Maschinelles Beweisen

Folienkopien zur Vorlesung im SS 1995

Joachim Biskup
Universität Hildesheim
Samelsonplatz 1
31141 Hildesheim

Vorwort

Meine Vorlesung über Maschinelles Beweisen stützt sich ganz wesentlich auf das folgende Buch:

> Dieter Hofbauer, Ralf D. Kutsche,
> Grundlagen des maschinellen Beweisens,
> Vieweg, Braunschweig - Wiesbaden,
> 2., verb. Aufl., 1991,
> ISBN 3-528-14718-0

Ich habe aus dem Buch die Gliederung des Stoffes, im wesentlichen die Bezeichnungen und Redeweisen und sogar die Numerierungen von Kapiteln, Definitionen und Aussagen übernommen. Mein eigener Beitrag beschränkt sich auf die Stoffauswahl, gelegentliche kleine Einschübe und häufige Verkürzungen der im Buch genau ausgearbeiteten technischen Einzelheiten auf mehr oder weniger anschaulich Verstehbares.

Darüber hinaus entspringt nur die Aufbereitung zu im Original farbigen, häufig auch mehrschichtig zu verwendenen Folien meiner eigenen Anstrengung.

Diese Folienkopien sollen weder das Buch von D. Hofbauer und R. D. Kutsche noch die Vorlesung selbst ersetzen. Ganz im Gegenteil rate ich allen Studenten, das Buch im voraus, begleitend und nacharbeitend genau zu studieren und in der Vorlesung aufmerksam dem gesprochenen Wort zuzuhören. Ich hoffe, daß die Hörer der Vorlesung durch eigenes, vom Mitschreiben befreites Mitdenken beim mehr oder weniger anschaulichen Vortrag zusammen mit dem Studium des Buches eine gute Einführung in das Maschinelle Beweisen erhalten.

Hildesheim, 1995 Joachim Biskup

Maschinelles Beweisen

1. Aufgabe des maschinellen Beweisens

   Syntax der Prädikatenlogik

2. Semantik der Prädikatenlogik

3. Ableitungsregeln

   Schnittregel

4. Substitutionsregel

   Unifizierbarkeit

5. Unifikation

6. Resolution

7. Gleichheitsstrukturen

8. Paramodulation

9. Termersetzung

10. Ersetzungssysteme

11. Kritische Paare

12. Terminierung

Maschinelles Beweisen

V3 : Grundzüge der Theorie

Ü1 : Ausarbeitungen,
Ergänzungen,
prototypische Implementierung

für Diplomprüfung

- "Praktische" Informatik A : Grundlagen für
  "logischen Programmierung",
  "Expertensysteme",
  "Künstliche Intelligenz"

- Vertiefungsfach "Informationssysteme"

Grundlage:

D. Hofbauer / R.-D. Kutsche,

Grundlagen des maschinellen Beweisens,

Vieweg, Braunschweig / Wiesbaden,

1. Auflage : 1989,

2. Auflage : 1991..

Inhalt:

0. Einführung : Aufgabe, Geschichte
1. Prädikatenlogik
2. Resolution
5. Paramodulation
6. Termersetzung

weitere Literatur:

- Chang / Lee: Symbolic Logic and Mechanical Theorem Proving, Academic Press, 1973.
- Loveland: Automated Theorem Proving, North Holland, 1978.
- Lloyd: Foundations of Logic Programming, Springer, 1987.
- Richter: Logikkalküle, Teubner, 1978.
- Boyer / Moore: A Computational Logic, Academic Press, 1979
- Comm. of the ACM 35,3 (March 1992), Special Issue on Logic Programming.

0. Einführung

Der Traum des maschinellen Beweisens:

1. Der Mensch behauptet eine Aussage.
2. Die Maschine beweist sie.

mögliche Anwendungen:

- Mathematik
- Programmverifikation
- logische Programmierung (→ PROLOG, logische Datenbanken)
- Expertensysteme, Künstliche Intelligenz

⋮

1. Der Mensch behauptet eine Aussage:

- die eigentliche Aussage muß formalisiert werden;
- alle weiteren Annahmen, Voraussetzungen, usw. müssen ebenfalls ausdrücklich genannt und formalisiert werden;
- diese Formalisierungen müssen als (endliches!) Wort über einem geeigneten Alphabet der Maschine eingegeben werden.

2. Die Maschine beweist diese Aussage:

- die Maschine soll folgende Funktion berechnen:

  entscheide: Menge der die Aussagen und Voraussetzungen darstellenden Worte

  $\longrightarrow$ { Wahr, Falsch }

- die Maschine soll ferner die entsprechenden formalen Beweise oder formalen Widerlegungen liefern:

  beweise: Menge der die Aussagen und Voraussetzungen darstellenden Worte

  $\longrightarrow \Sigma^*$ (geeignetes Alphabet, um Beweise aufzuschreiben)

<u>also:</u> Vorgehensweise folgt altem Menschheits- (Wissenschafts-) Ziel:

Inhalte formalisieren und algorithmisieren!

<u>erfolgreiches Vorbild:</u>

Arithmetik (Grundrechenarten) durch Rechenkalküle im Stellenwertsystem betreiben;

statt z.B.: "drei" plus "fünf" ergibt "acht"

formal:

0 1 1	"drei"
+ 1 0 1	"fünf"
1 1	Überträge
1 0 0 0	"acht"

Entwicklung der Vorgehensweise

Inhalte formalisieren und algorithmisieren

in der Logik, d.h. der

Theorie der wahren Aussagen und ihrer Herleitungen:

17. Jh.: Descartes, Leibniz: Visionäre, in der Philosophie verwurzelt

19. Jh.: de Morgan, Boole: Kalküle der Aussagenlogik

Ende 19. Jh: Frege: "Begriffsschrift": Schritt zur Prädikatenlogik; tragisch gescheitert: er rannte einem unerfüllbaren Traum nach

Beginn 20. Jh.: Hilbert: formalisiert den "Traum" als mathematisches Arbeitsprogramm

30er Jahre: Gödel, Church, Turing: beweisen, daß "Traum" allgemein unerfüllbar, aber "Teilträume" erreichbar sind:

- "entscheide" (für Prädikatenlogik) nicht berechenbar!
- {A | entscheide (A) = W} (für Prädikatenlogik) rekursiv aufzählbar!

60er Jahre: Robinson, ... : Resolutionskalkül, um Elemente aus $\{A \mid \text{entscheide}(A) = W\}$ "effizient" zu erkennen

70er Jahre: Kowalski, Colmerauer: PROLOG, führt Beweise in einer Teilmenge der Prädikatenlogik

1. Prädikatenlogik

- die formale Sprache der Prädikatenlogik:

  Syntax, Semantik

- einige Grundbegriffe:

  Gültigkeit (einer Formel in einer Struktur),

  Modell,

  Erfüllbarkeit, Allgemeingültigkeit,

  (logische) Folgerung

- Normalformen von Formeln:

  konjunktive Normalform, Gentzenformel, Hornformel,

  pränexe Normalform, Skolem-Normalform

- Schnittregel und Substitutionsregel

- Herbrand-Modell, Satz von Herbrand

- Regelsysteme:

  Korrektheit, Vollständigkeit, Widerlegungsvollständigkeit

Signatur: $\Sigma = (S, F, P)$

S Sorten

F Operationszeichen

P Prädikatenzeichen

Terme: i) Konstantensymbole aus F

Variable

ii) ist $f(s_1, \dots, s_n) \to s$ aus Σ und sind $t_1, \dots, t_n$ Terme,

so ist auch $f(t_1, \dots, t_n)$ Terme

atomare Formeln: $P(\underbrace{t_1, \dots, t_n}_{\text{Terme}})$

P aus Σ

Formeln: i) atomare Formeln,

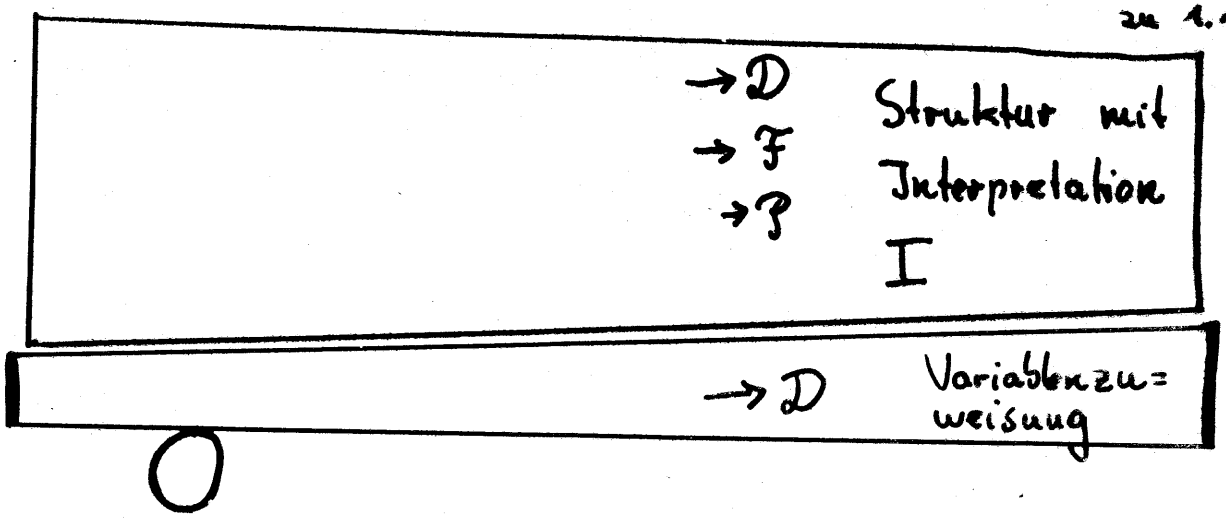
W, F

ii) sind A, B Formeln, so auch

$\neg A$, $A \wedge B$, $A \vee B$, $A \to B$, $A \leftrightarrow B$

iii) ist A Formel, die x frei enthält, so sind auch

$\exists x\, A$, $\forall x\, A$ Formeln


→ D
→ F
→ P
Struktur mit Interpretation I
→ D
Variablenzuweisung

Substitution

σ : Variablen $\longrightarrow$ $\text{Terme}_\Sigma(U)$ mit ① $x, \sigma(x)$ haben gleiche Sorte

② $\text{dom}\,\sigma = \{x \in V \mid x\sigma \neq x\}$ endlich

$$\sigma = \begin{pmatrix} x_1 & \dots & x_n \\ t_1 & \dots & t_n \end{pmatrix} \leftarrow \text{dom}\,\sigma \qquad [x_i / t_i]$$

Fortsetzung auf Terme, Formeln, Formelmengen

$x\sigma^* := x\sigma$ f. alle Variablen x

$[f(t_1, \dots, t_n)]\sigma^* := f(t_1\sigma^*, \dots, t_n\sigma^*)$ f. alle Funktionssz. f f. alle Terme t_i

$[P(t_1, \dots, t_n)]\sigma^* := P(t_1\sigma^*, \dots, t_n\sigma^*)$

$\vdots \qquad\qquad \vdots$

$M\sigma^* := \{m\sigma^* \mid m \in M\}$

Bsp: $\sigma = \begin{pmatrix} x & y & z \\ e & e & e \circ e \end{pmatrix}$ Grundsubstitution (keine Variablen in den Bildern)

$$[\circ(\circ(x,y), z)]\sigma^*$$

$$= \circ([\circ(x,y)]\sigma^*, z\sigma^*)$$

$$= \circ(\circ(x\sigma^*, y\sigma^*), z\sigma^*)$$

$$= \circ(\circ(e, e), e \circ e)$$

Eigenschaften von Substitutionen

$\sigma, \tau, \sigma_1, \sigma_2, \sigma_3$ Substitutionen

$[\,]$ identitische Substitution

t Term

i) $\sigma\,[\,] = [\,]\,\sigma = \sigma$ $[\,]$ neutrales Element bzg Komposition

ii) $(t\,\sigma)\,\tau = t\,(\sigma\tau)$ schrittweises Auswerten

iii) $(\sigma_1\,\sigma_2)\,\sigma_3 = \sigma_1\,(\sigma_2\,\sigma_3)$ Komposition ist assoziativ

(iv) <u>falls</u> $t\sigma = t\tau$ f. alle $t \in T_\Sigma(V)$

<u>dann</u> $\sigma = \tau$

(v) <u>falls</u> $\sigma\tau = \sigma$

<u>dann</u> $\tau|_{\text{Variablen im Bildbereich von } \sigma} = [\,]|_{\text{Variablen im Bildbereich von } \sigma}$

τ läßt Variablen im Bildbereich von σ unverändert

Ableitungsregel

Prämissen $G_1 \quad G_2 \quad \dots \quad G_n$ — Formeln (Formelschemas)

Konklusion G — Formel (Formelschema, enthält "Variable für Formeln)

heißt **Ableitungsregel** (-regelschema)

(⇒ siehe Post-Systeme)

Ableitung(en) von G — Formel
aus X — Formelmenge
mit R — Menge von Ableitungsregeln

(i) (G) für $G \in X$ (die Elemente aus X sind "Axiome")

(ii) ist $(C_1, \dots, C_k)$ Ableitung und

$$\frac{G_1 \dots G_n \quad \in X \cup \{C_1, \dots, C_k\} \quad \text{schon hergeleitet}}{G \qquad \in R}$$

so ist $(C_1, \dots, C_k, G)$ Ableitung

man schreibt dann kurz: $X \vdash_R G$; "G ableitbar aus X"

Semantik

zur Syntax $\Sigma = (S, F, P)$ (Sorten, Funktionszeichen, prädikatenzeichen)

Struktur $\mathfrak{M} = (\mathcal{D}, \mathcal{F}, \mathcal{P})$

mit Zuordnungen (Interpretation) $\mathcal{I}$

$\mathcal{I}(s) := \mathcal{D}_S \in \mathcal{D}$ f. alle $s \in S$

↑ nichtleere Individuenmenge (Datenmenge)

$\mathcal{I}(f) := f$ mit $f : \mathcal{D}_{s_1} \times \ldots \times \mathcal{D}_{s_n} \to \mathcal{D}_s$

↑ (getypte) Funktion

f. alle Funktionszeichen $f(s_1, \ldots, s_n) \to s$ aus $\mathbf{F}$

speziell $n = 0$:

$\mathcal{I}(c) := d$ mit $d \in \mathcal{D}_s$

f. alle Konstantenzeichen $c \to s$ aus $\mathbf{F}$

$\mathcal{I}(P) := p$ mit $p \subseteq \mathcal{D}_{s_1} \times \ldots \times \mathcal{D}_{s_n}$

↑ Relation, Prädikat

f. alle Prädikatenzeichen $P(s_1, \ldots, s_n)$ aus $\mathbf{P}$

$p : \mathcal{D}_{s_1} \times \ldots \times \mathcal{D}_{s_n} \to \{W, F\}$ als Wahrheitsfunktion

für $n = 0$: $p \in \{W, F\}$ Wahrheitswert

Beispiel: $\Sigma = (\{group\}, \{\circ, ^{-1}, e\}, \{=\})$

Sorte

Funktionszeichen

Gleichheitsprädikat

$I(group) := \underbrace{\{1, a, b, c\}}_{Z_4}$ $\quad \mathfrak{D} := \{Z_4\}$

$I(\circ)$	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

$\mathfrak{F} := \{ \underline{I(\circ)}, \underline{I(^{-1})}, 1 \}$

$I(^{-1})$	1	a	b	c
	1	c	b	a

$I(e) := 1$

$I(=) := \underbrace{\{(d,d) \mid d \in \{1,a,b,c\}\}}_{Identität(P_4)}$ $\quad \mathfrak{P} := \{Identität(P_4)\}$

sei $\mathcal{M} = (\mathcal{D}, \mathcal{F}, \mathcal{I})$ Struktur mit Interpretation I

(interpretiert "alles außer Variablen")

$\omega : \text{Variablen}_s \to \mathcal{D}_s$ Variablenzuweisung

(interpretiert Variablen)

dann <u>Wert</u> von allen Termen und Formeln bestimmt durch:

$\text{wert}^{\omega}_{\mathcal{M}}(c) := I(c)$ für Konstante c aus F

$\text{wert}^{\omega}_{\mathcal{M}}(x) := \omega(x)$ f.alle Variablen $x \in V$

Induktionsanfang durch I und ω bestimmt

$$\text{wert}^{\omega}_{\mathcal{M}}(f(t_1, \ldots, t_n)) = I(f)(\text{wert}^{\omega}_{\mathcal{M}}(t_1), \ldots, \text{wert}^{\omega}_{\mathcal{M}}(t_n))$$

Induktionsschritt bestimmt durch I und Induktionsvoraussetzung

f.alle f aus F

$t_1, \ldots, t_n$ passende Terme

d.h. $\text{wert}^{\omega}_{\mathcal{M}} : \text{Terme}_s \to \mathcal{D}_s$

Syntax — Semantik

$Wert^{\omega}_{\mathcal{M}}(P) := I(P) \in \{W, F\}$ f. alle Aussagenzeichen $P \in \mathbf{P}$

$Wert^{\omega}_{\mathcal{M}}(W) := W$; $Wert^{\omega}_{\mathcal{M}}(F) := F$

$Wert^{\omega}_{\mathcal{M}}(P(t_1, \dots, t_n)) := I(P)(wert^{\omega}_{\mathcal{M}}(t_1), \dots, wert^{\omega}_{\mathcal{M}}(t_n)) \in \{W, F\}$

↑ Wahrheitsfunktion

$Wert^{\omega}_{\mathcal{M}}(\neg A) := W$ gdw $Wert^{\omega}_{\mathcal{M}}(A) = F$

$Wert^{\omega}_{\mathcal{M}}(A \wedge B) := W$ gdw $Wert^{\omega}_{\mathcal{M}}(A) = W$ und $Wert^{\omega}_{\mathcal{M}}(B) = W$

⋮ ⋮

$Wert^{\omega}_{\mathcal{M}}(\forall x A) := W$ gdw $Wert^{\omega'}_{\mathcal{M}}(A) = W$ f. alle ω' mit "$\omega = \omega'$ bis auf x"

$Wert^{\omega}_{\mathcal{M}}(\exists x A) := W$ gdw es gibt ω' mit "$\omega = \omega'$ bis auf x" und $Wert^{\omega'}_{\mathcal{M}}(A) = W$

d.h. $Wert^{\omega}_{\mathcal{M}}$: Formeln $\longrightarrow \{W, F\}$

$Wert_{\mathcal{M}}$: geschlossene Formeln $\longrightarrow \{W, F\}$

(keine freien Variablen!)

$Wert_{\mathcal{M}}$ unabhängig von ω

G (Formel) **gilt in** $\mathcal{M}$ (Struktur)

$\mathcal{M}$ (Struktur) **ist Modell von** G (Formel)

gdw $\text{Wert}_{\mathcal{M}}(\forall G) = W$

Allabschluß der Formel G

$\mathcal{M}$ (Struktur) **ist Modell von** X (Formelmenge) gdw $\mathcal{M}$ ist Modell für alle $G \in X$

X ist **erfüllbar** gdw. es gibt ein Modell $\mathcal{M}$ von X

X und Y sind **erfüllbarkeitsgleich** gdw sie beide erfüllbar oder beide unerfüllbar sind

---

X ist **allgemeingültig** gdw jede Struktur (passend zu Σ) ist Modell von X

G (Formel) **folgt (logisch) aus** X (Formelmenge) gdw jedes Modell von X ist auch Modell von G

kurz: $X \models G$

Normalformen

konjunktive Normelform:

$$D_1 \wedge \ldots \wedge D_n$$

D_i hat Form $L_1 \vee \ldots \vee L_{i_r}$ mit L_i Literal

Gentzenformel:

$$P_1 \wedge \ldots \wedge P_n \longrightarrow Q_1 \vee \ldots \vee Q_m \quad \text{mit } P_i, Q_j \text{ atomar}$$

äquivalent zu

$$\neg P_1 \vee \ldots \vee \neg P_n \vee Q_1 \vee \ldots \vee Q_m$$

d.h. hat Form eines D_i aus konj. NF

Hornformel:

$$P_1 \wedge \ldots \wedge P_n \longrightarrow Q \quad \text{mit } P_i, Q \text{ atomar}$$

äquivalent zu

$$\neg P_1 \vee \ldots \vee \neg P_n \vee Q$$

Widerspruch:

$$W \longrightarrow F$$

kurz $\square$ Marke einer unerfüllbaren Formel

Traum vom automatischen Beweisen

① Mensch behauptet

② Maschine beweist

ein Ansatz:

zu ①: - Behauptung inhaltlich bestimmen

- Formalisierung der Grundgegebenheiten:

  Signatur $\Sigma = (S, F, P)$

  "worüber wir reden können"

- Formalisierung der Voraussetzungen:

  Formelmenge X über Σ

- Formalisierung der Konklusion: Formel G

- Formalisierung der Behauptung: $X \vdash G$

  z.B. X: Gruppenaxiome

  G: $\forall x (x \circ x^{-1} = e)$

  gdw

zu ①-②: Umformen: $X \cup \{\neg G\}$ unerfüllbar

Normalisieren: pränexe Normalform

Skolem Normalform

Matrix in konj. NF (Menge von Gentzenformeln)

zu ②: mit Regeln, die Erfüllbarkeit (Unerfüllbarkeit) erhalten,

□ ableiten

Lemma 1.30

Jede prädikatenlogische Formel läßt sich (effektiv) in eine dazu **äquivalente** in **pränexe Normalform** bringen, d.h. in die Gestalt

$$\underbrace{Q_1 \dots Q_n}_{\text{Quantoren}} \quad \underbrace{M}_{\text{quantorenfreie Matrix}}$$

Umformungsregeln:

1) $Qx\,P(x) \vee G$ (x nicht in G) ersetzen durch $Qx\,(P(x) \vee G)$

$Qx\,P(x) \wedge G$ (x nicht in G) ersetzen durch $Qx\,(P(x) \wedge G)$

$\neg\, \forall x\, P(x)$ ersetzen durch $\exists x \neg P(x)$

$\neg\, \exists x\, P(x)$ ersetzen durch $\forall x \neg P(x)$

Quantoren "wandern nach außen"

2) konfliktfreie Umbenennungen von Variablen

3) jeweils äquivalente Teilausdrücke (lokal) ersetzen

kein eindeutiges Ergebnis!

Beispiel:

$$\forall x \exists y \; P(x,y) \;\vee\; \exists x \, Q(x)$$

$$\forall x \exists y \; P(x,y) \;\vee\; \exists z \, Q(z) \qquad \text{Umbenennung}$$

$$\forall x \exists y \Big(P(x,y) \;\vee\; \underbrace{\exists z \, Q(z)}_{\text{ohne } x,\ \text{ohne } y} \Big)$$

$$\forall x \exists y \Big(\exists z \big(\underbrace{P(x,y)}_{\text{ohne } z} \vee Q(z) \big) \Big)$$

Vorsicht bei Umbenennungen: Konflikte, z.B.:

$$\forall x \, P(x) \;\vee\; \forall x \, Q(x) \quad \models \quad \forall x \big(P(x) \vee Q(x) \big)$$

aber: $\not\models$

z.B. bei Interpretation über natürlichen Zahlen:

alle Zahlen sind gerade $\vee$ alle Zahlen sind ungerade $\models$ alle Zahlen sind gerade oder ungerade

$\not\models$

Lemma 1.33

Jede Formel in pränexer Normalform läßt sich in eine (nur) erfüllbarkeitsgleiche Formel in Skolem-Normalform bringen:

entferne <u>von außen nach innen</u> alle Quantoren gemäß folgender Vorschrift:

(i) Allquantor: einfach weglassen (implizite Allquantifizierung)

(ii) Existenzquantor:

$$\exists y\, Q_1 \dots Q_k \; M(\underbrace{x_1, \dots, x_\ell}, y)$$

alle in M <u>frei vorkommenden</u> Variablen, gemäß (i) implizit allquantifiziert

mit f neues Funktionssymbol (als "Skolemfunktion")

ersetzen durch:

$$Q_1 \dots Q_k \; M(x_1, \dots, x_\ell, f(x_1, \dots, x_\ell))$$

f. alle $x_1, \dots, x_\ell$ gibt es y : $Q_1 \dots Q_k \; M(x_1, \dots, x_\ell, y)$

f beschreibt Zuordnung: $x_1, \dots, x_\ell \longmapsto y$

Beispiele:

1.) • $\forall x \exists y \forall z \left(P(x,y) \wedge Q(y,z) \rightarrow R(x,y,z) \right)$

• $\exists y \forall z \left(P(x,y) \wedge Q(y,z) \rightarrow R(x,y,z) \right)$

kommt frei vor — kommt frei vor

• $\forall z \left(P(x,f(x)) \wedge Q(f(x),z) \rightarrow R(x,f(x),z) \right)$

• $P(x,f(x)) \wedge Q(f(x),z) \rightarrow R(x,f(x),z)$

2) $\exists x \, P(x)$

$P(c)$

↑ neues Konstantenzeichen

Lemma 1.35

Jede quantorenfreie Formel läßt sich in eine dazu **äquivalente Menge** von Gentzenformeln transformieren.

siehe Rechnerstrukturen (Boolesche Algebra):

Distributivgesetze, Kommutativgesetze, Assoziativgesetze, Absorbtionsgesetze, (de Morgan'sche Gesetze) erlauben

konjunktive Normalform:

$$(L_{11} \vee \dots \vee L_{1k_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nk_n})$$

mit L_{ij} Literal (atomar, negiert atomar).

1) $\wedge \quad \hat{=} \quad$ Menge von Formeln

2) sind $L_{i,1}, \dots, L_{i,p}$ negiert atomar, $L_{i,j} \equiv \neg A_{i,j}$
$L_{i,p+1} \dots L_{i,k_i}$ atomar

so äquivalent zu $A_{i,1} \wedge \dots \wedge A_{i,p_i} \rightarrow L_{i,p+1} \vee \dots \vee L_{i,k_i}$

Normalisieren

1. pränexe Normalform : äquivalent
   (Quantoren herausziehen)

2. Skolem-Normalform : erfüllbarkeitsgleich
   (Existenzquantoren entfernen)

3. Menge von Gentzenformeln : äquivalent

---

erfüllbarkeitsgleich

$$\forall x \Big(animal(x) \rightarrow$$
$$\forall y \; (plants(y) \rightarrow eats(x,y)) \quad \vee$$
$$\forall z \; (animal(z) \wedge muchsmaller(z,x)$$
$$\wedge \exists u \; (plants(u) \wedge eats(z,u))$$
$$\rightarrow eats(x,z)) \Big)$$
$$\vdots$$

ein Anwendungsbeispiel:

→ Hofbauer / Kutsche

Schnittregel

$$\frac{A \to B \vee P \qquad P \wedge C \to D}{A \wedge C \to B \vee D}$$

$$\frac{\neg A \vee B \vee P \qquad \neg P \vee \neg C \vee D}{\neg A \vee \neg C \vee B \vee D}$$

in Klauselschreibweise:

$$\frac{\{\neg A, B, \boxed{P}\} \qquad \{\neg P, \neg C, D\}}{\{\neg A, \neg C, B, D\}}$$

wird "herausgeschnitten"

speziell:

$$\frac{\neg W \vee P \qquad \neg P \vee F}{\{P\} \qquad \{\neg P\}}$$

$$\square$$

$$\neg W \vee F$$

Substitutionsregel

$$\frac{G}{G\sigma}$$

G quantorenfreie Gentzenformel

σ Substitution

Syntax:

Signatur: $\Sigma = (S, F, P)$

- S: Sortensymbole
- F: Funktionssymbole
- P: Prädikatensymbole

Grundterme über Σ:

i) Konstantensymbole aus F

ii) ist $f(s_1, \ldots, s_n) \to s$ aus Σ und sind $t_1, \ldots, t_n$ Grundterme, so ist auch $f(t_1, \ldots, t_n)$ Grundterm

"gewinne Semantik aus syntaktischem Material",
"normalisierte Semantik", Herbrand-Struktur:

Herbrand-Universum: Grundterme über Σ, genauer:

$$\mathcal{U} := (\mathcal{U}_s)_{s \in S} \quad \text{mit} \quad \mathcal{U}_s := \{ t \mid t \text{ Grundterm zur Sorte } s \}$$

Herbrand-Interpretation:

$$I(s) := \mathcal{U}_s$$

$$I(f) := f_T \quad \text{mit} \quad f_T(t_1, \ldots, t_n) := f(t_1, \ldots, t_n)$$

$I(P)$ beliebig!

Herbrand-Basis:

$$\mathcal{B} := \{ P(t_1, \ldots, t_n) \mid P \text{ Prädikatensymbol}, t_i \text{ Grundterme} \}$$

Herbrand-Interpretation von Prädikatzeichen:

$$I(P): U_{s_1} \times \ldots \times U_{s_n} \to \{W, F\}$$

(
Grundterme zur Sorte s_1

entspricht eineindeutig

$$\mathcal{A} \subset \mathcal{B}$$

$$\mathcal{A} := \{ P(t_1, \ldots, t_n) \mid P(t_1, \ldots, t_n) \in \mathcal{B} \text{ und } I(P)(t_1, \ldots, t_n) = W \}$$

Satz 1.45

Eine Menge X quantorenfreier Formeln ist erfüllbar

genau dann, wenn

X ein Herbraud-Modell besitzt.

Beweis: „$\Leftarrow$": trivial

„$\Rightarrow$" o.B.d.A (Lemma 1.35) bestehe X aus Gentzenformeln, d.h. Formeln der Form $\Gamma \to \Delta$.

Sei $\mathfrak{M}$ Modell von X.

Definiere:

$$\mathcal{A} := \{ A \mid A \text{ Grundatom}, \ \text{Wert}_{\mathfrak{M}}(A) = W \}$$
$$\subset \mathcal{B} \quad \text{(Herbraud-Basis)}$$

$\mathcal{A}$ bestimmt Herbraud-Struktur $\mathfrak{H}$ (siehe oben).

Beh: $\mathfrak{H}$ ist Modell von X.

Bew (indirekt):

angenommen, $\mathcal{K}$ sei nicht Modell von $\forall \overbrace{K \to D}^{\in X}$

$\Rightarrow$ ex. Variablenzuweisung, d.h. Grundsubstitution σ

(wegen Form des Herbrand-Universums)

mit $Wert^{\sigma}_{\mathcal{K}}(K \to D) = F$

d.h. $Wert_{\mathcal{K}}(P\sigma) = W$, $Wert_{\mathcal{K}}(Q\sigma) = F$ } f. alle $P\sigma \in K\sigma$, $Q\sigma \in D\sigma$

d.h. $\mathcal{K}$ bestimmt durch $\mathcal{A}$: $P\sigma \in \mathcal{A}$, $Q\sigma \notin \mathcal{A}$ } f. alle $P\sigma \in K\sigma$, $Q\sigma \in D\sigma$

d.h. Definition von $\mathcal{A}$: $Wert_{\mathcal{M}}(P\sigma) = W$, $Wert_{\mathcal{M}}(Q\sigma) = F$ } f. alle $P\sigma \in K\sigma$, $Q\sigma \in D\sigma$

d.h. $\mathcal{M}$ ist nicht Modell von $K \to D$

$\Rightarrow \#$

Sei R Regelsystem

R heißt **korrekt**

: gdw wenn $X \vdash_R G$ syntaktisches Ableiten

dann $X \models G$ semantische Folgerung

R heißt **vollständig**

: gdw wenn $X \models G$

dann $X \vdash_R G$

R heißt **widerlegungsvollständig**

: gdw wenn X widersprüchlich (unerfüllbar)

dann $X \vdash_R \square$

Satz 149 Die Schnittregel

$$\frac{A \to B \vee P \quad \{\neg A, B, P\} \qquad P \wedge C \to D \quad \{\neg P, \neg C, D\}}{A \wedge C \to B \vee D \quad \{\neg A, \neg C, B, D\}}\ GS$$

ist für <u>variablenfreie</u> Gentzenformeln $\{\neg P_1, \dots, \neg P_n, Q_1, \dots, Q_m\}$

korrekt, d.h. wenn $X \vdash_{GS} G$, dann $X \vdash G$

und widerlegungsvollständig, d.h. wenn X widersprüchlich dann $X \vdash_{GS} \square$.

Beweis der Korrektheit: zu zeigen:

wenn M Modell von $\{\neg A, B, P\}$

und M Modell von $\{\neg P, \neg C, D\}$

dann M Modell von $\{\neg A, \neg C, B, D\}$!

da alle Formeln variablenfrei sind: entweder M Modell von P
oder M Modell von $\neg P$

Fall 1: M Modell von P

dann: M nicht Modell von $\neg P$ Semantik von $\neg$

dann: M Modell von $\{\neg C, D\}$ M Modell von $\{\neg P, \neg C, D\}$

dann: M Modell von $\{\neg A, \neg C, B, D\}$ Semantik von $\vee$

Fall 2: analog!

$\vee$ $\vee$

Beweis der Widerlegungsvollständigkeit:

zu zeigen: wenn X widersprüchlich dann $X \vdash_{GS} \square$!

Kontraposition: wenn $X \not\vdash_{GS} \square$ dann X erfüllbar !

gdw (Satz 1.45)

X besitzt Herbrand-Modell

Aufgabe: unter Annahme, daß aus X mit Hilfe der Schnittregel GS nicht $\square$ abgeleitet werden kann: "konstruiere" Herbrand-Modell für X !

Konstruktion:

sei $P_1, P_2, \ldots$ Aufzählung der Herbrand-Basis

$\mathcal{B} = \{ P(t_1, \ldots, t_n) \mid P$ Prädikatensymbol, t_i Grundterme $\}$

definiere: i) $X_0 := X$

ii) $X_{n+1} := X_n \cup \begin{cases} \{P_n\} & \text{falls } X_n \cup \{P_n\} \not\vdash_{GS} \square \\ \{\neg P_n\} & \text{sonst} \end{cases}$

iii) $\hat{X} := \bigcup_{n \geq 0} X_n$

es gilt: a) f. alle $n \geq 0$: $X_n \nvdash_{GS} \square$

Beweis: (Induktion über n)

$n=0$: $\underbrace{X}_{=X_0} \nvdash_{GS} \square$ nach Voraussetzung

$n+1$: **Fall 1:** $X_n \cup \{P_n\} \nvdash_{GS} \square$

dann: $X_{n+1} := X_n \cup \{P_n\}$

also: $X_{n+1} \nvdash_{GS} \square$

Fall 2: $X_n \cup \{P_n\} \vdash_{GS} \square$

dann: $X_{n+1} := X_n \cup \{\neg P_n\}$

indirekte Annahme: $X_n \cup \{\neg P_n\} \vdash_{GS} \square$

Konsistenzlemma (s.u): $X_n \vdash_{GS} \square$

also: #(zur Induktionsannahme)

es gilt: b) $\hat{X} \nvdash_{GS} \square$

Beweis: (indirekt) Annahme: $\hat{X} \vdash_{GS} \square$

dann: es gibt $\underbrace{\text{Ableitung}}_{\text{endlich!}}$ von $\square$ aus $\underbrace{\hat{X}}_{\text{d.h. nur endliche Teilmenge wird benutzt, etwa nur Elemente aus } X_n}$

also: ex. $n \in \mathbb{N}$: $X_n \vdash_{GS} \square$ #(zu a)

es gilt: c) f. alle Grundatome P : $P \notin \hat{X}$ gdw. $\neg P \in \hat{X}$

Beweis:

i) sei $P \equiv P_n$

Schritt ii) der Konstruktion

fügt **entweder** P_n **oder** $\neg P_n$ hinzu

ii) es werde o.B.d.A P_n hinzugefügt zu $\hat{X}$

indirekte Annahme:

$$\neg P_n \in X \quad , \text{ d.h. } \neg P_n \in X_0 \subset \hat{X}$$

dann $\dfrac{\overset{\in \hat{X}}{\{\neg P_n\}} \qquad \overset{\in \hat{X}}{\{P_n\}}}{\square}\, GS$

d.h. $\hat{X} \vdash_{GS} \square$

also # (zu b))

also: a) f.alle $n \geq 0$: $X_n \vdash_{GS} \square$

b) $\hat{X} \vdash_{GS} \square$

c) f.alle Grundatome P: $P \notin \hat{X}$ gdw. $\neg P \in \hat{X}$

sei $\hat{A}$:= Menge der Atome aus $\hat{X}$
(unnegierte Literale)

$\hat{A} \subset \mathcal{B}$ Herbrand-Basis

$\hat{A}$ entspricht eindeutig einer Herbrand-Struktur $\mathcal{H}$

Beh: $\mathcal{H}$ ist Modell von $\hat{X}$.

Bew.: (indirekt)

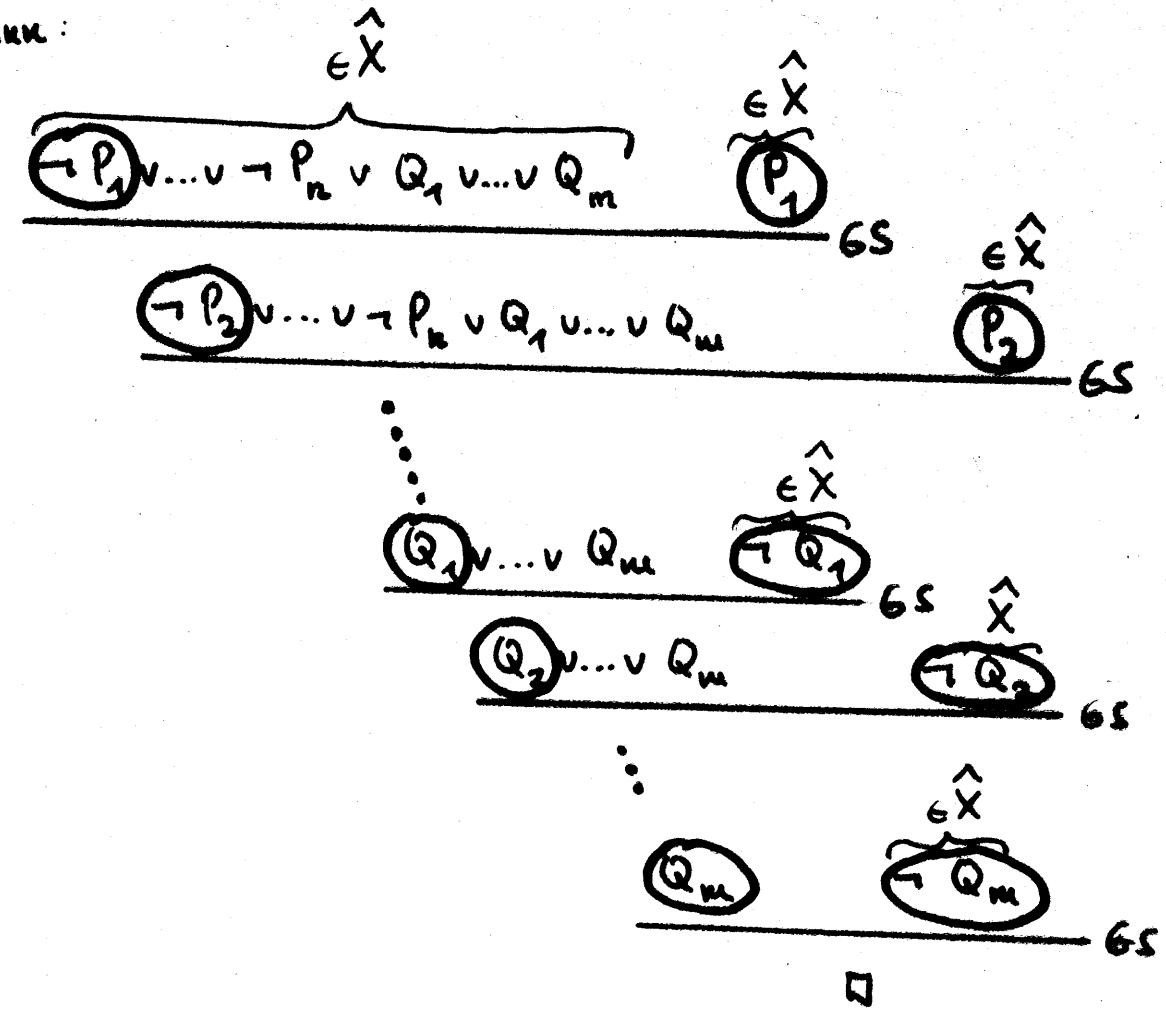
Annahme: $\mathcal{H}$ nicht Modell von $\hat{X}$

dann: ex $G := C \to D \in \hat{X}$ mit $Wert_{\mathcal{H}}(G) = F$

dann: $Wert_{\mathcal{H}}(P) = W$, $Wert_{\mathcal{H}}(Q) = F$ } f.alle $P \in C$, $Q \in D$

d.h. $P \in \hat{A} \subset \hat{X}$, $\neg Q \in \hat{X}$ } f.alle $P \in C$, $Q \in D$

dann:



d.h. $\hat{X} \vdash_{GS} \square$

also $\#(a \sqcap b))$

Lemma 1.50 Konsistenzlemma

Wenn $X \cup \{P\} \vdash_{GS} \square$

und $X \cup \{\neg P\} \vdash_{GS} \square$,

dann $X \vdash_{GS} \square$

Beweis: betrachte Ableitungsbaum für $X \cup \{P\} \vdash_{GS} \square$:

Fall 1: P wird nicht benutzt: Beh. folgt trivial

Fall 2: P wird benutzt, dann auch als Blatt, etwa so:

$$\dfrac{\Gamma_1 \cup \{\neg P\} \qquad \{P\}}{\Gamma_1}\,GS$$

$\vdots$

modifiziere Ableitungsbaum:

1. ersetze obigen Schritt einfach durch $\Gamma_1 \cup \{\neg P\}$
2. setze Änderung im Baum fort:

   entweder $\neg P$ wird in allen Zweigen herausgeschnitten

   oder $\neg P$ bleibt erhalten:

   dann $X \vdash_{GS} \{\neg P\}$

   füge Ableitungsbaum für $X \cup \{\neg P\} \vdash_{GS} \square$ hinzu:

   man erhält Ableitungsbaum für

   $X \vdash_{GS} \square$

Beispiel:

X sei in Klauselschreibweise gegeben:

$\{S\}$,
$\{\neg P, Q\}$
$\{\neg P, R\}$
$\{\neg Q, \neg R\}$
$\{\neg S, P\}$

i) es gilt: $X, \{P\} \vdash_{GS} \square$, z.B. vermöge Ableitung A1;

ii) es gilt: $X, \{\neg P\} \vdash_{GS} \square$ z.B. vermöge Ableitung A2;

A1:

$$\dfrac{\dfrac{\dfrac{\neg P, Q \qquad P}{Q} \qquad \neg Q, \neg R}{\neg R} \qquad \dfrac{\neg P, R \qquad P}{R}}{\square}$$

A2:

$$\dfrac{\dfrac{\neg S, P \qquad \neg P}{S} \qquad \neg S}{\square}$$

Beispiel:

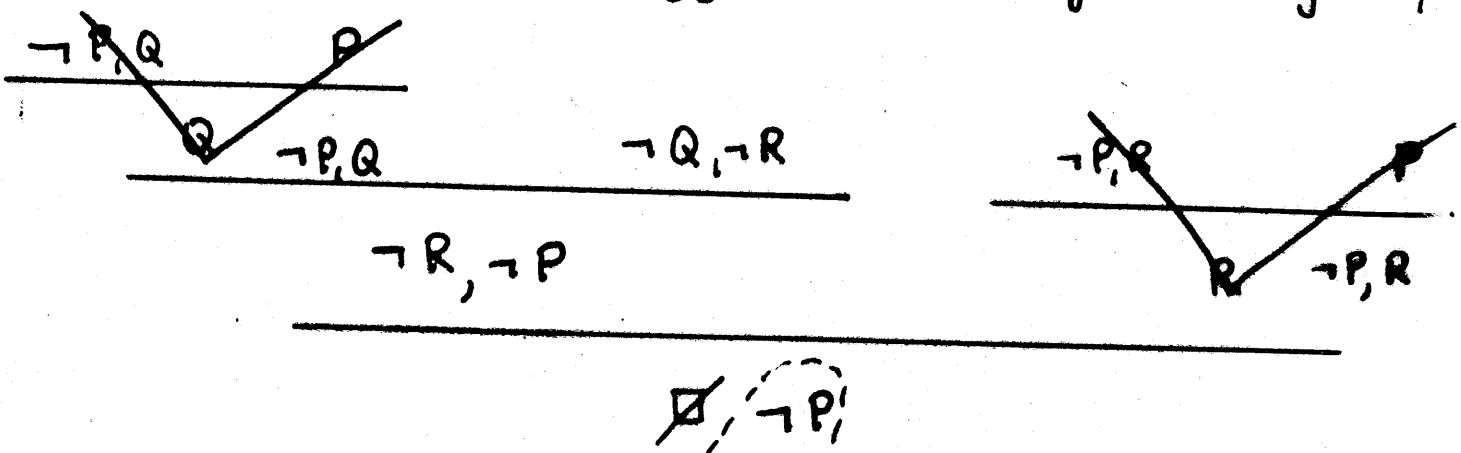
X sei in Klauselschreibweise gegeben:

$\{S\}$,
$\{\neg P, Q\}$
$\{\neg P, R\}$
$\{\neg Q, \neg R\}$
$\{\neg S, P\}$

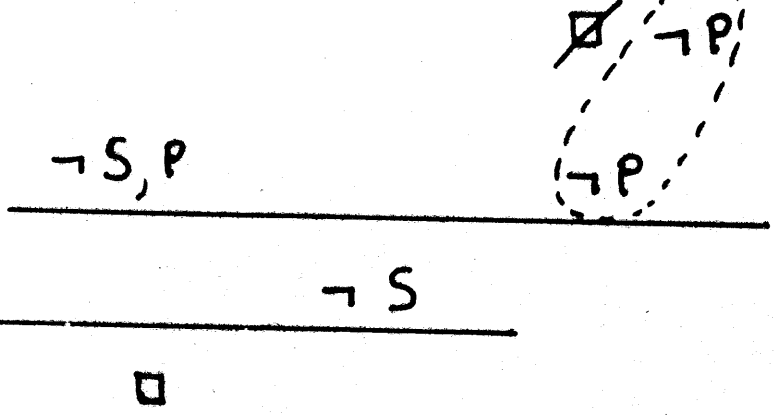
i) es gilt: $X, \{P\} \vdash_{GS} \square$, z.B. vermöge Ableitung A1;

ii) es gilt: $X, \{\neg P\} \vdash_{GS} \square$ z.B. vermöge Ableitung A2;

A1:



A2:



- modifiziere und leite $\neg P$ (anstelle von $\square$) ab!
- kombiniere Ableitungsbäume!

bislang: Schnittregel korrekt und widerlegungsvollständig für variablenfreie Gentzenformeln.

nunmehr: Gentzenformeln mit Variablen (implizit allquantifiziert!)

Sei X Menge von Gentzenformeln

$$\text{grund}(X) := \{ A\omega \mid A \in X, \; \omega: \text{Variablen} \to \text{Terme ist Grundsubstitution} \}$$

Lemma 1.52 [Folgerungen absenken]

Wenn X widersprüchlich, dann auch $\text{grund}(X)$.

Lemma 1.53 [Ableitungen hochheben]

Wenn $\text{grund}(X) \vdash_{GS} \square$, dann $X \vdash_{GS + \text{Substitution}} \square$.

Satz 1.55

(GS (Schnittregel für Gentzenformeln
+ Subst (Substitution))

ist widerlegungsvollständig für (beliebige) Gentzenformeln.

Lemma 1.52 [Folgerungen absenken]

Wenn X widersprüchlich, dann auch $\text{grund}(X)$.

zu zeigen (Kontraposition):

wenn $\text{grund}(X)$ ein Modell besitzt, dann auch X !

spezieller: gdw es ein Herbraud-Modell besitzt — wir können sogar das gleiche nehmen

wenn $\mathcal{H}$ ein Herbraud-Modell von $\text{grund}(X)$ ist,
dann ist $\mathcal{H}$ auch Modell von X.

Beweis: Sei $\mathcal{H}$ Herbraud-Modell von $\text{grund}(X)$.

Sei ω: Variablen $\longrightarrow$ Herbraud-Universum, $G \in X$.

zu zeigen: $\text{Wert}^{\omega}_{\mathcal{H}}(G) = W$

Bew.: $\text{Wert}^{\omega}_{\mathcal{H}}(G) = \text{Wert}_{\mathcal{H}}(G\omega)$ — ω ist auch Grundsubstitution

$= W$ — $G\omega \in \text{grund}(X)$ und $\mathcal{H}$ Modell von X

Lemma 1.53 [Ableitungen hochheben]

Wenn $\text{grund}(X) \vdash_{GS} \square$, dann $X \vdash_{GS+\text{Subst}} \square$.

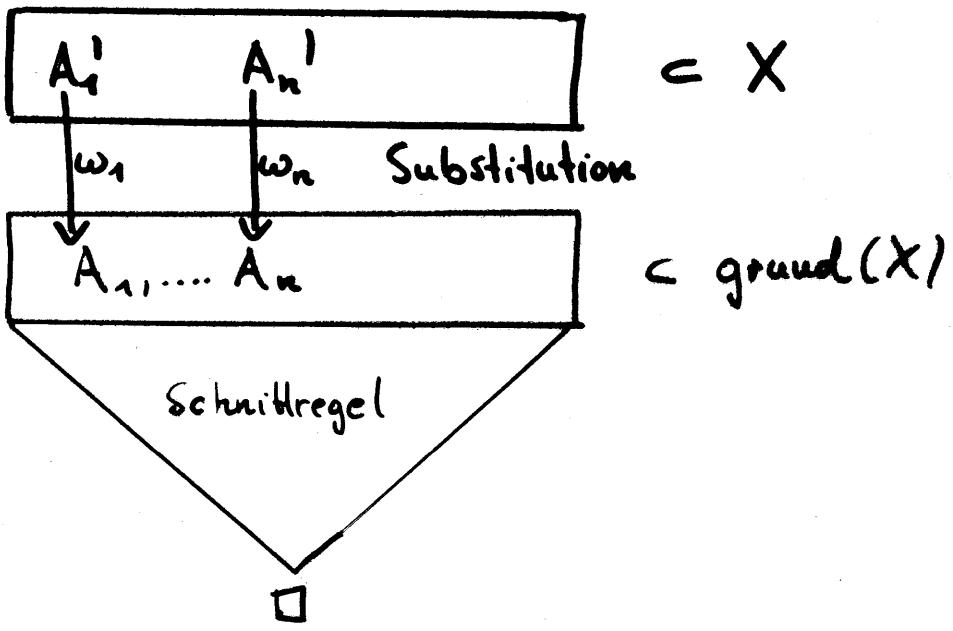
Beweis:

sei $A \in \text{grund}(X)$ ein Blatt in der Ableitung von $\square$

$$\left.\begin{array}{l} \text{ex } \omega : \text{Variablen} \to \text{Grundterme} \\ \text{ex } A' \in X \end{array}\right\} \; A = A'\omega$$

ersetze A durch $\dfrac{A'}{A}$ Subst mit Substitution ω

anschaulich:



Satz 1.54 [Lifting Theorem]

Sei R die Schnittregel (gemäß Satz 1.49 widerlegungsvollständig für variablenfreie Gentzenformeln)

oder eine ebenfalls noch für variablenfreie Gentzenformeln widerlegungsvollständige Spezialisierung.

Dann ist (R + Substitution) widerlegungsvollständig für beliebige Gentzenformeln.

zu zeigen: **wenn** X widersprüchliche Menge von Gentzenformeln

dann $X \vdash_{R+\text{Subst}} \square$.

Beweis: X widersprüchlich

dann: $\text{grund}(X)$ widersprüchlich — Folgerung absenken (Lemma 1.52)

dann: $\text{grund}(X) \vdash_R \square$ — R widerlegungsvollständig für variablenfreie Formeln (Satz 1.49)

dann: $X \vdash_{R+\text{Subst}} \square$ — Ableitungen hochheben (Lemma 1.53)

Satz von Herbrand

Sei X Menge von Gentzenformeln.

X ist widersprüchlich (prädikatenlogisch) gdw
es gibt endliche Menge $\overline{X}$ von Grundinstanzen von X
mit $\overline{X}$ widersprüchlich. (aussagenlogisch)

Beweisskizze:

"$\Rightarrow$" X widersprüchlich

dann: $X \vdash_{GS+Subst} \square$

GS + Subst widerlegungsvollständig (Satz 1.54)

dann: ex. (endliche) Ableitung von $\square$ aus X mit GS + Subst. Def. $\vdash$

- sei $X' \subset X$ die Menge der in der Ableitung benutzten Formeln: X' ist endlich
- "verschiebe" alle Anwendungen von Subst an die Blätter
- ersetze Anwendung von Subst durch entsprechende Instanzen
- ersetze verbliebene Variablen durch Konstantenzeichen

sei $\overline{X} \subset ground(X)$ die nunmehr in der Ableitung (die nur noch GS anwendet) benutzte Formelmenge:

$\overline{X}$ ist widersprüchlich (wie die Ableitung zeigt)

Traum vom automatischen Beweisen

⋮

Formalisierung der Behauptung: $X \models G$

X, G variablenfrei: $X \models G$

gdw $X \cup \{\neg G\}$ widersprüchlich

gdw $X \cup \{\neg G\} \vdash_{GS} \square$

X, G enthalten Variablen:

$X \models G$

gdw $X \models \forall G$

gdw $X \cup \{\neg \forall G\}$ widersprüchlich

↓ pränexe NF
↓ Skolem NF
↓ Menge von Grundformeln

gdw Y widersprüchlich

gdw $Y \vdash_{GS + Subst} \square$

Problem: "Suchraum" der möglichen Ableitungen einschränken

1. Versuch einer Algorithmisierung: einige Probleme:

[Initialisierung: wende Subst an]

$\overline{X}$:= endliche Menge von Grundinstanzen von X;
Subst nur mit Grundsubst.

while

[teste auf aussagenlogische Widersprüchlichkeit:
wende GS auf variablenfreie Formeln an]

$\overline{X} \vdash_{GS} \square$ [entscheidbar, da aus $\overline{X}$ nur endlich viele neue Formeln mit GS gebildet werden können]

st ge Trennung von GS und Subst

do [wende Subst an]

Subst nur mit Grundsubstitutionen

viele Grundinst. werden "nutzlos" erzeugt:

$\overline{X} := \overline{X} \cup$ endliche Menge weiterer Grundinstanzen von X

[$\overline{X}_{neu} \not\subseteq \overline{X}_{alt}$; falls kein Abbruch, wird ganz grund(X) ausgeschöpft]

für keinen Schritt brauchbar

end ;

[Satz von Herbrand: Abbruch gdw X widersprüchlich]

kein Abbruch bei erfüllbarem X: unvermeidbar, da Widersprüchlichkeit (Folgerung)

output ("X widersprüchlich"); **unentscheidbar!**

einige Probleme:

1. strenge Trennung von GS und Subst;

   Subst nur mit Grundsubstitutionen angewendet;

   vielen Grundinstanzen "nutzlos" erzeugt: für keinen Schritt brauchbar

   Lösungsansatz:

   - wende Subst "zielgerichtet" im Hinblick auf Schrittanwendung an
   - erzeuge mit Subst nicht alle (Grund-) Instanzen, sondern nur "allgemeinste" Repräsentanten von wirklich brauchbaren Instanzen

2. kein Abbruch bei erfüllbarem X

   - keine Lösung möglich: Widersprüchlichkeit ist unentscheidbar!!
   - aber: betrachte Spezialfälle, die Abbruch erlauben

Schnittregel:

$$\frac{\{\neg A, B, P(t_1,\dots,t_n)\} \quad \{\neg P(t_1,\dots,t_n), \neg C, D\}}{\{\neg A, \neg C, B, D\}}$$

Aufgabe:

- suche zwei Prämissen, in denen ein wegzuschneidendes Atom $P(t_1,\dots,t_n)$ einmal unnegiert und einmal negiert vorkommt!

  ("suche ein Paar komplementärer Literale")

- erzeuge solche Prämissen durch geeignete Substitutionen:

  gegeben: Terme $t_1,\dots,t_n$ in $P(t_1,\dots,t_n)$ und $t_1',\dots,t_n'$ in $\neg P(t_1',\dots,t_n')$

  gesucht: Substitution σ mit

  1. $t_i\sigma = t_i'\sigma$
  2. σ "allgemeinst"

  dann: $P(t_1,\dots,t_n)\sigma = P(t_1',\dots,t_n')\sigma$

  dann: Schnittregel anwendbar

Definition

Terme t, t' heißen **unifizierbar**

: gdw ex. Substitution σ mit $t\sigma = t'\sigma$

Termmenge M heißt **unifizierbar**

: gdw ex. Substitution σ mit $t\sigma = t'\sigma$

f. alle $t, t' \in M$

σ heißt dann **Unifikator** von t, t' bzw. M

Bsp:

1) $f(x, a)$ — x: Variable, a: Konstantensymbol

$f(g(y), y)$ — y: Variable

haben Unifikator $\begin{bmatrix} x & y \\ g(a) & a \end{bmatrix}$

2) $f(b, a)$ — b: Konstantensymbol, a: Konstantensymbol

$f(g(y), y)$ — y: Variable

besitzen keinen Unifikator:

um 2. Stelle zu unifizieren müßte y auf a abgebildet werden; aber $b \neq g(a)$!

Definition

1) Substitution σ ist allgemeiner als Substitution τ,

$\sigma \leq \tau$: gdw ex Substitution ρ mit $\sigma\rho = \tau$

Bsp: $\sigma = \begin{bmatrix} x & z \\ f(z) & a \end{bmatrix}$ $\tau = \begin{bmatrix} x & z \\ f(a) & a \end{bmatrix}$

($f(z)$: Variable; $f(a)$: Konstantensymbol)

für $\rho = \begin{bmatrix} z \\ a \end{bmatrix}$ gilt $\sigma\rho = \begin{bmatrix} x & z \\ f(a) & a \end{bmatrix} = \tau$

2) $\sigma \approx \tau$, σ äquivalent τ : gdw $\sigma \leq \tau$ und $\tau \leq \sigma$

3) $\sigma \sim \tau$, σ Variante von τ

: gdw ex. Variablenumbenennung $\rho = \underbrace{\begin{bmatrix} x_1, \dots, x_k \\ x_{i_1}, \dots, x_{i_k} \end{bmatrix}}_{\text{Permutation}}$

mit $\sigma\rho = \tau$

$\Downarrow$

$\sigma = \sigma\rho\rho^{-1} = \tau\rho^{-1}$

d.h. τ ist Variante von σ

also: "σ und τ sind Varianten"

Definition:

Substitution σ heißt **allgemeinster Unifikator** (most general unifier, **mgu**) der Termmenge M

: gdw 1. σ ist Unifikator von M,

d.h. $t\sigma = t'\sigma$ f. alle $t, t' \in M$

2. f. alle Unifikatoren τ von M gilt $\sigma \leq \tau$,

d.h. <u>falls</u> $t\tau = t'\tau$ f. alle $t, t' \in M$

<u>dann</u> ex. ϱ mit $\sigma\varrho = \tau$

<u>Bsp.</u> $f(x, y)$, $f(y, x)$ besitzen allgemeinsten Unifikator

$\sigma_1 = \begin{bmatrix} x & y \\ x & x \end{bmatrix}$ oder $\sigma_2 = \begin{bmatrix} x & y \\ y & y \end{bmatrix}$

σ_1, σ_2 sind Varianten vermöge $\varrho = \begin{bmatrix} x & y \\ y & x \end{bmatrix}$

sei τ irgendein Unifikator

$\Rightarrow x\tau = y\tau$

$\Rightarrow$ ex. ϱ mit $\sigma_1\varrho = \tau$

Lemma 2.5 $\sigma \approx \tau$ gdw $\sigma \sim \tau$

d.h. ex ρ_1, ρ_2 mit $\sigma\rho_1 = \tau$, $\tau\rho_2 = \sigma$ gdw ex. Permutation π mit $\sigma\pi = \tau$

Beweis: "$\Leftarrow$":

$$\left.\begin{array}{l} \sigma\pi = \tau \Rightarrow \sigma \preceq \tau \\ \tau\pi^{-1} = \sigma\pi\pi^{-1} = \sigma \Rightarrow \tau \preceq \sigma \end{array}\right\} \Rightarrow \sigma \approx \tau$$

"$\Rightarrow$":

$$\sigma\rho_1\rho_2 = \tau\rho_2 = \sigma$$

$\Rightarrow$ $\rho_1\rho_2$ läßt Variablen im Bildbereich von σ unverändert

$\Rightarrow$ • $\rho_1(x)$ ist Variable f. alle Variablen x im Bildbereich von σ

• ρ_1 ist injektiv auf den Variablen im Bildbereich von σ

sei π definiert durch

• π Erweiterung von ρ_1 auf den Variablen im Bildbereich von σ

• π Permutation auf endlicher Menge von Variablen

$\Rightarrow$ $\sigma\pi = \tau$

└ "tut das Gleiche wie ρ_1!"

$\Rightarrow$ $\sigma \sim \tau$

Satz 2.6.b [Eindeutigkeit allgemeinster Unifikatoren]

Sind σ und τ allgemeinste Unifikatoren von M, so sind σ und τ Varianten.

Beweis:

σ mgu von M und τ Unifikator von M: $\sigma \leq \tau$

τ mgu von M und σ Unifikator von M: $\tau \leq \sigma$

also: $\sigma \approx \tau$ [äquivalent]

Lemma 2.5: $\sigma \sim \tau$ [Varianten]

Satz 2.6.a [Existenz allgemeinster Unifikatoren]

Ist M unifizierbar, so existiert ein allgemeinster Unifikator für M.

Ansatz für einen Algorithmus:

1. bestimme Start-Gleichungsmenge

$$E_0 := \{ t \doteq t' \mid t \neq t', t \in M, t' \in M \}$$

Aufgabe: löse die Gleichungen simultan durch geeignete Substitution

2. wende wiederholt Umformungsregeln auf die laufende Gleichungsmenge an:

- geforderte Invarianz: i) Unifizierbarkeit
  ii) mgu
- Abbruch sicherstellen!

3. lies bei Abbruch aus dann vorliegender Gleichungsmenge ab,
   - ob unifizierbar [einfaches Kriterium]
   - falls unifizierbar, dann mgu

Umformungsregeln von Martelli-Montanari

t, t_i, t_i' : Terme

f : Operationssymbol

x : Variable

E : Gleichungsmenge

$\cup$: disjunkte Vereinigung

U1. Dekomposition:

$$\frac{E \cup \{ f(t_1,\dots,t_n) \equiv f(t_1',\dots,t_n') \}}{E \cup \{ t_1 \equiv t_1', \dots, t_n \equiv t_n' \}}$$

speziell:

$$\frac{E \cup \{ a \equiv a \}}{E}$$

entfernt triviale Gleichung für Konstantensymbol

U2. Variablen-Elimination:

falls x nicht in t ("occur check"), aber in E vorkommt:

$$\frac{E \cup \{ x \equiv t \}}{E\left[\begin{smallmatrix} x \\ t \end{smallmatrix}\right] \cup \{ x \equiv t \}}$$

U3. Umordnung:

falls t keine Variable ist:

$$\frac{E \cup \{ t \equiv x \}}{E \cup \{ x \equiv t \}}$$

U4. Elimination trivialer Gleichungen:

$$\frac{E \cup \{ x \equiv x \}}{E}$$

Anwendungen der Umformungsregeln:

$\{ f(x, g(y,z), a) \equiv f(g(v,z), x, z) \}$

Dekomposition

$\{ x \equiv g(v,z),\ \underbrace{g(y,z) \equiv x,\ a \equiv z}_{E} \}$

Variablen-Elimination $[x / g(v,z)]$

$\{ x \equiv g(v,z),\ g(y,z) \equiv g(v,z),\ a \equiv z \}$

Dekomposition

$\{ x \equiv g(v,z),\ y \equiv v,\ (z \equiv z),\ a \equiv z \}$

Elimination einer trivialen Gleichung

$\{ \underbrace{x \equiv g(v,z),\ y \equiv v}_{E},\ a \equiv z \}$

Umordnung, Variablen-Elimination $[z / a]$

$\{ x \equiv g(v,a),\ y \equiv v,\ z \equiv a \}$

Lemma 2.9 [Unifikations-Invarianz der Umformungsregeln]

Sei E'' aus E' durch Anwendung von U1, U2, U3 oder U4 entstanden.

1. σ unifiziert E'' gdw σ unifiziert E'
2. σ ist mgu von E'' gdw σ ist mgu von E'

Beweis von 1.

ut. Dekomposition : $\dfrac{E \cup \{ f(t_1,..,t_n) \equiv f(t_1',...,t_n') \}}{E \cup \{ t_1 \equiv t_1' , \dots , t_n \equiv t_n' \}}$

<u>zeige:</u> $f(t_1,..,t_n)\,\sigma = f(t_1',...,t_n')\,\sigma$

↑ Gleichheit als Zeichenkette

gdw $t_i \sigma = t_i' \sigma$ für $i = 1,..,n$

<u>Beweis</u> durch Induktion über den Aufbau von Termen

ud. Variablen-Elimination : $\dfrac{E \cup \{x \equiv t\}}{E\left[\begin{smallmatrix} x \\ t \end{smallmatrix}\right] \cup \{x \equiv t\}}$

mit: x kommt nicht in t, aber in E vor

für $\tau := \left[\begin{smallmatrix} x \\ t \end{smallmatrix}\right]$ gilt :

i) τ ist mgu von $\{x, t\}$

ii) $\tau\tau = \tau$ denn x kommt nicht in t vor

iii) <u>falls</u> σ Unifikator von $F \cup \{x \equiv t\}$.

<u>dann</u> i) ex. ρ mit $\sigma = \tau\rho$

$= \tau\tau\rho = \tau\sigma$

speziell für Unifikator σ von $E \cup \{x \equiv t\}$ bzw. $E\left[\begin{smallmatrix} x \\ t \end{smallmatrix}\right] \cup \{x \equiv t\}$:

$$(E \cup \{x \equiv t\})\sigma = E\sigma \cup \{x \equiv t\}\sigma$$

$$= E\tau\sigma \cup \{x \equiv t\}\sigma$$

$$= E[x/t]\sigma \cup \{x \equiv t\}\sigma = (E[x/t] \cup \{x \equiv t\})\sigma$$

U3. Umordnung: $\dfrac{E \cup \{t \equiv x\}}{E \cup \{x \equiv t\}}$ mit t ist keine Variable

Beh. trivial!

U4 Elimination trivialer Gleichungen: $\dfrac{E \cup \{x \equiv x\}}{E}$

Beh. trivial!

<u>Beweis von 2:</u> folgt direkt aus 1.

Unifikationsalgorithmus

Eingabe: M: endliche Menge von Termen

Ausgabe: σ: Substitution [mgu von M]

bzw. Text "M nicht unifizierbar"

Methode:

[initialisiere: bestimme Start-Gleichungsmenge]

$E := \{ t \equiv t' \mid t \neq t', t \in M, t' \in M \}$;

[wende wiederholt Umformungsregeln von Martelli-Montanari an]

while eine Umformungsregel U_i anwendbar

do $E :=$ Anwendungsergebnis von U_i auf E **end**;

[teste Unifizierbarkeit]

if E hat Gestalt $\{x_1 \equiv t_1, \ldots, x_k \equiv t_k\}$, $k \geq 0$,

x_i paarweise verschieden,

x_i kommt in t_i nicht vor [und damit auch in keinem t_j, $i \neq j$]

[E vollständig gelöst]

then [unifizierbar mit mgu] $\sigma := \begin{bmatrix} x_1 & \cdots & x_k \\ t_1 & & t_k \end{bmatrix}$;

output (σ)

else [nicht unifizierbar] output ("M nicht unifizierbar")

end;

Bsp. zu unifizieren: $M = \{ f(\underset{g(v,a)}{x}, g(\underset{v}{y}, \underset{a}{z}), a),\ f(g(\underset{a}{v}, \underset{a}{z}), \underset{g(v,a)}{x}, \underset{a}{z}) \}$

Start-Gleichungsmenge: $E_0 = \{ f(x, g(y,z), a) \equiv f(g(v,z), x, z) \}$

Ergebnis-Gleichungsmenge ist vollständig gelöst:

linke Seiten: paarweise verschiedene Variablen, die in keiner rechten Seite vorkommen

mgu: $\begin{bmatrix} x & y & z \\ g(v,a) & v & a \end{bmatrix}$

Satz (2.11) Der Unifikationsalgorithmus bricht stets ab und

(2.12) ist korrekt:

Eingabe M ist unifizierbar gdw Algorithmus liefert Substitution σ; diese ist dann mgu von M.

Beweis des Abbruchs:

wir zeigen, daß eine Regelanwendung die Gleichungsmenge "echt vereinfacht" im folgenden Sinne: definiere

$$E \mapsto (k, m, n) \quad \text{mit}$$

$k := \| \text{var}(E) \setminus \{x \mid x \text{ kommt in } E \text{ nur einmal vor, und zwar in } x \equiv t \text{ oder } t \equiv x\} \|$

$m :=$ Summe der "Größen" aller linken und rechten Seiten in E
("Größen" = #(Knoten) in Baumdarstellung)

$n := \| \{t \equiv x \mid t \equiv x \in E,\ x \text{ Variable},\ t \text{ keine Variable}\} \|$

Dekomposition:	verringert	m	[das gemeinsame f verschwindet]
Variablen-Elimination:	verringert	k	[durch Ersetzen von x durch t]
Umordnung:	verringert	n	[entfernt $t \equiv x$]
Elimination trivialer Gl.:	verringert	m	[durch Wegfall einer Gleichung]

Beweis der Korrektheit:

1. Sei E vollständig gelöst:

Dann gilt: $x_i\sigma = t_i = t_i\sigma$

$x_i\sigma = t_i$: Def σ

$t_i = t_i\sigma$: σ läßt t_i unverändert, da $dom(\sigma) \cap var(t_i) = \emptyset$

also: σ Unifikator von E

sei dann ρ beliebiger Unifikator von E

wir zeigen: $\sigma\rho = \rho$ [d.h. $\sigma \leq \rho$; also: σ allgemeinster Unifikator]

Bew: Fall 1: $x \notin dom\,\sigma \Rightarrow x\sigma\rho = x\rho$ (Fallannahme)

Fall 2: $x \in dom\,\sigma$, etwa $x = x_i$

$\Rightarrow x_i\sigma\rho = t_i\rho = x_i\rho$ (Def σ; ρ ist Unifikator)

Lemma 2.9 [Invarianz]: σ ist auch mgu von M

2. Sei E nicht vollständig gelöst [und keine Regel anwendbar !$_0$]:

dann enthält E eine Gleichung, die nicht dem "Unifizierbarkeits-test" genügt:

Fall 1: eine Gleichung nicht von Form $x \equiv t$:

Fall 1.1: von Form $t \equiv x$ $\Rightarrow$ U3. Umordnung anwendbar $\Rightarrow$ #

Fall 1.2: von Form $f(t_1,\dots,t_n) \equiv f(t_1',\dots,t_n')$ $\Rightarrow$ U1. Dekomposition anwendbar

$\Rightarrow$ #

Fall 1.3: von Form $f(t_1,\dots,t_n) \equiv g(t_1',\dots,t_m')$ mit $f \neq g$

$\Rightarrow$ E nicht unifizierbar [Operationszeichen verschieden]

Fall 2: alle Gleichungen von Form $x \equiv t$, aber ein x_i kommt in t_i vor

$\Rightarrow \{x_i, t_i\}$ und damit E nicht unifizierbar

[$x_i \equiv \underbrace{f(\dots, x_i, \dots)}_{t_i}$ nicht lösbar in Σ^*]

Lemma 2.9 [Invarianz]: M nicht unifizierbar

(pure) Resolution

P, Q Atome : 1) zu unifizieren,

2) dann wegzuschneiden

A, C Konjunktionen von Atomen

B, D Disjunktionen von Atomen

$$\frac{A \to B \vee P \qquad Q \wedge C \to D}{\neg A \vee B \vee P \qquad \neg Q \vee \neg C \vee D}\ \text{Res}$$

zu unifizierendes Paar komplementärer Literale

$$(A \wedge C\pi \to B \vee D\pi)\,\sigma$$

$$(\neg A \vee B \vee (\neg C \vee D)\pi)\,\sigma$$

σ ← mgu von P und $Q\pi$

↑ Umbenennung für Variablendisjunktheit

mit 1. π ist Umbenennung (von $Q \wedge C \to D$),
so daß die Prämissen variablendisjunkt werden

2. σ ist mgu von P und $Q\pi$

Bsp:

$$\frac{\neg R(x,a) \vee \neg P(y) \vee R(g(x,a),y) \qquad \neg R(x,x) \vee Q(x)}{\neg R(z,z) \vee Q(z)}\ \pi = \begin{bmatrix} x & z \\ z & x \end{bmatrix}$$

$$\frac{}{\neg R(x,a) \vee \neg P(g(x,a)) \vee Q(g(x,a))}\ \text{Res mit mgu}$$

$$\sigma = \begin{bmatrix} z & y \\ g(x,a) & g(x,a) \end{bmatrix}$$

volle Resolution

$P_1, \dots, P_n, Q_1, \dots, Q_m$ Atome : 1) unifizieren
2) dann wegzuschneiden

A, C Konjunktionen von Atomen
B, D Disjunktionen von Atomen

$A \to B \vee P_1 \vee \dots \vee P_n \qquad Q_1 \wedge \dots \wedge Q_m \wedge C \to D$

zu unifizierendes Mengenpaar komplementärer Literale

$$\frac{\neg A \vee B \vee (P_1 \vee \dots \vee P_n) \vee (\neg Q_1 \vee \dots \vee \neg Q_m) \vee \neg C \vee D}{(A \wedge C\pi \to B \vee D\pi)\sigma} \text{ Rob}$$

$(\neg A \vee B \vee (\neg C \vee D)\pi)\sigma$ ← mgu für $P_i, Q_j\pi$

└ Umbenennung für Variablendisjunktheit

mit 1. π ist Umbenennung, so daß die Prämissen variablendisjunkt werden

2. σ ist mgu von $\{P_1, \dots, P_n, Q_1\pi, \dots, Q_m\pi\}$

Bsp:
$$\frac{P(x) \vee P(y) \qquad \neg P(u) \vee \neg P(v)}{\square} \text{ Rob mit}$$

mgu

$$\sigma = \begin{bmatrix} x & y & v \\ u & u & u \end{bmatrix}$$

Faktorisierung

$P_1, \ldots, P_n$ Atome : zu unifizieren

A Konjunktion von Atomen

B Disjunktion von Atomen

$$\frac{A \to B \vee P_1 \vee \ldots \vee P_n \qquad \neg A \vee B \vee P_1 \vee \ldots \vee P_n}{(A \to B \vee P_1)\sigma \qquad (\neg A \vee B \vee P_1)\sigma}\ \text{Fak}$$

mit σ mgu von $\{P_1, \ldots, P_n\}$

dann:
$(P_1 \vee \ldots \vee P_n)\sigma$
$\equiv P_1\sigma \vee \ldots \vee P_n\sigma$
äquivalent: $P_1\sigma$

entsprechend:

$$\frac{P_1 \wedge \ldots \wedge P_n \wedge A \to B \qquad \neg P_1 \vee \ldots \vee \neg P_n \vee \neg A \vee B}{(P_1 \wedge A \to B)\sigma \qquad (\neg P_1 \vee \neg A \vee B)\sigma}\ \text{Fak}$$

mit σ mgu von $\{P_1, \ldots, P_n\}$

Satz 2.20 [Korrektheit und Widerlegungsvollständigkeit der Resolution]

Die Regelsysteme Res + Fak

und Rob

sind korrekt und widerlegungsvollständig für Gentzenformeln.

Beweis: 1. [Korrektheit]

eine Anwendung von Rob

kann durch hintereinander ausgeführte Anwendungen von Fak und Res simuliert werden:

eine Anwendung von Fak

ist eine spezielle Anwendung von Subst;

eine Anwendung von Res

kann durch hintereinander ausgeführte Anwendungen von Subst und GS simuliert werden;

da Subst und GS korrekt sind,

sind also auch Res + Fak bzw. Rob korrekt!

2. [Widerlegungsvollständigkeit]

zu zeigen: X widersprüchlich $\Rightarrow X \vdash_{\{\text{Res+Fak}\atop\text{Rob}} \square$

wir wissen bereits: $X \vdash_{GS+Subst} \square$ $\Rightarrow$ noch zu zeigen!

allgemeinere Beh.:

falls $X \vdash_{GS+Subst} G$

dann ex. G' mit

1. G ist Instanz von G'
2. $X \vdash_{Res+Fak} G'$

d.h. eine Ableitung mit GS+Subst läßt sich in eine allgemeinere mit Res+Fak umwandeln.

verwenden mgu's!

Bew.:
- folgendes Lifting-Lemma beweist Beh.

  für einen wesentlichen Schritt: Schnitt mit vorangehender Substitution
- dann Induktion über die Schrittzahl

Beispiel:

i)

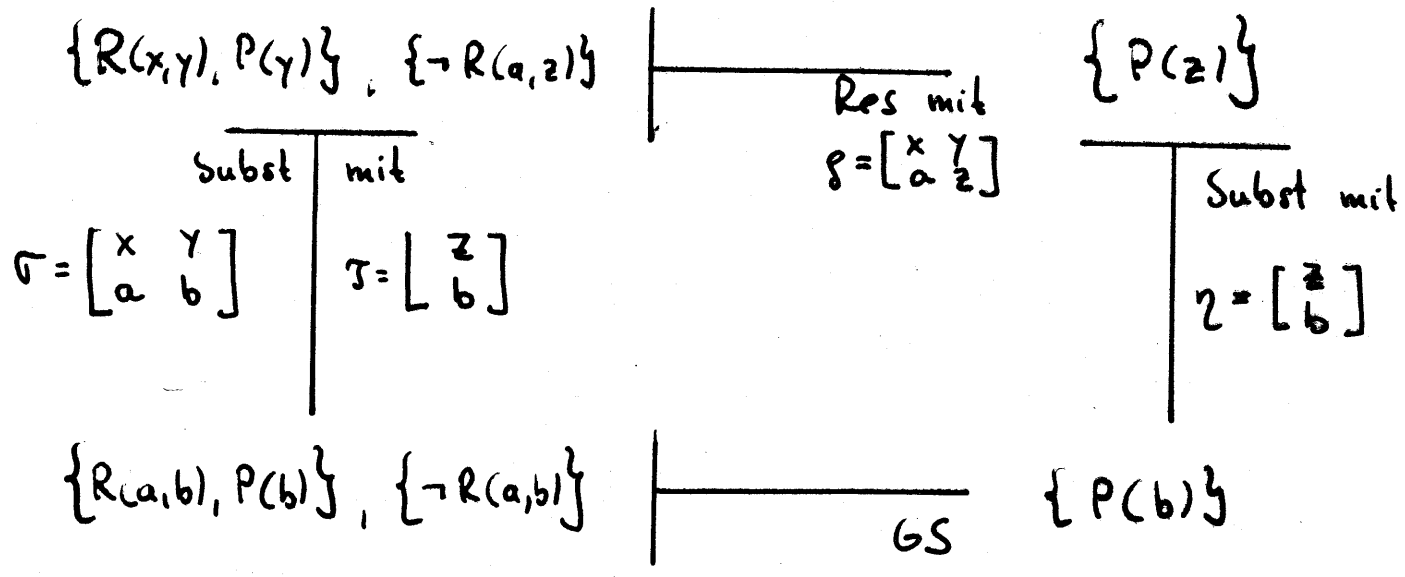
$$\dfrac{\dfrac{R(x,y),\ P(y)}{R(a,b),\ P(b)}\ \text{Subst mit } \sigma=\begin{bmatrix} x & y \\ a & b \end{bmatrix} \qquad \dfrac{\neg R(a,z)}{\neg R(a,b)}\ \text{Subst mit } \tau=\begin{bmatrix} z \\ b \end{bmatrix}}{P(b)}\ GS$$

ii)

$$\dfrac{R(x,y),\ P(y) \qquad \neg R(a,z)}{\underbrace{P(y)\,\varrho}_{P(z)}}\ \text{Res mit mgu } \varrho=\begin{bmatrix} x & y \\ a & z \end{bmatrix}$$

↳ gilt: $P(b)$ ist Instanz von $P(z)$

iii) folgendes Diagramm kommutiert:



Beispiel:

$\{\neg P(a), Q(y)\}$ $\{P(x), P(a)\}$

——— Subst mit $[\frac{x}{a}]$

——— Fak mit mgu $[\frac{x}{a}]$

$\{P(a)\}$

——— GS

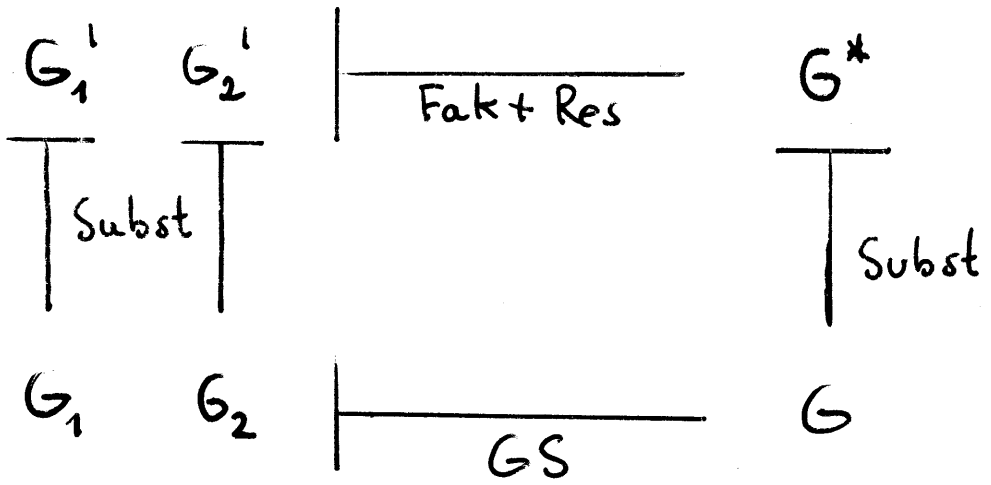
——— Res mit mgu $[\,]$

$Q(y)$

Lemma 2.21 [Lifting-Lemma]

Seien G_1' und G_2' Gentzenformeln mit Instanzen G_1 bzw. G_2, so daß der Schnitt $\dfrac{G_1 \quad G_2}{G}\,GS$ möglich ist.

Dann gibt es eine Gentzen-Formel G^*, die durch einen Resolutionsschritt aus Faktoren von G_1' bzw. G_2' entsteht, so daß G Instanz von G^* ist:



$\neg A, B, P(t_1), \ldots, P(t_n)$ $\qquad$ $\neg P(s_1), \ldots, \neg P(s_m), \neg C, D$

$\neg A\sigma^*, B\sigma^*, P(t_1)\sigma^*$ Fak mit mgu σ^* von t_i $\qquad$ $\neg P(s_1)\tau^*, \neg C\tau^*, D\tau^*$ Fak mit mgu τ^* von s_j

o.B.d.A variablendisjunkt

$\neg A\sigma, B\sigma,$ (P(t_1)σ) Subst mit $\sigma = \sigma^*\sigma_1$ unifiziert t_i $\qquad$ (¬P(s_1)τ), ¬Cτ, Dτ Subst mit $\tau = \tau^*\tau_1$ unifiziert s_j

komplementär, d.h. $t_1\sigma = s_1\tau$

Res mit mgu Θ:

$\neg A\sigma^*\Theta, B\sigma^*\Theta, \neg C\tau^*\Theta, D\tau^*\Theta$

$t_1\sigma^*, s_1\tau^*$ unifizierbar vermöge $\sigma_1 \cup \tau_1$, d.h. $\sigma_1 \cup \tau_1 = \Theta\Theta'$

Subst mit Θ'

$\neg A\sigma^*\Theta\Theta', B\sigma^*\Theta\Theta', \neg C\tau^*\Theta\Theta', D\tau^*\Theta\Theta'$

$\neg A\underbrace{\sigma^*\sigma_1}_{\sigma}, B\underbrace{\sigma^*\sigma_1}_{\sigma}, \neg C\underbrace{\tau^*\tau_1}_{\tau}, D\underbrace{\tau^*\tau_1}_{\tau}$

GS

$\neg A\sigma, B\sigma, \neg C\tau, D\tau$

Traum vom maschinellen Beweisen

⋮

Formalisierung der Behauptung : $X \models G$

logische Umformungen : Y widersprüchlich

Resolution korrekt und widerlegungsvollständig : $Y \vdash_{Rob} \square$

Algorithmisierung mit Resolution

[Initialisierung]

$\overline{Y} := Y$;

[teste auf Widersprüchlichkeit]

while $\square \notin \overline{Y}$

do [wende Resolution an]

select $G, H \in \overline{Y}$;

if Resolution anwendbar [Mengenpaar komplementärer Literale unifizierbar]

then $\overline{Y} := \overline{Y} \cup \{\text{Resolvente}(G, H)\}$

end

end ;

output ("Y widersprüchlich") ;

Problem 1: Auswahl im Suchraum einschränken!

Problem 2: Suchraum klein halten!

zu Problem 2: Suchraum klein halten!

Frage: welche Klauseln braucht man in den Suchraum nicht einzufügen, weil ein Beweis der Unerfüllbarkeit stets auch ohne sie möglich ist?

Versuch einer Antwort:

- Tautologien:
  eine Klausel C ist Tautologie : gdw
  sie ein komplementäres Literalpaar enthält,
  d.h. $C = \{ \ldots, L, \ldots, \neg L, \ldots \}$

- subsumierte Klauseln:
  eine Klausel C subsumiert eine Klausel D : gdw
  es gibt eine Substitution σ mit $C\sigma \subset D$.

Lemma 3.19

1. Wenn C subsumiert D,
   dann $C \models D$.

2. Die Umkehrung von 1. gilt im allgemeinen nicht.

3. Sind C und D variablenfrei, so gilt:
   C subsumiert D genau dann, wenn $C \models D$.

Beweis:

1. Sei σ eine Substitution mit $C\sigma \subset D$,
   und sei $\mathcal{M}$ ein Modell von C.
   zu zeigen: $\mathcal{M}$ ist auch Modell von D
   Bew.: $\mathcal{M}$ Modell von C
   dann: $\mathcal{M}$ Modell von $C\sigma$ — C implizit allquantifiziert
   dann: $\mathcal{M}$ Modell von D — $C\sigma \subset D$;
   Klauseln sind Disjunktionen

2. Gegenbeispiel: $C \equiv \{\neg P(x), P(f(x))\}$
   $D \equiv \{\neg P(x), P(f(f(x)))\}$

3. es gilt dann: C subsumiert D gdw $C \subset D$ gdw $C \vdash D$

Definition:

1. Klausel C subsumiert Klausel D :gdw
es gibt eine Substitution σ mit $C\sigma \subset D$.

2. Klauselmenge X subsumiert Klauselmenge Y :gdw
für alle $D \in Y$ gibt es $C \in X$ mit:
C subsumiert D.

einige Aussagen ohne Beweis:

Lemma 3.26 Wenn $Y \vdash_{\text{Res+Fak}} D$ und

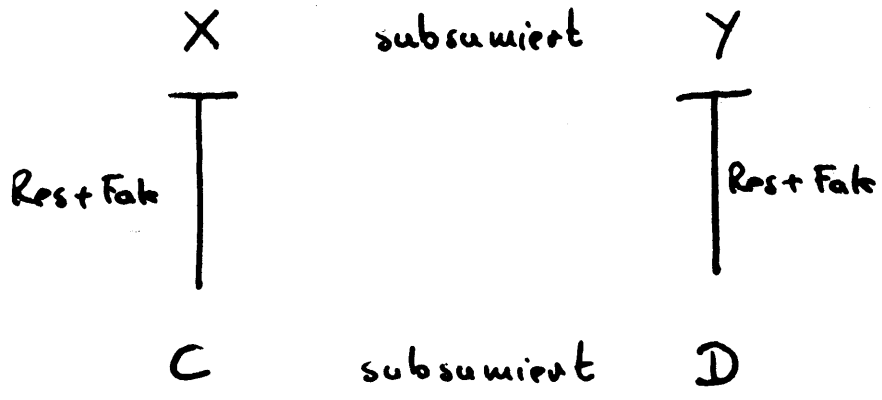
X subsumiert Y,

dann gibt es C mit:

$X \vdash_{\text{Res+Fak}} C$,

C subsumiert D.

also:



Korollar 3.27 Wenn $Y \vdash_{\text{Res+Fak}} \square$ und

X subsumiert Y,

dann $X \vdash_{\text{Res+Fak}} \square$.

Lemma 3.28 Wenn $Y \vdash_{\text{Res+Fak}} D$,

dann gibt es eine Klausel C mit

- C subsumiert D
- $Y \vdash_{\text{Res+Fak}} C$ vermöge einer Ableitung, in der keine Tautologie vorkommt

Korollar 3.29 Wenn $Y \vdash_{\text{Res+Fak}} \square$,

dann gibt es dafür eine Ableitung, in der keine Tautologie vorkommt.

ein (aussagenlogisches) Beispiel:

Aufgabe: • teste Y mit Klauseln

$$\{P, Q\}, \quad (1)$$

$$\{\neg P, Q\}, \quad (2)$$

$$\{P, \neg Q\}, \quad (3)$$

$$\{\neg P, \neg Q\} \quad (4)$$

auf Widersprüchlichkeit !

- verwende dabei die

  " Level-Saturation-Strategie ",

  d.h. eine "Breitensuche":

  - unterhalte Liste aller erzeugten Klauseln
  - Auswahl stufenweise
  - Tautologien und subsumierte Klauseln werden <u>nicht</u> angefügt !

(1) P, Q

(2) $\neg P, Q$

(3) $P, \neg Q$

(4) $\neg P, \neg Q$

(5) Q 1,2

(6) P 1,3

~~(7)~~ $Q, \neg Q$ 1,4 — Tautologie

~~(8)~~ $P, \neg P$ 1,4 — Tautologie

~~(9)~~ $Q, \neg Q$ 2,3 — Tautologie

~~(10)~~ $P, \neg P$ 2,3 — Tautologie

(11) $\neg P$ 2,4

(12) $\neg Q$ 3,4

~~(13)~~ P, Q ~~1,7~~

~~(14)~~ P, Q ~~1,8~~

~~(15)~~ P, Q ~~1,9~~

~~(16)~~ P, Q ~~1,10~~

~~(17)~~ Q 1,11 — subsumiert durch 5

~~(18)~~ P 1,12 — subsumiert durch 6

~~(19)~~ Q 2,6 — subsumiert durch 5

~~(20)~~ $\neg P, Q$ ~~2,7~~

~~(21)~~ $\neg P, Q$ ~~2,8~~

~~(22)~~ $\neg P, Q$ ~~2,9~~

~~(23)~~ $\neg P, Q$ ~~2,10~~

~~(24)~~ $\neg P$ 2,12 — subsumiert durch 11

~~(25)~~ P 3,5 — subsumiert durch 6

~~(26)~~ $P, \neg Q$ ~~3,7~~

~~(27)~~ $P, \neg Q$ ~~3,8~~

~~(28)~~ $P, \neg Q$ ~~3,9~~

~~(29)~~	$P, \neg Q$	3, ~~10~~		
~~(30)~~	$\neg Q$	3, 11	——	subsumiert durch 12
~~(31)~~	$\neg P$	4, 5	——	subsumiert durch 11
~~(32)~~	$\neg Q$	4, 6	——	subsumiert durch 12
~~(33)~~	$\neg P, \neg Q$	4, ~~7~~		
~~(34)~~	$\neg P, \neg Q$	4, ~~8~~		
~~(35)~~	$\neg P, \neg Q$	4, ~~9~~		
~~(36)~~	$\neg P, \neg Q$	4, ~~10~~		
~~(37)~~	Q	5, ~~7~~		
~~(38)~~	Q	5, ~~8~~		
(39)	$\square$	5, 12		

Syntax: $\Sigma = (S, F, P)$ (Sorten, Funktionszeichen, Prädikatenzeichen)

↳ kann insbesondere Gleichheitszeichen $\equiv_s$ für $s \in S$ enthalten

Semantik: $\mathcal{M} = (\mathcal{D}, \mathcal{F}, \mathcal{P})$

mit Interpretation I

soll dann jeweils das Gleichheitszeichen $\equiv_s$ durch die Identität auf $\mathcal{D}_s \in \mathcal{D}$ interpretieren

(wird aber durch den Begriff der Struktur nicht verlangt!)

Definition: Sei $\Sigma = (S, F, P)$ mit $\equiv_s$ aus P für $s \in S$.

$\mathcal{M} = (\mathcal{D}, \mathcal{F}, \mathcal{P})$ mit Interpretation I heißt

Gleichheitsstruktur : gdw

$I(\equiv_s) = \underbrace{\{(m,m) \mid m \in \mathcal{D}_s\}}_{\text{Identität auf } \mathcal{D}_s}$ für alle $s \in S$.

$\mathcal{M}$ ist Modell von G : gdw $\text{Wert}_{\mathcal{M}}(\forall G) = W$

G ist erfüllbar : gdw es gibt ein Modell von G

$\mathcal{M}$ ist ein <u>Gleichheitsmodell</u> von G : gdw

1. $\mathcal{M}$ ist Gleichheitsstruktur
2. $\mathcal{M}$ ist Modell von G

G ist <u>gleichheitserfüllbar</u> : gdw es gibt ein Gleichheitsmodell von G

<u>Bem. 1:</u> gleichheitserfüllbar $\Rightarrow$ erfüllbar

<u>Bem. 2:</u> erfüllbar $\not\Rightarrow$ gleichheitserfüllbar

Bsp: $X = \{ a \equiv b , P(a) , \neg P(b) \}$

ist erfüllbar, aber

<u>nicht</u> gleichheitserfüllbar!

gesucht:

Formelmenge GAX (Gleichheitsaxiome),
so daß für alle Mengen X von Gentzenformeln:

X gleichheitserfüllbar gdw $X \cup GAX$ erfüllbar

d.h. X hat kein Gleichheitsmodell gdw $X \cup GAX$ widersprüchlich
gdw $X \cup GAX \vdash_{Rob} \square$

gefunden:

GAX bestehe aus den folgenden Formeln
(über Signatur Σ), wobei x, y, z, x_i Variablen seien:

1. Reflexivität $x \equiv x$
2. Symmetrie $x \equiv y \rightarrow y \equiv x$
3. Transitivität $x \equiv y \wedge y \equiv z \rightarrow x \equiv z$
4. Kongruenz für Operationssymbole $x_i \equiv y \rightarrow f(x_1, \ldots, x_i, \ldots, x_n) \equiv f(x_1, \ldots, y, \ldots, x_n)$
5. Kongruenz für Prädikatensymbole $x_i \equiv y \wedge P(x_1, \ldots, x_i, \ldots, x_n) \rightarrow P(x_1, \ldots, y, \ldots, x_n)$

Satz 5.3 [Existenz von Gleichheitsmodellen]

Sei $\mathcal{M} = (\mathcal{D}, \mathcal{F}, \mathcal{P})$ ein Modell von GAX, und G die Menge der in $\mathcal{M}$ geltenden Formeln.

Dann gibt es eine Gleichheitsstruktur $\overline{\mathcal{M}} = (\overline{\mathcal{D}}, \overline{\mathcal{F}}, \overline{\mathcal{P}})$, die Modell von G ist
(und damit auch von GAX ist)

Beweis:

Sei $\equiv_s$ in $\mathcal{M}$ interpretiert durch $\approx_s$
(Syntax) (Semantik)

Die $\approx_s$ sind Kongruenzen bezüglich der Interpretation aus $\mathcal{F}$ und $\mathcal{P}$, weil in $\mathcal{M}$ GAX gilt.

Sei $\overline{\mathcal{M}} = (\overline{\mathcal{D}}, \overline{\mathcal{F}}, \overline{\mathcal{P}})$ die zugehörige Faktor-Struktur:
(siehe Diskrete Strukturen)

$$\overline{D}_s := \{ [d]_{\approx_s} \mid d \in D_s \}$$

$[d]_{\approx_s}$: Äquivalenzklasse von d

$$\overline{I}(f)([d_1], \ldots, [d_n]) := [I(f)(d_1, \ldots, d_n)]$$

$$([d_1], \ldots, [d_n]) \in \overline{I}(P) : \text{gdw } (d_1, \ldots, d_n) \in I(P)$$

zu zeigen:

1. $\overline{\mathfrak{M}}$ ist wohldefiniert

2. $\overline{\mathfrak{M}}$ ist Modell von G

zu 1.: Standardtechnik der Algebra

zu 2.: $\overline{\mathfrak{M}}$ identifiziert gerade die in $\mathfrak{M}$ ununterscheidbaren Elemente;

$\overline{\mathfrak{M}}$ ist daher Modell von G

(genauer Beweis durch Induktion über den Aufbau von Formeln)

Korollar 5.4

X gleichheitserfüllbar gdw $X \cup GAX$ erfüllbar

Beweis: "$\Rightarrow$": X gleichheitserfüllbar

dann: ex. Gleichheitsstruktur $\mathfrak{M}$: $\mathfrak{M}$ ist Modell von X
Def. gleichheitserfüllbar

dann: $\mathfrak{M}$ ist Modell von $X \cup GAX$
die Identität macht GAX wahr

dann: $X \cup GAX$ erfüllbar
Def. erfüllbar

"$\Leftarrow$": $X \cup GAX$ erfüllbar

dann: ex. Struktur $\mathfrak{M}$: $\mathfrak{M}$ ist Modell von $X \cup GAX$
Def. erfüllbar

dann: ex. Gleichheitsstruktur $\overline{\mathfrak{M}}$: $\overline{\mathfrak{M}}$ ist Modell von X
Satz 5.3

dann: X gleichheitserfüllbar
Def. gleichheitserfüllbar

Aufbau von Ableitungen:

man darf verwenden:

- vorgegebene Formeln: Axiome, Voraussetzungen
- Ableitungsregeln
- schon (früher) abgeleitete Formeln

Gleichheitsaxiome und Resolutionsregel sind nicht gut aufeinander abgestimmt:

- Resolution auf Formeln von GAX unanwendbar
  (bringt "meistens" nichts, da GAX erfüllbar ist, wir aber einen Widerspruch erzeugen wollen)

  Bsp:

$$\frac{X \equiv X \qquad \neg X \equiv Y \vee Y \equiv X \qquad \neg Z \equiv Y \vee Y \equiv Z}{X \equiv X} \text{ Rob mit } \begin{bmatrix} Z & Y \\ X & X \end{bmatrix}$$

  ← "wußten wir schon vorher"

- Ersetzen von Gleichem durch Gleiches mit Resolution umständlich

Beispiel: aus der Formel

$$P(f(g(a), g(g(y)), f(a,y,z))) \qquad V1$$

kann man mit der Gleichheit

$$g(a) \equiv g(g(a)), \qquad V2$$

wenn man speziell $y = a$ wählt, (Variablen sind stets allquantifiziert gedacht)

ableiten

$$P(f(g(a), g(g(g(a))), f(a,a,z)))$$

V2: $\boxed{g(a) \equiv g(g(a))}$ GAX4: $\neg x_1 \equiv y \vee g(x_1) \equiv g(y)$

$\begin{bmatrix} x_1 & y \\ g(a) & g(g(a)) \end{bmatrix}$

$g(g(a)) \equiv g(g(g(a)))$ GAX4: $\neg x_2 \equiv y \vee f(x_1, x_2, x_3) \equiv f(x_1, y, x_3)$

$\begin{bmatrix} x_2 & y \\ g(g(a)) & g(g(g(a))) \end{bmatrix}$

$f(x_1, g(g(a)), x_3) \equiv f(x_1, g(g(g(a))), x_3)$

GAX5: $\neg \overline{x_1} \equiv y \vee \neg P(\overline{x_1}) \vee P(y)$

$\begin{bmatrix} \overline{x_1} & y \\ f(x_1, g(g(a)), x_3) & f(x_1, g(g(g(a))), x_3) \end{bmatrix}$

$\neg P(f(x_1, g(g(a)), x_3)) \vee P(f(x_1, g(g(g(a))), x_3))$

V1: $\boxed{P(f(g(a), g(g(y)), f(a, y, z)))}$

$\begin{bmatrix} x_1 & \boxed{y} & x_3 \\ g(a) & \boxed{a} & f(a, a, z) \end{bmatrix}$

$P(f(g(a), g(g(g(a))), f(a, a, z)))$

Unifizierbarkeits-Test:

$$f(x_1, g(g(a)), x_3) \equiv f(g(a), g(g(y)), f(a,y,z))$$

Dekomposition

$$x_1 \equiv g(a) \qquad \frac{g(g(a)) \equiv g(g(y))}{\text{Dekomposition}} \qquad x_3 \equiv f(a,y,z)$$

$$\frac{g(a) \equiv g(y)}{\text{Dekomposition}}$$

$$\frac{a \equiv y}{\text{Umordnung}}$$

$$y \equiv a$$

Variable-Elimination

$$x_1 \equiv g(a) \qquad y \equiv a \qquad x_3 \equiv f(a,a,z)$$

Paramodulation von $l \approx r$ in P:

P Atom mit einer Stelle u

$l \approx r$ Gleichheitsatom

A, C Konjunktionen von Atomen
B, D Disjunktionen von Atomen

$$\frac{A \to B \vee P \qquad C \to D \vee l \approx r \qquad \neg A \vee B \vee P \qquad \neg C \vee D \vee l \approx r}{(A \wedge C\pi \to B \vee P[u \leftarrow r\pi] \vee D\pi)\sigma \qquad (\neg A \vee B \vee (\neg C \vee D)\pi \vee P[u \leftarrow r\pi])\sigma}\ \text{Para}$$

mit 1. π ist Umbenennung von $(C \to D \vee l \approx r)$, so daß die Prämissen <u>variablendisjunkt</u> werden

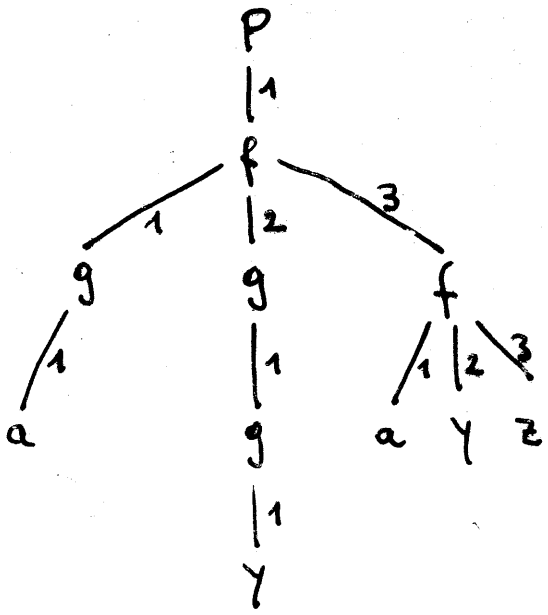
2. σ ist mgu vom Teilterm von P an der Stelle u, P/u, und $l\pi$

entsprechend:

$$\frac{A \wedge P \to B \qquad C \to D \vee l \approx r \qquad \neg A \vee \neg P \vee B \qquad \neg C \vee D \vee l \approx r}{(A \wedge P[u \leftarrow r\pi] \wedge C\pi \to B \vee D\pi)\sigma \qquad (\neg A \vee B \vee (\neg C \vee D)\pi \vee \neg P[u \leftarrow r\pi])\sigma}\ \text{Para}$$

Beispiel:

$P(f(g(a), g(g(y)), f(a,y,z)))$ mit Stelle 1.2.1.λ



$P/1.2.1.\lambda = g(y)$

$g(a) \equiv g(g(a))$

$(A, B, C, D$ seien alle leer!)

$P/1.2.1.\lambda$

$P(f(g(a), g(\boxed{g(y)}), f(a,y,z)))$ | $g(a) \equiv g(g(a))$

$\left(P(f(g(a), g(\underbrace{g(g(a))}_{\tau}), f(a,y,z))\right)\sigma$

Para mit mgu von $g(y)$ und $g(a)$:

$\sigma = \left[\begin{smallmatrix} y \\ a \end{smallmatrix}\right]$

$P(f(g(a), g(g(g(a))), f(a,a,z)))$

Beispiel [für eine Ableitung mit Resolution und Paramodulation]

Voraussetzungen (über natürliche Zahlen):

(1) $\text{Gerade}(x) \vee \text{Ungerade}(x)$,

(2) $\text{Gerade}(x) \wedge \text{Ungerade}(y) \rightarrow \text{Ungerade}(x+y)$

(3) $\text{Ungerade}(x) \wedge \text{Gerade}(y) \rightarrow \text{Ungerade}(x+y)$

(4) $(x+y)+z \equiv x+(y+z)$

(5) $2*x \equiv x+x$

(6) $\text{Gerade}(x) \rightarrow \text{Ungerade}(x+1)$

(7) $\text{Ungerade}(x) \rightarrow \text{Gerade}(x+1)$

Behauptung: $\forall x\ \text{Ungerade}((2*x)+1)$

negiert: $\exists x \neg\ \text{Ungerade}((2*x)+1)$

skolemisiert: $\neg\ \text{Ungerade}((2*c)+1)$

als Gentzenformel:

(8) $\text{Ungerade}((2*c)+1) \rightarrow F$

also gesucht: Widerlegung von (1),...,(8)

8: $\neg Ung((2*c)+1)$ 5: $2*x \equiv x+x$

Para mit mgu $\sigma_1 = \begin{bmatrix} x \\ c \end{bmatrix}$ von $2*c$ und $2*x$

$\{\neg Ung((x+x)+1)\}\sigma_1$

$\neg Ung((c+c)+1)$ 4: $(x+y)+z \equiv x+(y+z)$

Para mit mgu $\sigma_2 = \begin{bmatrix} x & y & z \\ c & c & 1 \end{bmatrix}$ von $(c+c)+1$ und $(x+y)+z$

$\{\neg Ung(x+(y+z))\}\sigma_2$

$\neg Ung(c+(c+1))$ 2: $\neg Ger(x) \vee \neg Ung(y) \vee Ung(x+y)$

Res mit mgu $\sigma_3 = \begin{bmatrix} x & y \\ c & c+1 \end{bmatrix}$ von $c+(c+1)$ und $x+y$

$\neg Ger(c) \vee \neg Ung(c+1)$ 6: $\neg Ger(x) \vee Ung(x+1)$

Res mit mgu $\sigma_4 = \begin{bmatrix} x \\ c \end{bmatrix}$ von $c+1$ und $x+1$

(12) $\boxed{\neg Ger(c)}$

$\neg Ung(c+(c+1))$ 3: $\neg Ung(x) \vee \neg Ger(y) \vee Ung(x+y)$

Res mit mgu $\sigma_5 = \begin{bmatrix} x & y \\ c & c+y \end{bmatrix}$ von $c+(c+1)$ und $x+y$

$\neg Ung(c) \vee \neg Ger(c+1)$ 7: $\neg Ung(x) \vee Ger(x+1)$

Res mit mgu $\sigma_6 = \begin{bmatrix} x \\ c \end{bmatrix}$ von $c+1$ und $x+1$

(13) $\boxed{\neg Ung(c)}$

$$\frac{13: \neg \mathrm{Ung}(c) \qquad 1: \mathrm{Ger}(x) \vee \mathrm{Ung}(x)}{} \text{ Res mit mgu } \sigma_7 = \begin{bmatrix} x \\ c \end{bmatrix} \text{ von } c \text{ und } x$$

$$\frac{\mathrm{Ger}(c) \qquad 12: \neg \mathrm{Ger}(c)}{} \text{ Res mit mgu } \sigma_8 = [\,]$$

□

Menge von Gentzenformeln : X

(positive) Resolution : $\dfrac{\neg A \vee B \vee P \qquad \neg Q \vee \neg C \vee D}{(\neg A \vee B \vee \neg C \vee D)\sigma}$

(positive) reicht aus für Widerlegungsvollständigkeit

↑ negativer Teil darf immer fehlen!

Res mit mgu σ von P, Q; Prämissen variablen = disjunkt

Faktorisierung : $\dfrac{\neg A \vee B \vee (\neg) P(t_1) \vee \ldots \vee (\neg) P(t_n)}{(\neg A \vee B \vee (\neg) P(t_1))\sigma}$

Fak mit mgu σ von $t_1, \ldots, t_n$

GAX 1. Reflexivität: $x \equiv x$

GAX 4. Kongruenz: $\neg x_i \equiv y \vee f(\ldots, x_i, \ldots) \equiv f(\ldots, y, \ldots)$

GAX 5. Kongruenz: $\neg x_i \equiv y \vee \neg P(\ldots, x_i, \ldots) \vee P(\ldots, y, \ldots)$

GAX 2, GAX 3 sind redundant (wenn man GAX 5 auch für $\equiv$ hat)

REF 1. (GAX 1) Reflexivität: $x \equiv x$

REF 2. Funktionale Reflexivität: $f(x_1, \ldots, x_n) \equiv f(x_1, \ldots, x_n)$

REF 2 ist für Widerlegungen nicht unbedingt notwendig

Paramodulation : $\dfrac{\neg A \vee B \vee (\neg) P \qquad \neg C \vee D \vee l \equiv r}{(\neg A \vee B \vee \neg C \vee D \vee (\neg) P(u \leftarrow r))\sigma}$

Para mit mgu σ von l und P/u, Prämissen variablendisjunkt

zu zeigen:

$X \cup GAX \vdash_{\text{Res + Fak}} \square$ gdw $X \cup REF \vdash_{\text{Res + Fak + Para}} \square$

positive Resolution, d.h.

$$\frac{B \vee P \qquad \neg Q \vee \neg C \vee D}{(B \vee (\neg C \vee D)\pi)\sigma}$$

mit 1. π ist Umbenennung, so daß die Prämissen variablendisjunkt werden

2. σ ist mgu von P und $Q\pi$

reicht aus für Widerlegungsvollständigkeit:

- Resolution faßt zusammen: Schnittregel
  Substitution
- Schnittregel ist widerlegungsvollständig für variablenfreie Gentzenformeln
- Beweis hiervon beruht auf Konsistenzlemma:

$$\left.\begin{array}{l} X \cup \{P\} \vdash_{GS} \square \\ X \cup \{\neg P\} \vdash_{GS} \square \end{array}\right\} \Rightarrow \quad X \vdash_{GS} \square$$

falls hier nur positiver Schnitt benutzt, dann auch hier nur positiver Schnitt benötigt

Lemma 5.13a

falls $X \cup GAX \vdash_{Res+Fak} \square$

dann $X \cup REF \vdash_{Res+Fak+Para} \square$.

Beweis: Sei gegeben eine Widerlegung von $X \cup GAX$ mit Resolution und Faktorisierung derart, daß

1. nur positive Resolution benutzt wird
   reicht für Widerlegungsvollständigkeit
2. nur GAX 1, 4, 5 vorkommen
   GAX 2, 3 sind redundant
3. die Prämissen für Regelanwendungen jeweils schon variablendisjunkt sind
   jeweils durch geeignete Umbenennungen erreichbar
4. die Widerlegung "subsumptionsfrei" ist
   ex. σ mit $C\sigma \subset D$ und $|C| \leq |D|$, dann kann D entfernt werden
5. die Widerlegung "geordnet" ist
   durch geeignete Umordnungen der Beweisschritte

zu konstruieren: Widerlegung von $X \cup REF$ mit Resolution, Faktorisierung und Paramodulation

Konstruktion: simuliere jeden einzelnen Schritt der gegebenen Ableitung;

(zeige: Konklusion in Simulation jeweils gleich der Konklusion in gegebener Ableitung)

Fallunterscheidung nach

- Art der Regel (1. Fak, 2. Res)
- Art der Prämissen (X-Formel, abgeleitete Formel, GAX-Formel)

Fall 1.1 Faktorisierung mit X-Formel oder abgeleiteter Formel:

auch für Simulation erlaubt!

Fall 1.2 Faktorisierung mit einer GAX-Formel G:

dann: G ist von Form GAX5, wobei P das Gleichheitssymbol ist

also: G hat Form: $\neg x_i \equiv y \vee \neg x_i \equiv z \vee y \equiv z$

also: Faktor hat Form: $\neg x_i \equiv w \vee w \equiv w$

also: Faktor wird subsumiert durch GAX1: $x \equiv x$

also: noch einleitender Voraussetzung kommt der Schritt gar nicht vor

Fall 2.1 Resolution mit X- oder abgeleiteter Formel und X- oder abgeleiteter Formel:

auch für Simulation erlaubt!

Fall 2.2 Resolution mit GAX1-Formel und X- oder abgeleiteter Formel:

auch für Simulation erlaubt, da GAX1 gleich REF1!

Fall 2.3 Resolution mit GAX4-Formel und GAX1- oder X oder abgeleiteter Formel:
(GAX4-, GAX5-Formeln sind nicht möglich!)

dann liegt folgende Situation vor:

$$\frac{B \vee l \equiv r \qquad GAX4: \neg x_i \equiv y \vee f(\ldots, x_i, \ldots) \equiv f(\ldots, y, \ldots)}{B \vee f(\ldots, l, \ldots) \equiv f(\ldots, r, \ldots)}\ \text{Res mit mgu } \sigma$$

↑ nicht positiv:
also: andere Prämisse positiv
also: wegzuschneidendes Literal ist $\neg x_i \equiv y$
also: $\sigma = \begin{bmatrix} x_i & y \\ l & r \end{bmatrix}$ ist mgu von $l \equiv r$ und $x_i \equiv y$

Simulation mit Paramodulation und REF2:

$$\frac{\text{REF2: } f(\ldots, x_i, \ldots) \equiv f(\ldots \textcircled{x_i} \ldots) \qquad B \vee l \equiv r}{\{B \vee f(\ldots, x_i, \ldots) \equiv f(\ldots, r, \ldots)\}\sigma_4}\ \text{Para mit mgu } \sigma = \begin{bmatrix} x_i \\ l \end{bmatrix} \text{ von } x_i \text{ und } l \text{ an Stelle } \textcircled{\ }$$

$B \vee f(\ldots, l, \ldots) \equiv f(\ldots, r, \ldots)$

Fall 2.4 Resolution mit GAX5-Formel und GAX1- oder X- oder abgeleiteter Formel:

(GAX4; GAX5-Formeln sind nicht möglich)

dann liegt eine der folgenden Situationen vor:

(a) [$\neg x_i \equiv y$ wird zuerst geschnitten]

$B_1 \vee l \equiv r$ GAX5: $\neg x_i \equiv y \vee \neg P(\ldots, x_i, \ldots) \vee P(\ldots, y, \ldots)$

↑ nicht positiv

also: andere Prämisse positiv

also: wegzuschneidendes Literal ist negativ (gemäß (a): $\neg x_i \equiv y$)

Res mit mgu $\sigma_1 \equiv \begin{bmatrix} x_i & y \\ t & r \end{bmatrix}$

$B_2 \vee P(t_1, \ldots, t_i, \ldots, t_n)$ $\underbrace{\neg P(\ldots, l, \ldots)}$ $\vee P(\ldots, r, \ldots) \vee B_1$

"geordnete" Widerlegung: sofort wegschneiden!

Res mit mgu σ_2 von $P(t_1, \ldots, t_i, \ldots, t_n)$ und $P(\ldots, l, \ldots)$

$\underbrace{\{P(\ldots, r, \ldots) \vee B_1 \vee B_2\}\sigma_2}$

$\{P(t_1, \ldots, r, \ldots, t_n) \vee B_1 \vee B_2\}\sigma_2^*$

mit σ_2^* mgu von t_i und l, entsteht durch Weglassen der Variablen $x_1, \ldots, x_n$, die nicht in B_1, B_2, t_i, r, l vorkommen

Simulation mit Paramodulation:

$$\frac{B_2 \vee P(t_1, \ldots, \textcircled{t_i}, \ldots, t_n) \qquad B_1 \vee l \equiv r}{\{P(t_1, \ldots, r, \ldots, t_n) \vee B_1 \vee B_2\}\sigma_2^*}$$

Para mit mgu σ_2^* von t_i und l, an der Stelle ○

(b) [$\neg P(\ldots, x_i, \ldots)$ wird zuerst geschnitten]

$$\frac{B_2 \vee P(t_1, \ldots, t_i, \ldots, t_n) \qquad \text{GAX5: } \neg x_i \equiv y \vee \neg P(\ldots, x_i, \ldots) \vee P(\ldots, y, \ldots)}{\text{Res mit mgu } \sigma_1 = \begin{bmatrix} x_1 \ldots x_i \ldots x_n \\ t_1 \ldots t_i \ldots t_n \end{bmatrix}}$$

$$\frac{B_1 \vee l \equiv r \qquad \neg t_i \equiv y \vee P(t_1, \ldots, y, \ldots, t_n) \vee B_2}{\text{Res mit mgu } \sigma_2 = \begin{bmatrix} y \\ r \end{bmatrix} \cdots}$$

$$\underbrace{\{P(t_1, \ldots, r, \ldots, t_n) \vee B_1 \vee B_2\}\sigma_2}$$

$$\{P(t_1, \ldots, r, \ldots, t_n) \vee B_1 \vee B_2\}\sigma_2^* \quad \text{mit } \sigma_2^* \text{ mgu von } t_i \text{ und } l$$

Simulation mit Paramodulation:

siehe oben!

Lemma 5.13 b

falls $X \cup REF \vdash_{Res+Fak+Para} \square$

dann $X \cup GAX \vdash_{Res+Fak} \square$

Beweis:

man kann zeigen: Res+Fak+Para mit REF ist gleichheitskorrekt

[d.h. falls $X \cup REF \vdash_{Res+Fak+Para} C$

dann ist jedes Gleichheitsmodell von X auch Modell von C]

dann gilt:

falls: $X \cup REF \vdash_{Res+Fak+Para} \square$

dann: X hat kein Gleichheitsmodell
(siehe oben)

dann: $X \cup GAX$ widersprüchlich
(Korollar 5.4)

dann: $X \cup GAX \vdash_{Res+Fak} \square$
(Resolution widerlegungsvollständig)

Beispiel:

Voraussetzungen (über Gruppen)

(1) $x \circ (y \circ z) \equiv (x \circ y) \circ z$, assoziativ

(2) $e \circ x \equiv x$ e linksneutral

(3) $x^{-1} \circ x \equiv e$ Existenz von Linksinversen

Behauptung: $\forall x \quad x \circ e \equiv x$ e rechtsneutral

negiert: $\exists x \neg\, x \circ e \equiv x$

skolemisiert:

(4) $\neg\, c \circ e \equiv c$

also gesucht: Widerlegung von (1), (2), (3), (4)

2: $\textcircled{e} \circ x \equiv x$

Paramodulation mit $\pi_1 = \begin{bmatrix} x \\ u \end{bmatrix}$ und mgu $\sigma_1 = [\,]$ von $\textcircled{e}$ und $\boxed{e}$

3: $x^{-1} \circ x \equiv e$

$u^{-1} \circ u \equiv \boxed{e}$

$(u^{-1} \circ u) \circ x \equiv x$

Paramodulation mit $\pi_2 = \begin{bmatrix} x & y & z \\ \bar{x} & \bar{y} & \bar{z} \end{bmatrix}$ und mgu $\sigma_2 = \begin{bmatrix} \bar{x} & \bar{y} & \bar{z} \\ u^{-1} & u & x \end{bmatrix}$ von $\circ, \square$

1: $x \circ (y \circ z) \equiv (x \circ y) \circ z$

$\bar{x} \circ (\bar{y} \circ \bar{z}) \equiv \boxed{(\bar{x} \circ \bar{y}) \circ \bar{z}}$

$u^{-1} \circ (\textcircled{u \circ x}) \equiv x$

Para mit $\pi_3 = \begin{bmatrix} x \\ v \end{bmatrix}$ und mgu $\sigma_3 = \begin{bmatrix} u & x \\ v^{-1} & v \end{bmatrix}$ von $\circ, \square$

3: $x^{-1} \circ x \equiv e$

$\boxed{v^{-1} \circ v} \equiv e$

$\{u^{-1} \circ e \equiv x\}\ \sigma_3$

(5) $(v^{-1})^{-1} \circ \textcircled{e} \equiv v$

Para mit mgu $\sigma_4 = \begin{bmatrix} x \\ e \end{bmatrix}$ von $\circ, \square$

2: $e \circ x = \boxed{x}$

$\{(v^{-1})^{-1} \circ (e \circ x) \equiv v\}\ \sigma_4$

$(v^{-1})^{-1} \circ (e \circ e) \equiv v$

$(v^{-1})^{-1} \circ (e \circ e) \equiv v$

Para mit mgu

$\sigma_5 = \begin{bmatrix} x & y & z \\ (v^{-1})^{-1} & e & e \end{bmatrix}$ von $\bigcirc, \square$

1: $\boxed{x \circ (y \circ z)} \equiv (x \circ y) \circ z$

$((v^{-1})^{-1} \circ e) \circ e \equiv v$

Para mit $\pi_6 = \begin{bmatrix} v \\ \tilde{v} \end{bmatrix}$ und mgu

$\sigma_6 = \begin{bmatrix} \tilde{v} \\ v \end{bmatrix}$ von $\bigcirc, \square$

5: $(v^{-1})^{-1} \circ e \equiv v$

$\boxed{(\tilde{v}^{-1})^{-1} \circ e} \equiv \tilde{v}$

$\{\tilde{v} \circ e \equiv v\}\sigma_6$

$v \circ e \equiv v$

Resolution mit mgu

$\sigma_7 = \begin{bmatrix} v \\ c \end{bmatrix}$ von

4: $\boxed{\neg\, c \circ e \equiv c}$

$\square$

ein Hilfssatz für spätere Zwecke:

Lemma

① $\{ t_1 \equiv t_2 \} \cup REF \vdash_{Para} t_2 \equiv t_1$

② $\{ t_1 \equiv t_2 , t_2 \equiv t_3 \} \cup REF \vdash_{Para} t_1 \equiv t_3$

③ $REF \vdash_{Para} t \equiv t$

④ $\{ t_1 \equiv t_2 \} \cup REF \vdash_{Para} t_1\sigma \equiv t_2\sigma$

Beweis:

zu ①:

$$\frac{\underset{\text{REF1}}{\textcircled{x} \equiv x} \qquad \underset{\text{Voraus.}}{t_1 \equiv t_2}}{\underbrace{(t_2 \equiv x)\sigma}} \text{ Para}$$

$$t_2\sigma \equiv x\sigma$$

$$t_2 \equiv t_1$$

Def. σ

1. o.B.d.A variablendisjunkt
2. $\sigma = \begin{bmatrix} x \\ t_1 \end{bmatrix}$ ist mgu von x und t_1

variablendisjunkt: x kommt in t_2 nicht vor

zu ②:

Vorauss. $t_1 \equiv t_2$; Vorauss. $t_2 \equiv t_3$

$(t_1 \equiv t_3\pi)\pi^{-1}$

$t_1\pi^{-1} \equiv t_3\pi\pi^{-1}$

$t_1 \equiv t_3$

variablendisjunkt:

$\pi^{-1}(x) = x$ f. alle Variablen aus t_1

Para mit

1. π Umbenennung, die die Prämissen variablendisjunkt macht
2. π^{-1} ist mgu von t_2 und $t_2\pi$

zu ③: (durch Induktion über die Höhe von t)

Induktionsanfang: Höhe von $t = 1$

Zwei Fälle sind möglich:

falls t Variable ist, dann ist $t \equiv t$ REF 1;

falls t Konstante ist, dann ist $t \equiv t$ REF 2.

Also: REF $\vdash_{\text{Para}}$ $t \equiv t$

Induktionsschritt:

t hat Form $f(t_1, \dots, t_n)$

REF2:

$$f(x_1, x_2, \dots) \equiv f(x_1, x_2, \dots)$$

Ind. Annahme $t_1 \equiv t_1$

$$\underbrace{\left(f(t_1, x_2, \dots) \equiv f(x_1, x_2, \dots)\right)\sigma}$$

Para mit
1. o.B.d.A variablendisjunkt
2. mgu $\sigma = [\,^{x_1}_{t_1}]$ von x_1 und t_1

$$f(t_1, x_2, \dots) \equiv f(t_1, x_2, \dots)$$

Para

•

•

•

$$f(t_1, \dots, x_n) \equiv f(t_1, \dots, x_n)$$

Ind. Annahme $t_n \equiv t_n$

Para

$$f(t_1, \dots, t_n) \equiv f(t_1, \dots, t_n)$$

zu ⑤:

Beispiel: t_1 : $f(x,y)$

t_2 : $g(x,y)$

$$\sigma = \begin{bmatrix} x & y \\ a & h(z) \end{bmatrix}$$

Voraussetzung

$f(x,y) \equiv g(x,y)$ — REF 2: $a \equiv a$

Para mit $\sigma_1 = \begin{bmatrix} x \\ a \end{bmatrix}$

① $h(z) \equiv h(z)$ — Para mit $\sigma_2 = \begin{bmatrix} y \\ h(z) \end{bmatrix}$

$f(a,y) \equiv g(a,y)$

$f(a,h(z)) \equiv g(a,h(z))$

$t_1\sigma$ $\quad$ $t_2\sigma$

allgemein:

- wie im Beispiel σ "variablenweise" durchführen
- dabei Variablenkollisionen vermeiden

maschinelles Beweisen für Gleichheitsaussagen

bislang behandelte Ansätze:

- Resolution mit Gleichheitsaxiomen GAX
- Resolution und Paramodulation mit Reflexivaxiomen REF

Frage: Braucht man neben der Paramodulation zusätzlich noch die Resolution?

weiterer Ansatz:

- Termersetzung!

zur Frage:

Satz Sei E eine Menge von Gleichheitsatomen und t_1, t_2 Terme.

Dann gilt:

$$E \cup GAX \vdash_{Res} t_1 \equiv t_2$$

gdw.

$$E \cup REF \vdash_{Para} t_1 \equiv t_2$$

Beweis:

Man übertrage die Beweisidee des vorangehenden Satzes, d.h. die Simulation von

Resolution mit GAX

durch

Resolution und Paramodulation mit REF

auf die hier vorliegenden Verhältnisse.

zum weiteren Ansatz: **Termersetzung**

- Paramodulation benutzt

  Gleichung $l \equiv r$ als "Ersetzungsvorschrift":

  unter einer geeigneten Substitution wird

  die linke Seite l

  durch die rechte Seite r

  ersetzt.

- Termauswertung, etwa in der Arithmetik,

  ersetzt, von innen nach außen,

  "unausgewertete Terme"

  durch ihre Werte.

kleines Eins-und-Eins:

$((1+3)+4)-8$

$1+3 \rightarrow 4$

$(4+4)-8$

$4+4 \rightarrow 8$

$8-8$

$8-8 \rightarrow 0$

0

Definition

Sei $T_\Sigma(V)$ Menge der Terme
über der Signatur Σ
mit Variablen aus V.

1. $R \subset \{ \underbrace{l \longrightarrow r}_{\text{Regel}} \mid l, r \in T_\Sigma(V) \}$
(linke Seite, rechte Seite)

heißt Termersetzungssystem.

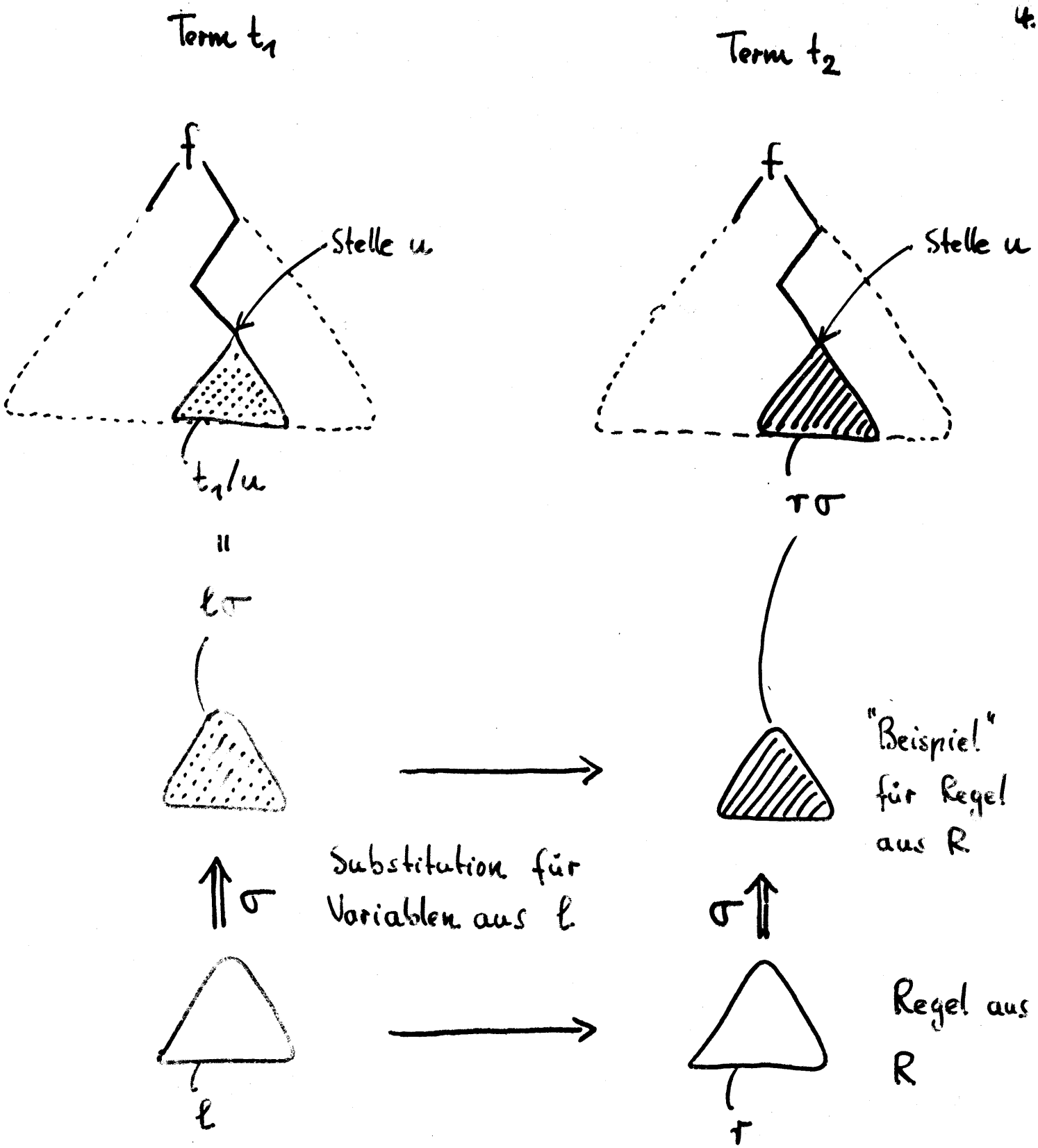
2. Für $t_1, t_2 \in T_\Sigma(V)$ heißt

t_1 (in einem Schritt) mit R reduzierbar zu t_2,

$t_1 \longrightarrow_R t_2$: gdw ex. Stelle u in t_1,
ex. Regel $l \to r \in R$,
ex. Substitution σ :

"match" von t_1/u mit $l\sigma$ 1) $t_1/u = l\sigma$

ersetze an Stelle u
$l\sigma$ durch $r\sigma$ 2) $t_2 = t_1[u \leftarrow r\sigma]$


Term t_1
Term t_2
f
Stelle u
t_1/u
=
$\ell\sigma$
f
Stelle u
$r\sigma$
"Beispiel" für Regel aus R
σ
Substitution für Variablen aus ℓ
σ
ℓ
r
Regel aus R

3. $\xrightarrow{+}_R$ transitiver Abschluß von R

$\xrightarrow{*}_R$ transitiver, reflexiver Abschluß von R:

$t_1 \xrightarrow{*}_R t_2$: gdw $t_1 \xrightarrow{+}_R t_2$ oder $t_1 = t_2$

$\longleftrightarrow_R$ symmetrischer Abschluß von R:

$t_1 \longleftrightarrow_R t_2$: gdw $t_1 \to t_2$ oder $t_2 \to t_1$

$\xleftrightarrow{*}_R$ Äquivalenzabschluß von R

(transitiver, reflexiver Abschluß von $\longleftrightarrow_R$)

Beispiel:

Termersetzungssystem R (etwa für natürliche Zahlen):

(1) $x + 0 \to x$

(2) $x + s(y) \to s(x+y)$ — successor, Nachfolger, "+1"

(3) $x * 0 \to 0$

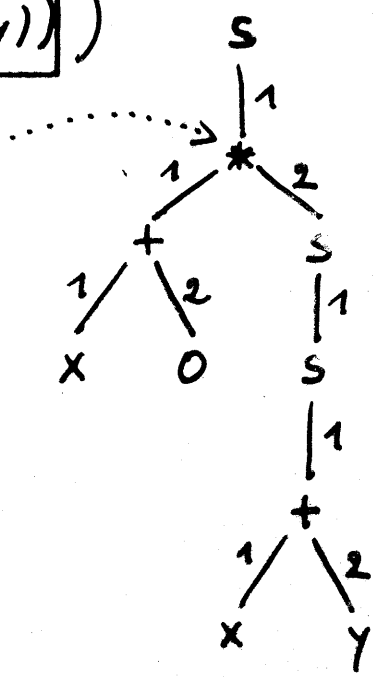
(4) $x * s(y) \to x + (x * y)$

Term t_1: $s(\boxed{(x+0) * s(s(x+y))})$ — t_1/u

Stelle u: $1.\lambda$

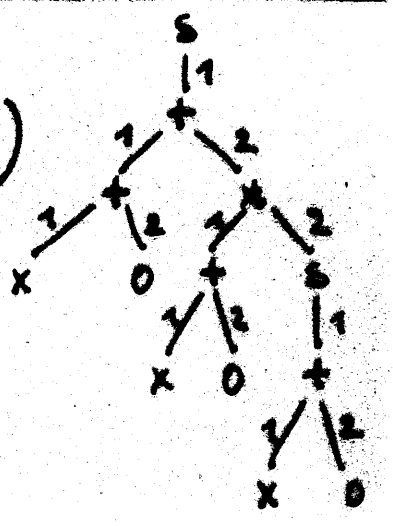
Regel $l \to r$: $x * s(y) \to x + (x * y)$

Substitution σ: $\begin{bmatrix} x & y \\ (x+0) & s(x+y) \end{bmatrix}$



Beispiel der Regel: $\boxed{(x+0) * s(s(x+y))}_{l\sigma} \to \boxed{(x+0) + ((x+0) * s(x+y))}_{r\sigma}$

Term t_2: $s(\boxed{(x+0) + ((x+0) * s(x+y))}_{r\sigma})$

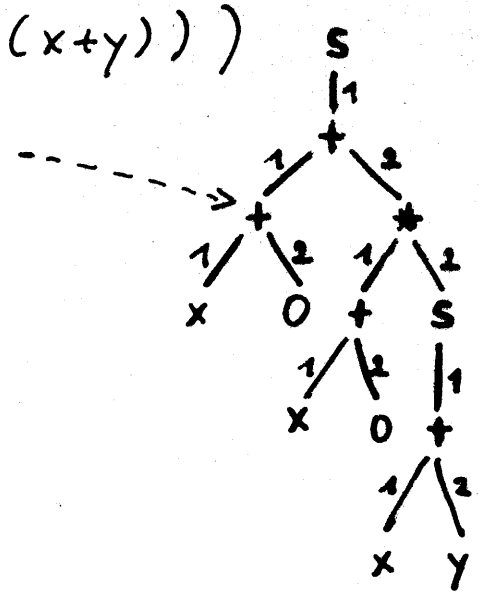


Term t_2 : $s(\boxed{(x+0)} + ((x+0) * s(x+y)))$ — t_2/u

Stelle u : $1.1.\lambda$

Regel $l \to r$: $x + 0 \to x$

Substitution σ : $[]$



Beispiel der Regel : $\boxed{x+0}^{l\sigma} \to \boxed{x}^{r\sigma}$

Term t_3 : $s(\boxed{x} + ((x+0) * s(x+y)))$ — $r\sigma$

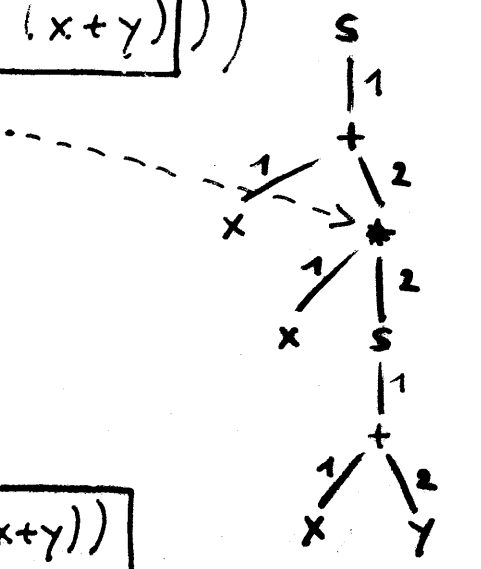
analog kann man t_4 erhalten; dann fortfahren:

Term t_4 : $s(x + (\boxed{x * s(x+y)}))$ — t_4/u

Stelle u : $1.2.\lambda$

Regel $l \to r$: $x * s(y) \to x + (x * y)$

Substitution σ : $\begin{bmatrix} x & y \\ x & x+y \end{bmatrix}$



Beispiel der Regel : $\boxed{x * s(x+y)}^{l\sigma} \to \boxed{x + (x * (x+y))}^{r\sigma}$

Term t_5 : $s(x + (\boxed{x + (x * (x+y))}))$ — $r\sigma$

Achtung: Klammern sind "freihändig" gesetzt !

Beispiel aus Gruppentheorie:

(1) $x \circ (y \circ z) \to (x \circ y) \circ z$ — $\circ$ assoziativ

(2) $e \circ x \to x$ — e linksneutral

(3) $x^{-1} \circ x \to e$ — $^{-1}$ liefert Linksinverses

Ziel: $x \circ e \overset{*}{\leftrightarrow} x$ — e rechtsneutral

Ableitung mit Hilfe des Termersetzungssystems (1), (2), (3):

$x \circ e \leftarrow (\ e \circ x\ ) \circ e$ (2), $\sigma = [\,]$

$\leftarrow ((x^{-1})^{-1} \circ x^{-1}) \circ x\ ) \circ e$ (3), $\sigma = \begin{bmatrix} x \\ x^{-1} \end{bmatrix}$

$\leftarrow (\ (x^{-1})^{-1} \circ (\ x^{-1} \circ x)) \circ e$ (1), $\sigma = \begin{bmatrix} x & y & z \\ (x^{-1})^{-1} & x^{-1} & x \end{bmatrix}$

$\to (\ (x^{-1})^{-1} \circ \quad e \quad) \circ e$ (3), $\sigma = [\,]$

$\leftarrow \quad (x^{-1})^{-1} \circ (\ e \quad \circ e\ )$ (1), $\sigma = \begin{bmatrix} x & y & z \\ (x^{-1})^{-1} & e & e \end{bmatrix}$

$\to \quad (x^{-1})^{-1} \circ \quad e$ (2), $\sigma = \begin{bmatrix} x \\ e \end{bmatrix}$

$\leftarrow \quad (x^{-1})^{-1} \circ (\ x^{-1} \circ x\ )$ (3), $\sigma = [\,]$

$\to ((x^{-1})^{-1} \circ \quad x^{-1}) \circ x$ (1), $\sigma = \begin{bmatrix} x & y & z \\ (x^{-1})^{-1} & x^{-1} & x \end{bmatrix}$

$\to \quad e \quad \circ x$ (3), $\sigma = \begin{bmatrix} x \\ x^{-1} \end{bmatrix}$

$\to \quad x$ (2), $\sigma = [\,]$

Lemma 6.5 [Verträglichkeit von $\rightarrow_R$ mit Substitution und Termbildung]

1. Falls $t_1 \rightarrow_R t_2$, dann $t_1\sigma \rightarrow_R t_2\sigma$.
2. Falls $t_1 \rightarrow_R t_2$, dann $f(\ldots t_1 \ldots) \rightarrow_R f(\ldots t_2 \ldots)$

Analoge Aussagen gelten dann für:

$\overset{}{\longleftrightarrow}_R$

$\overset{+}{\longrightarrow}_R$

$\overset{*}{\longrightarrow}_R$

$\overset{*}{\longleftrightarrow}_R$

zu 1: Sei $t_1 \to_R t_2$.

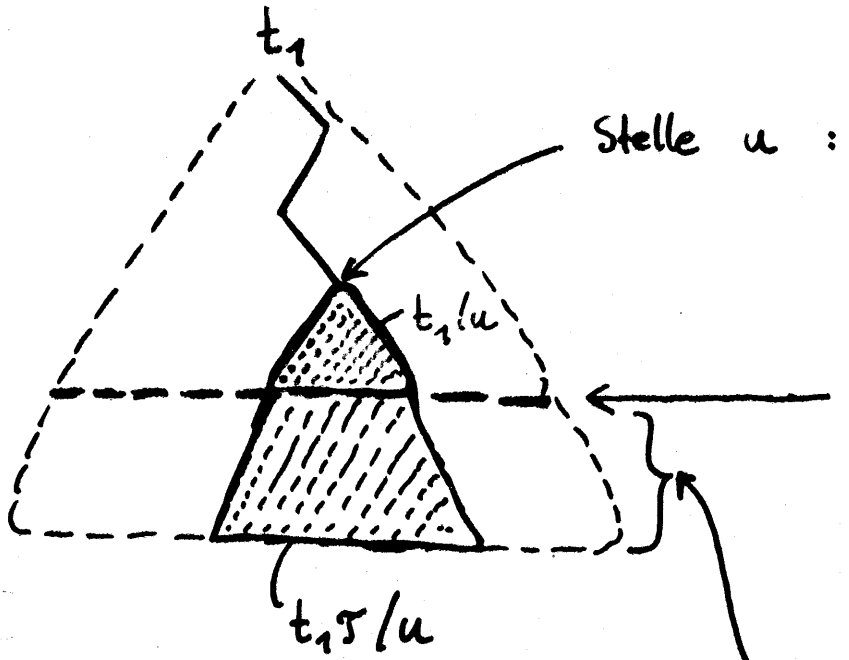
Dann ex. Stelle u in t_1,

ex. Regel $l \to r \in R$,

ex Substitution σ:

1) $t_1 / u = l\sigma$

2) $t_2 = t_1[u \leftarrow r\sigma]$



Stelle u : ist auch Stelle von $t_1\tau$

"Rand" von t_1 (Blätter): nur hier kommen Variable vor

Wirkung von Substitution τ : jeweils kontextfreie Ersetzung

Dann folgt:

1*) $t_1\tau/u = (t_1/u)\tau \overset{1)}{=} l\sigma\tau$

2*) $t_2\tau \overset{2)}{=} (t_1[u \leftarrow r\sigma])\tau$

$= t_1\tau[u \leftarrow r\sigma\tau]$

Also: $t_1\tau \to_R t_2\tau$ vermöge Substitution $\sigma\tau$

zu 2: Sei $t_1 \to_R t_2$.

Dann ex. Stelle u in t_1,

ex. Regel $\ell \to r \in R$,

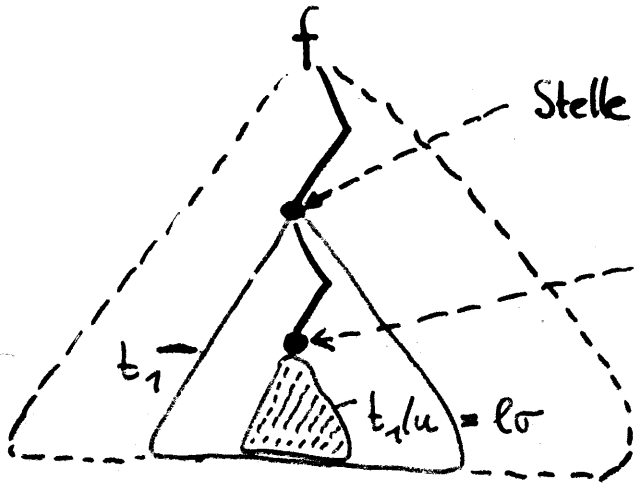
ex. Substitution σ :

1) $t_1/u = \ell\sigma$

2) $t_2 = t_1[u \leftarrow r\sigma]$

Wir betrachten nun $f(\ldots t_1 \ldots)$.

Sei v diejenige Stelle mit $t_1 = f(\ldots t_1 \ldots)/v$.



Stelle v in $f(\ldots t_1 \ldots)$

Stelle u in t_1
= "Stelle" $v.u$ in $f(\ldots t_1 \ldots)$

Dann folgt:

1*) $f(\ldots t_1 \ldots)/v.u = t_1/u \overset{1)}{=} \ell\sigma$

2*) $f(\ldots t_2 \ldots) = f(\ldots t_1 \ldots)[v \leftarrow t_2]$

$\overset{2)}{=} f(\ldots t_1 \ldots)[v \leftarrow t_1[u \leftarrow r\sigma]]$

$= f(\ldots t_1 \ldots)[v.u \leftarrow r\sigma]$

Also: $f(\ldots t_1 \ldots) \to_R f(\ldots t_2 \ldots)$

maschinelles Beweisen für Gleichheitsaussagen:

gegeben: • Termersetzungssystem

$$R = \{ l_1 \to r_1, \ldots, l_k \to r_k \}$$

• Terme t_1, t_2

entscheide: $t_1 \overset{*}{\underset{R}{\longleftrightarrow}} t_2$

Zusammenhang mit Paramodulation:

• für eine Menge E von Gleichheitsatomen der Form $s \equiv t$

sei $R_E := \{ s \to t \mid s \equiv t \in E \}$

• für eine Menge R von Termersetzungs-Regeln der Form $s \to t$

sei $E_R := \{ s \equiv t \mid s \to t \in R \}$

Satz 6.8 [Äquivalenz von Paramodulation und Termersetzung für Gleichungen]

Sei E eine Menge von Gleichheitsatomen, und seien t_1, t_2 Terme. Dann gilt:

$$E \cup \underset{\substack{x=x \\ f(\ldots)=f(\ldots)}}{\text{REF}} \vdash_{\text{Para}} t_1 \equiv t_2 \quad \text{gdw} \quad t_1 \overset{*}{\underset{R_E}{\longleftrightarrow}} t_2$$

"$\Rightarrow$" (durch Induktion über die Struktur der Paramodulation - Ableitung)

erweiterte Behauptung:

falls $E \cup REF \vdash_{Para} t_1 \equiv t_2$

dann
- $t_1 \overset{*}{\underset{R_E}{\longleftrightarrow}} t_2$
- in der Paramodulation - Ableitung kommen nur Gleichheitsatome vor

Beweis:

Induktionsanfang: Wir betrachten ein Blatt einer Paramodulation - Ableitung.

Zwei Fälle sind möglich:

1. falls $t_1 \equiv t_2 \in E$,

   dann $t_1 \longrightarrow t_2 \in R_E$, Definition R_E

   dann $t_1 \overset{*}{\underset{R_E}{\longleftrightarrow}} t_2$ Definition $\overset{*}{\underset{R_E}{\longleftrightarrow}}$

2. falls $t_1 \equiv t_2 \in REF$,

   dann $t_1 = t_2$, Definition REF
   ↖ als Zeichenkette gleich!

   dann $t_1 \overset{*}{\underset{R_E}{\longleftrightarrow}} t_2$ Definition $\overset{*}{\underset{R_E}{\longleftrightarrow}}$

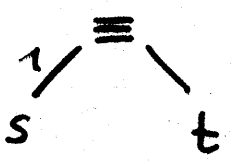
Induktionsschritt: Wir betrachten einen inneren Knoten einer Paramodulation-Ableitung, d.h. eine Anwendung der Paramodulation.

Sei also $t_1 \equiv t_2$ durch Paramodulation von $l \equiv r$ in $s \equiv t$ entstanden:

$$\frac{s \equiv t \qquad\qquad l \equiv r}{\underbrace{(s[u \leftarrow r] \equiv t)\,\sigma}_{t_1 \equiv t_2}}\ \text{Para}$$

mit
1. o.B.d.A seien $s \equiv t$ und $l \equiv r$ variablendisjunkt
2. σ ist mgu von s/u und l
3. $EuREF \vdash_{Para} s \equiv t$ und $EuREF \vdash_{Para} l \equiv r$

genauer: im Atom $s \equiv t$



wird an einer Stelle w paramoduliert:
diese Stelle sei o.B.d.A im linken Zweig, d.h. von der Form $w = 1.u$!

Dann gilt:

$t_1 = s[u \leftarrow r]\,\sigma$ — t_1 ist linke Seite des Ergebnisses der Paramodulation

$= s\sigma\,[u \leftarrow r\sigma]$ — σ ersetzt "kontextfrei"

$\overset{*}{\underset{R_E}{\longleftrightarrow}}\; s\sigma\,[u \leftarrow l\sigma]$

- gemäß Induktionsannahme: $l \overset{*}{\underset{R_E}{\longleftrightarrow}} r$
- Verträglichkeit von $\overset{*}{\underset{R_E}{\longleftrightarrow}}$ mit Substitution und Termbildung

$= s\sigma$ — σ mgu von s/u und l

$\overset{*}{\underset{R_E}{\longleftrightarrow}}\; t\sigma$

- gemäß Induktionsannahme: $s \overset{*}{\underset{R_E}{\longleftrightarrow}} t$
- Verträglichkeit von $\overset{*}{\underset{R_E}{\longleftrightarrow}}$ mit Substitution

$= t_2$ — t_2 ist rechte Seite des Ergebnisses der Paramodulation

"$\Leftarrow$": Beh: falls $t_1 \overset{*}{\underset{R_E}{\longleftrightarrow}} t_2$, dann $E \cup REF \vdash_{Para} t_1 \equiv t_2$

zu zeigen:

1. falls $t_1 \underset{R_E}{\longrightarrow} t_2$, dann $E \cup REF \vdash_{Para} t_1 \equiv t_2$
2. dann allgemein für $\overset{*}{\underset{R_E}{\longleftrightarrow}}$

Beweis:

zu 2.: folgt aus 1. mit ①, ②, ③ durch Induktion.

zu 1.: Sei $t_1 \underset{R_E}{\longrightarrow} t_2$.

Dann ex. Stelle u in t_1,
ex. Regel $l \to r \in R_E$, o.B.d.A variablendisjunkt zu t_1, t_2
ex. Substitution σ:

1) $t_1/u = l\sigma$
2) $t_2 = t_1[u \leftarrow r\sigma]$

Dann:

$$\frac{\dfrac{\dfrac{\dfrac{}{t_1[u \leftarrow l] \equiv t_1[u \leftarrow \textcircled{r}]}\ ③ \qquad \overset{E}{l \equiv r}}{t_1[u \leftarrow l] \equiv t_1[u \leftarrow r]}\ \text{Para mit mgu } []}{\vdots}\ \text{Para}}{t_1[u \leftarrow l]\sigma \equiv t_1[u \leftarrow r]\sigma}\ \text{Para}\ \Big\}\ \text{gemäß ④}$$

$t_1[u \leftarrow l]\sigma \equiv t_1[u \leftarrow r]\sigma$ gemäß "variablendisjunkt"

$t_1[u \leftarrow l\sigma] \equiv t_1[u \leftarrow r\sigma]$

1): t_1 2): t_2

Korollar 6.9

Sei E eine Menge von Gleichheitsatomen, und seien t_1, t_2 Terme.

Dann sind folgende Aussagen äquivalent:

1. In allen Gleichheitsmodellen von E gilt $t_1 \equiv t_2$.
2. $E \cup GAX \vdash_{Res} t_1 \equiv t_2$
3. $E \cup REF \vdash_{Para} t_1 \equiv t_2$
4. $t_1 \overset{*}{\underset{R_E}{\longleftrightarrow}} t_2$

Beweis:

"3. ⇔ 4.": Satz 6.8

"2. ⇔ 3.": ein vorangehender Satz

"2. ⇒ 1.": Korrektheit der Resolution

1. ⇒ 2. (Skizze):

Es gelte: In allen Gleichheitsmodellen von E gilt $t_1 \equiv t_2$

dann: $E \cup \{(\neg\, t_1 \equiv t_2)\,\theta\}$ hat kein Gleichheitsmodell

↑ geeignete Substitution für Skolemisierung

dann gemäß Korollar 5.5:

$$E \cup \{(\neg\, t_1 \equiv t_2)\,\theta\} \cup GAX \vdash_{Res+Fak} \square$$

↑ braucht man für vorkommende Formeln nicht

dann durch "Normalisierung" der Ableitung:

$$E \cup GAX \vdash_{Res} t_1' \equiv t_2'$$

für geeignete Substitution σ mit $(t_1' \equiv t_2')\,\sigma = t_1 \equiv t_2$

dann analog zu ④:

$$E \cup GAX \vdash_{Res} t_1 \equiv t_2$$

maschinelles Beweisen für Gleichheitsaussagen:

gegeben: Termersetzungssystem $R = \{ \ell_1 \to r_1, \ldots, \ell_k \to r_k \}$

Terme t_1, t_2

entscheide: $t_1 \overset{*}{\underset{R}{\longleftrightarrow}} t_2$

Satz: Das Problem $t_1 \overset{*}{\underset{R}{\longleftrightarrow}} t_2$ ist unentscheidbar.

Beweisidee: simuliere Turingmaschinen durch geeignete Ersetzungssysteme!

daher gesucht:

"schöne Eigenschaften" für R,

die hinreichend sind für die

Entscheidbarkeit von $\{ (t_1, t_2) \mid t_1 \overset{*}{\underset{R}{\longleftrightarrow}} t_2 \}$

im folgenden allgemeiner:

$\to$ Relation auf Menge T

später anwenden auf: $\to_R$ und $T_\Sigma(V)$

Definition

1. $R = (T, \to)$ mit T Menge

$\to \subset T \times T$ Relation auf T

heißt Ersetzungssystem.

2. $\xrightarrow{*}$ transitiver, reflexiver Abschluß von $\to$

$\xleftrightarrow{*}$ Äquivalenzabschluß

3. $R = (T, \to)$ heißt terminierend

(fundiert, Noethersch)

: gdw es gibt keine unendliche Folge

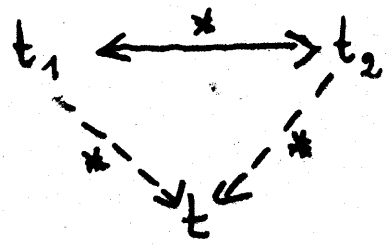
$t_0, t_1, t_2, \ldots$ aus T mit

$t_0 \to t_1 \to t_2 \to \ldots$

4. $R = (T, \to)$ heißt Church-Rosser

: gdw für alle $t_1, t_2 \in T$ mit $t_1 \xleftrightarrow{*} t_2$

ex. $t \in T$ mit $t_1 \xrightarrow{*} t$ und $t_2 \xrightarrow{*} t$.



5. $t \in T$ heißt irreduzibel

: gdw es gibt kein $t' \in T$ mit $t \to t'$

6. $t' \in T$ heißt Normalform von $t \in T$

: gdw 1) $t \xrightarrow{*} t'$

2) t' ist irreduzibel

7. Hat $t \in T$ eine eindeutige Normalform,
so werde sie mit $t \downarrow R$ bezeichnet.

Satz 6.12a [Church-Rosser impliziert Eindeutigkeit von Normalformen]

Sei $R = (T, \to)$ Church-Rosser,

$t \in T$.

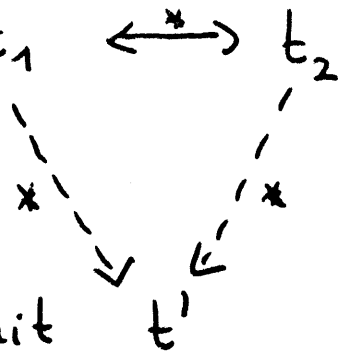
Dann hat t höchstens eine Normalform.

Beweis: Seien t_1, t_2 Normalformen von t, d.h.

1) $t \xrightarrow{*} t_1$, $t \xrightarrow{*} t_2$

2) t_1 irreduzibel , t_2 irreduzibel

Dann:



1), $\overset{*}{\leftrightarrow}$ Äquivalenzabschluß

Church-Rosser

Also: $t_1 = t'$ 2) irreduzibel

$t_2 = t'$

d.h $t_1 = t_2$

Satz 6.12 b [terminierend impliziert Existenz von Normalformen]

Sei $R = (T, \to)$ terminierend,
$t \in T$.
Dann hat t (mindestens) eine Normalform.

Beweis:

indirekt: angenommen t hat keine Normalform.

wir konstruieren eine unendliche Folge
$t_0, t_1, t_2 \ldots$ aus T mit $t_0 \to t_1 \to t_2 \to \ldots$

also: Widerspruch zu "terminierend"

i) $t_0 := t$: es gilt $t \xrightarrow{*} t_0$

ii) sei t_i schon konstruiert:

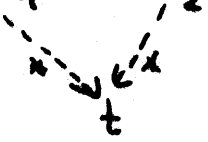
dann: • $t \xrightarrow{*} t_i$ Induktionsannahme

• t_i nicht irreduzibel indirekte Annahme: sonst wäre t_i Normalform von t

also: ex. t_{i+1} mit $t_i \longrightarrow t_{i+1}$ Def. irreduzibel
es gilt: $t \xrightarrow{*} t_{i+1}$ $\xrightarrow{*}$ transitiv

Satz Sei $R = (T, \to)$

terminierend, d.h. es gibt keine unendlichen Ketten
$t_0 \to t_1 \to t_2 \to \ldots$,

und Church-Rosser, d.h. für alle $t_1, t_2 \in T$ mit $t_1 \overset{*}{\longleftrightarrow} t_2$
ex. $t \in T$ mit 

Dann gilt:

1. Jedes $t \in T$ hat eindeutige Normalform, $t{\downarrow}R$.

2. $t_1 \overset{*}{\longleftrightarrow} t_2$ gdw. $t_1{\downarrow}R = t_2{\downarrow}R$.

3. Ist $t \longmapsto t{\downarrow}R$ eine berechenbare Funktion
(insbesondere also falls R endlich ist),
so ist $t_1 \overset{*}{\longleftrightarrow} t_2$ entscheidbar.

Beweis:

1. terminierend impliziert Existenz (Satz 6.12 b)

   Church-Rosser impliziert Eindeutigkeit (Satz 6.12 a)

2. "$\Leftarrow$": Sei $t := t_1 \downarrow R = t_2 \downarrow R$

   Dann $t_1 \xrightarrow{*} t \xleftarrow{*} t_2$ Def. $t_i \downarrow R$

   Also $t_1 \overset{*}{\longleftrightarrow} t_2$ $\overset{*}{\longleftrightarrow}$ Äquivalenzabschluß

"$\Rightarrow$"

Sei $t_1 \overset{*}{\longleftrightarrow} t_2$.

Gemäß 1. haben t_1, t_2 eindeutige Normalformen $t_1 \downarrow R$, $t_2 \downarrow R$

Also: $t_1 \overset{*}{\longleftrightarrow} t_2$

$*\downarrow$ $\quad \downarrow *$

$t_1 \downarrow R \qquad t_2 \downarrow R$ mit $t_i \downarrow R$ irreduzibel

Also: $t_1 \downarrow R \overset{*}{\longleftrightarrow} t_2 \downarrow R$ $\overset{*}{\longleftrightarrow}$ Äquivalenzabschluß

$*\searrow \quad \swarrow *$

ex. $t \in T$: $\quad t$ Church-Rosser

dann: $t_1 \downarrow R = t = t_2 \downarrow R$ $t_i \downarrow R$ irreduzibel

3. Entscheidungsverfahren:

Eingabe: t_1, t_2

Methode:

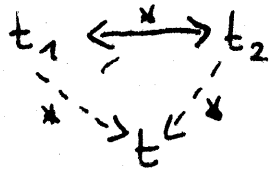
- berechne Normalformen $t_1 \downarrow R$, $t_2 \downarrow R$
- teste $t_1 \downarrow R$ und $t_2 \downarrow R$ auf Gleichheit

[gemäß 2.: $t_1 \downarrow R = t_2 \downarrow R$:gdw $t_1 \overset{*}{\leftrightarrow} t_2$]

wünschenswerte Eigenschaften von Ersetzungssystemen:

1. terminierend — keine unendlichen Ketten $t_0 \to t_1 \to t_2 \to \ldots$

2. Church-Rosser



Problem:

- Wie kann man erkennen, daß $R = (T, \to)$ diese Eigenschaften besitzt?

- Gibt es andere Eigenschaften (vielleicht spezieller, leichter zu erkennen), die ebenfalls Existenz und Eindeutigkeit von Normalformen implizieren?

Definition $R = (T, \to)$ heißt konfluent

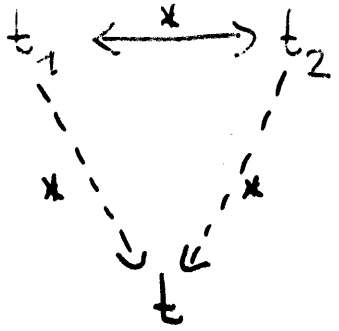
: gdw für alle $t_0, t_1, t_2 \in T$

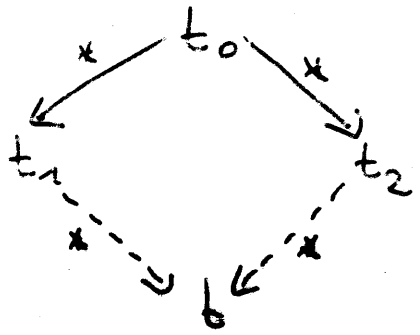
mit $t_0 \xrightarrow{*} t_1$, $t_0 \xrightarrow{*} t_2$

ex. $t \in T$ mit $t_1 \xrightarrow{*} t$, $t_2 \xrightarrow{*} t$

Satz 6.16

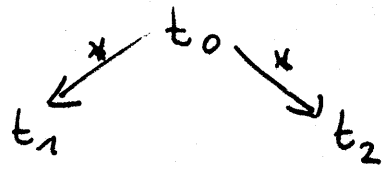
R ist Church-Rosser gdw R ist konfluent.





Beweis:

"⇒": konfluent ist spezieller als Church-Rosser:

Wenn 

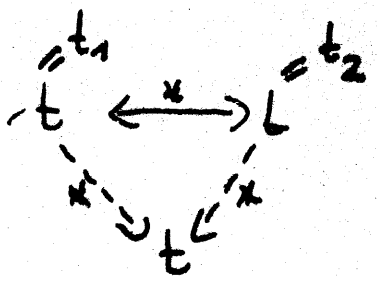
dann auch $t_1 \xleftrightarrow{*} t_2$

"$\Leftarrow$" (Induktion über die Länge n
der "Verbindung" von t_1 und t_2)

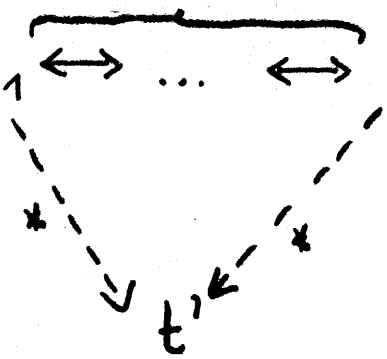
$n = 0$: Sei $t_1 \overset{*}{\longleftrightarrow} t_2$ mit $t_1 = t_2$.

Wähle $t := t_1$.

Dann gilt trivialerweise:



$n > 0$: Sei $t_1 \longleftrightarrow \dots \longleftrightarrow s \longleftrightarrow t_2$ (Länge $n-1$)



Induktionsannahme:
ex. t' mit

Fall 1: $s \longleftarrow t_2$

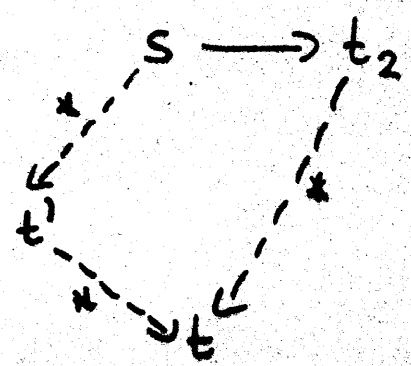
Dann: $t_2 \longrightarrow s$ — Fall 1

$\overset{*}{\longrightarrow} t'$ — Ind. Annahme

Also: $t := t'$ hat geforderte Eigenschaften

Fall 2: $s \longrightarrow t_2$

Da R konfluent, ex. $t \in T$ mit:



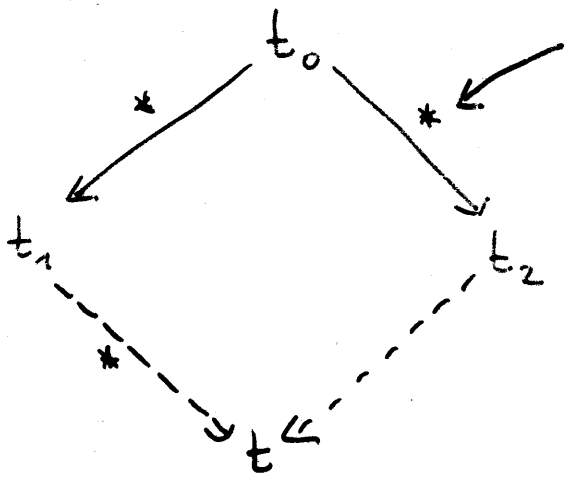
Also: t hat geforderte Eigenschaften

$R = (T, \to)$ konfluent

:gdw für alle $t_0, t_1, t_2 \in T$

mit $t_0 \xrightarrow{*} t_1$, $t_0 \xrightarrow{*} t_2$

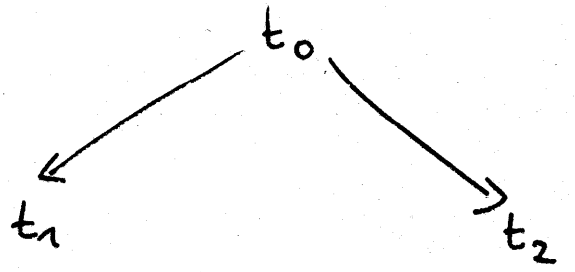
ex. $t \in T$ mit $t_1 \xrightarrow{*} t$, $t_2 \xrightarrow{*} t$



transitiver, reflexiver Abschluß:

i. allg. "unbegrenzt viele" Situationen zu betrachten

<u>Frage:</u> reicht es aus, nur folgende Situationen zu betrachten:



Definition $R = (T, \to)$ heißt lokal konfluent

: gdw für alle $t_0, t_1, t_2 \in T$

mit $t_0 \to t_1$, $t_0 \to t_2$

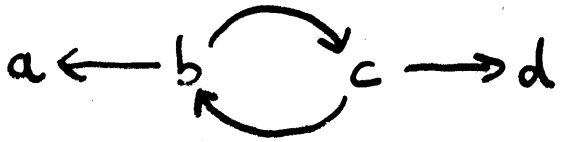
ex. $t \in T$ mit $t_1 \xrightarrow{*} t$, $t_2 \xrightarrow{*} t$

Bemerkung 1: konfluent impliziert lokal konfluent

Bemerkung 2: Es gibt ein Ersetzungssystem R mit

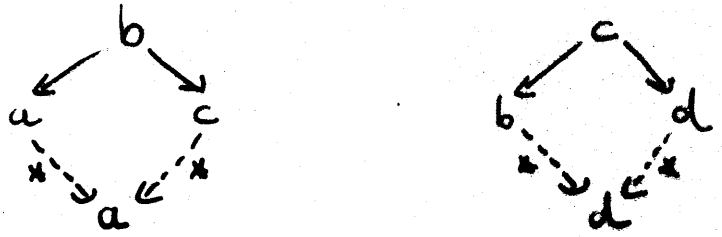
1. lokal konfluent, aber
2. nicht konfluent:

$R = (\{a, b, c, d\}, \{b \to a, b \to c, c \to b, c \to d\})$

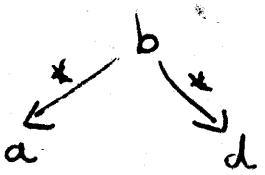


beachte:
R ist nicht terminierend

lokal konfluent: nur b und c haben Ausgrad ≥ 2, d.h.
nur folgende Situationen zu betrachten:



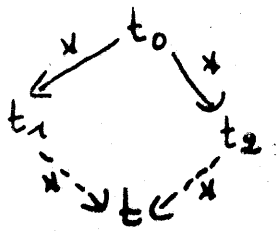
nicht konfluent:

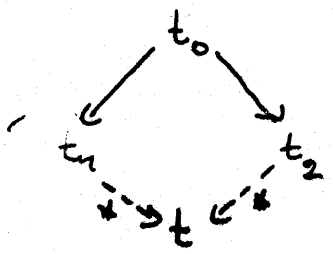


; a, d irreduzibel ; $a \neq d$

Satz 6.17 Sei $R = (T, \to)$ terminierend. Dann

R konfluent gdw R lokal konfluent

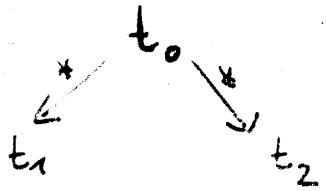




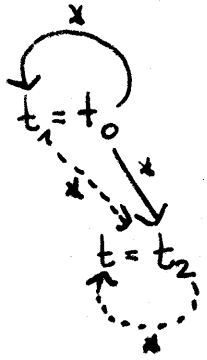
Beweis: "$\Rightarrow$": trivial

"$\Leftarrow$" (durch Induktion über die "Tiefe" von t_0:
möglich da R terminierend ist, d.h. keine
unendlichen Ketten besitzt)

Sei also



Fall 1: $t_0 = t_1$: wähle $t = t_2$, denn:



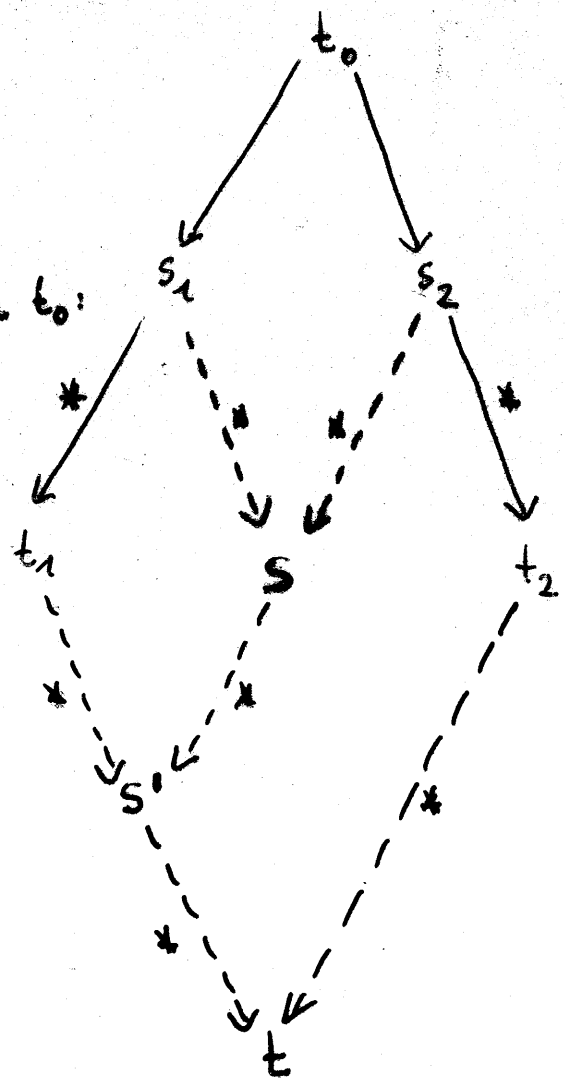
Fall 2: $t_0 = t_2$: wähle $t = t_1$

Fall 3: $t_0 \xrightarrow{+} t_1$ und $t_0 \xrightarrow{+} t_2$: also

ex. s_1, s_2 : $t_0 \to s_1 \xrightarrow{*} t_1$, $t_0 \to s_2 \xrightarrow{*} t_2$

dann: "Tiefe" von s_i kleiner als "Tiefe" von t_0.

Dann:



"Tiefe" von s_1 kleiner als von t_0:

Ind. Annahme:

ex. s' mit

$s_1 \xrightarrow{*} s'$,

$s \xrightarrow{*} s'$

lokal konfluent:

ex. s mit

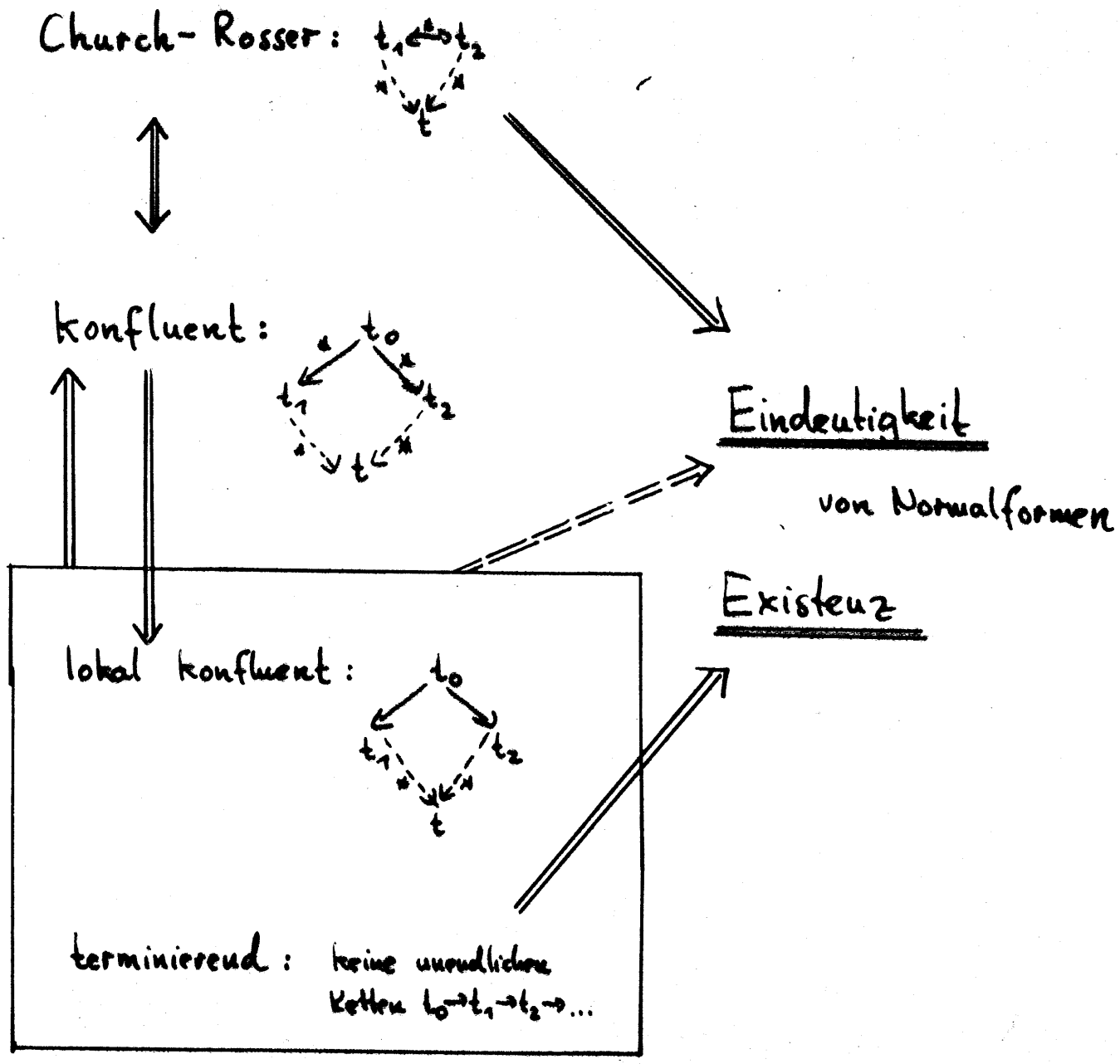
$s_1 \xrightarrow{*} s$, $s_2 \xrightarrow{*} s$

"Tiefe" von s_2 kleiner als von t_0:

Ind. Annahme:

ex. t mit

$s' \xrightarrow{*} t$, $t_2 \xrightarrow{*} t$


Church-Rosser:
konfluent:
lokal konfluent:
terminierend: keine unendlichen Ketten $t_0 \to t_1 \to t_2 \to \ldots$
Eindeutigkeit
von Normalformen
Existenz

maschinelles Beweisen für Gleichheitsaussagen:

gegeben: Termersetzungssystem $R = \{ l_1 \to r_1, \ldots, l_k \to r_k \}$

Terme t_1, t_2

entscheide: $t_1 \overset{*}{\underset{R}{\longleftrightarrow}} t_2$

ein Ansatz aus der Theorie (allgemeiner) Ersetzungssysteme:

- berechne Normalformen $t_1 \downarrow R$, $t_2 \downarrow R$
- teste $t_1 \downarrow R$ und $t_2 \downarrow R$ auf Gleichheit

notwendige Voraussetzung dafür:

Existenz und Eindeutigkeit von Normalformen

hinreichend dafür:

terminierend und lokal konfluent

Problem: Wie kann man erkennen,
daß ein Termersetzungssystem R
diese Eigenschaften besitzt ?

zunächst: lokal konfluent
später : terminierend

Beispiel:

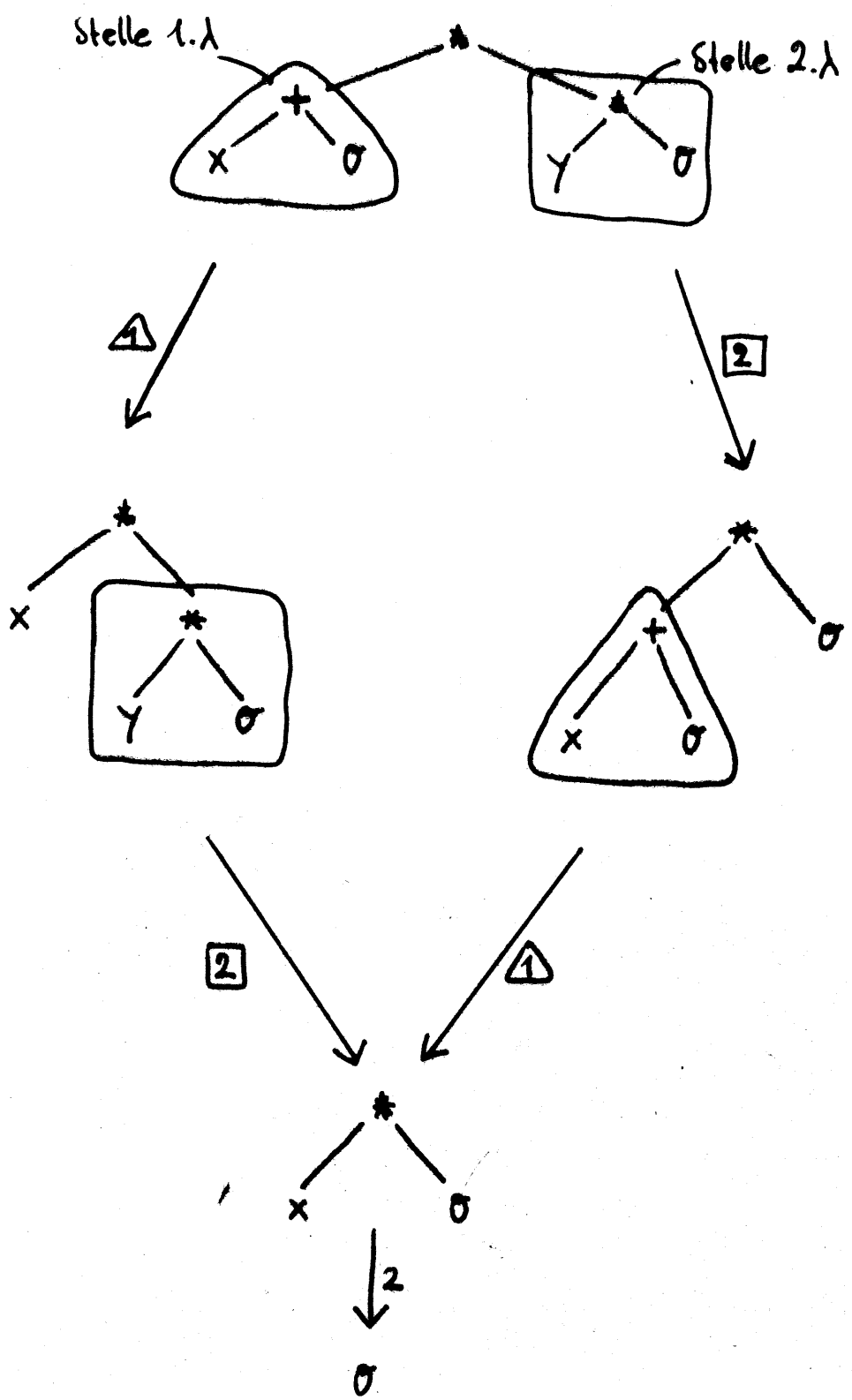
1) $x + 0 \rightarrow x$

2) $x * 0 \rightarrow 0$

3) $s(x) + y \rightarrow s(x+y)$

4) $x * (y+x) \rightarrow (x * y) + (x * x)$

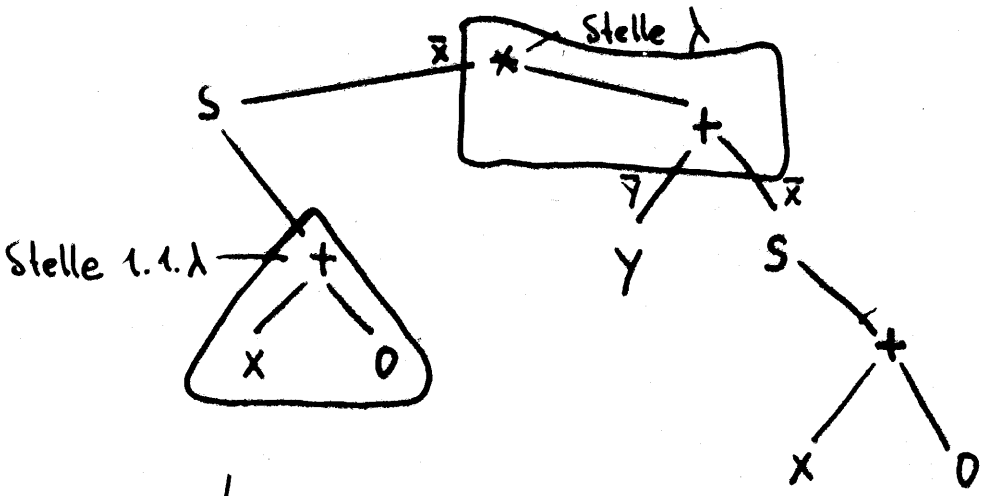
betrachte $(x + 0) * (y * 0)$



die Stellen
1.λ und 2.λ
△ □
sind unabhängig:

1.λ kein Anfang von 2.λ
2.λ kein Anfang von 1.λ

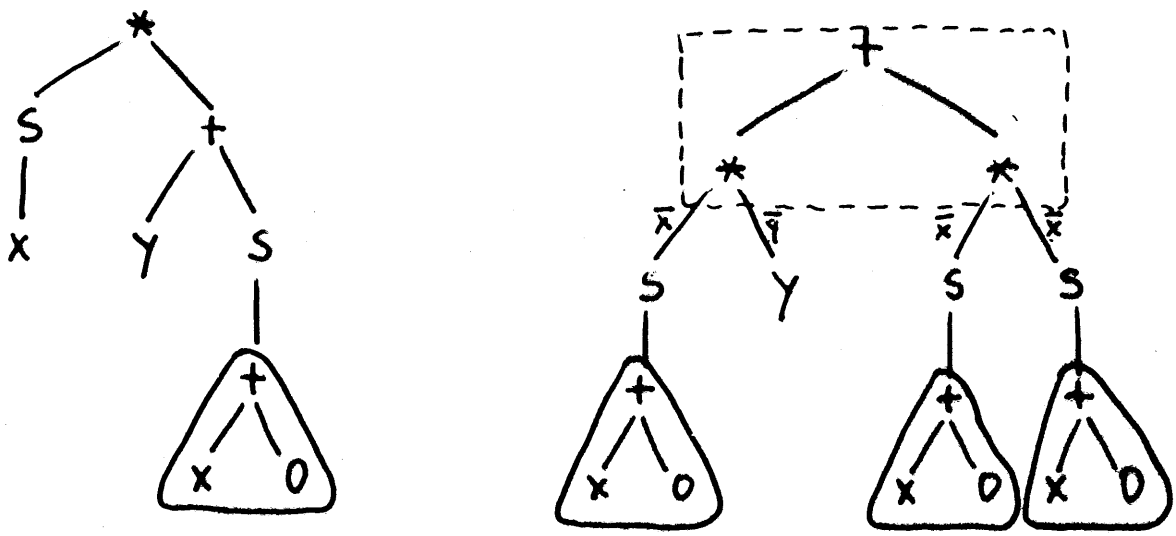
$$s(x+0) * (y + s(x+0))$$



die Stellen
λ und 1.1.λ
sind abhängig:
λ ist Anfang von 1.1.λ
aber: □ und △
überlappen sich nicht

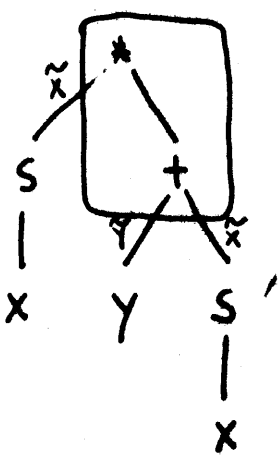
1

Ψ mit $\bar{x} = s(x+0)$
$\bar{y} = y$

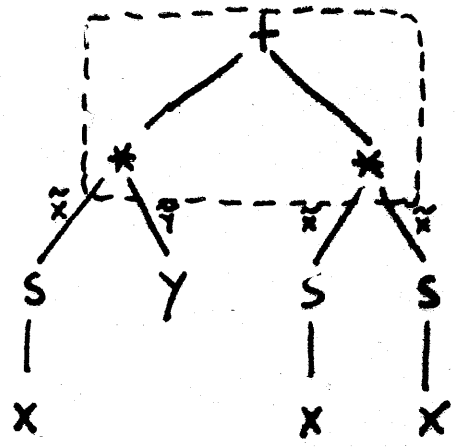


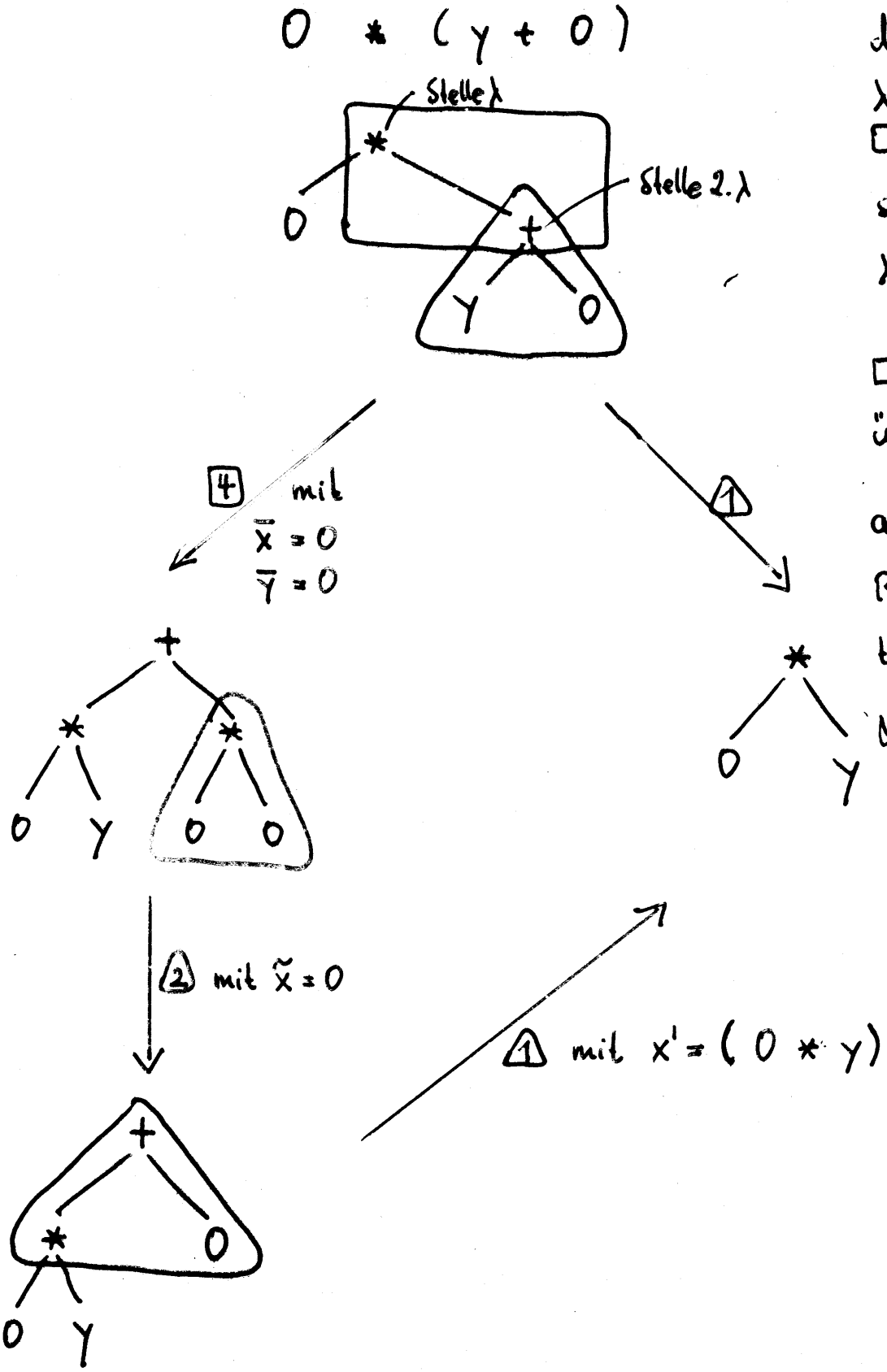
1

1 *



Ψ mit
$\tilde{x} = s(x)$
$\tilde{y} = y$



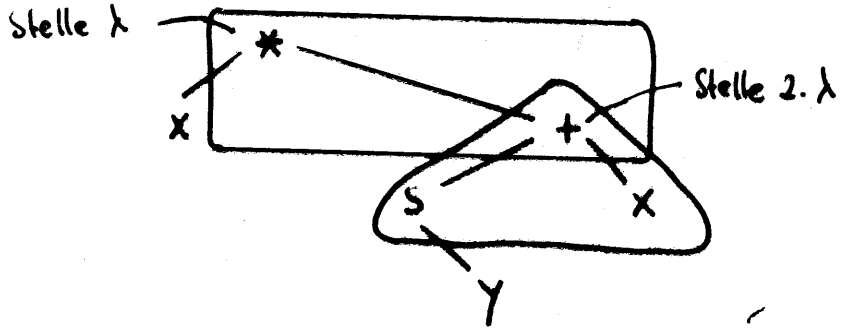


die Stellen
λ und 2.λ
□ △
sind abhängig:
λ ist Anfang von 2.λ;

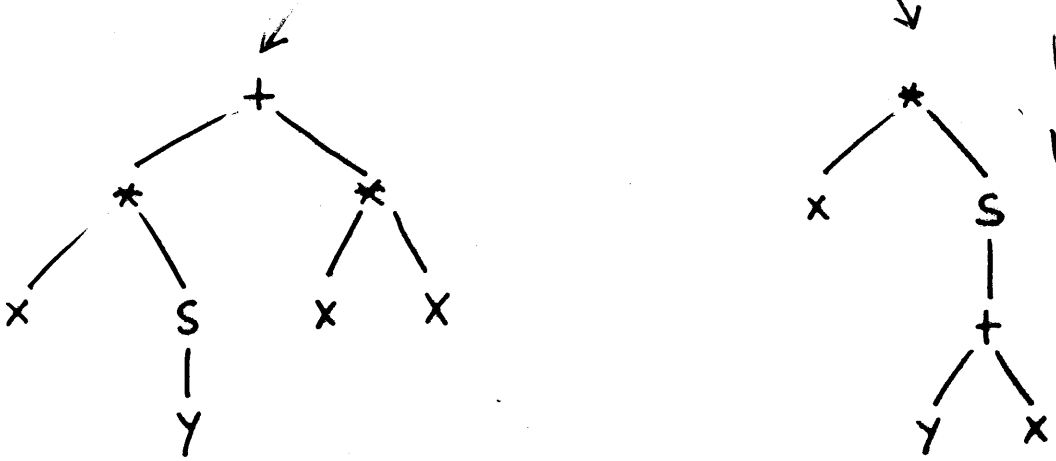
□ und △
überlappen sich;

aber: in diesem
Beispiel wird
trotzdem eindeutige
Normalform erreicht!

$x * (s(y) + x)$



die Stellen
λ und 2.λ
□ △
sind abhängig:
λ ist Anfang von 2.λ;
▭ und △
überlappen sich;
in diesem Beispiel
keine eindeutige
Normalform



in beiden Zweigen ist keine Regel mehr anwendbar:

also hat $x * (s(y)+x)$

zwei verschiedene Normalformen.

Definition [kritische Paare]

Sei R Termersetzungssystem,

$\ell_1 \to r_1$
$\ell_2 \to r_2$ Regeln aus R, o.B.d.A variablendisjunkt,

u eine Stelle in ℓ_1 mit:
ℓ_1 / u ist keine Variable;

σ mgu von ℓ_1 / u und ℓ_2.

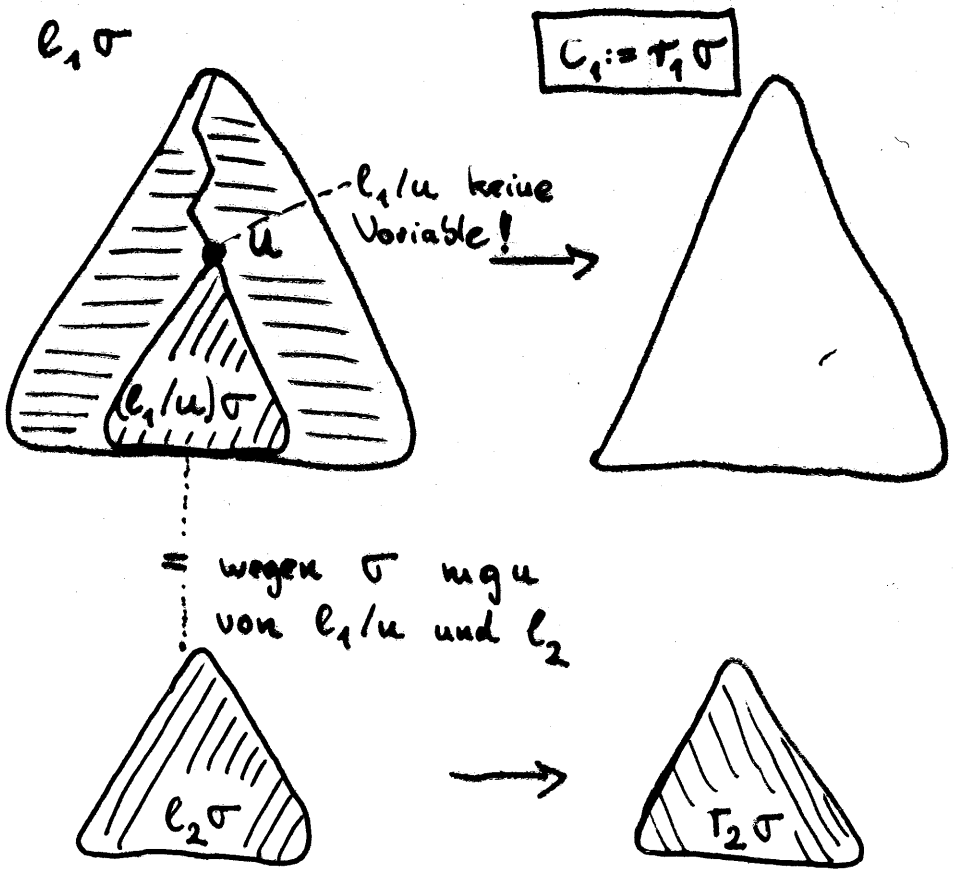
Dann heißt das Termpaar (c_1, c_2) mit

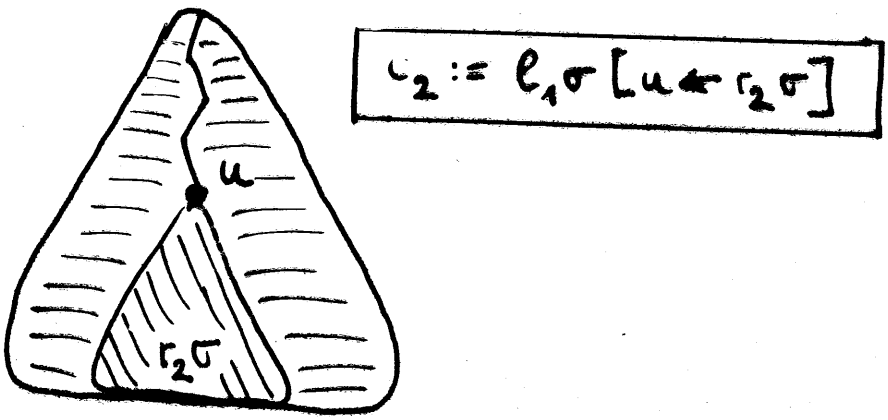
(1) $c_1 := r_1 \sigma$

(2) $c_2 := \ell_1 [u \leftarrow r_2] \sigma = \ell_1 \sigma [u \leftarrow r_2 \sigma]$

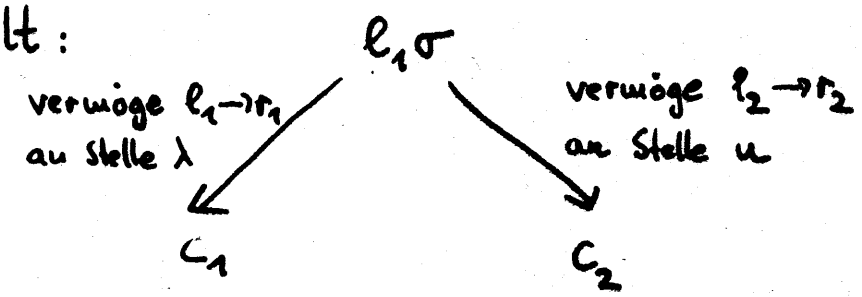
kritisches Paar bzg. R,
entstanden aus Überlagerung

von $\ell_2 \to r_2$
auf $\ell_1 \to r_1$
an der Stelle u.





offensichtlich gilt:



wir werden zeigen: es reicht, lokale Konfluenz für solche kritischen Paare zu verlangen

altes Beispiel:

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x) + y \to s(x + y)$

(4) $x * (y + x) \to (x * y) + (x * x)$

altes Beispiel:

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x) + y \to s(x+y)$

(4) $x * (y+x) \to (x*y) + (x*x)$

Überlagerung von (1) $z + 0 \to z$

auf (3) $s(x)+y \to s(x+y)$

an der Stelle λ

ergibt mit mgu $\sigma = \begin{bmatrix} z & y \\ s(x) & 0 \end{bmatrix}$

von $s(x)+y\,/\lambda = s(x)+y$

und $z + 0$

kritisches Paar

$c_1 = s(x+y)\,\sigma = s(x+0)$

$c_2 = s(x)+y\,[\lambda \leftarrow z]\,\sigma$

$= z\,\sigma$

$= s(x)$

altes Beispiel:

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x) + y \to s(x + y)$

(4) $x * (y + x) \to (x * y) + (x * x)$

Überlagerung von (3) $s(x)+y \to s(x+y)$

auf (1) $z+0 \to z$

an der Stelle λ

ergibt mit mgu $\sigma = \begin{bmatrix} z & y \\ s(x) & 0 \end{bmatrix}$

von $z+0/\lambda = z+0$

und $s(x)+y$

kritisches Paar

$c_1 = z\sigma = s(x)$

$c_2 = z+0\,[\lambda \leftarrow s(x+y)]\,\sigma$

$= s(x+y)\,\sigma$

$= s(x+0)$

altes Beispiel:

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x) + y \to s(x + y)$

(4) $x * (y + x) \to (x * y) + (x * x)$

Überlagerung von (1) $z + 0 \to z$

auf (4) $x * (y+x) \to (x * y) + (x * x)$

an der Stelle $2.\lambda$

ergibt mit mgu $\sigma = \begin{bmatrix} z & x \\ y & 0 \end{bmatrix}$

von $x * (y+x) / 2.\lambda = y + x$

und $z + 0$

kritisches Paar

$$c_1 = (x * y) + (x * x)\,\sigma$$
$$= (0 * y) + (0 * 0)$$

$$c_2 = x * (y + x)\,[2.\lambda \leftarrow z]\,\sigma$$
$$= (x * z)\,\sigma$$
$$= 0 * y$$

altes Beispiel:

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x) + y \to s(x + y)$

(4) $x * (y + x) \to (x * y) + (x * x)$

Überlagerung von (3) $s(z) + w \to s(z + w)$

auf (4) $x * (y + x) \to (x * y) + (x * x)$

an der Stelle $2.\lambda$

ergibt mit mgu $\sigma = \begin{bmatrix} y & x \\ s(z) & w \end{bmatrix}$

von $x * (y + x) \,/\, 2.\lambda = y + x$

und $s(z) + w$

kritisches Paar

$$c_1 = (x * y) + (x * x)\ \sigma$$

$$= (w * s(z)) + (w * w)$$

$$c_2 = x * (y + x)\ [2.\lambda \leftarrow s(z + w)]\ \sigma$$

$$= x * s(z + w)\ \sigma$$

$$= w * s(z + w)$$

altes Beispiel:

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x) + y \to s(x + y)$

(4) $x * (y + x) \to (x * y) + (x * x)$

hat kritische Paare:

c_1	c_2
$s(x+0)$	$s(x)$
$s(x)$	$s(x+0)$
$(0*y)+(0*0)$	$0*y$
$(w * s(z)) + (w*w)$	$w * s(z+w)$

denn es gibt keine weiteren

Unifikationen von linker Regelseite l_2

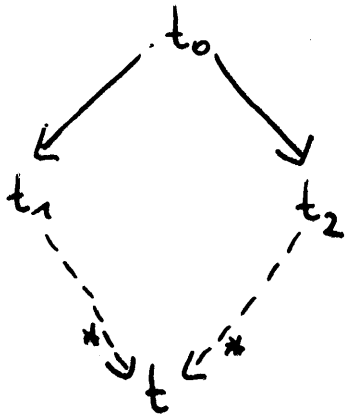
, mit Unterterme von linker Regelseite l_1

(außer den trivialen!)

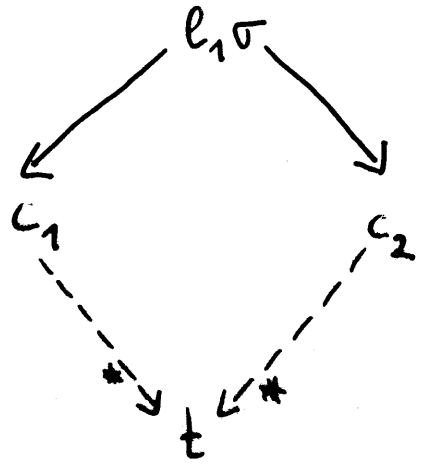
Satz 6.23 Sei R Termersetzungssystem. Dann gilt

R ist lokal konfluent gdw für alle kritischen Paare (c_1, c_2) bzg. R, entstanden aus Überlagerung von $l_2 \to r_2$ auf $l_1 \to r_1$ an der Stelle u mit mgu σ,

für alle t_0, t_1, t_2 mit $t_0 \to t_1$, $t_0 \to t_2$ ex. ein Term t mit



ex. ein Term t mit



es reicht also, lokale Konfluenz nur für kritische Paare zu prüfen

Beweis: "⇒": Sei (c_1, c_2) kritisches Paar,

entstanden aus
Überlagerung von $\ell_2 \to r_2$
auf $\ell_1 \to r_1$
an der Stelle u
mit mgu σ,

d.h.

(1) $c_1 = r_1\sigma$,

(2) $c_2 = \ell_1[u \leftarrow r_2]\sigma = \ell_1\sigma[u \leftarrow r_2\sigma]$.

Dann gilt:

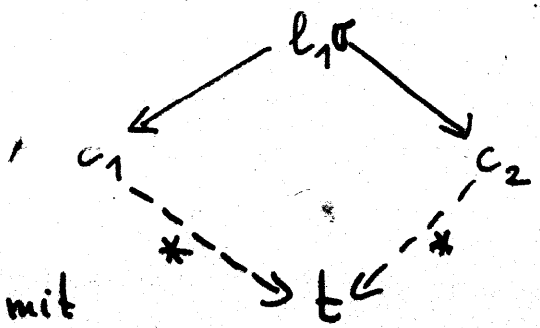
(3) $\ell_1\sigma \to r_1\sigma$ wende für Stelle λ von $\ell_1\sigma$ die Regel $\ell_1 \to r_1 \in R$ mit Substitution σ an:

1) $\ell_1\sigma / \lambda = \ell_1\sigma$

2) $r_1\sigma = \ell_1\sigma[u \leftarrow r_1\sigma]$

(4) $\ell_1\sigma \to \ell_1\sigma[u \leftarrow r_2\sigma]$ wegen $\ell_2 \to r_2 \in R$

Also:

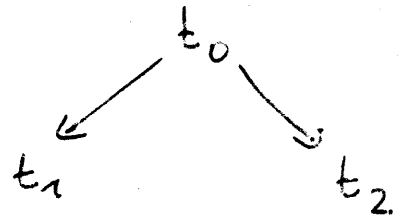


wegen (3), (1)
bzw. (4), (2)

ex. t mit wegen lokal konfluent

"$\Leftarrow$": Beweisidee entsprechend obigen Beispielen:

Sei



Fallunterscheidung nach Art des Entstehens von t_1, t_2 aus t_0:

Fall 1: Entstehung an unabhängigen Stellen.

Fall 2: Entstehung an abhängigen Stellen, aber ohne Überlappung der linken Regelseiten.

Fall 3: Entstehung an abhängigen Stellen mit Überlappung:

Gemäß Voraussetzung gilt:

ex. Stelle u_1 in t_0,
ex. Regel $\ell_1 \to r_1 \in R$,
ex. Substitution σ_1:

(1) $t_0 / u_1 = \ell_1 \sigma_1$

(2) $t_1 = t_0 [u_1 \leftarrow r_1 \sigma_1]$

ex. Stelle u_2 in t_0,
ex. Regel $\ell_2 \to r_2 \in R$,
ex. Substitution σ_2:

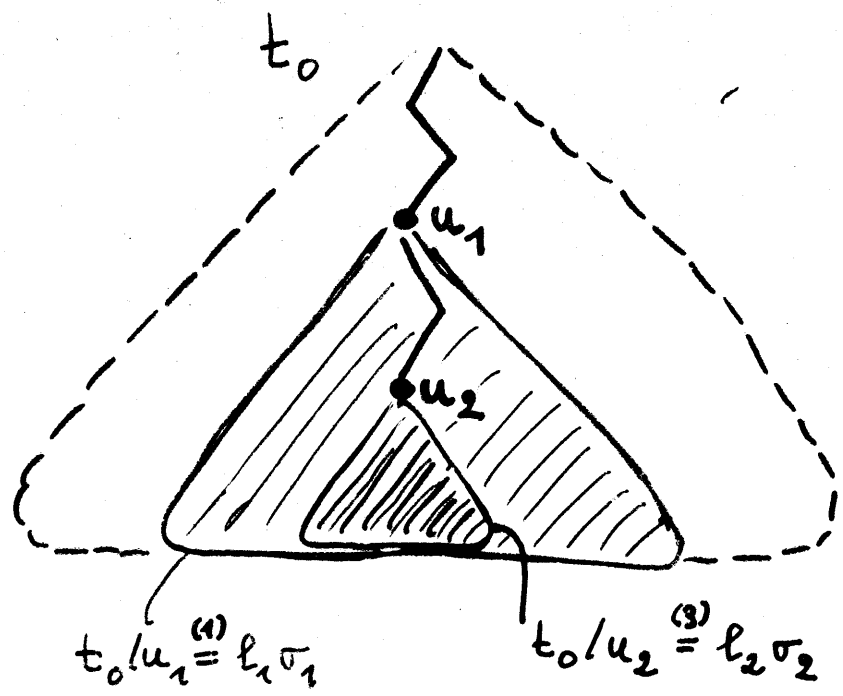
(3) $t_0 / u_2 = \ell_2 \sigma_2$

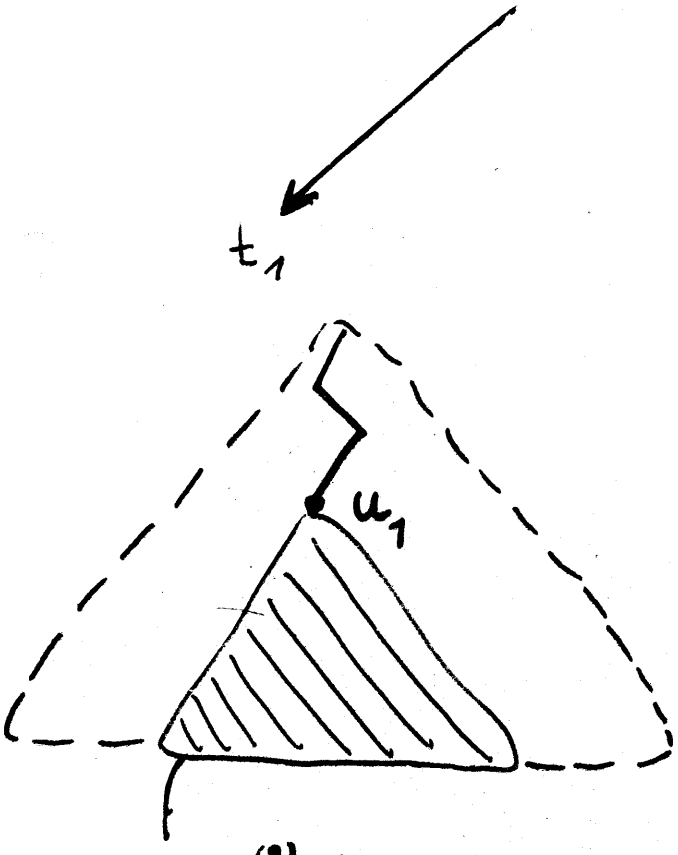
(4) $t_2 = t_0 [u_2 \leftarrow r_2 \sigma_2]$

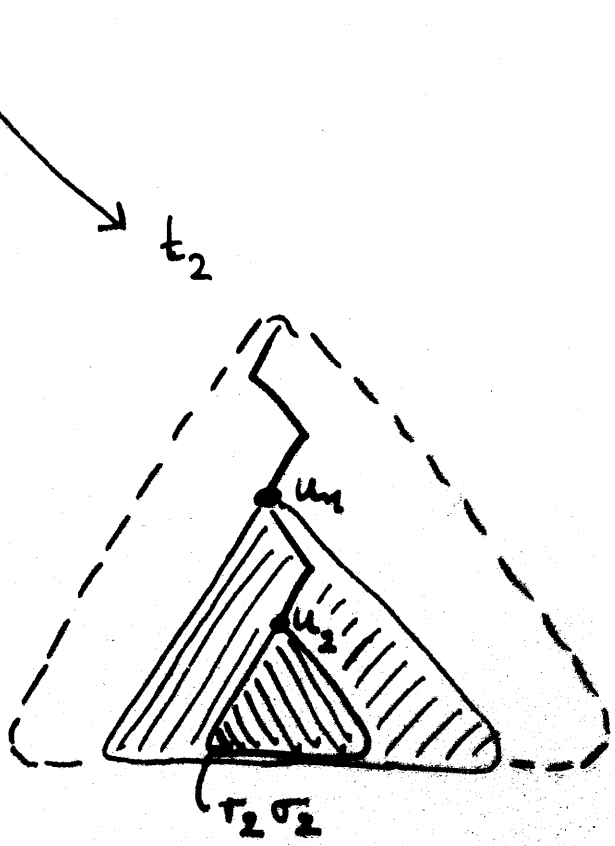
gemäß Fallannahme: Entstehung an abhängigen Stellen

also (o.B.d.A): u_1 ist Anfang von u_2

also liegt folgende Situation vor:







(5) $t_2/u_1 \overset{(4)}{=} t_0/u_1\,[\bar{u}_2 \leftarrow r_2\sigma_2] \overset{(1)}{=} l_1\sigma_1\,[\bar{u}_2 \leftarrow r_2\sigma_2]$

(6) $t_2 = t_0\,[u_1 \leftarrow l_1\sigma_1\,[\bar{u}_2 \leftarrow r_2\sigma_2]]$

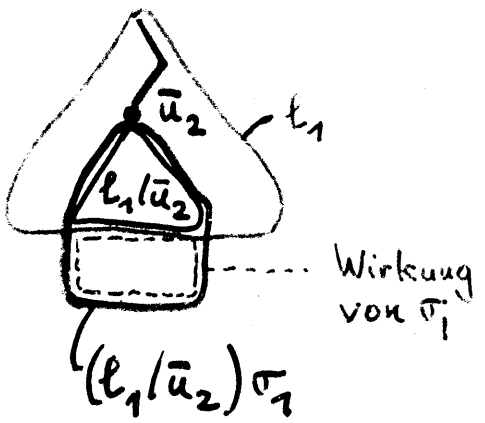
Dabei ist $\bar{u}_2$ das "Endstück von u_2 ab u_1".

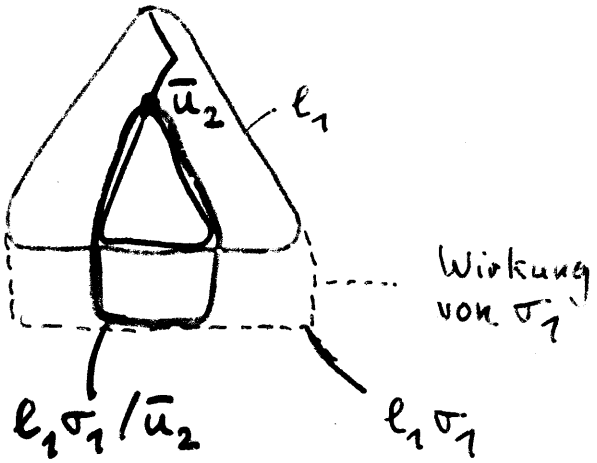
Beh: $l_1 / \bar{u}_2$ und l_2 sind unifizierbar.

Beweis: $l_2 \sigma_2 \overset{(3)}{=} t_0 / u_2$

$\overset{(1)}{=} l_1 \sigma_1 / \bar{u}_2$

$= (l_1 / \bar{u}_2)\, \sigma_1$





Seien dann o.B.d.A l_1 und l_2 variablendisjunkt.

Dann folgt: $l_2 (\sigma_1 \cup \sigma_2) = (l_1 / \bar{u}_2)(\sigma_1 \cup \sigma_2)$

↑ o.B.d.A. wirkungslos — ↑ o.B.d.A. wirkungslos

also: $\sigma_1 \cup \sigma_2$ ist Unifikator

Sei dann σ mgu von $l_1 / \bar{u}_2$ und l_2

und $\sigma_1 \cup \sigma_2 = \dot{\sigma}\, \tilde{\sigma}$ (7)

Wir betrachten dann das kritische Paar (c_1, c_2) mit

(8) $\quad c_1 := r_1 \sigma$

(9) $\quad c_2 := l_1 \sigma [\bar{u}_2 \leftarrow r_2 \sigma]$

Gemäß Voraussetzung: ex. t mit

(10) $\quad c_1 \xrightarrow{*} t$

(11) $\quad c_2 \xrightarrow{*} t$

Dann folgt:

(12) $\quad r_1 \sigma_1 \overset{(7)}{=} r_1 \sigma \tilde{\sigma} \overset{(8)}{=} c_1 \tilde{\sigma} \overset{(10)}{\xrightarrow{*}} t \tilde{\sigma}$

(13) $\quad l_1 \sigma_1 [\bar{u}_2 \leftarrow r_2 \sigma_2] \overset{(7)}{=} l_1 \sigma \tilde{\sigma} [\bar{u}_2 \leftarrow r_2 \sigma \tilde{\sigma}]$

$= \left(l_1 \sigma [\bar{u}_2 \leftarrow r_2 \sigma] \right) \tilde{\sigma}$

$\overset{(9)}{=} c_2 \tilde{\sigma}$

$\overset{(10)}{\xrightarrow{*}} t \tilde{\sigma}$

Wegen (2) und (12): $\quad t_1 \xrightarrow{*} t_0 [u_1 \leftarrow t \tilde{\sigma}]$

Wegen (6) und (13): $\quad t_2 \xrightarrow{*} \underbrace{t_0 [u_1 \leftarrow t \tilde{\sigma}]}$

dies ist das gesuchte Element!

(1) $x + 0 \to x$

(2) $x * 0 \to 0$

(3) $s(x)+y \to s(x+y)$

(4) $x * (y+x) \to (x * y) + (x * x)$

hat <u>kritische Paare</u> mit <u>beteiligten Regeln</u>,

wobei die angegebenen Ableitungen möglich sind:

$s(x+0) \xrightarrow{(1)} \boxed{s(x)}$ in Normalform — (1) auf (3) (und umgekehrt)

$(0*y)+(0*0) \xrightarrow{(2)} (0*y)+0 \xrightarrow{(1)} \boxed{0*y}$ in Normalform — (1) auf (4)

$\boxed{(w * s(z))+(w*w)}$ in Normalform $\quad \boxed{w * s(z+w)}$ in Normalform — (3) auf (4)

also gemäß Satz 6.23:

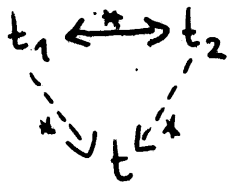
- (1), (2), (3), (4) nicht lokal konfluent
- (1), (2), (3) lokal konfluent
- (1), (2), (4) lokal konfluent

Korollar 6.24 Sei R terminierendes Termersetzungssystem. Dann sind äquivalent:

R Church-Rosser

6.16 ⇕ f.alle Ersetzungssysteme

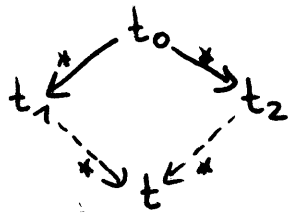
f.alle t_1, t_2 ex. t:



R konfluent

6.11 ⇕ terminierend

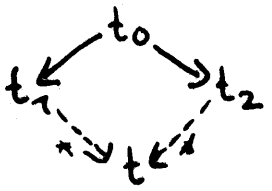
f. alle t_0, t_1, t_2 ex. t:



R Lokal konfluent

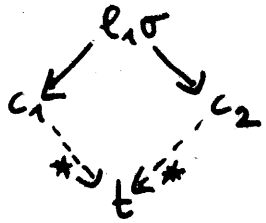
6.23 ⇕ Termersetzungssystem

f. alle t_0, t_1, t_2 ex. t:



R für kritische Paare konfluent

f. alle kritischen Paare (c_1, c_2) entstanden aus ... $\ell_1 \to \sigma_1$ ... mit σ ex. t:



Korollar 6.25

Ist R ein terminierendes
Termersetzungssystem
mit endlich vielen Regeln,

dann ist die Konfluenz von R entscheidbar.

Beweis: Dies ist ein Entscheidungsverfahren für Konfluenz:

1. Bestimme alle kritischen Paare (c_1, c_2).

   [Da R endlich ist, gibt es nur endlich viele kritische Paare, die sich effektiv berechnen lassen.]

2. Für jedes kritische Paar (c_1, c_2):

   teste, ob $\text{Normalformen}(c_1) \cap \text{Normalformen}(c_2) \neq \emptyset$.

   [Da R endlich und terminierend ist, hat jeder c_i nur endlich viele Normalformen, die sich effektiv berechnen lassen.]

3. Falls alle Durchschnitte nichtleer : konfluent;
   sonst : nicht konfluent.

   [Da R Termersetzungssystem, liefert Satz 6.23 die Entscheidung.]

Problem: Wie kann man erkennen,

daß ein Termersetzungssystem R

terminierend ist ?

es gibt keine unendliche Folge

$t_0, t_1, t_2, \ldots$ aus der Termmenge mit

$t_0 \to t_1 \to t_2 \to \ldots$

Ein Ersetzungssystem $R = (T, \rightarrow)$ heißt

terminierend : gdw es keine unendliche Folge $t_0, t_1, t_2, \ldots$ aus T gibt mit

$$t_0 \rightarrow t_1 \rightarrow t_2 \rightarrow \ldots$$

Beispiele:

1. Das durch die Regel $f(x) \rightarrow x$ definierte Termersetzungssystem ist terminierend:

   jede Regelanwendung vermindert die Anzahl der Funktionszeichen

2. Das durch die Regeln $a \rightarrow b$, $b \rightarrow a$ definierte Termersetzungssystem ist nicht terminierend:

   $a \rightarrow b \rightarrow a \rightarrow b \rightarrow \ldots$
   ist eine unendliche Folge

Lemma 7.2

Sei $R = (T_\Sigma(V), \to)$ ein Termersetzungssystem.

R ist terminierend gdw

es keine unendliche Folge
$\tilde{t}_0, \tilde{t}_1, \tilde{t}_2, \ldots$ von Grundtermen aus $T_\Sigma(V)$
gibt mit $\tilde{t}_0 \to \tilde{t}_1 \to \tilde{t}_2 \to \ldots$

Beweis:

"$\Rightarrow$": trivial

"$\Leftarrow$"

falls $t_0 \to t_1 \to t_2 \to \ldots$ aus beliebigen Termen gebildet ist,

so kann man durch Grundsubstitution daraus eine Folge $\tilde{t}_0 \to \tilde{t}_1 \to \tilde{t}_2 \to \ldots$ von Grundtermen gewinnen

Satz 7.5

Sei $R = (T_\Sigma(V), \rightarrow)$ ein Termersetzungssystem.

R ist terminierend gdw

es gibt eine

monotone, f. alle Terme r, s, t,
f. alle Zahlen i gilt:

$$s > t \Rightarrow \underbrace{r[i.\lambda \leftarrow s]}_{f(\ldots, s, \ldots)} > \underbrace{r[i.\lambda \leftarrow t]}_{f(\ldots, t, \ldots)}$$

fundierte es gibt keine unendlichen absteigenden Ketten

Ordnung $>$ auf $T_\Sigma(V)$ irreflexiv, transitiv

mit

$l\sigma > r\sigma$ f. alle Regeln $l \rightarrow r$ aus R,
f. alle (Grund-) Substitutionen σ

(es reicht also, alle Beispiele der Regeln zu untersuchen)

Beweis:

"$\Rightarrow$": $\xrightarrow[R]{+}$ hat die gewünschten Eigenschaften:

irreflexiv, transitiv	:	Def $\xrightarrow[R]{+}$
monoton	:	Lemma 6.5
fundiert	:	R terminierend

"$\Leftarrow$" Sei $>$ Terminationsordnung, d.h. $>$ hat die angegebenen Eigenschaften

<u>zu zeigen:</u> $l\sigma > r\sigma$ f. alle $l \to r$ aus R f. alle Substitutionen σ $\overset{!}{\Longrightarrow}$ $s \to_R t \Rightarrow s > t$ f. alle $s,t \in T_\Sigma(V)$

$\Longrightarrow$ R terminierend

$>$ fundiert

<u>Bew:</u> sei $s \to_R t$, d.h. ex. Stelle u in s

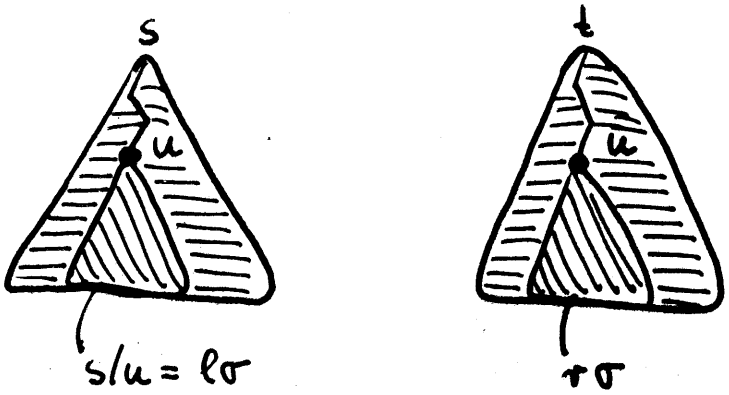
Regel $l \to r$ aus R

Substitution σ mit

1) $s/u = l\sigma$

2) $s[u \leftarrow r\sigma] = t$

<u>also:</u>



$s = s[u \leftarrow l\sigma]$ $\quad$ $t = s[u \leftarrow r\sigma]$

nach Voraussetzung: $l\sigma > r\sigma$

$>$ monoton : $s > t$

(mit Induktion)

Hilfssatz:

R **monoton**, d.h. f. alle Terme r, s, t,
f. alle Zahlen i gilt:

$$s > t \Rightarrow r[i.\lambda \leftarrow s] > r[i.\lambda \leftarrow t]$$

$\overset{!}{\Longrightarrow}$

f. alle Terme r, s, t
f. alle Stellen u gilt:

$$s > t \Rightarrow r[u \leftarrow s] > r[u \leftarrow t]$$

Beweis: Induktion über u:

$u = \lambda$: trivial, denn

$$r[\lambda \leftarrow s] = s \underset{\uparrow}{>} t = r[\lambda \leftarrow t]$$

Voraussetzung

$u = i.\tilde{u}$: betrachte $r_i := r/i.\lambda$

nach Ind. Annahme: $r/i.\lambda[\tilde{u} \leftarrow s] > r/i.\lambda[\tilde{u} \leftarrow t]$

dann gilt:

$$r[i.\tilde{u} \leftarrow s]$$

$$= r[i.\lambda \leftarrow r/i.\lambda[\tilde{u} \leftarrow s]]$$

Ind.Ann. / Monotonie: $$> r[i.\lambda \leftarrow r/i.\lambda[\tilde{u} \leftarrow t]]$$

$$= r[i.\tilde{u} \leftarrow t]$$

Korollar 7.7

Sei $R = (T_\Sigma(V), \to)$ ein Termersetzungssystem.

R ist terminierend gdw

es gibt (eine Terminierungsfunktion)
$\Gamma: T_\Sigma(V) \to W$ mit:

- W ist fundierte Ordnung
- f. alle Terme r, s, t gilt:

$$\Gamma(s) > \Gamma(t) \Rightarrow \Gamma(r[i.\lambda \leftarrow s]) > \Gamma(r[i.\lambda \leftarrow t])$$

- $\Gamma(l\sigma) > \Gamma(r\sigma)$ f. alle Regeln $l \to r$ aus R,
  f. alle (Grund-) Substitutionen σ

Beweis:

"$\Rightarrow$": Satz 7.5 mit $\Gamma := id_{T_\Sigma(V)}$

"$\Leftarrow$": Satz 7.5 mit $s > t$: gdw $\Gamma(s) > \Gamma(t)$

Beispiele:

$\Gamma_1(t)$:= Anzahl Operationssymbole in t

$\Gamma_2(t)$:= Anzahl Blätter (im Termbaum) von t

a) betrachte Regel

$$\overbrace{g(f(f(x)), a, f(f(x)))}^{=:\ell} \rightarrow \underbrace{g(a, g(x,a,x), a)}_{=:r}$$

$\Gamma_1(\ell) = 6$
$\Gamma_1(r) = 5$
} Γ_1 als Terminierungsfunktion geeignet

$\Gamma_2(\ell) = 3$
$\Gamma_2(r) = 5$
} Γ_2 als Terminierungsfunktion nicht geeignet

b) betrachte Regel

$$g(a, g(x,a,x), a) \rightarrow g(f(f(x)), a, f(f(x)))$$

Γ_1 als Terminierungsfunktion nicht geeignet

Γ_2 als Terminierungsfunktion geeignet