaben für dieses Problem an. Wichtig ist lediglich, dass die Eingabelänge nur logarithmisch mit der Größe der Zahlen wächst. Dies erreicht man beispielsweise dadurch, dass man die Zahlen binär codiert.

Theorem 3.19. *Das Problem SUBSETSUM ist NP-vollständig.*

Beweis. Man sieht leicht ein, dass SUBSETSUM zu NP gehört, denn für eine gegebene Menge I kann effizient überprüft werden, ob $\sum_{i \in I} a_i = b$ gilt.

Wir zeigen nun, dass $3\text{-SAT} \leq_p \text{SUBSETSUM}$ gilt. Sei dazu φ eine beliebige Eingabe für 3-SAT, also eine Formel in konjunktiver Normalform, in der jede Klausel maximal drei Literale enthält. Es seien $\{x_1, \dots, x_N\}$ die Variablen, die in φ vorkommen, und es seien $\{C_1, \dots, C_M\}$ die Klauseln von φ . Wir erzeugen aus φ eine Eingabe für SUBSETSUM mit $n = 2N + 2M$ Zahlen (b nicht mitgezählt), in der jede Zahl mit $N + M$ Ziffern im Dezimalsystem codiert werden kann. Für eine Zahl z und einen Index $j \in \{1, \dots, N + M\}$ bezeichnen wir im Folgenden mit $z(j)$ die j -te Ziffer der Zahl z im Dezimalsystem.

- Für jede Variable x_i mit $i \in \{1, \dots, N\}$ erzeugen wir zwei Zahlen a_i und \bar{a}_i . Für $j \in \{1, \dots, N\}$ setzen wir

$$a_i(j) = \bar{a}_i(j) = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Für $j \in \{1, \dots, M\}$ setzen wir

$$a_i(N + j) = \begin{cases} 1 & \text{falls } x_i \text{ in } C_j \text{ enthalten ist,} \\ 0 & \text{sonst} \end{cases}$$

und

$$\bar{a}_i(N + j) = \begin{cases} 1 & \text{falls } \neg x_i \text{ in } C_j \text{ enthalten ist,} \\ 0 & \text{sonst.} \end{cases}$$

- Für jedes $i \in \{1, \dots, M\}$ erzeugen wir zwei Zahlen h_i und h'_i . Es sei $h_i(N + i) = h'_i(N + i) = 1$ und alle anderen Ziffern seien 0.
- Wir setzen

$$b(j) = \begin{cases} 1 & \text{falls } j \leq N, \\ 3 & \text{falls } j > N. \end{cases}$$

In dieser Reduktion spielt die Reihenfolge der Ziffern keine Rolle, da es bei der Addition der erzeugten Zahlen zu keinen Überläufen kommen kann. Dies liegt daran, dass es für jede Position maximal fünf Zahlen (b nicht mitgezählt) gibt, die an der Position eine 1 enthalten. Abbildung 3.1, die wir aus [5] übernommen haben, stellt diese Reduktion noch einmal schematisch dar.

Die Zahlen, die wir konstruiert haben, sind sehr groß, da sie aus jeweils $N + M$ Ziffern im Dezimalsystem bestehen und somit Werte in der Größenordnung von 10^{N+M} annehmen können. Binär (oder dezimal) codiert können wir die Zahlen dennoch in polynomieller Zeit aus der gegebenen Formel φ erzeugen.

Es bleibt zu zeigen, dass es genau dann eine Teilmenge I der Zahlen $a_i, \bar{a}_i, h_i, h'_i$ gibt, deren Summe genau b ist, wenn es eine erfüllende Belegung für φ gibt.

	1	2	3	...	N	$N+1$	$N+2$...	$N+M$
a_1	1	0	0	...	0	1	0
a'_1	1	0	0	...	0	0	0
a_2	0	1	0	...	0	0	1
a'_2	0	1	0	...	0	1	0
a_3	0	0	1	...	0	1	1
a'_3	0	0	1	...	0	0	0
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_N	0	0	0	...	1	0	0
a'_N	0	0	0	...	1	0	1
h_1	0	0	0	...	0	1	0	...	0
h'_1	0	0	0	...	0	1	0	...	0
h_2	0	0	0	...	0	0	1	...	0
h'_2	0	0	0	...	0	0	1	...	0
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
h_M	0	0	0	...	0	0	0	...	1
h'_M	0	0	0	...	0	0	0	...	1
b	1	1	1	...	1	3	3	...	3

Abbildung 3.1: Schematische Darstellung der Reduktion $3\text{-SAT} \leq_p \text{SUBSETSUM}$ [5]: In diesem Beispiel gilt $C_1 = x_1 \vee \neg x_2 \vee x_3$ und $C_2 = x_2 \vee x_3 \vee \neg x_N$.

- Sei x^* eine erfüllende Belegung für φ . Wir konstruieren daraus eine Teilmenge I mit der gewünschten Summe. Gilt $x_i^* = 1$, so nehmen wir a_i in die Teilmenge I auf. Gilt $x_i^* = 0$, so nehmen wir \bar{a}_i in die Teilmenge I auf.

Bezeichnen wir mit A die Summe der bisher ausgewählten Zahlen, so gilt $A(j) = 1$ für alle $j \in \{1, \dots, N\}$, da wir entweder a_j oder \bar{a}_j ausgewählt haben. Ferner folgt aus der Konstruktion, dass $A(N+j)$ für alle $j \in \{1, \dots, M\}$ angibt, wie viele Literale der Klausel C_j von der Belegung x^* erfüllt werden. Dementsprechend gilt $A(N+j) \in \{1, 2, 3\}$ für alle $j \in \{1, \dots, M\}$. Falls $A(N+j) = 2$ gilt, so fügen wir der Menge I noch die Zahl h_j hinzu. Gilt $A(N+j) = 1$, so fügen wir der Menge I noch die Zahlen h_j und h'_j hinzu. Danach hat die j -te Ziffer der Summe den Wert 3. Alle anderen Ziffern werden durch die Hinzunahme von h_j und h'_j nicht verändert.

Insgesamt haben wir so eine Teilmenge der Zahlen konstruiert, deren Summe gleich b ist.

- Sei nun andersherum I eine Teilmenge der Zahlen, deren Summe gleich b ist. Wir konstruieren daraus eine erfüllende Belegung x^* für φ . Zunächst beobachten wir, dass für jedes $j \in \{1, \dots, N\}$ genau eine der Zahlen a_j und \bar{a}_j in I enthalten ist, da sonst die j -te Ziffer der Summe der Zahlen aus I nicht gleich $b(j) = 1$ sein könnte. Wir setzen

$$x_j^* = \begin{cases} 1 & \text{falls } a_j \text{ in } I \text{ enthalten ist,} \\ 0 & \text{falls } \bar{a}_j \text{ in } I \text{ enthalten ist.} \end{cases}$$

Um zu sehen, dass x^* eine erfüllende Belegung von φ ist, betrachten wir die Summe A der Zahlen a_i und \bar{a}_i , die in I enthalten sind. Für jedes $j \in \{1, \dots, M\}$ gilt $A(N + j) \geq 1$, da ansonsten die $(N + j)$ -te Ziffer der Summe der Zahlen aus I nicht gleich $b(N + j) = 3$ sein könnte. Da $a_i(N + j) = 1$ oder $\bar{a}_i(N + j) = 1$ nur dann gilt, wenn C_j das Literal x_j bzw. $\neg x_j$ enthält, folgt daraus, dass die Belegung x^* mindestens ein Literal jeder Klausel erfüllt.

Damit ist der Beweis abgeschlossen.

□

Literaturverzeichnis

- [1] Norbert Blum: **Einführung in formale Sprachen, Berechenbarkeit, Informations- und Lerntheorie**. Oldenbourg, 2007.
- [2] John E. Hopcroft, Rajeev Motwani und Jeffrey D. Ullman: **Einführung in Automatentheorie, Formale Sprachen und Berechenbarkeit**. Pearson Studium, 3. Auflage, 2007.
- [3] Christos H. Papadimitriou: **Computational Complexity**. Addison Wesley, 1993.
- [4] Alan M. Turing: **On Computable Numbers, with an Application to the Entscheidungsproblem**. Proceedings of the London Mathematical Society, 42:230–265, 1937.
- [5] Berthold Vöcking: **Berechenbarkeit und Komplexität**, Vorlesungsskript, RWTH Aachen, Wintersemester 2013/14. <http://algo.rwth-aachen.de/Lehre/WS1314/VBuK/BuK.pdf>.
- [6] Ingo Wegener: **Theoretische Informatik – eine algorithmenorientierte Einführung**. Teubner, 3. Auflage, 1993.