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 $w(\in \mid \notin) L$ 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
- $Phalt \leq P \land PHalt \leq \bar{P} \Rightarrow$ 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: $\forall \theta : \sigma \leq \theta$
- 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, $\neg F$, $F \land G, ..., \forall x.F$ 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: $\Delta^{\mathcal{I}} = \mathbb{N}$, $c^{\mathcal{I}} = 299.792.458$, $\leq_4^{\mathcal{I}} = \{0, 1, 2, 3, 4\}$,
  even$^{\mathcal{I}} = \{n | n \equiv 0 \pmod 2\}$
- Zuweisung: $\mathcal{Z} : V \rightarrow \Delta^{\mathcal{I}}$, $\mathcal{Z}[x \mapsto \delta]$, für $x \in V$, $\delta \in \Delta^{\mathcal{I}}$
- Kompaktheitssatz:
  $|T| = \infty, T \models F, F \models G, G \subset T, |G| = \infty$

Formelformen

- geschlossene Formel/Satz: Formel ohne freie Variablen
- negation normal Form (NNF): nur $(\neg, \land, \lor)$, $\neg$ 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: $(... \lor ... \lor ...) \land (... \lor ...) \land ...$
- Klauselform: $(x \lor y) \land \neg z \rightarrow \{\{x, y\}, \{\neg z\}\}$
- 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)
- $F \equiv G \Leftrightarrow F \models G \land G \models F$
- 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: $F \models G \rightarrow H \Leftrightarrow F \cup \{G\} \models H$
- $F \land G \models H \Leftrightarrow F \models G \rightarrow H$
- $F \equiv G \Leftrightarrow \models F \leftrightarrow G$
- $T \models F \equiv T \cup \{\neg F\}$ unerf. ? $\equiv (\land_{G \in T} G \rightarrow F$ Tautologie ?

Herbrand

- Satz in Skolemform erf $\Leftrightarrow$ F hat HB-Model
- Herbrand-Expansion:
  $HE(F) := \{G\{x_1 \mapsto t_1, ..., x_n \mapsto t_n\} | t_1, ..., t_n \in \Delta_F\}$
  z.B. $p(a, f(a, s, t)) \vee q(b)) \mid s, t \in \Delta_G\}$
- Satz v. Göd, Her, Sko: F in SkF erf. $\Leftrightarrow$ HE(F) aussagenlog. erf
- Herbrand-Universum: für F, Menge aller var.freien Terme, die man mit Konst. und Funk. symbolen in $F \cup \{a\}$ bilden kann
- Herbrand-Interpretation: $\Delta^{\mathcal{I}} = \Delta_F, \forall t \in \Delta_F : t^{\mathcal{I}} = t$

Clique NPC

- Clique $\in$ NP: Clique ist Cert.
- Clique NP-hard: SAT $\leq_p$ Clique
- G_F hat Clique der Größe l$\Leftrightarrow$ F ist erf.
- $F = \left((L_1^1 \vee ... \vee L_{n_1}^1) \wedge ... \wedge (L_1^l \vee ... \vee L_{n_l}^l)\right)$
- Knoten: $V = \{(L_j^i) \mid i \in \{1...l\}, j \in \{1, ..., n_i\}\}$
- Kanten: $E = \{(L, i) - (L', j) \mid i \neq j, L \wedge L'$ erf. $\}$
- ez auf unabh. Menge reduz. $\rightarrow$ Komplement

Basic Logikregeln

- De-Morgan: $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- De-Morgan: $\neg(A \vee B) \equiv \neg A \wedge \neg B$
- $A \rightarrow B \equiv \neg A \vee B$
- $A \leftrightarrow B \equiv A \wedge B \vee \neg A \wedge \neg B$
- $\neg\neg A \equiv A$

Teilmengen Summe NPC

- $F = (C_1 \wedge ... \wedge C_n)$
- $v(t_i) := a_1...a_n c_1...c_k$
- $a_j = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}, \quad c_j = \begin{cases} 1, p_i \in C_j \\ 0, else \end{cases}$
- $v(f_i) := a_1...a_n c_1...c_k$
- $a_j = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}, \quad c_j = \begin{cases} 1, \neg p \in C_j \\ 0 else \end{cases}$
- für $r := |C_i| - 1$, def: $m_{i,1}, ..., m_{i,r}$
- $v(m_{i,j}) := c_i...c_k$
- $c_l = \begin{cases} 1, l = i \\ 0, l \neq i \end{cases}$
- $S := \left\{t_i, f_i \,\middle|\, 1 \leq i \leq n\right\} \cup \left\{m_{i,j} \,\middle|\, 1 \leq i \leq k, 1 \leq j \leq |C_i| - 1\right\}$
- $z := a_1...a_n c_1...c_k$ mit $a_i := 1, c_i = |C_i|$

PCP Steine

- $$\begin{cases} \begin{bmatrix} qa \\ bp \end{bmatrix} \rightarrow \delta(q, a) = \langle p, b, R \rangle, \\ \begin{bmatrix} cqa \\ pcb \end{bmatrix} \rightarrow \delta(q, a) = \langle p, b, L \rangle \text{ und } c \in \Gamma \text{ beliebig}, \\ \begin{bmatrix} qa \\ pb \end{bmatrix} \rightarrow \delta(q, a) = \langle q, b, N \rangle \end{cases}$$
- $$\begin{cases} \begin{bmatrix} \#qa \\ \#bp \end{bmatrix} \rightarrow \delta(q, a) = \langle p, b, L \rangle \text{ anstoßen am linken Rand}, \\ \begin{bmatrix} q\# \\ q\_\# \end{bmatrix} \rightarrow \forall q \in Q \text{ unendlich nach rechts} \end{cases}$$
- Kopierregel: $\begin{bmatrix} x \\ x \end{bmatrix} \rightarrow \forall x \in \Gamma \cup \{\#\}$

Datalog

- Konsequenzoperator: T_p
- $T_p^0 = \emptyset$, if $T_p^i = T_p^{i+1} \rightarrow T_p^\infty$
- n-spaltige Tabelle wird zu n-stelligem Prädikat
- Schlussfolgerung $P \vDash F$ in Datalog in ExpTime
- für jeden Fakt $F \in T_p^\infty$ ex. min ein Ableitungsbaum
- für P ist T_p^∞ das kleinste Herb. Modell
  $\rightarrow F \in T_p^\infty \Leftrightarrow$ F in jeden Heb. Mod. vorkommt $\Leftrightarrow P \vDash F$
- Datenbankanfragen in präd. Log. ist PSpace-Complete (im Bezug auf Größe der Datenbank und Formel)
- Zeitkomplexität: ExpTime
- Bsp: Anfrage:
  $Q_o[x] = \exists x_0, z_{linie}.verbindung(x_0, x_1, z_{linie}) \wedge Q_0[x_0])$
- gesuchte Var wird quantifiziert
- bei Bool wird alles quantifiziert, das gesuchte mit $\exists$