Reduktionen

- turing red.: $P \leq_T Q$ P kann mit Q als subroutine gelößt werden
- poly. m-red.: $P \leq_p Q \Leftrightarrow \forall w \in \Sigma^* : w \in P \leftrightarrow f(w) \in Q$
- L ist NP-hard: $\forall L' \in$ NP : $L' \leq_p L$ (alle L' aus NP sind auf L p.m.r.)
- L element NP: ex. ein poly. Verifikator (Cert. überprüfbar in P)
- L ist NP-complete: $L \in$ NP und L NP-hard
- Jede m-red ist eine t-red (aber nicht anders herum)
  ex. P s.d. $P \leq_T Q$ aber nicht $P \leq_m Q$

(Un)Entscheidbarkeit

- entscheidbar: ex. TM, die f.a. inputs $w(\in | \notin)L$ hält
- (co)-semi-entscheidbar: ex. TM, die f.a. inputs $w(\notin) \in L$ hält
- $P \leq Q$, Q (un)entscheidbar $\Rightarrow$ P (un)entscheidbar
- semi- + co-semi = entscheidbar = L und $\bar{L}$ entscheidbar
- $Phalt \leq P \wedge PHalt \leq \bar{P} \Rightarrow$ vollständig unentscheidbar
- Satz v. Rice: E nicht-triviale Eigenschaft, TM M mit L=L(M) hat L die E ? $\Rightarrow$ Unentscheidbar

Beziehungen von Klassen

- L $\subseteq$ NL $\subseteq$ P $\subseteq$ NP $\subseteq$ PSpace $\subseteq$ NPSpace $\subseteq$ EXP $\subseteq$ NEXP
- Satz von Savitch: NSpace(f(n)) $\subseteq$ DSpace(f(n)^2)
- NL $\subsetneq$ PSpace, P $\subsetneq$ EXP, NP $\subsetneq$ NEXP (folgt auf THT/SHT)
- Satz von Immerman, Szelepcsenyi: NL $=$ coNL
- $L \in$ DTIME/DSPACE $\Leftrightarrow \bar{L} \in$ DTIME/DSPACE
- wenn NP $=$ coNP $\rightarrow$ P $=$ NP

Halteproblem

- PHalt = geg. M, w hält M auf w ?
- Assume: PHalt entscheidbar $\rightarrow$ ex. Entscheider H
- Konstruiere d. Diagonalisierung TM D s.d.
- - prüfe ob Eingabe TM ist
- - Simuliere H auf <M,<M» $\rightarrow$ hält M auf <M> ?
- - Ja $\rightarrow$ Endlosschleife, Nein $\rightarrow$ akzeptiere
- *Simuliere D auf <D>* $\rightarrow$ Wiederspruch

PCP

- Menge Dominosteine, ex. Anordnung s.d. oben = unten
- $PHalt \leq mPCP \leq PCP$
- mPCP: PCP aber mit festem Startstein
- idee: Kodieren TM-lauf (config. seq) als seq. von Wortpaaren, s.d oben eine config zurücl liegt
- -> TM hält $\rightarrow$ Lauf endlich, ex. Lösung (+ vice versa)
- MPCP hat lsg. $\rightarrow$ PCP hat lsg. + $\forall$ Sym. umgeben mit #
- PCP hat lsg. $\rightarrow$ mPCP hat lsg. + da PCP mit erstem Stein anfangen muss, da nur dieser oben = unten + # weglassen

Unifikation

- Löschen: $\{x = x\} \rightarrow \{\}$ (gleiches weglassen)
- Zerlegung:
  $\{f(x_1, ..., x_n) = f(y_1, ..., y_n)\} \rightarrow \{x_1 = y_1, ..., x_n = y_n\}$
- Orientierung: $\{x = y\} \rightarrow \{y = x\}$ (vertauschen)
- Eliminierung: $\{x = y\} \rightarrow \{x = y\} \cup G\{x \mapsto y\}$ (einsetzen)
- σ is min. so allgemein wie θ, wenn $\exists \lambda : \sigma \circ \lambda = \theta$,
- MGU: $\forall \theta : \sigma \preceq \theta$
- alle MGU's sind bis auch Umbenennung der Vars gleich
- gelößte Form: wenn RS nicht in LS vorkommt, RS ist Variable

Prädikatenlogik Definitionen

- V...Variablen, C...Konstanten, P...Prädikatensymbole
- Atom: $p(t_1, ..., t_n) \quad p \in P,\ t_i \in V \cup C$ (t...Terme)
- Formel: Induktiv, Atom ist Formel, $\neg F, F \wedge G, ..., \forall x.F$ auch
- gebundene Variable: steht im Scope eines Quantors
  default: Variablen in Atomen sind frei
- Interpretation $\mathcal{I}$: $\langle \Delta^{\mathcal{I}}, \cdot^{\mathcal{I}} \rangle$
- - $\Delta^{\mathcal{I}}$: Domäne/Grunmenge
- - $\cdot^{\mathcal{I}}$: Interpretationsfunktion
- $\mathcal{I}$ mapped jede Konstante auf ein Domänenelement und jedes Prädikatensymbol auf eine Relation (Menge)
- Bsp: $\Delta^{\mathcal{I}} = \mathbb{N}$, $c^{\mathcal{I}} = 299.792.458$, $\leq_4^{\mathcal{I}} = \{0, 1, 2, 3, 4\}$,
  $\text{even}^{\mathcal{I}} = \{n | n \equiv 0 \pmod 2\}$
- Zuweisung: $\mathcal{Z} : V \rightarrow \Delta^{\mathcal{I}}$, $\mathcal{Z}[x \mapsto \delta]$, für $x \in V, \delta \in \Delta^{\mathcal{I}}$

Formelformen

- geschlossene Formel/Satz: Formel ohne freie Variablen
- negation normal Form (NNF): nur $(\neg, \wedge, \vee)$, $\neg$ nur vor Atomen
- bereinigte Form: keine Variable kommt gebunden und frei vor keine Variable wird von mehr als einem Quantor gebunden
- Pränexform: Alle Quantoren stehen am Anfang
- Skolemform: Pränexform + alle $\exists$ entfernt
  n-stelliges Funktionssymbol mit n = Anz. der $\forall$ davor
- KNF: $(... \vee ... \vee ...) \wedge (... \vee ...) \wedge ...$
- Klauselform: $(x \vee y) \wedge \neg z \rightarrow \{\{x, y\}, \{\neg z\}\}$
- F in Pränex erfüllbar $\Leftrightarrow$ Skolemisierung erfüllbar
- Skolemisierung is keine äquiv. Umf., nur erfüllbarkeitserhalte

Logisches Schließen

- $\mathcal{I}$ is ein Modell für F wenn $\mathcal{I}$ F erfüllt ($\mathcal{I} \models F$)
- $\mathcal{I} \models \mathcal{T}$ wenn $\forall F \in \mathcal{T} : \mathcal{I} \models F$
- logische Konsequenz: $F \models G$, jedes Modell für F ist eins für G
- Alle Tautologien $\models F$ sind äquivalent (ebenso für unerf. F)
- $F \equiv G \Leftrightarrow F \models G \wedge G \models F$
- Monotonie: Mehr Sätze $\Leftrightarrow$ weniger Modele, mehr Schlussfolgerungen
  $\rightarrow$ Tautologien sind in jeder $\mathcal{I}$ wahr, log. Kons. von allem
  $\rightarrow$ Unerf. F haben kein Model, haben alle Sätze als Kons.
- Deduktionstheorem: $F \models G \rightarrow H \Leftrightarrow F \cup \{G\} \models H$
- $F \wedge G \models H \Leftrightarrow F \models G \rightarrow H$
- $F \equiv G \Leftrightarrow \models F \leftrightarrow G$
- $T \models F \equiv T \cup \{\neg F\}$ unerf. ? $\equiv (\wedge_{G \in \mathcal{T}} G \rightarrow F$ Tautologie ?