Korrespondenzproblem von Post

§9.14 Definition (PCP und Lösung; *Post correspondence pairs*)

PCP sind Folge $P = \langle (u_1, w_1), \dots, (u_k, w_k) \rangle$ von Paaren nichtleerer Wörter $(u_i, w_i) \in \Sigma^+ \times \Sigma^+$.
Folge $(i_1, \dots, i_n)$ mit $n \geq 1$ und $i_1, \dots, i_n \in \{1, \dots, k\}$ ist **Lösung** der PCP P falls $u_{i_1} \cdots u_{i_n} = w_{i_1} \cdots w_{i_n}$

Emil Leon Post (* 1897; † 1954)

- Poln.-amer. Mathematiker & Logiker
- Entwickelte universelles Berechnungsmodell
- Korrespondenzproblem

Korrespondenzproblem von Post

Beispiel

- PCP $P = \langle (0, 101), (11, 00), (01, 1) \rangle$

Paar 1:	0	Paar 2:	11	Paar 3:	01
	101		00		1

- Unlösbar (keine Lösung) da alle Paare verschieden beginnen

Weiteres Beispiel

- PCP $P = \langle (0, 010), (1, 101), (0101, 01) \rangle$

Paar 1:	0	Paar 2:	1	Paar 3:	0101
	010		101		01

- Lösbar — Lösung $(3, 1)$ denn

  01010
  01010

Korrespondenzproblem von Post

Letztes Beispiel

- PCP $P = \langle (001, 0), (01, 011), (01, 101), (10, 001) \rangle$

Paar 1:	001	Paar 2:	01	Paar 3:	01	Paar 4:	10
	0		011		101		001

- Lösbar — minimale Lösung Länge 66
  $(2, 4, 3, 4, 4, 2, 1, 2, 4, 3, 4, 3, 4, 4, 3, 4, 4, 2, 1, 4, 4, 2, 1, 3, 4, 1, 1, 3, 4, 4, 4, 2, 1, 2, 1, 1, 1, 3, 4, 3, 4, 1, 2, 1, 4, 4, 2, 1, 4, 1, 1, 3, 4, 1, 1, 3, 1, 1, 3, 1, 2, 1, 4, 1, 1, 3)$

Korrespondenzproblem von Post

Korrespondenzproblem von Post

- Frage: Sind geg. PCP P lösbar?
- Problem $L = \{P \mid \text{PCP } P \text{ lösbar}\}$
- Aufzählung $\rho_L \colon \Sigma^* \dashrightarrow \{0, 1\}$ mit

$$\rho_L(P) = \begin{cases} 1 & \text{falls } P \text{ lösbar} \\ \text{undef} & \text{sonst} \end{cases}$$

- Berechenbarkeit von ρ_L berechenbar (Alle Indexfolgen probieren)
- Semi-Entscheidbarkeit von L semi-entscheidbar

§9.15 Theorem

Korrespondenzproblem von Post semi-entscheidbar

Modifiziertes Korrespondenzproblem von Post

§10.1 Definition (starke Lösung; *strong solution*)

Seien $P = \langle (u_1, w_1), \dots, (u_k, w_k) \rangle$ PCP.
Lösung $(i_1, \dots, i_n)$ der PCP P **stark** *(strong)* falls $i_1 = 1$

Modifiziertes Korrespondenzproblem von Post

- Frage: Sind geg. PCP P stark lösbar? (d.h. gibt es starke Lösung)
- Problem $L_{\text{MPCP}} = \{P \mid P \text{ stark lösbare PCP}\}$

Reduktion MPCP auf PCP

Illustration

- PCP $P = \langle (0101, 01), (1, 101), (0, 010) \rangle$

Paar 1:	0101	Paar 2:	1	Paar 3:	0
	01		101		010

- Lösbar — (schwache) Lösung $(2, 1)$ denn

$$\underbrace{1}_{2}\underbrace{0101}_{1} = \underbrace{101}_{2}\underbrace{01}_{1}$$

- Stark lösbar — starke Lösung $(1, 1, 3, 2)$ denn

$$\underbrace{0101}_{1}\underbrace{0101}_{1}\underbrace{0}_{3}\underbrace{1}_{2} = \underbrace{01}_{1}\underbrace{01}_{1}\underbrace{010}_{3}\underbrace{101}_{2}$$

Reduktion MPCP auf PCP

Idee

- Anfangs- & Zwischenmarkierung mit spez. Symbol $\#$
- Endmarkierung mit weiterem Symbol $\$$
- Seien $P = \langle (u_1, w_1), \dots, (u_k, w_k) \rangle$ PCP
  - Wort u_i erste Komponente $\#$ hinter jedes Symbol
  - Wort w_i zweite Komponente $\#$ vor jedes Symbol
- Jede Sequenz $w'_{i_1} \cdots w'_{i_n}$ beginnt mit $\#$, aber kein u_i beginnt mit $\#$
- 1 Kopie von u'_1 mit $\#$ am Anfang, Lösung muss damit beginnen

Reduktion MPCP auf PCP

Illustration

- PCP $P = \langle (0101, 01), (1, 101), (0, 010) \rangle$

Paar 1:	0101	Paar 2:	1	Paar 3:	0
	01		101		010

- Neue PCP

#0#1#0#1#	0#1#0#1#	1#	0#	$
#0#1	#0#1	#1#0#1	#0#1#0	#$

- Neue PCP nur starke Lösungen
- Originale PCP stark lösbar gdw. neue PCP lösbar

Reduktion MPCP auf PCP

§10.2 Theorem

$L_{\text{MPCP}} \preceq L_{\text{PCP}}$

Beweis (1/2)

Seien $P = \langle (u_1, w_1), \dots, (u_k, w_k) \rangle$ PCP und $\#, \$$ neue Symbole. Für jedes Wort $w = (\sigma_1, \dots, \sigma_n) \in \Sigma^*$ seien

$$\begin{aligned} {}^{\#}w &= \#\sigma_1\# \cdots \#\sigma_n && \text{(\# vor jedem Symbol)} \\ w^{\#} &= \sigma_1\# \cdots \#\sigma_n\# && \text{(\# hinter jedem Symbol)} \\ {}^{\#}w^{\#} &= \#\sigma_1\# \cdots \#\sigma_n\# && \text{(\# vor und hinter jedem Symbol)} \end{aligned}$$

Wir definieren Reduktion von MPCP auf PCP vermittels Funktion f

$$f(P) = \langle ({}^{\#}u_1^{\#}, {}^{\#}w_1), (u_1^{\#}, {}^{\#}w_1), \dots, (u_k^{\#}, {}^{\#}w_k), (\$, \#\$) \rangle$$

mit $k + 2$ Elementen. f offensichtlich total und berechenbar

Reduktion MPCP auf PCP

Beweis (2/2)

$$f(P) = \langle ({}^{\#}u_1^{\#}, {}^{\#}w_1), (u_1^{\#}, {}^{\#}w_1), \dots, (u_k^{\#}, {}^{\#}w_k), (\$, \#\$) \rangle$$

Zu zeigen P stark lösbar gdw. $f(P)$ lösbar. Seien P stark lösbar und $(1, i_2, \dots, i_m)$ Lösung. Dann $(1, i_2 + 1, \dots, i_m + 1, k + 2)$ Lösung für $f(P)$

$$\begin{array}{ccccccccccc} u_1 & u_{i_2} & \cdots & u_{i_m} & & = & w_1 & w_{i_2} & \cdots & w_{i_m} & \\ {}^{\#}u_1^{\#} & u_{i_2}^{\#} & \cdots & u_{i_m}^{\#} & \$ & = & {}^{\#}w_1 & {}^{\#}w_{i_2} & \cdots & {}^{\#}w_{i_m} & \#\$ \end{array}$$

Seien $f(P)$ lösbar und $(i_1, \dots, i_m)$ kürzeste Lösung. Dann $i_1 = 1$, $i_2, \dots, i_{m-1} \in \{2, \dots, k+1\}$ und $i_m = k + 2$.
Also $(1, i_2 - 1, \dots, i_{m-1} - 1)$ starke Lösung für P

$$\begin{array}{ccccccccccc} {}^{\#}u_1^{\#} & u_{i_2}^{\#} & \cdots & u_{i_{m-1}}^{\#} & \$ & = & {}^{\#}w_1 & {}^{\#}w_{i_2} & \cdots & {}^{\#}w_{i_{m-1}} & \#\$ \\ u_1 & u_{i_2} & \cdots & u_{i_{m-1}} & & = & w_1 & w_{i_2} & \cdots & w_{i_{m-1}} & \square \end{array}$$

Reduktion Halteproblem auf MPCP

Idee

- 1. Paar für Initialsituation
- Kopiere Symbole & simuliere Ableitungsschritte
- 2. Komponente (unten) hat 1 Schritt Vorsprung

Illustration

$$\begin{aligned} &\$\square\square qabba\square\# \\ = \; &\$\square\square qabba\square\#\square\square\square q_a bba\square\square\#\square \end{aligned}$$

für Übergang $(q, a) \to (q_a, \square, \triangleright) \in \Delta$

Reduktion Halteproblem auf MPCP

§10.3 Theorem

$H_\varepsilon \preceq L_{\text{MPCP}}$ (Halteproblem auf leerem Band reduzierbar auf L_{MPCP})

Beweis (1/4)

Wir reduzieren vom Halteproblem auf leerem Band vermittels Funktion $f\colon \{0,1\}^* \to (V^+ \times V^+)^+$ mit

$$f(v) = \langle (u_1, w_1), \dots, (u_k, w_k) \rangle \qquad \text{für alle } v \in \{0,1\}^*$$

wobei $\text{decode}(v) = (Q, \Sigma, \Gamma, \Delta, \square, q_0, q_+, q_-)$ geeignet kodierte det. TM mit $Q \cup \Gamma \cup \{\$, \#\} \subseteq V$ und $\{\$, \#\} \cap (Q \cup \Gamma) = \emptyset$

Reduktion Halteproblem auf MPCP

Beweis (2/4)

Wir konstruieren PCP $f(v)$

1. $(u_1, w_1) = (\$, \$\Box\Box q_0\Box\#)$ Initialsituation
2. Für alle $\gamma \in \Gamma$ existiert i mit $(u_i, w_i) = (\gamma, \gamma)$ Kopierpaare
3. Für alle $(q, \gamma) \to (q', \gamma', \diamond) \in \Delta$ existiert i mit $(u_i, w_i) = (q\gamma, q'\gamma')$
   Für alle $(q, \gamma) \to (q', \gamma', \triangleright) \in \Delta$ existiert i mit $(u_i, w_i) = (q\gamma, \gamma' q')$
   Für alle $(q, \gamma) \to (q', \gamma', \triangleleft) \in \Delta$ und $\gamma'' \in \Gamma$ existiert i mit $(u_i, w_i) = (\gamma'' q\gamma, q'\gamma''\gamma')$ Transitionspaare
4. Existiert i mit $(u_i, w_i) = (\#, \Box\#\Box)$ Erweiterung um $\Box$
5. Für alle $\gamma \in \Gamma$ und $f \in \{q_+, q_-\}$ existiert i mit $(u_i, w_i) = (\gamma f, f)$
   Für alle $\gamma \in \Gamma$ und $f \in \{q_+, q_-\}$ existiert i mit $(u_i, w_i) = (f\gamma, f)$
   Löschregeln
6. Für alle $f \in \{q_+, q_-\}$ existiert i mit $(u_i, w_i) = (f\#\#, \#)$ Abschluss
7. Keine weiteren Paare in $f(v)$

Reduktion Halteproblem auf MPCP

Beweis (3/4)

Zu zeigen $\mathrm{decode}(v)$ hält auf leerem Band gdw. $f(v)$ stark lösbar
Zunächst halte $M = \mathrm{decode}(v)$ auf leerem Band. Dann existiert Folge Konfigurationen $\xi_1, \dots, \xi_n$ mit

- $\xi_1, \dots, \xi_n \in \Gamma^* Q \Gamma^*$ und $|\xi_i| = 2(i+1) + 1$
- $\Box\Box q_0 \Box \vdash_M \xi_1 \vdash_M \cdots \vdash_M \xi_n$
- $\xi_n \in \Gamma^* \{q_+, q_-\} \Gamma^*$

Lösungswort

$$\$\Box\Box q_0\Box\#\xi_1\#\cdots\#\xi_n\#\xi_n^{(1)}\#\xi_n^{(2)}\#\cdots\#f\#\#$$

wobei $f \in \{q_+, q_-\}$, $\xi_n^{(0)} = \xi_n$ und $\xi_n^{(i)}$ aus $\xi_n^{(i-1)}$ entsteht indem Symbol links oder rechts vom Endzustand f gelöscht wird.

Reduktion des Halteproblems auf MPCP

Beweis (4/4)

Zu zeigen $\mathrm{decode}(v)$ hält auf leerem Band gdw. $f(v)$ stark lösbar
Umgekehrt sei $(i_1, \dots, i_n)$ starke Lösung von $f(v)$. Also $i_1 = 1$ und Lösungswort beginnt mit $\#\Box\Box q_0\Box\#$. Damit beiden Sequenzen übereinstimmen müssen folgende Paare verwendet werden

1. Kopierpaare kopieren Bandinhalt bis Zustand (oder bis Zeichen vor Zustand) passend auf “oberen” String
2. Transitionspaar simuliert Übergang
   (Kopie Ausgangskonfiguration oben; Folgekonfiguration unten)
3. Kopierpaare kopieren verbleibenden Bandinhalt

Letztlich muss Endzustand erreichen, denn nur dessen Paare haben längere obere Sequenzen als untere Sequenzen. Damit erreicht also M Endzustand und hält auf leerem Band. $\Box$

Unentscheidbarkeit des PCP

§10.4 Theorem

Korrespondenzproblem von Post unentscheidbar

Beweis

Theorem §9.11 zeigt Halteproblem H_ε auf leerem Band unentscheidbar. Weiterhin $H_\varepsilon \preceq L_{\mathrm{MPCP}}$ (Theorem §10.3) und damit L_{MPCP} unentscheidbar nach Theorem §9.9. Außerdem $L_{\mathrm{MPCP}} \preceq L_{\mathrm{PCP}}$ (Theorem §10.2) und damit L_{PCP} unentscheidbar $\Box$

Schnittproblem kontextfreier Sprachen

Leerheit Schnitt kontextfreier Sprachen

- Frage: Ist $L(G) \cap L(G') \neq \emptyset$ für geg. kontextfreie Grammatiken G und G'?
- Problem $L_{\text{CFI}} = \{\langle G, G' \rangle \mid G \text{ und } G' \text{ kontextfrei}, L(G) \cap L(G') \neq \emptyset\}$

Reduktion vom PCP

- Schnittsprache enthält Worte der Form $\underline{i}^{\text{R}} u \$ w^{\text{R}} \underline{\ell}$, wobei $\underline{i}$ und $\underline{\ell}$ Indexsequenzen und u und w korrespondierende Zeichenreihen
- 1. Sprache sichert Korrespondenz Indexsequenz & Zeichenreihe
- 2. Sprache sichert Gleichheit Indexsequenzen $\underline{i}$ und $\underline{\ell}$ und Gleichheit Zeichenreihen u und w

Schnittproblem kontextfreier Sprachen

§10.5 Theorem

$L_{\text{PCP}} \preceq L_{\text{CFI}}$

Beweis (1/2)

Seien $P = \langle (u_1, w_1), \dots, (u_k, w_k) \rangle$ PCP über Σ, $\Gamma = \Sigma \cup \{\$, 1, \dots, k\}$
Konstruiere 2 kontextfreie Grammatiken G und G' über Γ mit folgenden Produktionen für G

$$S \to A\$B \qquad A \to 1Au_1 \mid 1u_1 \mid \cdots \mid kAu_k \mid ku_k$$
$$B \to w_1^{\text{R}}B1 \mid w_1^{\text{R}}1 \mid \cdots \mid w_k^{\text{R}}Bk \mid w_k^{\text{R}}k$$

Sprache von G

$$L(G) = \{\underbrace{i_n \cdots i_1 u_{i_1} \cdots u_{i_n}}_{A} \$ \underbrace{(w_{\ell_1} \cdots w_{\ell_m})^{\text{R}} \ell_1 \cdots \ell_m}_{B} \mid \cdots\}$$

Schnittproblem kontextfreier Sprachen

Beweis (2/2)

Grammatik G' verwendet folgende Produktionen

$$S \to 1S1 \mid \cdots \mid kSk \mid T \qquad T \to \$ \mid \sigma T \sigma \qquad \text{für alle } \sigma \in \Sigma$$

Sprache von G'

$$L(G') = \{u \underbrace{w\$w^{\text{R}}}_{T} u^{\text{R}} \mid u \in \{1, \dots, k\}^*, w \in \Sigma^*\}$$

Schnitt $L(G) \cap L(G') = \{\ell^{\text{R}} w \$ w^{\text{R}} \ell \mid \ell \text{ erzeugt beidseitig } w \text{ in } P\}$ womit jedes Element von $L(G) \cap L(G')$ Lösung samt Lösungswort repränsentiert. Damit P lösbar gdw. $L(G) \cap L(G') \neq \emptyset$ und damit $L_{\text{PCP}} \preceq L_{\text{CFI}}$ □

Schnittproblem kontextfreier Sprachen

§10.6 Theorem

Schnittproblem L_{CFI} kontextfreier Sprachen unentscheidbar

Beweis

Theorem §10.5 zeigt $L_{\text{PCP}} \preceq L_{\text{CFI}}$ und Korrespondenzproblem L_{PCP} von Post unentscheidbar nach Theorem §10.4. Also Schnittproblem L_{CFI} unentscheidbar nach Theorem §9.9 □

Schnittproblem kontextfreier Sprachen

Unendlichkeit Schnitts kontextfreier Sprachen

- Frage: Ist $L(G) \cap L(G')$ unendlich für geg. kontextfreie Grammatiken G und G'?
- Problem $L'_{\text{CFI}} = \{\langle G, G' \rangle \mid L(G) \cap L(G') \text{ unendlich}\}$
- Reduktion vom PCP wie bisher

$$\text{PCP } P \text{ lösbar} \iff \text{PCP } P \text{ unendlich viele Lösungen}$$

In Reduktion repräsentiert $L(G) \cap L(G')$ Lösungen und damit auch Reduktion von L_{PCP} auf L'_{CFI}

§10.7 Theorem

Unendlichkeitsproblem L'_{CFI} Schnitt kontextfreier Sprachen unentscheidbar

Inklusion kontextfreier Sprachen

Inklusion kontextfreier Sprachen

- Frage: Gilt $L(G') \subseteq L(G)$ für geg. kontextfreie Grammatiken G' und G?
- Problem $L_{\text{CFT}} = \{\langle G', G \rangle \mid L(G') \subseteq L(G)\}$
- Offenbar $L(G') \cap L(G) \neq \emptyset$ gdw. $L(G') \not\subseteq \overline{L(G)}$
- Versuch Reduktion von L_{CFI} auf $\overline{L_{\text{CFT}}}$

$$f(\langle G', G \rangle) = \langle G', \overline{G} \rangle$$

mit $\overline{G}$ (Typ-0)-Grammatik für Komplement $\overline{L(G)}$; also $L(\overline{G}) = \overline{L(G)}$
Funktion f ist total & berechenbar

- Allerdings

$$f^{-1}(\overline{L_{\text{CFT}}}) = \{\langle G', G \rangle \in L_{\text{CFI}} \mid \overline{L(G)} \text{ kontextfrei}\} \subsetneq L_{\text{CFI}}$$

Inklusion kontextfreier Sprachen

Inklusion kontextfreier Sprachen

- Frage: Gilt $L(G') \subseteq L(G)$ für geg. kontextfreie Grammatiken G' und G?
- Problem $L_{\text{CFT}} = \{\langle G', G \rangle \mid L(G') \subseteq L(G)\}$
- Reduktion f von L_{PCP} auf L_{CFI}; sei $f(P) = \langle G_1, G_2 \rangle$
  Reduktion g von L_{PCP} auf $\overline{L_{\text{CFT}}}$ per $g(P) = \langle G_1, \overline{G_2} \rangle$
  (Komplement $\overline{L(G_2)}$ ebenso kontextfrei; siehe Übung)

$$\begin{aligned} P \text{ lösbar} &\iff L(G_1) \cap L(G_2) \neq \emptyset &&\iff f(P) \in L_{\text{CFI}} \\ &\iff L(G_1) \not\subseteq L(\overline{G_2}) &&\iff g(P) \in \overline{L_{\text{CFT}}} \end{aligned}$$

Also $L_{\text{PCP}} \preceq \overline{L_{\text{CFT}}}$

Inklusion kontextfreier Sprachen

§10.8 Theorem

Inklusionsproblem L_{CFT} kontextfreier Sprachen unentscheidbar

Beweis

Wir wissen $L_{\text{PCP}} \preceq \overline{L_{\text{CFT}}}$ und Korrespondenzproblem L_{PCP} von Post unentscheidbar (Theorem §10.4). Damit auch Komplement $\overline{L_{\text{CFT}}}$ Inklusionsproblem unentscheidbar (Theorem §9.9). Wäre L_{CFT} entscheidbar, dann Komplement $\overline{L_{\text{CFT}}}$ entscheidbar nach Theorem §8.6. Also Inklusionsproblem L_{CFT} unentscheidbar □

Gleichheit kontextfreier Sprachen

Äquivalenz kontextfreier Sprachen

- Frage: Gilt $L(G) = L(G')$
  für geg. kontextfreie Grammatiken G und G'?
- Problem $L_{\mathsf{CFE}} = \{\langle G, G' \rangle \mid L(G) = L(G')\}$
- Reduktion f von L_{PCP} auf L_{CFI}; sei $f(P) = \langle G_1, G_2 \rangle$
  Reduktion g von L_{PCP} auf $\overline{L_{\mathsf{CFE}}}$ per $g(P) = \langle G_1 \cup \overline{G_2}, \overline{G_2} \rangle$
  $(L(\overline{G_2}) = \overline{L(G_2)}$ und $L(G_1 \cup \overline{G_2}) = L(G_1) \cup \overline{L(G_2)})$

$$\begin{aligned} P \text{ lösbar} &\iff L(G_1) \cap L(G_2) \neq \emptyset \\ &\iff L(G_1) \not\subseteq L(\overline{G_2}) \\ &\iff L(G_1) \cup L(\overline{G_2}) \neq L(\overline{G_2}) \iff g(P) \in \overline{L_{\mathsf{CFE}}} \end{aligned}$$

Also $L_{\mathsf{PCP}} \preceq \overline{L_{\mathsf{CFE}}}$

Gleichheit kontextfreier Sprachen

§10.9 Theorem

Äquivalenzproblem L_{CFE} kontextfreier Sprachen unentscheidbar

Für kontextfreie Sprachen unentscheidbar

- Leerheit Schnitt
- Endlichkeit Schnitt
- Inklusion
- Äquivalenz
- Kontextfreiheit Komplements
- Regularität

Leerheit kontextsensitiver Sprachen

Leerheit kontextsensitiver Sprachen

- Frage: Ist $L(G) = \emptyset$ für geg. kontextsensitive Grammatik G?
- Problem $L_{\mathsf{CSE}} = \{G \mid L(G) = \emptyset\}$
- Reduktion von L_{CFI}

$$f(\langle G, G' \rangle) = G'' \qquad \text{mit} \qquad L(G'') = L(G) \cap L(G')$$

  (Kontextsensitive Sprachen sind unter Schnitt abgeschlossen)
- $L(G) \cap L(G') \neq \emptyset$ gdw. $f(\langle G, G' \rangle) \neq \emptyset$
  Also $L_{\mathsf{CFI}} \preceq \overline{L_{\mathsf{CSE}}}$
- Damit L_{CSE} unentscheidbar

Satz von Church

Erinnerung Prädikatenlogik erster Stufe $(\forall x, \exists x,$ etc.)

§10.10 Theorem (Satz von Church)

Erfüllbarkeit geg. Formel Prädikatenlogik erster Stufe unentscheidbar

Alonzo Church (* 1903; † 1995)

- Amer. Mathematiker & Logiker
- Entwickelte λ-Kalkül (nicht vorgestellt)
- Doktorvater von Stephen Kleene & Alan Turing

© Princeton University

Arithmetik

§10.11 Definition (Arithmetische Terme; *arithmetic terms*)

Folgende Ausdrücke sind **arithmetische Terme**

- Jede natürliche Zahl $n \in \mathbb{N}$ und jede Variable $x \in X$
- $(t + t')$ und $(t \cdot t')$ für arithmetische Terme t, t'
- Keine weiteren arithmetischen Terme

Für Variablenbelegung $\theta\colon X \to \mathbb{N}$ sei

$$x\theta = \theta(x) \qquad n\theta = n \qquad x \in X;\ n \in \mathbb{N}$$
$$(t + t')\theta = t\theta + t'\theta \qquad (t \cdot t')\theta = t\theta \cdot t'\theta$$

Beispiele

- $t_1 = 5$ $\qquad t_1\theta = 5$
- $t_2 = (x_2 \cdot 3) + x_1$ $\qquad t_2\theta = 3\theta(x_2) + \theta(x_1)$
- $t_3 = (3 \cdot 2) + 0$ $\qquad t_3\theta = 6$

Arithmetik

§10.12 Definition (Arithmetische Formeln; *arithmetic formulas*)

Arithmetische Formeln sind

- $t = t'$ für arithmetische Terme t, t'
- $\neg F$ und $F \vee F'$ für arithmetische Formeln F, F'
- $\exists x F$ für $x \in X$ und arithmetische Formel F
- Keine weiteren arithmetischen Formeln

Variablenbelegung $\theta\colon X \to \mathbb{N}$ **erfüllt** Formel F, kurz $\theta \models F$, falls

$$\begin{aligned}
&\theta \models (t = t') && \text{gdw. } t\theta = t'\theta \\
&\theta \models \neg F && \text{gdw. } \theta \not\models F \\
&\theta \models (F \vee F') && \text{gdw. } \theta \models F \text{ oder } \theta \models F' \\
&\theta \models \exists x.F && \text{gdw. } n \in \mathbb{N} \text{ existiert mit } \theta_{[x \mapsto n]} \models F
\end{aligned}$$

Arithmetik

Beispiele (wir nutzen wie üblich auch $\forall x$ und $\wedge$)

- $2 + 3 = 5$ — wahr
- $\forall x_1.\forall x_2.(x_1 \cdot x_2) = (x_2 \cdot x_1)$ — wahr
- $\exists x_1.\forall x_2.(x_1 + x_2) = x_2$ — wahr
- $\exists x_1.\forall x_2.(x_1 \cdot x_2) = (x_2 \cdot x_2)$ — falsch

Notizen

- **Satz** = Formel ohne freie Variablenvorkommen
- Für Satz F und Variablenbelegungen θ, θ' gilt $\theta \models F$ gdw. $\theta' \models F$
- Satz F also wahr, kurz $\models F$, oder falsch, kurz $\not\models F$
- $\theta_{[x \mapsto n]}$ ist Variablenbelegung θ außer Zuordnung Wert n zu x

$$\theta_{[x \mapsto n]}(y) = \begin{cases} n & \text{falls } y = x \\ \theta(y) & \text{sonst} \end{cases}$$

Arithmetik

§10.13 Definition (arithm. repräsentierbar; *arithm. representable*)

Partielle Funktion $f\colon \mathbb{N}^k \dashrightarrow \mathbb{N}$ **arithmetisch repräsentierbar** falls arithmetische Formel F mit freien Variablen $x, x_1, \dots, x_k$ existiert, so dass für alle $n, n_1, \dots, n_k \in \mathbb{N}$

$$f(n_1, \dots, n_k) = n \quad \text{gdw. } \mathbf{0}_{[x \mapsto n, x_1 \mapsto n_1, \dots, x_k \mapsto n_k]} \models F$$

Notizen

- $\mathbf{0}\colon X \to \mathbb{N}$ ist Variablenbelegung mit $\mathbf{0}(x) = 0$ für alle $x \in X$
- Falls für $n_1, \dots, n_k \in \mathbb{N}$ kein $n \in \mathbb{N}$ mit $\mathbf{0}_{[x \mapsto n, x_1 \mapsto n_1, \dots, x_k \mapsto n_k]} \models F$ existiert, dann $f(n_1, \dots, n_k)$ undefiniert

Arithmetik

§10.14 Theorem

While-berechenbare partielle Funktionen arithmetisch repräsentierbar

Arithmetik

§10.15 Theorem

Wahre arithm. Sätze $\mathrm{WA} = \{F \mid \text{Satz } F, \models F\}$ <u>nicht</u> rekursiv aufzählbar

Beweis (per Widerspruch)

Sei WA rekursiv aufzählbar und $a \colon \mathbb{N} \to \mathrm{WA}$ berechenbare surjektive Funktion. Sei F beliebiger arithmetischer Satz. Entweder $\models F$ oder $\models \neg F$. Da a surjektiv, existiert Index $n \in \mathbb{N}$ mit $a(n) \in \{F, \neg F\}$. Also WA entscheidbar per Suche nach Index n. Weiterhin L_{PCP} semi-entscheidbar (Theorem §9.15). Nach Theorem §10.14 existiert arithmetische Formel F', die $\rho_{L_{\mathrm{PCP}}}$ repräsentiert

$$P \in L_{\mathrm{PCP}} \iff \rho_{L_{\mathrm{PCP}}}(P) = 1 \iff \mathbf{0}_{[x \mapsto 1, x_1 \mapsto P]} \models F' \\ \iff F'[x \mapsto 1, x_1 \mapsto P] \in \mathrm{WA}$$

Damit $L_{\mathrm{PCP}} \preceq \mathrm{WA}$ und WA unentscheidbar. Widerspruch ↯ □