Notizen zur Vorlesung
Theoretische Informatik und Logik

Zusammenfassung

Notizen zur Vorlesung https://iccl.inf.tu-dresden.de/web/Theoretische_Informatik_und_Logik_(SS2017).

Ich versuche möglichst ohne formelle Symbole und Definitionen zu arbeiten, daher verweisen die Markierungen jeweils auf die Vorlesungsnummer in FS bzw. TIL. Obwohl der Schwerpunkt auf TheoLog liegt, habe ich ein paar Definitionen aus Formale Systeme mit einbezogen, da TheoLog diese weiterverwendet.

Einige Formulierungen habe ich aus den hervorragenden Folien von Prof. Krötzsch geliehen. Quellen dieser Folien sind auf Github zu finden unter https://github.com/mkroetzsch und sind unter der Lizenz CC BY 3.0 DE verwendbar. Für diese gilt: „(C) Markus Krötzsch, https://iccl.inf.tu-dresden.de/web/TheoLog2017, CC BY 3.0 DE“.

Inhaltsverzeichnis

Autor	Dominik Pataky
Dozent	Prof. Markus Krötzsch
Ort	Fakultät Informatik, TU Dresden
Zeit	Sommersemester 2017
Letztes Update	21. Juni 2017
Lizenz	CC BY-SA 4.0

1 Formale Systeme

1.1 Sprachen und Automaten

(formale) Sprache Menge von Wörtern/Symbolen/Tokens, z.B. Programmiercode oder natürliche Sprache. Zusätzliche Begriffe: Konkatenation, Präfix/Suffix/Infix, leeres Wort FS 1

Symbol Token der Sprache, z.B. if/else, +/-, True/False, "Hello World"-String

Alphabet nichtleere, endliche Menge von Symbolen

Wort endliche Sequenz von Symbolen

Grammatik formelle Spezifikation einer Sprache. Aus einer Grammatik kann man widerum eine Sprache erzeugen FS 2

Rechenoperationen Vereinigung, Schnitt, Komplement, Produkt, Potenz, Kleene-Abschluss

Abschlusseigenschaft Beispiel: Wenn Sprache A und Sprache B regulär sind, wäre dann auch der Schnitt der beiden Sprachen wieder regulär? FS 5

Automat Beginnt von einem Startzustand und folgt je nach Eingabe seinen Übergängen in die jeweiligen Zustände. Akzeptiert, wenn letzter Zustand ein akzeptierter Endzustand.

Deterministischer endlicher Automat (DFA) erkennen reguläre Sprachen FS 3

nichtdeterministischer endlicher Automat (NFA) „rät" die richtigen Übergänge, arbeitet parallel. Nichtdeterminismus sinnvoll? Kompaktere Darstellungen, Start für Entwicklung DFA, kann bei Untersuchung Komplexität/Berechenbarkeit helfen FS 4

Kellerautomat (PDA) PDA erweitern endliche Automaten um einen unbeschränkt großen Speicher, der aber nur nach dem LIFO-Prinzip verwendet werden kann. PDAs erkennen genau die kontextfreien Sprachen. FS 15

Turingmaschine (TM) liefert allgemeines Modell der Berechnung. Liest und schreibt in einem Schritt, hat unendlichen Speicher, kann beliebig auf Speicher zugreifen (im Gegensatz zu LIFO bei PDA). Kann ein Band oder mehrere Bänder haben. Kann deterministisch (DTM) oder nichtdeterministisch (NTM) sein. Alle Varianten der TM können die selben Funktionen berechnen (Probleme lösen) - einzig der Aufwand ist unterschiedlich (NTM kann DTM darstellen, NTM kann durch DTM simuliert werden etc.). Siehe auch Church-Turing-These. FS 18

Kardinalität Unterscheidung abzählbar (mit natürlichen Zahlen) und überabzählbar

Chomsky-Hierarchie Kategorische Einteilung von Sprachen je nach Komplexität ihrer Grammatik. Hierarchie 0 > 1 > 2 > 3. These: „Die meisten Sprachen können nicht mit Grammatiken beschrieben werden (abzählbar viele Grammatiken vs. überabzählbar viele Sprachen)". FS 2

Typ 0 beliebige Grammatiken (Turingmaschinen)

Typ 1 kontextsensitive Grammatiken

Typ 2 kontextfreie Grammatiken (CYK, Kellerautomaten)

Typ 3 reguläre Grammatiken (DFA, NFA, Pumping Lemma)

Probleme Probleme formulieren Berechnungsfragen.

Wortproblem Wortproblem für eine Sprache über einem Alphabet ist die Bestimmung der Ausgabe „ja, Wort ist in Sprache" oder „nein, Wort ist nicht in Sprache", für die Eingabe eines Wortes gebildet aus dem Alphabet FS 3

Leerheitsproblem (DFA, NFA) Entscheidung für „ja, Automat erzeugt Sprache" oder „nein, durch den Automaten erzeugte Sprache ist leer" (es wird nie ein Endzustand erreicht). FS 10

Inklusionsproblem (DFA, NFA) Entscheidung für „ja, Sprache A eines Automaten ist eine Teilmenge der Sprache B eines anderen Automaten" oder „nein, Sprache A ist keine Teilmenge der Sprache B". FS 10

Äquivalenzproblem (DFA, NFA) Entscheidung für „ja, Sprache A eines Automaten ist gleich der Sprache B eines anderen Automaten" oder „nein, Sprache A unterscheidet sich von Sprache B". FS 10

Endlichkeitsproblem (DFA, NFA) Entscheidung für „ja, erzeugte Sprache eines Automaten ist endlich“ oder „nein, erzeugte Sprache ist nicht endlich“ (z.B., wenn Zyklen auf dem Pfad von Start- zu Endzustand existieren). FS 10

Universalitätsproblem (DFA, NFA) Entscheidung für „ja, erzeugte Sprache eines Automaten ist Σ^*“ oder „nein, erzeugte Sprache ist nicht Σ^*“ (heißt, Komplement der erzeugten Sprache ist leer). FS 10

Halteproblem (TM) Entscheidet, ob eine Turingmaschine für eine Eingabe jemals hält oder nicht. Unentscheidbar. FS 19

Church-Turing-These Die Turingmaschine kann alle Funktionen berechnen, die intuitiv berechenbar sind. Auch: „Eine Funktion ist genau dann im intuitiven Sinne berechenbar, wenn es eine Turingmaschine gibt, die für jede mögliche Eingabe den Wert der Funktion auf das Band schreibt und anschließend hält.“ FS 18

Entscheidbarkeit Eine Sprache L ist entscheidbar / berechenbar / rekursiv, wenn es eine Turingmaschine gibt, die das Wortproblem der Sprache L entscheidet. D.h. die Turingmaschine ist Entscheider und die Sprache L ist gleich der durch die Turingmaschine erkannten Sprache. Andernfalls heißt die Sprache L unentscheidbar.
Die Sprache L ist semi-entscheidbar / Turing-erkennbar / rekursiv aufzählbar, wenn es eine Turingmaschine gibt, deren erkannte Sprache zwar L ist, jedoch die Turingmaschine kein Entscheider sein muss. FS 19

Satz von Rice Sei E eine Eigenschaft von Sprachen, die für manche Turing-erkennbare Sprachen gilt und für manche Turing-erkennbare Sprachen nicht gilt (= „nicht-triviale Eigenschaft“).
Dann ist das folgende Problem unentscheidbar: die Eingabe besteht aus einer Turingmaschine. Wir wollen prüfen, ob die durch diese Turingmaschine erkannte Sprache die Eigenschaft E besitzt. Der Beweis für die Unentscheidbarkeit dieses Problems ist eine Reduktion vom Halteproblem. FS 20

1.2 Aussagenlogik

Die Aussagenlogik untersucht logische Verknüpfungen von atomaren Aussagen. FS 21

Atomare Aussage Behauptungen, die wahr oder falsch sein können.
Auch: aussagenlogische Variablen, Propositionen, Atome

Operatoren, Junktoren Verknüpfung von atomaren Aussagen.
Negation, Konjunktion, Disjunktion, Implikation, Äquivalenz.
Können auch äquivalent durch andere Junktoren ausgedrückt werden (de Morgan). FS 22
Eine Disjunktion von Literalen nennt man **Klausel**.
Eine Konjunktion von Literalen nennt man **Monom**.

Formel Jedes Atom ist eine Formel, jede durch Junktoren verknüpfte Formeln sind wieder Formeln. Diese zusammengesetzten Formeln bestehen dann wieder aus Teilformeln (auch: Unterformeln, $Sub(F)$). Eine Formel, die nur aus einem Atom besteht, nennt man auch **Literal**. Literale können die Form x oder $\neg x$ (für x Atom) annehmen.

unerfüllbar Formel hat keine Modelle

erfüllbar Formel hat mindestens ein Modell

allgemeingültig alle Interpretationen sind Modelle für Formel. Auch: **Tautologie**, $\models F$

widerlegbar Formel ist nicht allgemeingültig

Syntax „Sprache einer Logik“ (Formeln mit logischen Operatoren). Wichtig: Klammerung.

Semantik Definition der Bedeutung. Wertzuweisung von Wahrheitswerten zu Atomen mit Hilfe der Interpretation. „Die Bedeutung einer Formel besteht darin, dass sie uns Informationen darüber liefert, welche Wertzuweisungen möglich sind, wenn die Formel wahr sein soll.“

Interpretation eine Funktion w, die von einer Menge Atome auf die Menge {0, 1} abbildet.

Wahrheitstabelle Schrittweise Auflösung einer Formel durch Lösen ihrer Teilformeln.

Modell eine Interpretation, dessen Abbildung eine Formel nach 1 löst.

Logische Konsequenz eine Formel G ist eine logische Konsequenz einer Formel F ($F \models G$), wenn jedes Modell von F auch ein Modell für G ist.

Logische Äquivalenz zwei Formeln F und G sind semantisch äquivalent ($F \equiv G$), wenn sie genau dieselben Modelle haben FS 22

Normalform jede Formel lässt sich in eine äquivalente Formel in Normalform umformen.
Für die Umformungen gibt es Algorithmen, siehe FS 22

Negationsnormalform (NNF) enthält nur UND, ODER und Negation, wobei Negation nur direkt vor Atomen vorkommt.

Konjunktive Normalform (KNF) Formel ist eine Konjunktion von Disjunktionen von Literalen.

Disjunktive Normalform (DNF) Disjunktion von Konjunktionen von Literalen.

1.3 Komplexität

Turingmaschinen sind begrenzt durch die Anzahl ihrer Speicherzellen (Speicher) und der Anzahl möglicher Berechnungsschritte (Zeit). Schranken sind Funktionen gerichtet nach der Länge der Angabe. FS 24

O-Notation charakterisiert Funktionen nach ihrem Verhalten und versteckt Summanden kleinerer Ordnung und lineare Faktoren. Beispiel: ein Polynom $n^4 + 2n^2 + 150$ wird zu $O(n^4)$.

$O(f)$-zeitbeschränkt es gibt eine Funktion $g \in O(f)$, so dass eine DTM/NTM bei beliebiger Eingabe der Länge n nach einer maximalen Anzahl Schritte $g(n)$ anhält.

$O(f)$-speicherbeschränkt es gibt eine Funktion $g \in O(f)$, so dass eine DTM/NTM bei beliebiger Eingabe der Länge n nur eine maximale Anzahl Speicherzellen $g(n)$ verwendet.

Sprachklassen Einteilung von Sprachen nach der Möglichkeit der Entscheidbarkeit.
„Klasse aller Sprachen, welche…“

- **DTIME**$(f(n))$ …durch eine $O(f)$-zeitbeschränkte DTM entschieden werden können
- **DSPACE**$(f(n))$ …durch eine $O(f)$-speicherbeschränkte DTM entschieden werden können
- **NTIME**$(f(n))$ …durch eine $O(f)$-zeitbeschränkte NTM entschieden werden können
- **NSPACE**$(f(n))$ …durch eine $O(f)$-speicherbeschränkte NTM entschieden werden können

Komplexitätsklassen erfassen Sprachklassen je nach ihrer Komplexität. Stehen untereinander in Beziehung und bilden quasi Hierarchie. FS 24

- **PTime (P)** deterministisch, polynomielle Zeit
- **ExpTime (Exp)** deterministisch, exponentielle Zeit
- **LogSpace (L)** deterministisch, logarithmischer Speicher
- **PSpace** deterministisch, polynomieller Speicher
- **NPTime (NP)** nichtdeterministisch, polynomielle Zeit
- **NExpTime (NExp)** nichtdeterministisch, exponentielle Zeit
- **NLogSpace (NL)** nichtdeterministisch, logarithmischer Speicher
- **NPSpace** nichtdeterministisch, polynomieller Speicher (gleich PSpace)

SAT Boolean Satisfiability Problem. Problem, welches ein Modell für eine Formel auf Erfüllbarkeit untersucht. In NP. Interessant für Untersuchung, da SAT ein Problem darstellt, für welches es wahrscheinlich schwierig ist eine Lösung zu finden, jedoch sehr einfach ist eine Lösung auf Korrektheit zu prüfen. FS 25

Reduktion Rückführung eines Problems auf ein anderes. Beispiel Drei-Farben-Problem ist auf SAT reduzierbar, da sich die Farb-Zustände als Formeln ausdrücken kodieren lassen. „Alle Probleme in NP können polynomiell auf SAT reduziert werden“ (**Cook, Levin**)

Härte und Vollständigkeit für P und NP FS 25

- **NP-hart** Sprache ist NP-hart, wenn jede Sprache in NP polynomiell darauf reduzierbar ist (Beispiel Halteproblem und jedes weitere unentscheidbare Problem).
- **NP-vollständig** Sprache ist NP-hart und liegt selbst in NP (Beispiel SAT).
- **P-hart** Sprache ist P-hart, wenn jede Sprache in P mit logarithmischem Speicherbedarf auf diese reduzierbar ist.
- **P-vollständig** Sprache ist P-hart und liegt selbst in P (Beispiel HornSAT).

Zusammenfassung aller Themenkomplexe, Hierarchien und Zusammenhänge in FS 26.

2 Theoretische Informatik

2.1 Turingmaschinen

Turingmaschine deterministisch als DTM oder nichtdeterministisch als NTM.
Definiert als Tupel $(Q, \Sigma, \Gamma, \delta, q_0, F)$ mit endlicher Menge von Zuständen Q, Eingabealphabet Σ, Arbeitsalphabet Γ, Übergangsfunktion δ, Startzustand q_0 und Menge von akzeptierenden Endzuständen F. Können ein oder mehrere Bänder haben. Siehe auch Church-Turing-These. FS 18 TIL 1

Funktion Turingmaschine kann eine Funktion von Eingaben auf Ausgabewörter definieren. Wenn eine TM bei Eingabe w anhält und die Ausgabe der Form $v\sqcup\sqcup\ldots$ entspricht, hat diese TM die Funktion berechnet.

Sprache die von einer Turingmaschine erkannte Sprache ist die Menge aller Wörter, die von dieser TM akzeptiert werden (d.h. in einem Endzustand hält).

Konfiguration der „Gesamtzustand" einer TM, bestehend aus Zustand, Bandinhalt und Position des Lese-/Schreibkopfs; geschrieben als Wort (Bandinhalt), in dem der Zustand vor der Position des Kopfes eingefügt ist. Beispiel $\sqcup\sqcup q_0 aaba\sqcup\sqcup$.

Übergangsrelation Beziehung zwischen zwei Konfigurationen wenn die TM von der ersten in die zweite übergehen kann (deterministisch oder nichtdeterministisch)

Lauf mögliche Abfolge von Konfigurationen einer TM, beginnend mit der Startkonfiguration; kann endlich oder unendlich sein

Halten Ende der Abarbeitung, wenn die TM in einer Konfiguration keinen Übergang mehr zur Verfügung hat.

Transducer Ausgabe der Turingmaschine ist Inhalt des Bandes, wenn TM hält, ansonsten undefiniert. Endzustände sind irrelevant.

Entscheider Ausgabe der Turingmaschine ist „Akzeptiert", wenn TM in Endzustand hält, ansonsten „verwirft" (beinhaltet auch „TM hält nicht"). Bandinhalt ist irrelevant.

Aufzähler ist eine DTM, die bei Eingabe des leeren Bandes immer wieder (d.h. bis zum letzten Wort bei endlichen Sprachen) einen Zustand $q_{Ausgabe}$ erreicht, in welchem das aktuelle Band ein Wort aus der Sprache dieser DTM ist. Die Sprache dieser DTM ist dann die Menge der so erzeugten Wörter. Diese DTM muss nicht halten, die Sprache kann unendlich sein. Wörter dürfen mehrfach ausgegeben werden.

Berechenbarkeit bezogen auf Funktionen. Eine Funktion F heißt berechenbar, wenn es eine DTM gibt, die F berechnet. Ist durch geeignete Kodierung (z.B. binär) erweiterbar auf natürliche Zahlen, Wörterlisten und andere Mengen. TIL 2

rekursiv eine berechenbare totale Funktion ist rekursiv.

partiell rekursiv eine berechenbare partielle Funktion ist partiell rekursiv.

Entscheidbarkeit bezogen auf Sprachen. TIL 2

entscheidbar / berechenbar / rekursiv es existiert eine Turingmaschine, die das Wortproblem der Sprache entscheidet. D.h. die Turingmaschine ist Entscheider und die Sprache ist gleich der Sprache der TM.

semi-entscheidbar / Turing-erkennbar / Turing-akzeptierbar / rekursiv aufzählbar es existiert eine Turingmaschine, deren erzeugte Sprache gleich der Sprache ist, jedoch die TM kein Entscheider ist.
Eine Sprache ist genau dann semi-entscheidbar, wenn es einen Aufzähler für diese Sprache gibt.

unentscheidbar sonst.
„Es gibt Sprachen und Funktionen, die nicht berechenbar sind." Beweis anhand der abzählbaren Menge von Turingmaschinen im Vergleich zur Überabzählbarkeit der Menge der Sprachen über jedem Alphabet.

Probleme der Kategorie „Unentscheidbar bzw. unberechenbar, nicht berechenbar". TIL 2

Busy-Beaver-Funktion ist nicht berechenbar und wächst sehr schnell. Die Funktion nimmt eine natürliche Zahl n und gibt die maximale Anzahl x-Symbole, welche eine DTM mit n Zuständen und dem Arbeitsalphabet $\{x, \sqcup\}$ bis zu ihrem Halt schreiben kann, zurück.

2.2 LOOP und WHILE

LOOP und WHILE sind eine Erfindung von Schöning und sind quasi eine pädagogische Brücke zwischen den Ultra-low-level Turingmaschinen und High-level Programmiersprachen. WHILE baut auf LOOP auf. TIL 3

LOOP Besteht aus Variablen, Wertzuweisungen und Schleifen. Die Eingabe einer Menge von natürlichen Zahlen wird in $x_1, x_2, \dots$ gespeichert. Die Ausgabe ist eine natürliche Zahl, gespeichert in x_0. Alle weiteren Variablen haben den Wert 0. LOOP terminiert immer in endlich vielen Schritten. Berechnet eine totale Funktion.

Variablen Menge $\{x_0, x_1, \dots\}$ oder auch $\{x, y, myVariable\}$. Haben als Wert eine natürliche Zahl.

Wertzuweisungen in der Form $x := y + n$ oder $x := y - n$, wobei n eine natürliche Zahl ist. Eine Wertzuweisung ist bereits ein LOOP-Programm.

Schleifen in der Form LOOP x DO P END, wobei P wieder ein LOOP-Programm ist. Der Wert der Variable x kann in P nicht geändert werden. Daher terminiert ein LOOP-Programm immer in endlich vielen Schritten.

Hintereinanderausführung wenn P_0 und P_1 LOOP-Programme, dann auch $P_0; P_1$.

Syntax-Erweiterung Die Syntax lässt sich zur Vereinfachung erweitern.

Wertzuweisung $x := y$ $x := y + 0$

Rücksetzen $x := 0$ LOOP x DO $x := x - 1$ END

Wertzuweisung Zahl $x := n$ $x := 0; x := x + n$. Alternativ $x := null + n$

Variablen-Addition $x := y + z$ $x := y$; LOOP z DO $x := x + 1$ END

Bedingung **IF** $x \neq 0$ **THEN** LOOP x DO $y := 1$ END ; LOOP y DO P END

Berechenbarkeit eine Funktion heißt LOOP-berechenbar, wenn es ein LOOP-Programm gibt, welches die Funktion berechnet. Auch hier ist mit geeigneter Kodierung wieder mehr machbar, als nur die natürlichen Zahlen in Betracht zu ziehen (Beispiel Wortproblem, Probleme in NP, gängige Algorithmen). Es gibt berechenbare totale Funktionen, die nicht LOOP-berechenbar sind (vgl. Ackermannfunktion).

WHILE Basiert auf LOOP und erweitert dieses. Jedes LOOP-Programm ist auch ein WHILE-Programm.

Schleifen in der Form WHILE $x \neq 0$ DO P WHEN, wobei P wieder WHILE-Programm. Im Gegensatz zu LOOP kann in WHILE der Wert von x in P zur Laufzeit geändert werden. Es kann also passieren, dass das Programm nicht terminiert wenn x nie auf 0 gesetzt wird.

Konvertierung LOOP-Schleifen können in WHILE-Schleifen konvertiert werden. Eine DTM kann WHILE-Programme simulieren und ein WHILE-Programm DTMen simulieren.

Berechenbarkeit Eine partielle Funktion heißt WHILE-berechenbar, wenn es ein WHILE-Programm gibt, welches bei einem definierten $f(n_0, n_1, \dots)$ terminiert und bei einem nicht definierten Wertebereich nicht terminiert. Wenn eine partielle Funktion WHILE-berechenbar ist, ist sie **Turing-berechenbar**.

2.3 Universalität

Universalmaschine U eine Turingmaschine, die andere TM als Eingabe kodiert erhält und diese simuliert. Die Kodierung ist dabei z.B. binär, mit dem Trennsymbol $\#$. Hat vier Bänder: Eingabeband von U mit kodierter TM und kodierter Eingabe w, Arbeitsband von U, Band 3 mit aktuellem Zustand der simulierten TM und Band 4 als Arbeitsband der simulierten TM.
Für die Arbeitsweise siehe TIL 4

2.4 Unentscheidbare Probleme und Reduktionen

Beweis durch Diagonalisierung, Reduktionen TIL 4

Probleme der Kategorie „unentscheidbar“.

Halteproblem $\mathbf{P}_{Halt}$ Frage: „Gegeben eine Turingmaschine M und ein Wort w. Wird die Turingmaschine M für die Eingabe w jemals anhalten?“. Das Halteproblem $\mathbf{P}_{Halt}$ der Turingmaschine M für das Wort w kann formal kodiert werden als $enc(M)\#\#enc(w)$ und einer universellen Turingmaschine zur Überprüfung übergeben werden. Beweise für Unentscheidbarkeit anhand Diagonalisierung und Reduktion in TIL 4

Goldbachsche Vermutung Beispiel für ein auf das Halteproblem reduzierbares Problem. Besagt, dass jede gerade Zahl $n \geq 4$ die Summe zweier Primzahlen ist. Zum Beispiel ist $4 = 2 + 2$ und $100 = 47 + 53$. Lässt man nun eine Turingmaschine diese Vermutung systematisch beginnend bei 4 testen, würde ein Anhalten bei Misserfolg $\mathbf{P}_{Halt}$ und „die Vermutung stimmt nicht“ gleichzeitig lösen. Gäbe es demnach ein Programm, welches $\mathbf{P}_{Halt}$ lösen kann (entscheidet), wäre eine separate Überprüfung der Goldbachschen Vermutung nicht nötig. Die Frage der Goldbachschen Vermutung wäre sofort beantwortet.

ϵ **-Halteproblem** „Gegeben sei eine Turingmaschine. Wird diese TM für die leere Eingabe ϵ jemals anhalten?“. Unentscheidbar.

Beweismethoden zum Nachweis der Unentscheidbarkeit.

Kardinalität Beweis von Aussagen anhand der unterschiedlichen Kardinalitäten.

Diagonalisierung Berechenbarkeit annehmen und einen paradoxen Algorithmus für das Problem konstruieren.

Reduktion Rückführung eines unentscheidbaren Problems auf das gegebene. Die Reduktion ist ein Entscheidbarkeitsalgorithmus. Siehe auch *1.3 Komplexität*. TIL 4

Turing-Reduktion Ein Problem **P** ist Turing-reduzierbar auf ein Problem **Q** (in Symbolen: $\mathbf{P} \leq_T \mathbf{Q}$), wenn man **P** mit einem Programm lösen könnte, welches ein Programm für **Q** als Unterprogramm (auch: Subroutine) aufrufen darf. Das Programm für **Q** muss hierbei nicht existieren.

Many-One-Reduktion Eine berechenbare totale Funktion $f : \Sigma^* \to \Sigma^*$ ist eine Many-One-Reduktion von einer Sprache **P** auf eine Sprache **Q** (in Symbolen: $\mathbf{P} \leq_m \mathbf{Q}$), wenn für alle Wörter $w \in \Sigma^*$ gilt: $w \in \mathbf{P}$ gdw. $f(w) \in \mathbf{Q}$.
Schwächer als Turing-Reduktion, jede Many-One-Reduktion kann als Turing-Reduktion ausgedrückt werden (dies gilt jedoch nicht andersherum).

Satz von Rice Siehe *1.1 Sprachen und Automaten*. TIL 5
„Praktisch alle interessanten Fragen zu Sprachen von Turingmaschinen sind unentscheibar“. Eingabe ist eine Turingmaschine, Ausgabe „hat die Sprache der TM die Eigenschaft?“.

2.5 Semi-Entscheidbarkeit

Hinweis: Hierzu gibt es im Schöning gute graphische Darstellungen. TIL 5

Komplement einer Sprache L: $\overline{L} = \{w \in \Sigma^* \mid w \notin L\}$ (Achtung: auf Kontext achten. Komplement des Halteproblems ist z.B. anderer Form). Die Turing-Reduktionen $\overline{L} \leq_T L$ bzw. $L \leq_T \overline{L}$ sind mit einer Turingmaschine überprüfbar. Für eine Eingabe w entscheidet diese, ob $w \in L$ und invertiert das Ergebnis.

Semi-Entscheidbarkeit Beispiel anhand des Halteproblems: simuliere eine Turingmaschine und deren Eingabe, kodiert als $enc(M)\#\#enc(w)$. Wenn M hält, hält auch die universelle Turingmaschine und akzeptiert. Eine Sprache L ist entscheidbar, wenn sowohl L als auch $\overline{L}$ semi-entscheidbar sind.

Co-Semi-Entscheidbarkeit Wenn eine Sprache L unentscheidbar, jedoch semi-entscheidbar ist, kann $\overline{L}$ nicht semi-entscheidbar sein.

2.6 Postsches Korrespondenzproblem

Auch: **PCP**. Ein unentscheidbares Problem ohne direkten Bezug zu einer Berechnung. TIL 5

PCP Bei diesem Problem nimmt man eine Reihe von 2-Tupeln (anschaulich vergleichbar mit Dominosteinen) mit je einem Wert oben und einem unten. Ziel der Lösung ist nun, die gegebenen Tupel so anzuordnen, dass oben und unten die gleiche Wortkette entsteht. Beispiel: wir haben die drei Tupel (AB, B), (B, BBB) und (BB, BA). Eine Anordnung mit zehn Tupeln ergibt dann die Lösung. Es kann vorkommen, dass das Problem keine Lösung besitzt.

MPCP Hilfskonstruktion. Wir nutzen MPCP, um das Halteproblem auf MPCP zu reduzieren. Folgend reduzieren wir MPCP auf PCP. Beim MPCP wird PCP verwendet, jedoch das Start-Tupel vorgegeben. Die Lösung eines MPCP ist auch eine Lösung des entsprechenden PCP, welche mit dem gegebenen Start-Tupel beginnt.

2.7 Unentscheidbare Probleme formaler Sprachen

In diesem Kapitel wird wieder auf *1.1 Sprachen und Automaten* zurückgegriffen. Eine durch eine Grammatik G erzeugte Sprache wird als $L(G)$ bezeichnet. Für Beweise der folgenden Sätze siehe Vorlesung. Siehe auch Chomsky-Hierarchie in *1.1 Sprachen und Automaten*. TIL 6

- Das Schnittproblem regulärer Grammatiken (Typ 3) ist entscheidbar.
- Das Schnittproblem kontextfreier Grammatiken (Typ 2, **CFG**) ist unentscheidbar. Beweis durch Many-One-Reduktion vom PCP.
- Das Leerheitsproblem für kontextfreie Grammatiken ist entscheidbar.
- Kontextfreie Sprachen sind unter Vereinigung abgeschlossen.
- Deterministische kontextfreie Sprachen sind unter Komplement abgeschlossen.
- Das Äquivalenzproblem kontextfreier Grammatiken ist unentscheidbar.

2.8 Komplexitätstheorie

Untersuchung von Problemkomplexitäten und Suche nach Methoden zur Bestimmung der Komplexität eines Problems. Klassierung zwischen „leicht lösbar“ bis „schwer lösbar“. Einteilung von berechenbaren Problemen entsprechend der Menge an Ressourcen, die zu ihrer Lösung nötig sind. Einführung anhand von Beispielen. TIL 7

Eulerpfad Ein Eulerpfad ist ein Pfad in einem Graphen, der jede Kante genau einmal durchquert. Ein Eulerkreis ist ein zyklischer Eulerpfad. Ein Graph hat genau dann einen Eulerschen Pfad, wenn er maximal zwei Knoten ungeraden Grades besitzt und zusammenhängend ist.

Hamiltonpfad Ein Hamiltonpfad ist ein Pfad in einem Graphen, der jeden Knoten genau einmal durchquert. Ein Hamiltonkreis ist ein zyklischer Hamiltonpfad.

Schranken von Turingmaschinen in Zeit und Raum. Siehe *1.3 Komplexität*.

Speicher Zahl der verwendeten Speicherzellen

Zeit Zahl der durchgeführten Berechnungsschritte

O-Notation Siehe *1.3 Komplexität*.

Linear Speedup Theorem Sei M eine Turingmaschine mit $k > 1$ Bändern, die bei Eingaben der Länge n nach maximal $f(n)$ Schritten hält. Dann gibt es für jede natürliche Zahl $c > 0$ eine äquivalente k-Band Turingmaschine M', die nach maximal $\frac{f(n)}{c} + n + 2$ Schritten hält.
Bedeutet: in der Theorie kann jedes Programm mit Hilfe mehrerer Bänder „beliebig schneller“ gemacht werden. Dies ist praktisch nicht umsetzbar, da eine Turingmaschine nicht beliebig große Datenmengen in einem Schritt lesen und nicht beliebig komplexe Zustandsübergänge in konstanter Zeit realisieren kann.

2.9 Beziehungen der Komplexitätsklassen

Siehe *1.3 Komplexität* für eine Übersicht der Klassen. TIL 7

Nichtdeterministische Klassen $NL \subseteq NP \subseteq NPSpace \subseteq NExp$

DTM auch als NTM, d.h. nichtdet. stärker $L \subseteq NL$, $P \subseteq NP$, $PSpace \subseteq NPSpace$, $Exp \subseteq NExp$

Satz von Savitch Speicherbeschränkte NTM können durch DTMs nur mit quadratischen Mehrkosten simuliert werden. Insbesondere gilt damit $PSpace = NPSpace$.

Zusammenfassend: $L \subseteq NL \subseteq P \subseteq NP \subseteq PSpace = NPSpace \subseteq Exp \subseteq NExp$.
Jedoch ist zu beachten:

- Wir wissen nicht, ob irgendeines dieser $\subseteq$ sogar $\subsetneq$ ist.
- Insbesondere wissen wir nicht, ob $P \subsetneq NP$ oder $P = NP$.
- Wir wissen nicht einmal, ob $L \subsetneq NP$ oder $L = NP$.

2.10 Zeit und Raum

Zusammenhänge zwischen Zeitklassen und Speicherklassen bzw. deren Beschränkungen. TIL 8
Es gilt für beliebige Funktionen $f : \mathbb{N} \to \mathbb{R}$:

- $\mathrm{DTIME}(f) \subseteq \mathrm{DSPACE}(f)$
- $\mathrm{DSPACE}(f) \subseteq \mathrm{DTIME}(2^{O(f)})$

Robustheit von Zeitklassen Setzt sich aus zwei Erkenntnissen zusammen:

- Konstante Faktoren haben keinen Einfluss auf die Probleme, die eine zeitbeschränkte Mehrband-TM lösen kann, sofern mindestens lineare Zeit erlaubt ist (Linear Speedup Theorem). Sofern nicht einmal lineare Zeit zur Verfügung stände, könnte die TM nicht einmal die Eingabe lesen!
- Die Anzahl der Bänder hat lediglich einen polynomiellen (quadratischen) Einfluss auf die Probleme, die eine zeitbeschränkte TM lösen kann.

Robustheit von Speicherklassen Weder konstante Faktoren, noch die Anzahl der Bänder haben Einfluss auf die Probleme, welche eine speicherbeschränkte TM lösen kann.

3 Prädikatenlogik

Die Prädikatenlogik erweitert die Aussagenlogik. Neben den neuen Mengen **V**, **C** und **P** kommen der Allquantor $\forall$ und der Existenzquantor $\exists$ hinzu. **Hinweis:** In dieser Vorlesung entfallen Funktionssymbole! TIL 13

3.1 Syntax

Im Gegensatz zu der unendlichen Menge von Atomen in der Aussagenlogik gibt es in der Prädikatenlogik mehrere betrachtete Mengen. Diese Mengen sind abzählbar unendlich und die Elemente disjunkt. Formeln sind, ausgenommen genannter Ausnahmen, eindeutig zu klammern. TIL 13

Variablen Die Menge **V**, bestehend aus $x, y, z \ldots$. Variablen können frei oder gebunden vorkommen (oder bei mehrfachem Auftreten einer Variable in einer Formel auch beides). **Freie** Variablen sind durch keinen Quantor gebunden. **Gebundene** Variablen befinden sich innerhalb des „Scope" eines Quantors. Beispiel: in der Formel $p(x) \wedge \exists x.q(x)$ kommt x sowohl frei ($p(x)$) als auch gebunden ($q(x)$) vor.

Konstanten Die Menge **C**, bestehend aus $a, b, c, \ldots$

Prädiktensymbole Die Menge **P**, bestehene aus $p, q, r, \ldots$. Bei nullstelligen Prädiktensymbolen lassen wir die leeren Klammern weg.

Quantoren Der Allquantor $\forall$ beschreibt, dass die betreffende Formel für alle möglichen Interpretationen der Variable gelten muss. Der Existenzquantor $\exists$ beschreibt, dass es mindestens eine gültige Interpretation der Variable geben muss. Wenn ein Quantor vor einer Formel mehrere Variablen betrifft, schreiben wir diese als Liste ($\forall x, y.F$ statt $\forall x.\forall y.F$).

Atom Ein prädikatenlogisches Atom ist ein Ausdruck $p(t_1, \ldots, t_n)$ für ein n-stelliges Prädiktensymbol $p \in \mathbf{P}$ und **Terme** $t_1, \ldots, t_n \in \mathbf{V} \cup \mathbf{C}$

Formel Jedes Atom ist eine Formel. Wenn nun $x \in \mathbf{V}$ und F und G Formeln, dann sind auch $\neg F$, $(F \wedge G)$, $(F \vee G)$, $(F \to G)$, $(F \leftrightarrow G)$, $\exists x.F$ und $\forall x.F$ Formeln. Die äußersten Klammern von Formeln dürfen weggelassen werden. Klammern innerhalb von mehrfachen Konjunktionen oder Disjunktionen dürfen weggelassen werden. Hat eine Formel keine freie Variablen ist sie **geschlossen** und wird **Satz** genannt, ansonsten ist sie eine **offene** Formel.

Teilformel Teilformeln einer Formel sind alle Teilausdrücke einer Formel, welche selbst Formeln sind.

3.2 Semantik

Der Wahrheitswert von Formeln ergibt sich aus den Wahrheitswerten der Atome in dieser Formel. TIL 13

Interpretation Interpretation $\mathcal{I}$ ist ein Paar $\langle \Delta^{\mathcal{I}}, \cdot^{\mathcal{I}} \rangle$.
Die nichtleere Menge $\Delta^{\mathcal{I}}$ wird auch **Domäne** genannt.
Die Funktion $\cdot^{\mathcal{I}}$ heißt **Interpretationsfunktion**. Diese bildet jede Konstante $a \in \mathbf{C}$ auf ein Element $a^{\mathcal{I}} \in \Delta^{\mathcal{I}}$ und jedes n-stellige Prädiktensymbol $p \in \mathbf{P}$ auf eine Relation $p^{\mathcal{I}} \in (\Delta^{\mathcal{I}})^n$ ab.

Zuweisung Zuweisung $\mathcal{Z}$ für eine Interpretation $\mathcal{I}$ ist eine Funktion $\mathcal{Z} : \mathbf{V} \to \Delta^{\mathcal{I}}$, sie bildet also Variablen auf Elemente der Domäne ab. Bei $x \in \mathbf{V}$ und $\delta \in \Delta^{\mathcal{I}}$ schreiben wir für die Zuweisung von x auf δ und für alle $y \neq x$ auf $\mathcal{Z}(y)$: $\mathcal{Z}[x \mapsto \delta]$.

Wahrheitsbestimmung Die Wahrheitsbestimmung von Atomen und Formeln unter einer Interpretation und einer Zuweisung werden rekursiv aufgelöst.

- Für Konstanten c benötigen wir nur die Interpretation: $c^{\mathcal{I},\mathcal{Z}} = c^{\mathcal{I}}$
- Für Variablen x benötigen wir nur die Zuweisung: $x^{\mathcal{I},\mathcal{Z}} = \mathcal{Z}(x)$
- Für Prädikate/Atome $p(t_1, \ldots, t_n)$ setzen wir nun rekursiv:
  $p(t_1, \ldots, t_n)^{\mathcal{I},\mathcal{Z}} = 1$ wenn $\langle t_1^{\mathcal{I},\mathcal{Z}}, \ldots, t_n^{\mathcal{I},\mathcal{Z}} \rangle \in p^{\mathcal{I}}$ bzw.
  $p(t_1, \ldots, t_n)^{\mathcal{I},\mathcal{Z}} = 0$ wenn $\langle t_1^{\mathcal{I},\mathcal{Z}}, \ldots, t_n^{\mathcal{I},\mathcal{Z}} \rangle \notin p^{\mathcal{I}}$

Für eine Formel gilt nun:
eine Interpretation $\mathcal{I}$ und eine Zuweisung $\mathcal{Z}$ **erfüllen** eine Formel F, geschrieben „$\mathcal{I}, \mathcal{Z} \models F$", wenn die Rekursion mit Atomen, Operationen und Quantoren zu Wahr auflöst.

3.3 Semantische Grundbegriffe

Wir wollen in der Prädikatenlogik wenn möglich nur mit Sätzen arbeiten, d.h. mit geschlossenen Formeln ohne ungebundene Variablen. TIL 14

Modelltheorie Wir unterscheiden grob zwischen der Prädikatenlogik mit und ohne offenen Formeln. Bei der Prädikatenlogik mit Sätzen können wir auf Zuweisungen verzichten. Formeln sind Behauptungen, die wahr oder falsch sein können. Modelle sind mögliche Welten (prädikatenlogische Interpretationen und ggf. Zuweisungen), in denen manche Behauptungen gelten und andere nicht. (**Intuition**)

Typen von Formeln Siehe hierzu auch die Graphen „Modelle $\models$ Formeln“ in TIL 14

- allgemeingültig (tautologisch): Eine Formel, die in allen Modellen wahr ist
- widersprüchlich (inkonsistent): Eine Formel, die in keinem Modell wahr ist
- erfüllbar: Eine Formel, die in einem Modell wahr ist
- widerlegbar: Eine Formel, die in einem Modell falsch ist

Logisches Schließen Bei der Analyse von Modellen für Formeln und andersherum können in Wechselwirkung Konsequenzen hergestellt werden.

a) Wenn $\mathcal{I}$ die Formel F erfüllt, also $\mathcal{I} \models F$, dann ist $\mathcal{I}$ ein Modell für F.

b) $\mathcal{I}$ kann mehrere Formeln erfüllen, d.h. sie kann Modell für eine Formelmenge $\mathcal{T}$ sein, wenn $\mathcal{I}$ alle Formen in $\mathcal{T}$ erfüllt.

c) Eine Formel F ist nun eine **logische Konsequenz** aus einer Formel bzw. Formelmenge G, d.h. $G \models F$, wenn jedes Modell $\mathcal{I}$ von G auch ein Modell von F ist, d.h. $\mathcal{I} \models G \implies \mathcal{I} \models F$. Sonderfall: Ist F eine Tautologie, dann schreiben wir nur $\models F$.

Beispiel 1: Gegeben sind vier Modelle $\mathcal{I}_i$ und vier Formeln F_j. $\mathcal{I}_2$ und $\mathcal{I}_3$ sind alle erfüllenden Modelle für F_3. $\mathcal{I}_2$ und $\mathcal{I}_3$ sind aber u.a. auch Modelle für F_2. Das bedeutet, wenn F_3 erfüllt ist, ist auch immer F_2 erfüllt. Es gilt $F_3 \models F_2$.

Beispiel 2: Im Beispiel der Logelei „Wir sind alle vom gleichen Typ“ haben wir fünf Formeln gegeben. Drei davon ergeben sich aus den gegebenen Aussagen („gegebene Theorie“) und die anderen beiden sind Allquantor-Behauptungen für „alle sagen die Wahrheit“ bzw. „alle lügen.“. Wir können anhand der Modelle „LL“, „WL“ und „WW“ und der Theorie Konsequenzen erstellen und somit über das Modell „WW“ die Behauptung „$\forall x.W(x)$“ als logische Konsequenz für unsere Theorie identifizieren.

d) Zwei Formelmengen F und G können auch semantisch äquivalent sein, d.h. $F \equiv G$, wenn sie genau die gleichen Modelle haben ($\mathcal{I} \models F$ gdw. $\mathcal{I} \models G$ für alle Modelle $\mathcal{I}$).

Semantische Äquivalenz Eine Äquivalenzrelation $\equiv$ ist reflexiv, symmetrisch und transitiv. Alle Tautologien sind semantisch äquivalent. Alle unerfüllbaren Formeln sind semantisch äquivalent. Äquivalenz $F \equiv G$ gdw. $F \models G$ und $G \models F$.

Problem logischen Schließens in der Prädikatenlogik Die zwei Fragen „Model checking“ (Überprüfung eines Modells auf Erfüllung einer Formel) und „Logische Folgerung (Entailment)“ (Überprüfung ob zwei Formeln oder Formelmengen eine logische Konsequenz sind) sind in der Prädikatenlogik schwerer zu lösen als in der Aussagenlogik.

Monotonie und Tautologie Aus der Definition von $\models$ folgt die Monotonie: je mehr Sätze in einer logischen Theorie gegeben sind, desto weniger Modelle können die gesamte Theorie erfüllen und desto mehr Schlussfolgerungen kann man aus der logischen Theorie ziehen. D.h. mehr Annahmen führen zu mehr Schlussfolgerungen. Extremfälle sind hierbei Tautologien (sind in jedem Modell wahr und daher logische Konsequenz jeder Theorie) und unerfüllbare Formeln (sind in keinem Modell wahr und haben daher alle anderen Sätze als Konsequenz).

Gleichheit Es gibt ein spezielles Gleichheitsprädikat $\approx$. In Interpretationen $\mathcal{I}$ gilt $\approx^{\mathcal{I}} = \{\langle\delta, \delta\rangle | \delta \in \Delta^{\mathcal{I}}\}$. Dies kann z.B. zum Erzwingen von gleicher Interpretation von Konstanten verwendet werden. Auch gibt es $\not\approx$, Definition $\forall x, y.(x \not\approx y \leftrightarrow \neg x \approx y)$. Man kann aber mit Hilfe anderer Definitionen der Prädikatenlogik sowohl Gleichheit als auch Ungleichheit einsparen. TIL 14 TIL 15

3.4 Prädikatenlogik als Universalsprache

Die Entwicklung der Logik hat ein zentrales Motiv: Logik als eine universelle, präzise Sprache. Die Entwicklung begann bei Aristoteles als Grundlage der philosophischen Argumentation, ging in Leibniz Sinne in Richtung „rechnen“ und wurde von Hilbert und Russell schließlich zusammen mit der Mathematik formalisiert. Wenn nun die Mathematik in logischen Formeln formuliert wird, wird logisches Schließen zur Kernaufgabe der Mathematik. Eine zentrale Frage des Schließens ist hierbei die Überprüfung auf Erfüllbarkeit einer Formel bzw. einer Formelmenge. TIL 15

Strukturelle Induktion Diese Induktion kann man über jede induktiv definierte syntaktische Struktur durchführen (z.B. Formeln, Terme, Programme,...).

- In der „klassischen Induktion“ wird eine Eigenschaft E untersucht, wobei (1) „0 hat E“ geprüft und darauf aufbauend (2) für alle $n > 0$ im Falle von „$n-1$ hat E“ geprüft wird.
- In der **strukturellen Induktion auf Formeln** prüfen wir nun ob (1) alle atomaren Formeln E haben und (2) alle nicht-atomaren Formeln F ebenfalls E haben, wenn alle ihre echten Teilformeln E haben.

Im Beispiel „Induktion auf der Insel der Wahrheitssager und Lügner. Ein Einwohner verkündet: 'Was ich jetzt sage, das habe ich schon einmal gesagt.' Welchen Typ hat er?“ muss der Einwohner ein Lügner sein, da er mindestens beim ersten Mal lügt.

3.5 Unentscheidbarkeit des logischen Schließens

Erinnerung: F ist logische Konsequenz von G ($F \models G$), wenn alle Modelle von F auch Modelle von G sind. (1) Es ist nicht offensichtlich, wie man das überprüfen sollte, denn es gibt unendliche viele Modelle. (2) Ebenso schwer erscheinen die gleichwertigen Probleme der Erfüllbarkeit und Allgemeingültigkeit.

Intuition: prädikatenlogisches Schließen ist unentscheidbar. Beweis durch Reduktion eines bekannten unentscheidbaren Problems, z.B. Halteproblem, PCP, Äquivalenz kontextfreier Sprachen u.a.

Der Beweis in der Vorlesung zeigt die Reduktion vom CFG-Schnittproblem. Hierfür werden Wörter ω aus der Modellmenge (Modellstruktur) $\mathcal{I}$ als Ketten von binären Relationen kodiert und untersucht, ob das Wort ω in der Schnittmenge zweier kontextfreier Grammatiken G_1 und G_2 vorkommt.
Beispiel: wir haben auf der Insel z.B. das Modell mit Kombination „LLWWW“ (drei sagen die Wahrheit, zwei lügen), und wir wollen wissen ob $F \models G$. Wir kodieren die erfüllenden Modelle der Formeln F und G wie o.g. und erhalten G_1 und G_2. Nach Kodierung müssten also in beiden Grammatiken die Übergänge $\langle L_1, L_2\rangle, \langle L_2, W_1\rangle, \langle W_1, W_2\rangle, \langle W_2, W_3\rangle$ vorkommen. Ist dies der Fall, dann erfüllt dieses Modell beide Formeln. (*Vergleich und Notation nicht nach VL!*)
Zusammenfassend lassen sich demnach logische Konsequenzen auf diese Probleme reduzieren und da CFG unentscheidbar gilt auch: Logisches Schließen (Erfüllbarkeit, Allgemeingültigkeit, logische Konsequenz) in der Prädikatenlogik ist unentscheidbar. TIL 15

3.6 Gödel

Gödelscher Vollständigkeitssatz und Unvollständigkeitssätze. TIL 15

Gödelscher Vollständigkeitssatz „Es gibt ein konsistentes Verfahren, das alle Konsequenzen einer prädikatenlogischen Theorie effektiv beweisen kann.“ (1) Alle wahren Sätze können endlich bewiesen werden. (2) Prädikatenlogisches Schließen ist semi-entscheidbar.

1. Gödelscher Unvollständigkeitssatz „Es gibt kein konsistentes Verfahren, das alle Konsequenzen der elementaren Arithmetik effektiv beweisen kann.“ (1) Für jedes Verfahren gibt es Sätze über elementare arithmetische Zusammenhänge, die weder bewiesen noch widerlegt werden können. (2) Die Wahrheit elementarer arithmetischer Zusammenhänge ist nicht semi-entscheidbar.

2. Gödelscher Unvollständigkeitssatz

3.7 Algorithmen zum logischen Schließen

Resolution TIL 16

3.8 Syntaktische Umformungen

Ersetzungstheorem, Junktoren wie in Aussagenlogik.
Neu: Äquivalenzen mit Quantoren TIL 16
Negationsnormalform (NNF), bereinigte Formel TIL 16
Pränexform, Skolemisierung, Einführung Funktionssymbole TIL 17
Konjunktive NF, Klauselform TIL 17

4 Repetitorien

4.1 Repetitorium I

Aufgabe A

Wiederholung von Begriffen Einband Turing-Maschine, Mehrband Turing-Maschine, Entscheidungsproblem, Unentscheidbarkeit, Aufzählbarkeit, Abzählbarkeit und Halteproblem.

Aufgabe B

Zeigen Sie: Wenn es möglich ist, für zwei beliebige Turing-Maschinen zu entscheiden, ob sie dieselbe Sprache akzeptieren, so ist es auch möglich, für beliebige Turing-Maschinen zu entscheiden, ob sie die leere Sprache akzeptieren. Seien K, M_1, M_2 Turingmaschinen, so dass $K(enc(M_1)\#\#enc(M_2))$ akzeptiert $\Leftrightarrow L(M_1) = L(M_2)$ und K hält auf jeder Eingabe.
Lösung: Sei M Turingmaschine und sei $M_\emptyset$ eine Turingmaschine, so dass $L(M_\emptyset) = \emptyset$.
Dann gilt $K(enc(M)\#\#enc(M_\emptyset))$ akzeptiert $\Leftrightarrow L(M) = \emptyset$, also $\mathbf{P}_{Leer} \leq_m \mathbf{P}_{\ddot{A}quiv}$.

Aufgabe C

Zeigen Sie, dass $\{1\}^*$ unentscheidbare Teilmengen besitzt.
Lösung: $\{1\}^*$ ist abzählbar unendlich, also ist $\mathfrak{P}(\{1\}^*)$ überabzählbar. Es gibt aber nur abzählbar unendlich viele entscheidbare Sprachen (auch: abzählbar viele nicht-äquivalente Turingmaschinen). Also sind einige (fast alle) dieser Sprachen unentscheidbar.

Aufgabe D

a) „Jedes LOOP-Programm terminiert." – Richtig. Definition von LOOP sagt, dass Anzahl Durchläufe nicht mehr während der Laufzeit geändert werden kann, demnach gibt es eine endliche Anzahl Durchläufe.

b) „Zu jedem WHILE-Programm gibt es ein äquivalentes LOOP-Programm." – Falsch, nicht zu jedem WHILE-Programm gibt es immer ein äquivalentes LOOP-Programm. Dies liegt daran, dass LOOP keine partiellen Funktionen verarbeiten kann.
Beispiel anhand von Division: LOOP terminiert immer, jedoch wäre Division durch 0 (ebenfalls in $\mathbb{N}$) undefiniert. Kann demnach nur mit WHILE gelöst werden (Fall $x_2 = 0$ für $div(x_1, x_2)$ landet in Endlosschleife).

c) „Die Anzahl der Ausführungen von P in der LOOP-Schleife LOOP x_i DO P END kann beeinflusst werden, indem x_i in P entsprechend modifiziert wird." – Falsch, Anzahl Schleifen kann laut Definition von LOOP nicht während Laufzeit geändert werden.

d) „Die Ackermannfunktion ist total und damit LOOP-berechenbar." – Falsch, die Ackermannfunktion ist zwar total, jedoch nicht LOOP-berechenbar (jedoch berechenbar). Die Funktion wurde gezielt gesucht und gefunden, um genau diesen Fall zu zeigen.

Aufgabe E

Geben Sie eine Turing-Maschine A_{mod2} an, die die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(x) = (x \ mod \ 2)$ berechnet. Stellen Sie dabei die Zahlen in unärer Kodierung dar.
Lösung: $A_{mod2} = (\{q_0, \ldots, q_f\}, \{x\}, \{x, \sqcup\}, \delta, q_0, \{q_f\})$. Die Turingmaschine liest die eingegebenen x (unäre Kodierung) und wechselt zwischen q_0 und q_1. Sobald auf ein $\sqcup$ gestoßen wird, weiß die TM, ob eine gerade oder ungerade Anzahl x eingegeben wurde. Wenn gerade, lösche alle x und ende in leerem Band. Wenn ungerade, lösche alle x und schreibe zum Abschluss ein x auf das Band.

Aufgabe F

Es sei $f : \mathbb{N} \to \mathbb{N}$ mit $f(x) = \lfloor \log_{10}(x) \rfloor$. Geben Sie ein WHILE-Programm an, welches f berechnet.
Lösung: Erst eine endlose WHILE-Schleife für die Eingabe $x = 0$. Dann Lösung mit $div(x, 10)$.

Aufgabe G

a) „Die Menge der Instanzen des Postschen Korrespondenzproblems, welche eine Lösung haben, ist semi-entscheidbar.“ – Richtig. Wenn eine Lösung existiert, kann diese (z.B. durch Breitensuche) auch gefunden werden.

b) „Das Postsche Korrespondenzproblem ist bereits über dem Alphabet $\Sigma = \{a, b\}$ nicht entscheidbar.“ – Richtig, denn Instanzen können über Σ kodiert werden, ohne die Entscheidbarkeit zu beeinflussen.

c) „Es ist entscheidbar, ob eine Turingmaschine nur Wörter akzeptiert, die Palindrome sind.“ – Falsch, Satz von Rice (die Akzeptanz von Palindromen ist eine **Eigenschaft**). Eigenschaft E ist „L besteht nur aus Palindromen“, diese Eigenschaft ist nicht-trivial: erfüllt z.B. durch $L = \emptyset$, jedoch nicht durch $L = \{ab\}$.

d) „ $\mathbf{P}_{Halt}$ ist semi-entscheidbar“ – Richtig, da es universelle Turingmaschinen gibt, die beliebige TM simulieren können.

e) „Es ist nicht entscheidbar, ob die von einer deterministischen Turing-Maschine berechnete Funktion total ist.“ – Richtig, denn sonst wäre das Halteproblem entscheidbar ($\mathbf{P}_{Halt} \leq_m \mathbf{P}_{Total}$).
Reduktion: M, w gegeben, baue Turingmaschine M' mit
$M' =$ bei Eingabe x
$\rightarrow$ simuliere M auf w
$\rightarrow$ akzeptiere mit leerem Band
M hält auf $w \Rightarrow M'$ berechnet $f(x) = \epsilon$
M hält nicht auf $w \Rightarrow M'$ berechnet Abbildung, die nirgends definiert ist.
Reduktion demnach $enc(M)\#\#enc(w) \mapsto enc(M')$.

f) „Es gibt reguläre Sprachen, die nicht semi-entscheidbar sind.“ – Falsch. Reguläre Sprachen sind immer entscheidbar, da Turingmaschinen endliche Automaten simulieren können.

Aufgabe H

Sei L eine unentscheidbare Sprache. Zeigen Sie:

a) „L hat eine Teilmenge $T \subseteq L$, die entscheidbar ist.“: $T = \emptyset$.

b) „L hat eine Obermenge $O \supseteq L$, die entscheidbar ist.“: $O = \Sigma^*$.

c) „Es gibt jeweils nicht nur eine sondern unendlich viele entscheidbare Teilmengen bzw. Obermengen wie in (a) und (b).“ – Es gilt: L ist unendlich. Dann ist die Menge der endlichen Teilmengen von L unendlich. Alles diese sind entscheidbar. Genauso für **b)**, z.B. muss $\Sigma^* \setminus L$ unendlich sein. Die Menge der endlichen Teilmengen E von $\Sigma^* \setminus L$ ist unendlich, für jede ist $\Sigma^* \setminus E$ entscheidbar.

4.2 Repetitorium II (02.06.2017)

Aufgabe α

a) P: Menge aller Entscheidungsprobleme, die von einer deterministischen TM in polynomieller Zeit entschieden werden können. (entschieden: der Algorithmus hält immer)

b) NP: Wie P, nur mit NTM. Menge aller Entscheidungsprobleme, so dass für Instanzen ein Zertifikat in polynomieller Zeit geraten und überprüft werden kann. (NP ist Menge aller Suchprobleme, bei denen ich weiß wann ich angekommen bin)

c) $PSpace$: Menge aller Entscheidungsprobleme, die von einer DTM in polynomiellem Platz entschieden werden können.

d) $P \subseteq NP \subseteq PSpace$: DTM „sind" auch NTM $\rightarrow P \subseteq NP$. NTP, die polynomiell-zeitbeschränkt sind, können in deterministisch polynomiellem Platz simuliert werden $\rightarrow NP \subseteq PSpace$. (Auch anhand der Anzahl möglicher Lesevorgänge begründbar). Außerdem Satz von Savitch: $NP \subseteq NPSpace \subseteq PSpace$.

e) $\mathcal{C}$-hart: ein Entscheidungsproblem ist $\mathcal{C}$-hart, wenn alle Probleme in in $\mathcal{C}$ in polynomieller Zeit auf dieses reduzierbar sind. Es ist $\mathcal{C}$-vollständig, wenn es $\mathcal{C}$-hart ist und selbst in $\mathcal{C}$ liegt. Am Beispiel von SAT sehen wir, dass SAT $\mathcal{C}$-vollständig ist, da es selbst in NP liegt und kein Problem in NP schwerer ist (und somit alle auf SAT reduzierbar sind) als SAT. Es kann vorkommen, dass mehrere Probleme $\mathcal{C}$-vollständig sind, wenn diese in polynomiell äquivalenter Zeit lösbar sind.

Aufgabe β

Zeigen, dass NP unter Kleene-Stern abgeschlossen. $\forall L \in NP : L^* \in NP$
Sei $L \in NP$ und sei M eine polynomiell-zeitbeschränkte TM, so dass $L = L(M)$.
Definiere $N =$ bei Eingabe ω

- rate Zerlegung $\omega = \omega_1, \ldots, \omega_n$ (beim leeren Wort: $n = 0$) (nicht-deterministisch)
- simuliere M auf ω_i für $i = 1, \ldots, n$ (nicht-deterministisch)
- akzeptiere, falls alle Simulationen akzeptieren

N ist polynomiell-zeitbeschränkt und $L(N) = L^*$

Aufgabe γ

Aufgabe mit Problem **K**: zwei gerichtete Graphen G_1 und G_2 sowie eine Zahl $k \in \mathbb{N}$. Gesucht: Teilmengen und Bijektion.

a) $K \in NP$ da Teilmengen $V_1^{'}$ und $V_2^{'}$ und die Zuordnung f geraten werden kann und in polynomieller Zeit überprüfbar ist ob $f : V_1 \rightarrow V_2$ eine Bijektion ist, so dass $(u, v) \in E_1 \implies (f(u), f(v)) \in E_2$.

b) Sei G ein Graph und $n \in \mathbb{N}$. Gefragt ist dann, ob G eine **CLIQUE** der Größe n als Untergraph enthält.
Sei $f(enc(G)\#\#enc(n)) := enc(G)\#\#enc(K_n)\#\#enc(n)$ wobei K_n der vollständige Graph auf n Knoten ist. Dann gilt: f ist polynomiell-zeitbeschränkt und G hat **CLIQUE** der Größe $n \iff enc(G)\#\#enc(K_n)\#\#enc(n) \in K$. Also ist f eine polynomiell-zeitbeschränkte Many-One-Reduktion von **CLIQUE** auf K und damit ist K auch NP-hart.
Liste bekannter Probleme: SAT/3SAT/CNFSAT, CLIQUE/IndepententSet/HamiltonCircle, 3-Färbbarkeit

Aufgabe δ

a) Entscheider für L_1: $N =$ bei Eingabe ω

- berechne Reduktion $f(\omega)$ (polynomielle Zeit)
- entscheide, ob $f(\omega) \in L_2$

N ist polynomiell-platzbeschränkt, da:

- f polynomiell-zeitbeschränkt
- $f(\omega) \in L_2$ kann in polynomiellem Platz entschieden werden.

N ist auch Entscheider, da es einen polynomiell-platzbeschränkten Entscheider für L_2 gibt. Also ist $L_1 \in PSpace$.

b) Sei $L \in PSpace$. Dann ist $L \leq_p L_1 \leq_p L_2$ also $L \leq_p L_2$ (transitiv). Also ist jedes Problem in PSpace auf L_2 in polynomieller Zeit reduzierbar und L_2 damit PSpace-hart.

Aufgabe ϵ

a) „Jedes PSpace-harte Problem ist NP-hart“ – Richtig, da $NP \subseteq PSpace$.

b) „Es gibt kein NP-hartes Problem, welches in PSpace liegt“ – Falsch, z.B. gilt $SAT \in PSpace$ und SAT ist NP-hart.

c) „Jedes NP-vollständige Problem liegt in PSpace“ – Richtig, da $NP \subseteq PSpace$ und alle NP-vollständigen Probleme liegen in NP.

d) „Es gilt $NP = PSpace$, wenn es ein PSpace-hartes Problem in NP gibt“ – Richtig, $NP \subseteq PSpace$ ist bekannt. Sei L ein PSpace-hartes Problem in NP. Sei $L' \in PSpace$. Dann gilt $L' \leq_p L$ und da NP unter polynomieller Zeitreduktion abgeschlossen ist, folgt $L' \in NP$. Also gilt $PSpace \subseteq NP$ und damit auch $NP = PSpace$.

e) „Wenn $P \neq NP$ gilt, dann gibt es kein NP-hartes Problem in P“ – Richtig, sonst wäre $P = NP$.

f) „Sei L ein PSpace-vollständiges Problem. Dann gilt $L \in P \iff P = PSpace$“ – Richtig.

Aufgabe ζ

Tic-Tac-Toe-Spiel. Die Beschreibung einer Gewinnstrategie erfolgt mit Hilfe eines Baumes, auf dem die möglichen Abläufe skizziert werden. Alle Möglichen Spielzüge von X und O führen zum Sieg von X.

Aufgabe η

„Zeigen Sie, dass für jedes PSpace-vollständige Problem **L** auch das Komplement $\overline{\mathbf{L}}$ ein PSpace-vollständiges Problem ist.“ $\mathbf{L} \in PSpace \rightarrow \overline{\mathbf{L}} \in PSpace$. $\overline{\mathbf{L}}$ ist PSpace-hart:

$$\begin{aligned} \mathbf{H} \in PSpace &\Longrightarrow \overline{\mathbf{H}} \in PSpace \\ &\Longrightarrow \overline{\mathbf{H}} \leq_p L \\ &\Longrightarrow \mathbf{H} \leq_p \overline{\mathbf{L}} \end{aligned}$$

Also ist $\overline{\mathbf{L}}$ PSpace-vollständig.

Aufgabe θ

„Zeigen Sie: ist $P = NP$, dann sind alle Sprachen $\mathbf{L} \in P \setminus \{\emptyset, \Sigma^*\}$ NP-vollständig.“
Sei $\mathbf{L} \in P \setminus \{\emptyset, \Sigma^*\}$. Sei $K \in NP$. Wir zeigen, dass $\mathbf{K} \leq_p \mathbf{L}$, unter der Annahme, dass $P = NP$.

Seien $x_1 \in \mathbf{L}, x_2 \in \Sigma^* \setminus \mathbf{L}$. Definiere $f(\omega) = \begin{cases} x_1 \; falls \; \omega \in \mathbf{K} \\ x_2 \; sonst \end{cases}$

Da $\mathbf{K} \in P$ ist die Abbildung f in polynomieller Zeit berechenbar. Es gilt $\omega \in \mathbf{K} \iff f(\omega) \in \mathbf{L}$. Also ist f eine polynomiell-zeitbeschränkte Many-One-Reduktion von **K** auf **L**. Also ist **L** auch NP-vollständig.