Inferenzmethoden

Teil IV

Jenseits von Prädikatenlogik

Klassische Prädikatenlogik ist oft zu einfach

- **Universelle Sprache mit sehr wenigen Vorgaben**
  – Man kann sehr viel damit beschreiben
  – Nur die logischen Konnektive haben eine feste Bedeutung
  – Es gibt keine Unterstützung für vordefinierte Begriffe
- **Viele Anwendungen benötigen andersartige Logiken**
  – Zusätzliche logische Konnektive oder andere Bedeutung
- **Es gibt viele grundlegende mathematische Konzepte**
  – Gleichheit von Werten, Zahlen, Datenstrukturen
- **Wie kann man Beweisverfahren entsprechend anpassen?**
  – Idealerweise als universelles Verfahren mit spezifischen Modulen

Forschungsnahe Thematik mit viel Spezialliteratur

Logiken jenseits der klassischen Prädikatenlogik

- **Konstruktive Logik: mehr als nur Wahrheit**
  - Interpretiere logische Symbole als Konstruktion eines Nachweises
  - Gut verwendbar als Logik der Berechnung und Programmierung
  - Ursprünglicher Name: Intuitionistische Logik
- **Modallogiken: zusätzliche Quantoren $\Diamond$, $\Box$**
  - Ist Gültigkeit einer Aussage möglich oder zwingend notwendig?
- **Logik höherer Stufe: freie Quantifizierung**
  - Formeln dürfen auch über Funktionen und Prädikate quantifizieren
- **Lineare Logik: andere Strukturregeln**
  - Formeln können in Argumenten nicht mehrfach verwendet werden
  - Gut als Logik von Resourcen
- **... und noch vieles mehr**
  - Nichtmonotone, Relevanz-, Beschreibungs-, Temporallogik, ...
  - Kombinationen: konstruktive Logik höherer Stufe, Typentheorie, ...

Voraussetzungen für nichtklassisches Beweisen

- **Normalformen sind nicht immer möglich**
  - In konstruktiver Logik ist jede Formel in DNF ungültig
    - Eine Klausel müsste, für sich alleine betrachtet, gültig sein
  - In linearer Logik gibt es mehrere Konjunktionsbegriffe
- **Beweise müssen mehr Information enthalten**
  - In konstruktiver Logik enthalten Beweise algorithmische Lösungen
  - In Modallogiken entstehen gesicherte Aussagen aus Möglichkeiten
  - Lineare Logik beschreibt die Verarbeitung von Ressourcen
- **Konnektionsmethode muß erweitert werden**
  - Beweissuchverfahren für Nichtnormalform-Matrizen
  - Verwaltung logik-spezifischer Zusatzinformation in den Literalen und Verallgemeinerung des Komplementaritätsbegriffs
  - Komplementaritätstest mit erweiterten Unifikationsverfahren

Inferenzmethoden

Einheit 12

Konstruktive Logik

1. Unterschiede zur klassischen Logik
2. Intuitionistische Präfixe
3. Erweiterung des Extensionsverfahrens

Intuitionistische Logik im Überblick

- **Konstruktiver Begriff von Beweisbarkeit** (**Logik des Rechnens**)
  - F ist gültig, wenn ein expliziter Nachweis konstruiert werden kann
    Aussschluß des Gegenteils (F kann nicht falsch sein) reicht nicht
  - Führt zu anderer Interpretation von $\vee$, $\Rightarrow$, $\exists$
  - Unterstützt Repräsentation und Ausführung von Algorithmen
- **Beweise haben größere Aussagekraft**
  - Jede intuitionistisch gültige Formel ist auch klassisch gültig
  - Umkehrung gilt nicht: $P \vee \neg P$ **ist kein Theorem**
- **Gödel-Transformation τ bettet klassische Logik ein**
  - F klassisch gültig gdw. $\tau(F)$ intuitionistisch gültig
  - Umgekehrte Einbettung auf Umweg über Modallogiken
- **Mögliche Beweisverfahren**
  - (Interaktive gesteuerte) Sequenzen-/Tableauxkalküle
  - Klassisches Extensionsverfahren für transformierte Formel
  - Extensionsverfahren mit “konstruktiver Zusatzinformation”

Semantische Unterschiede zur klassischen Logik

- **Ursprüngliche Interpretation der logischen Konnektive**
  - $\iota(A \vee B)$ ist wahr, falls $\iota(A)$ = wahr oder $\iota(B)$ = wahr
  - $\iota(A \Rightarrow B)$ ist wahr, falls aus $\iota(A)$ = wahr immer $\iota(B)$ = wahr folgt
  - $\iota(\exists x\, A)$ ist wahr, falls $\iota_x^u(A)$ = wahr für ein $u \in \mathcal{U}$

  Klassisch ist $A \vee B \;\equiv\; \neg(\neg A \wedge \neg B)$, $\quad A \Rightarrow B \;\equiv\; \neg(A \wedge \neg B)$, $\quad \exists x\, A \;\equiv\; \neg(\forall x\, \neg A)$

- **Viele klassische Gesetze sind nicht konstruktiv**

  $\boldsymbol{A \vee \neg A}$ würde bedeuten, daß man jede Aussage entscheiden kann

  $\boldsymbol{\neg\neg A \Rightarrow A}$ heißt, daß jede nicht widerlegte Aussage wahr ist

  $\boldsymbol{\neg(\forall x\, \neg A) \;\Rightarrow\; \exists x\, A}$ heißt, daß man den Zeugen x für A kennt,
  wenn man weiß, daß A nicht immer falsch ist

- **Viele klassische Beweise sind unnötig unkonstruktiv**
  - *Es gibt zwei irrationale Zahlen x und y so daß x^y rational ist"*

    Beweis: Ist $\sqrt{2}^{\sqrt{2}}$ rational, dann wähle $x{=}y{=}\sqrt{2}$, sonst $x{=}\sqrt{2}^{\sqrt{2}}$, $\;y{=}\sqrt{2}$
  - Am Ende des Beweises sind x und y nach wie vor unbekannt

WAS LÄUFT "FALSCH" IN KLASSISCHEN BEWEISEN?

- **Block Tableaux für konstruktiv ungültige Formeln**

$$A \vee \neg A^F \;\big|\; A^F,\ \neg A^F \;\big|\; A^F,\ A^T \;\big|\; \times$$

$$\neg\neg A \Rightarrow A^F \;\big|\; \neg\neg A^T,\ A^F \;\big|\; \neg A^F,\ A^F \;\big|\; A^T,\ A^F \;\big|\; \times$$

$$\neg(\forall x\, \neg A) \Rightarrow \exists x\, A^F \;\big|\; \neg(\forall x\, \neg A)^T,\ \exists x\, A^F \;\big|\; (\forall x\, \neg A)^F,\ \exists x\, A^F \;\big|\; \neg A[a/x]^F,\ \exists x\, A^F \;\big|\; \neg A[a/x]^F,\ A[a/x]^F \;\big|\; A[a/x]^T,\ A[a/x]^F \;\big|\; \times$$

  – Manche Beweisknoten enthalten zwei mit ^{F} markierte Formeln

  – Beweis verfolgt eine von zwei alternativen Beweisbehauptungen und "zeigt" anschließend die andere

- **Konstruktive Beweise müssen eine Behauptung verfolgen**

  – Kalkül darf nur eine mit ^{F} markierte Formel zulassen

  – Regeln müssen modifiziert werden und ggf. ^{F}-Formeln fallen lassen

Kalküle für Intuitionistische Logik

Block Tableau		Refinement Logik	
T	F	$-L$	$-R$
$\dfrac{S,A\wedge B^T}{S,A^T,\ B^T}$	$\dfrac{S,A\wedge B^F}{S,A^F \mid S,B^F}$	$\dfrac{H,\ A\wedge B\vdash C}{H,\ A,\ B\vdash C}$	$\dfrac{H\vdash A\wedge B}{H\vdash A \mid H\vdash B}$
$\dfrac{S,A\vee B^T}{S,A^T \mid S,B^T}$	$\dfrac{S,A\vee B^F}{S,A^F \ \textit{oder}\ S,B^F}$	$\dfrac{H,\ A\vee B\vdash C}{H,A\vdash C \mid H,B\vdash C}$	$\dfrac{H\vdash A\vee B}{H\vdash A\ \textit{oder}\ H\vdash B}$
$\dfrac{S,A\Rightarrow B^T}{\boldsymbol{S^T},A^F \mid S,B^T}$	$\dfrac{S,A\Rightarrow B^F}{S,A^T,B^F}$	$\dfrac{H,\ A\Rightarrow B\vdash C}{H\vdash A \mid H,B\vdash C}$	$\dfrac{H\vdash A\Rightarrow B}{H,A\vdash B}$
$\dfrac{S,\neg A^T}{\boldsymbol{S^T},A^F}$	$\dfrac{S,\neg A^F}{S,A^T}$	$\dfrac{H,\ \neg A\vdash C}{H\vdash A}$	$\dfrac{H\vdash \neg A}{H,\ A\vdash \mathsf{ff}}$
$\dfrac{S,\forall x A^T}{S,A[t/x]^T}$	$\dfrac{S,\forall x A^F}{S,A[a/x]^F}$	$\dfrac{H,\ \forall x A\vdash C}{H,\ A[t/x]\vdash C}$	$\dfrac{H\vdash \forall x A}{H\vdash A[a/x]}$
$\dfrac{S,\exists x A^T}{S,A[a/x]^T}$	$\dfrac{S,\exists x A^F}{S,A[t/x]^F}$	$\dfrac{H,\ \exists x A\vdash C}{H,\ A[a/x]\vdash C}$	$\dfrac{H\vdash \exists x A}{H\vdash A[t/x]}$
$\dfrac{S,X^T,X^F}{\times}$		$\dfrac{H,\ X\vdash X}{\times}$	
$\boldsymbol{S^T} = \{X^T \mid X^T\in S\}$		*H ist Menge von Formeln, C eine (Ziel-)formel*	

Beweisführung in konstruktiver Logik

- **Manche klassisch gültige Formel wird unbeweisbar**

  $A \vee \neg A$: Konstruktiver Beweis müsste entweder A oder $\neg A$ zeigen

  $\neg\neg A \Rightarrow A$: Bei Auflösung von $\neg\neg A^T$ geht das Beweisziel A^F verloren

$$\begin{array}{c} A \vee \neg A^F \\ | \\ A^F \\ | \\ ?? \end{array} \qquad \begin{array}{c} A \vee \neg A^F \\ | \\ \neg A^F \\ | \\ A^T \\ | \\ ?? \end{array} \qquad \begin{array}{c} \neg\neg A \Rightarrow A^F \\ | \\ \neg\neg A^T,\ A^F \\ | \\ \neg A^F \\ | \\ A^T \\ | \\ ?? \end{array}$$

  – Beide Formeln sind intuitionistisch nicht gültig

  – Auch DeMorgan-Regeln wie $\neg A \vee B \;\Leftrightarrow\; A \Rightarrow B$ gelten nicht

- **Manche konstruktiv gültige Formel benötigt neue Beweise**

  – Der klassisch naheliegenste Beweis ist nicht konstruktiv $\mapsto$ Folie 6

  – Die gleiche Schrittfolge führt im konstruktiven Beweis nicht zum Ziel

$$(S \wedge (\neg(T \Rightarrow R) \Rightarrow P)) \Rightarrow (\neg((P \Rightarrow Q) \wedge (T \Rightarrow R)) \Rightarrow (S \wedge \neg\neg P))$$

Klassischer (Block) Tableaux Beweis

$$(S \wedge (\neg(T \Rightarrow R) \Rightarrow P)) \Rightarrow (\neg((P \Rightarrow Q) \wedge (T \Rightarrow R)) \Rightarrow (S \wedge \neg\neg P))^F$$

$$S \wedge (\neg(T \Rightarrow R) \Rightarrow P)^T,\ \neg((P \Rightarrow Q) \wedge (T \Rightarrow R)) \Rightarrow (S \wedge \neg\neg P)^F$$

$$S \wedge (\neg(T \Rightarrow R) \Rightarrow P)^T, \neg((P \Rightarrow Q) \wedge (T \Rightarrow R))^T,\ S \wedge \neg\neg P^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T, \neg((P \Rightarrow Q) \wedge (T \Rightarrow R))^T,\ S \wedge \neg\neg P^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T,\ S \wedge \neg\neg P^F, (P \Rightarrow Q) \wedge (T \Rightarrow R)^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T,\ S \wedge \neg\neg P^F, P \Rightarrow Q^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T, P^T,\ S \wedge \neg\neg P^F, Q^F$$

$$\boxed{S^T}, \neg(T \Rightarrow R) \Rightarrow P^T, P^T,\ \boxed{S^F}, Q^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T, P^T,\ \neg\neg P^F, Q^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T, P^T, \neg P^T,\ Q^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T, \boxed{P^T},\ \boxed{P^F}, Q^F$$

$$S^T, \neg(T \Rightarrow R) \Rightarrow P^T,\ S \wedge \neg\neg P^F, T \Rightarrow R^F$$

$$S^T,\ \neg(T \Rightarrow R)^F, S \wedge \neg\neg P^F, T \Rightarrow R^F$$

$$S^T, \boxed{T \Rightarrow R^T},\ S \wedge \neg\neg P^F, \boxed{T \Rightarrow R^F}$$

$$S^T, P^T,\ S \wedge \neg\neg P^F, T \Rightarrow R^F$$

$$\boxed{S^T}, P^T,\ \boxed{S^F}, T \Rightarrow R^F$$

$$S^T, P^T,\ \neg\neg P^F, T \Rightarrow R^F$$

$$S^T, P^T, \neg P^T,\ T \Rightarrow R^F$$

$$S^T, \boxed{P^T},\ \boxed{P^F}, T \Rightarrow R^F$$

$(S\wedge(\neg(T\Rightarrow R)\Rightarrow P))\Rightarrow(\neg((P\Rightarrow Q)\wedge(T\Rightarrow R))\Rightarrow(S\wedge\neg\neg P))$

KONSTRUKTIVER BEWEISANSATZ

$(S\wedge(\neg(T\Rightarrow R)\Rightarrow P))\Rightarrow(\neg((P\Rightarrow Q)\wedge(T\Rightarrow R))\Rightarrow(S\wedge\neg\neg P))^F$

$S\wedge(\neg(T\Rightarrow R)\Rightarrow P)^T,\ \neg((P\Rightarrow Q)\wedge(T\Rightarrow R))\Rightarrow(S\wedge\neg\neg P)^F$

$S\wedge(\neg(T\Rightarrow R)\Rightarrow P)^T,\ \neg((P\Rightarrow Q)\wedge(T\Rightarrow R))^T,\ S\wedge\neg\neg P^F$

!! $S^T,\ \neg(T\Rightarrow R)\Rightarrow P^T,\ \neg((P\Rightarrow Q)\wedge(T\Rightarrow R))^T,\ S\wedge\neg\neg P^F$

$S^T,\ \neg(T\Rightarrow R)\Rightarrow P^T,\ (P\Rightarrow Q)\wedge(T\Rightarrow R)^F$

- $S^T,\ \neg(T\Rightarrow R)\Rightarrow P^T,\ P\Rightarrow Q^F$
  - $S^T,\ \neg(T\Rightarrow R)\Rightarrow P^T,\ P^T,\ Q^F$
    - !! $S^T,\ P^T,\ \neg(T\Rightarrow R)^F$
      - $S^T,\ P^T,\ T\Rightarrow R^T,\ \mathtt{ff}^F$
        - ???
    - $S^T,\ P^T,\ Q^F$
      - ???
- $S^T,\ \neg(T\Rightarrow R)\Rightarrow P^T,\ T\Rightarrow R^F$
  - !! $S^T,\ \neg(T\Rightarrow R)^F$
    - $S^T,\ T\Rightarrow R^T,\ \mathtt{ff}^F$
      - $S^T,\ R^T,\ T^F$
        - ???
  - $S^T,\ P^T,\ T\Rightarrow R^F$
    - $S^T,\ P^T,\ T^T,\ R^F$
      - ???

$\neg^T$ und $\Rightarrow^T$ "zerstören" bisherige ^{F}-Formeln (Ziele)

– Einige der nachfolgenden Regeln sind nicht mehr anwendbar

– Ursprünglicher klassischer Beweis ist nicht konstruktiv durchführbar

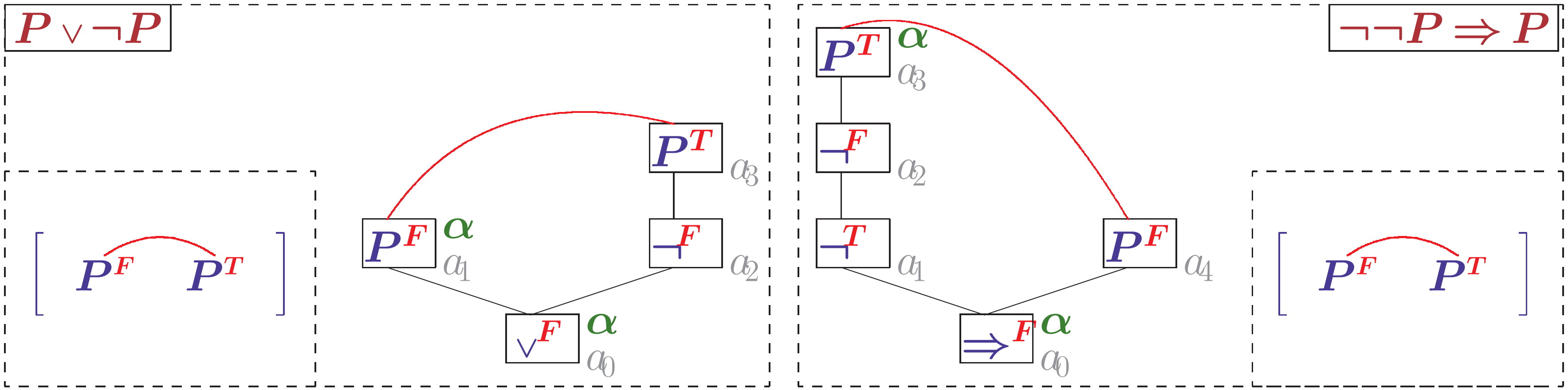
– Eine andere Beweisreihenfolge führt dagegen zum Erfolg $\mapsto$ Übung

Warum sind konstruktive Beweise komplizierter?

- **Beweise konzentrieren sich auf eine Zielaussage**
  – Klassische Beweise dürfen mitten im Beweis das Ziel wechseln
- **Manche Beweisregeln sind destruktiv**
  – Anwendung der Regeln $\neg^T$ und $\Rightarrow^T$ entfernt Informationen, die im klassischen Beweis erhalten blieben
  – Nachfolgende Regeln können diese Formeln nicht mehr verwenden
  – Beweis ist evtl. möglich, wenn $\neg^T$ und $\Rightarrow^T$ später angewandt werden
- **Der intuitionistische Beweiskalkül ist nicht konfluent**
  – Reihenfolge der Regelanwendungen ist wichtig
- **Intuitionistisches Extensionsverfahren wird aufwendiger**
  – Suche nach Konnektionen identifiziert nur beweisrelevante Formelteile
  – Zusätzlich muß Reihenfolge der Regelanwendungen bestimmt werden, die einen Beweis ohne Verwendung mehrerer ^{F}-Formeln ermöglicht
  – Matrixcharakterisierung der Gültigkeit ist entsprechend zu erweitern
  – Beweisverfahren muß zusätzliche Mechanismen bereitstellen

Matrixcharakterisierung konstruktiver Beweise

Was unterscheidet $P\vee\neg P$ und $\neg\neg P\Rightarrow P$ von $P\Rightarrow P$?

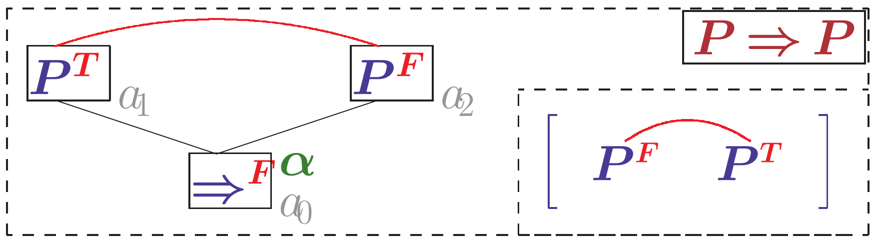


– Gleiche zweidimensionale Matrix aber verschiedene Formelbäume

– σ-komplementäre Konnektion allein kann Unterschied nicht aufdecken

– Beweise für $P\vee\neg P$ und $\neg\neg P\Rightarrow P$ nicht konstruktiv durchführbar, da auf Weg zu konnektierten Atomen zwei ^{F}-Knoten gleichzeitig vorkämen

– Beweis für $P\Rightarrow P$ erzeugt P^T und P^F direkt in einem Schritt



Matrix muß Constraints an konstruktive Beweise codieren

Wann existieren konstruktive Beweise?

- **Matrix muß konstruktive Block-Tableaux verdichten**
  - Konnektierte Atome müssen gleichzeitig freigelegt sein
  - Alle übergeordneten Knoten müssen zuvor freigelegt werden
  - Dabei dürfen keine zwei ^{F}-Positionen gleichzeitig vorkommen

  Analysiere Knoten zwischen Wurzel und konnektierten Atomen
- **Präfix konnektierter Atome beschreibt kritische Knoten**
  - Es reicht, Knoten markiert mit $\neg$, $\Rightarrow$, $\forall$ oder Atomen zu betrachten
    - Polaritäten konnektierter Atome sind verschieden
    - Nur Regeln für $\neg$, $\Rightarrow$ ändern die Polarität
  - Codiert kritische Regelanwendungen, die Atom im Beweis freilegen
- **Anforderungen an Präfixe konnektierter Atome**
  - Verzahnung beider Präfixe ergibt Reihenfolge der Regeln im Beweis
  - Nach Verzweigung dürfen verschiedene ^{F}-Knoten nicht kollidieren
  - Destruktive Regeln $\neg^T$, $\Rightarrow^T$ sollten möglichst spät vorkommen, damit beweisrelevante ^{F}-Teilformeln nicht vorzeitig entfernt werden

Wie findet man die richtige Regelreihenfolge?

- **Formelbaum liefert partielle Ordnung der Regeln**
  – Übergeordnete Knoten müssen vor ihren Nachfolgern freigelegt sein
- **Termsubstitution codiert Reihenfolge der γ-/δ-Regeln**
  – Substitution σ weist γ-Variablen einen Term zu
  – δ-Variablen in diesem Term müssen vor der γ-Variablen freigelegt sein
- **Bestimme Reihung intuitionistischer Regeln analog**
  – Unifiziere Präfixe konnektierter Atome durch Einfügen kritischer Knoten, um endgültige Kette der Beweisregeln zu beschreiben
  – Knoten markiert mit $\neg^T$, $\Rightarrow^T$, $\forall^T$ (und ^{T}-Atome) sind verschiebbar
  Mögliche Konflikte entstehen bei $\neg^F$, $\Rightarrow^F$, $\forall^F$ (und ^{F}-Atomen)

  Behandle ^{T}-Knoten als Variablen und ^{F}-Knoten als Konstante
  – Bestimme Substitution der Variablen durch Folge anderer Knoten, die beide Präfixstrings gleich machen (d.h. Atome können gleichzeitig erreicht werden)
  – Zugewiesene Konstante müssen dann im Beweis “vor der Variablen” durch Anwendung einer Regel verarbeitet werden

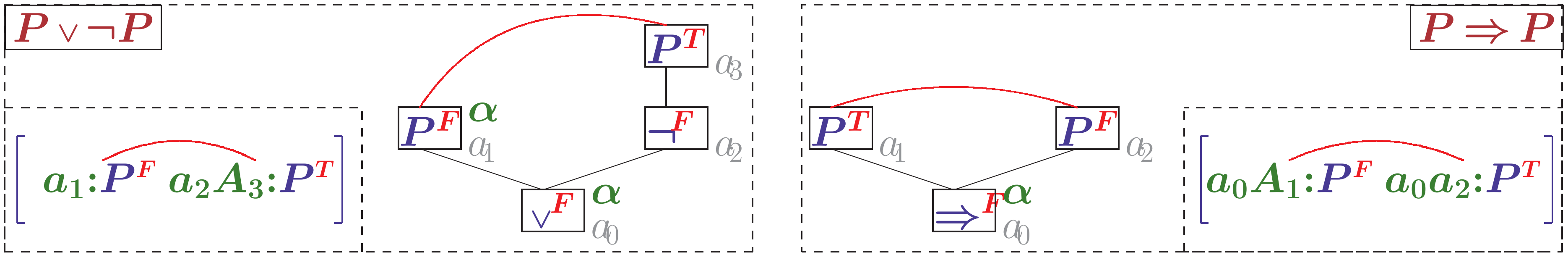
INTUITIONISTISCHES EXTENSIONSVERFAHREN

- **Erweitere Matrixcharakterisierung der Gültigkeit**
  - ***F* ist gültig gdw. alle Pfade durch *F* komplementär**
  - Betrachtung von Nichtnormalform-Matrizen ist sinnvoll (nicht zwingend)
  - Komplementaritätsbegriff muß ergänzt werden
    - · Unifizierbarkeit der konnektierten Terme für Quantorenbehandlung
    - · Unifizierbarkeit der zugehörigen Präfixstrings für Konstruktivität

- **Erweitere zugehöriges Beweissuchverfahren**
  - Unverändertes konnektionen-orientiertes Pfadüberprüfungsverfahren
    - · Uniformes Verfahren für Nichtnormalform-Matrizen sinnvoll
  - Erweiterter Komplementaritätstest
    - · Termunifikation liefert Substitution σ_Q von γ-Variablen durch Terme
    - · Präfixunifikation liefert Substitution σ_J für Präfixe einer Positionen

  Substitutionen codieren Einschränkungen an Reihenfolge der Regeln

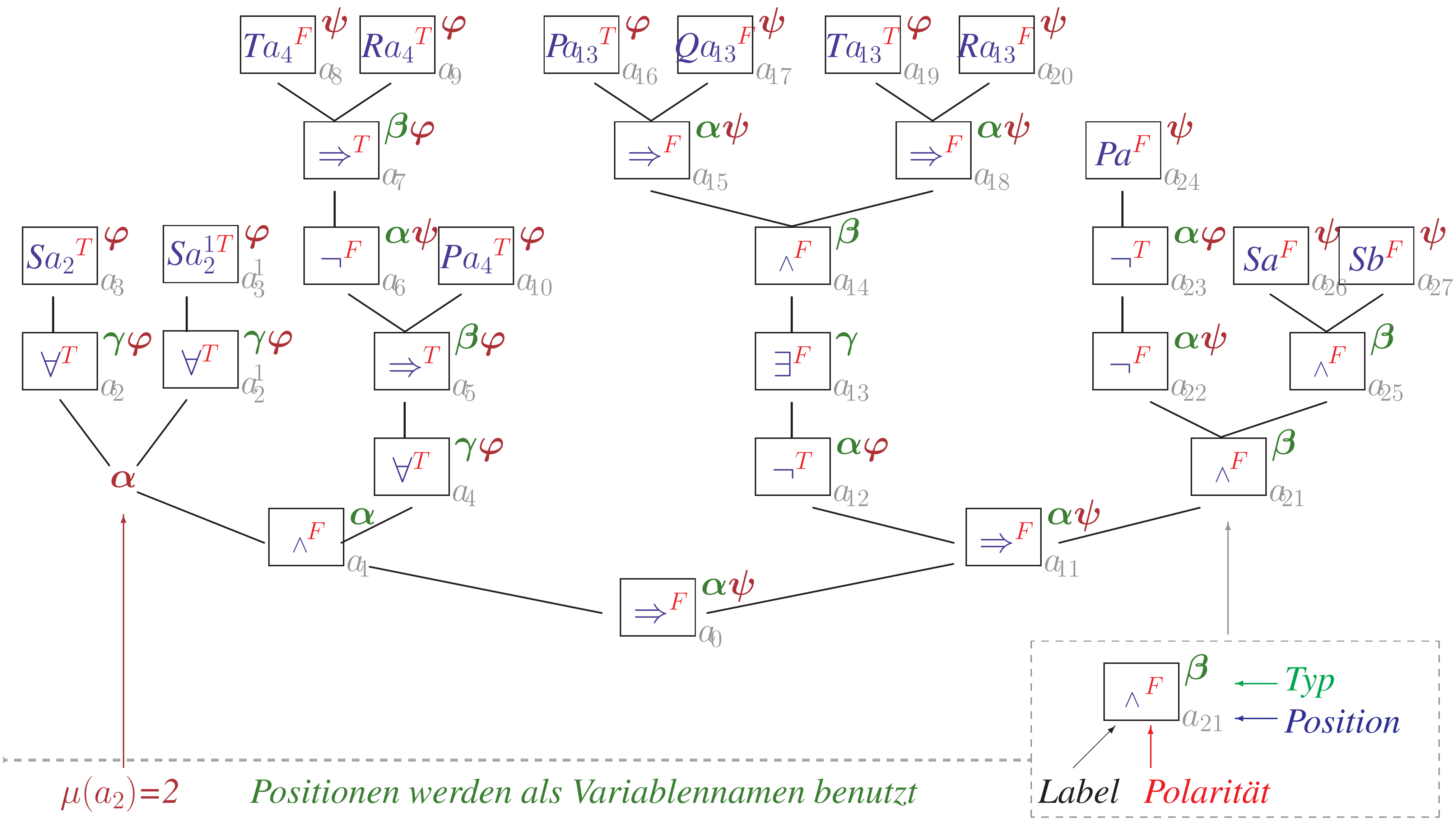
Intuitionistische Präfixe präzisiert



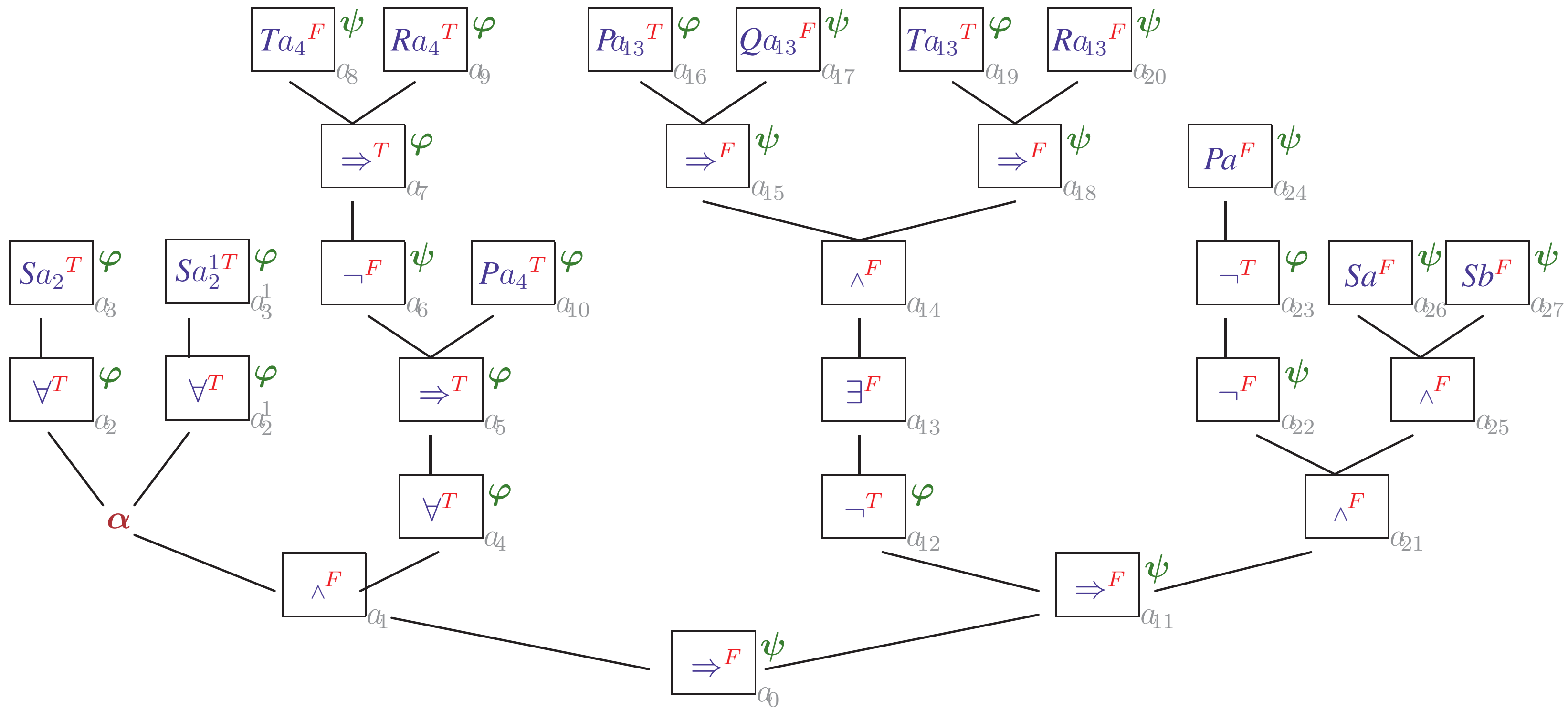
- **Weise Positionen intuitionistische Typen zu**
  - **Typ φ**: Positionen markiert mit $\neg^T$, $\Rightarrow^T$, $\forall^T$, ^{T}-Atomen
  - **Typ ψ**: Positionen markiert mit $\neg^F$, $\Rightarrow^F$, $\forall^F$, ^{F}-Atomen
  - φ-Positionen gelten als Variablen (Großbuchstaben)
  - ψ-Positionen gelten als Konstante (Kleinbuchstaben)
- **Definiere Präfix eines Atoms P**
  - Liste (String) der intuitionistischen Positionen zwischen Wurzel und P
- **Definiere intuitionistische Substitution σ_J**
  - Abbildung von φ-Positionen in Strings intuitionistischer Positionen
  - σ_J induziert Reduktionsordnung $\sqsubseteq_J$ auf intuitionistischen Positionen:
    Ist $\sigma_J(u) = v_1 ... v_n$ dann gilt $v_i \sqsubseteq_J u$ für jede ψ-Position v_i
    Dh. die Positionen v_i müssen (analytisch) vor u durch Regeln verarbeitet werden

Formelbaum mit intuitionistischen Positionen

$$(\forall x Sx) \wedge (\forall y \neg(Ty \Rightarrow Ry) \Rightarrow Py) \Rightarrow \neg(\exists z(Pz \Rightarrow Qz) \wedge (Tz \Rightarrow Rz)) \Rightarrow \neg\neg Pa \wedge Sa \wedge Sb$$



Matrix mit intuitionistischen Präfixen



$$
\left[
a_0A_2A_3{:}\,Sa_2^{\,T}\quad
a_0A_2^1A_3^1{:}\,Sa_2^{1T}\quad
\left[\begin{array}{l}
a_0A_4A_5a_6A_7a_8{:}\,Ta_4^{\,F}\\
a_0A_4A_5a_6A_7A_9{:}\,Ra_4^{\,T}\\
a_0A_4A_5A_{10}{:}\,Pa_4^{\,T}
\end{array}\right]
\left[\begin{array}{l}
\left[\;a_0a_{11}A_{12}a_{15}A_{16}{:}\,Pa_{13}^{\,T}\quad a_0a_{11}A_{12}a_{15}a_{17}{:}\,Qa_{13}^{\,F}\;\right]\\
\left[\;a_0a_{11}A_{12}a_{18}A_{19}{:}\,Ta_{13}^{\,T}\quad a_0a_{11}A_{12}a_{18}a_{20}{:}\,Ra_{13}^{\,F}\;\right]
\end{array}\right]
\left[\begin{array}{l}
a_0a_{11}a_{27}{:}\,Sb^{F}\\
a_0a_{11}a_{26}{:}\,Sa^{F}\\
a_0a_{11}a_{22}A_{23}a_{24}{:}\,Pa^{F}
\end{array}\right]
\right]
$$

Präfixe konnektierter Literale müssen durch intuitionistische Substitutionen gleich gemacht werden können

Intuitionistische Komplementarität und Gültigkeit

- **Komplementarität unter $\sigma = (\sigma_Q, \sigma_J)$**
  - Terme konnektierter Literale sind unter σ_Q unifizierbar, Präfixe unter σ_J
  - $\boldsymbol{\sigma_Q}$: Ersetze quantifizierte γ-Variablen durch Terme
    - · Termunifikation versucht Terme konnektierter Atome gleich zu machen
    - · σ_Q induziert Reduktionsordnung $\sqsubseteq_Q$ zwischen γ- und δ-Positionen
  - $\boldsymbol{\sigma_J}$: Ersetze φ-Variablen durch Strings
    - · Präfixunifikation versucht Präfixe konnektierter Atome gleich zu machen
    - · σ_J induziert Reduktionsordnung $\sqsubseteq_J$ zwischen ψ- und φ-Positionen
- **Zulässigkeit von (σ_Q, σ_J)**
  - Gesamte Reduktionsordnung $\lhd := (< \cup \sqsubseteq_Q \cup \sqsubseteq_J)^+$ ist azyklisch
  - Kommt eine δ-Position v in $\sigma_Q(u)$ vor, so gilt $|\sigma_J(pre_v)| \leq |\sigma_J(pre_u))|$
- **Intuitionistische Multiplizität $\mu_J(a_i)$**
  - Anzahl der Kopien des φ-Knotens im Baum

F ist intuitionistisch gültig, wenn es eine Multiplizität μ=(μ_Q, μ_J), eine zulässige Substitution σ=(σ_Q, σ_J) und eine Menge $\mathcal{C}$ σ-komplementärer Konnektionen gibt, so daß jeder Pfad durch F ein Element von $\mathcal{C}$ enthält

Extensionsverfahren für intuitionistische Logik

- **Pfadüberprüfungsverfahren bleibt unverändert**
  - Nicht-Normalform-Verfahren aus Einheit 6
- **Komplementaritätstest wird erweitert**
  - Bekanntes Termunifikationsverfahren (Robinson / Martelli-Montanari)
  - Neues Präfixunifikationsverfahren (Otten)
  - Überprüfung der Zulässigkeit

$$
\left[\; a_0a_2a_3{:}Sa_2{}^T \quad a_0a_2^1a_3^1{:}Sa_2^1{}^T \quad
\begin{bmatrix} a_0a_4a_5a_6a_7a_8{:}Ta_4{}^F \\ a_0a_4a_5a_6a_7a_9{:}Ra_4{}^T \\ a_0a_4a_5a_{10}{:}Pa_4{}^T \end{bmatrix}
\begin{bmatrix} \left[\, a_0a_{11}a_{12}a_{15}a_{16}{:}Pa_{13}{}^T \quad a_0a_{11}a_{12}a_{15}a_{17}{:}Qa_{13}{}^F \,\right] \\ \left[\, a_0a_{11}a_{12}a_{18}a_{19}{:}Ta_{13}{}^T \quad a_0a_{11}a_{12}a_{18}a_{20}{:}Ra_{13}{}^F \,\right] \end{bmatrix}
\begin{bmatrix} a_0a_{11}a_{27}{:}Sb^F \\ a_0a_{11}a_{26}{:}Sa^F \\ a_0a_{11}a_{22}a_{23}a_{24}{:}Pa^F \end{bmatrix}
\;\right]
$$

- $\sigma_Q = [b/a_2]$, $\sigma_J = [\epsilon/A_2,\ a_{11}a_{27}/A_3]$
- $\sigma_Q = [a/a_2^1]$, $\sigma_J = [\epsilon/A_2^1,\ a_{11}a_{26}/A_3^1]$
- $\sigma_Q = [a_{13}/a_4]$ $\sigma_J = [\epsilon/A_4,\ a_{11}X/A_5,\ a_{18}Y/A_7,\ Xa_6/A_{12},\ Ya_8/A_{19}]$
- $\sigma_Q = []$, $\sigma_J = [\epsilon/A_9a_{11}X/A_5,\ a_{20}/Y]$
- $\sigma_Q = [a/a_4,\ a/a_{13}]$, $\sigma_J = [a_{22}/X,\ A_{23}a_{24}/A_{10}]$
- $\sigma_Q = []$, $\sigma_J = [a_6a_{15}/A_{23},\ a_{24}/A_{16}]$

Intuitionistischer Matrixbeweis

$$\left[\; a_0A_2A_3{:}\,Sa_2^{T} \quad a_0A_2^1A_3^1{:}\,Sa_2^{1T} \quad \begin{bmatrix} a_0A_4A_5a_6A_7a_8{:}\,Ta_4^{F} \\ a_0A_4A_5a_6A_7A_9{:}\,Ra_4^{T} \\ a_0A_4A_5A_{10}{:}\,Pa_4^{T} \end{bmatrix} \quad \begin{bmatrix} \left[\, a_0a_{11}A_{12}a_{15}A_{16}{:}\,Pa_{13}^{T} \quad a_0a_{11}A_{12}a_{15}a_{17}{:}\,Qa_{13}^{F} \,\right] \\ \left[\, a_0a_{11}A_{12}a_{18}A_{19}{:}\,Ta_{13}^{T} \quad a_0a_{11}A_{12}a_{18}a_{20}{:}\,Ra_{13}^{F} \,\right] \end{bmatrix} \quad \begin{bmatrix} a_0a_{11}a_{27}{:}\,Sb^{F} \\ a_0a_{11}a_{26}{:}\,Sa^{F} \\ a_0a_{11}a_{22}A_{23}a_{24}{:}\,Pa^{F} \end{bmatrix} \;\right]$$

- **6 Konnektionen decken alle 18 Pfade ab**
  - $\mathcal{C} = \{\ \{a_3a_{27}\}, \{a_3^1a_{26}\}, \{a_8a_{19}\}, \{a_9a_{20}\}, \{a_{10}a_{24}\}, \{a_{16}a_{24}\}\ \}$
- **Terme gleich unter $\sigma_Q = [b/a_2,\ a/a_2^1,\ a/a_4,\ a/a_{13}]$**
  - $\sqsubseteq_Q$ ist leer, da keine δ-Positionen vorhanden
- **Präfixe gleich unter**

$$\begin{aligned} \sigma_J \;=\; [&\epsilon/A_2,\ \epsilon/A_2^1,\ a_{11}a_{27}/A_3,\ a_{11}a_{26}/A_3^1,\ \epsilon/A_4,\\ &a_{11}a_{22}/A_5,\ a_{18}a_{20}/A_7,\ \epsilon/A_9,\ a_6a_{15}a_{24}/A_{10},\\ &a_{22}a_6/A_{12},\ a_{24}/A_{16},\ a_{20}a_8/A_{19},\ a_6a_{15}/A_{23}] \end{aligned}$$

  - Induzierte Reduktionsordnung ist azyklisch
  - Zusatzbedingung für Zulässigkeit entfällt (keine δ-Positionen)
- **Die Formel ist intuitionistisch gültig**

Präfix-Unifikation

Unifiziere Präfix-Strings konnektierter Atome

- **Allgemeine String Unifikation ist sehr kompliziert**
  - Es kann unendlich viele allgemeinste Unifikatoren geben
- **Präfixe erfüllen spezielle Restriktionen**
  - Eindeutigkeit: jedes Symbol erscheint maximal einmal im Präfix-String
  - Baumeigenschaft: gleiche Symbole nur am Anfang zweier Präfix-Strings
  - Unifikationsverfahren wird deutlich einfacher als String-Unifikation
    - z.B. $taSTeFuL$ und $tabUlAR$ ist unifiziert zu $tableaux$ mit $\sigma = [b/S, l/T, a/F, x/L, \epsilon/U, ea/A, ux/R]$
    - Viele andere Unifikatoren möglich
- **Betrachte allgemeinste Unifikatoren**
  - aX und Yb unifizierbar mit $\sigma_1 = [b/X, a/Y]$ und $\sigma_2 = [cb/X, ac/Y]$ allgemeinster Unifikator $\sigma = [Zb/X, aZ/Y]$ liefert aZb
  - Mgu's verhindern vorzeitige Festlegung im Extensionsverfahren
- **Präfix-Unifikationstheorie ist finitär**
  - Maximal $\frac{1}{2}\,\frac{(2n)!}{(n!)^2}$ (also $\mathcal{O}(\frac{2^{2n}}{\sqrt{n}})$) allgemeinste Unifikatoren

Präfixunifikation – bildhaft

Systematische Aufzählung aller Kombinationen

- **Schreibe ersten String in Titelzeile einer Tabelle**
  – Konstanten belegen einen kleinen Slot (ein Symbol)
  – Variablen belegen einen großen (dehnbaren) Slot
- **Verteile zweiten String auf die Zeilen der Tabelle**
  – Identische Anfangsstrings werden identisch verteilt
  – Konstanten müssen im Bereich von Variablen erscheinen
  – Variablenbereiche sind beliebig dehnbar
  – Beginne mit kürzester Ausdehnung der Variablenbereiche
  – Verlängere Variablenbereiche systematisch und lese Substitution ab
- **Unifiziere Präfixe von $Ra_4{}^T$ und $Ra_{13}{}^F$ in Schritt 3**

$\boxed{a_0}$ A_4 | A_5 $\boxed{a_6}$ A_7 | A_9	σ_J
$\boxed{a_0}\boxed{a_{11}}$ —— A_{12} —— $\boxed{a_{18}}\boxed{a_{20}}$ ε	$[a_{11}X/A_4, Y/A_5, XYa_6/A_{12}, a_{18}a_{20}/A_7, \varepsilon/A_9]$
$\boxed{a_0}\boxed{a_{11}}$ —— A_{12} ———— $\boxed{a_{18}}\boxed{a_{20}}$	$[a_{11}X/A_4, Y/A_5, XYa_6Z/A_{12}, Za_{18}/A_7, a_{20}/A_9]$
$\boxed{a_0}\boxed{a_{11}}$ —— A_{12} ————— $\boxed{a_{18}}\boxed{a_{20}}$	$[a_{11}X/A_4, Y/A_5, XYa_6A_7/A_{12}, a_{18}a_{20}/A_9]$
$\boxed{a_0}\boxed{a_{11}}$ —— A_{12} —————— $\boxed{a_{18}}\boxed{a_{20}}$	$[a_{11}X/A_4, Y/A_5, XYa_6A_7Z/A_{12}, Za_{18}a_{20}/A_9]$
$\boxed{a_0}$ $\boxed{a_{11}}$ — A_{12} — $\boxed{a_{18}}\boxed{a_{20}}$ ε	$[\varepsilon/A_4, a_{11}X/A_5, Xa_6/A_{12}, a_{18}a_{20}/A_7, \varepsilon/A_9]$
$\vdots$ $\vdots$ $\vdots$ $\vdots$	$\vdots$

Präfixunifikation – systematisch

Transformationsverfahren wie Martelli-Montanari

Eingabe		*Menge von Präfix-Gleichungen* $\{E_1, ..E_n\}$
	wobei	$E_i \equiv p_i{=}\varepsilon\vert q_i$ *markierte Gleichung*
Initialisierung		*Setze* $EQ \leftarrow \{E_1, ..E_n\}$, $\sigma \leftarrow \epsilon$
Transformation	*Solange*	*eine der Transformationsregeln* $R_1, .., R_{10}$
		(Folie 22) anwendbar ist
		Transformiere EQ, σ *entsprechend*
Ergebnis	*Falls*	$EQ = \emptyset$
	dann	σ *ist allgemeinster Unifikator von* $\{E_1, ..E_n\}$
	sonst	$\{E_1, ..E_n\}$ *ist nicht unifizierbar*

- **Verfahren ist nichtdeterministisch und vollständig**
  - Menge möglicher Resultate ist Menge idempotenter mgus von $\{E_1, ..E_n\}$
- **Verfahren ist uniform anwendbar**
  - Viele Logiken durch unterschiedliche Transformationsregeln verarbeitbar

PRÄFIXUNIFIKATION – TRANSFORMATIONSREGELN FÜR $\mathcal{J}$

R_1	$\{\varepsilon = \varepsilon \vert \varepsilon\}, \sigma$	$\leadsto$	$\{\}, \sigma$
R_2	$\{\varepsilon = \varepsilon \vert t^+\}, \sigma$	$\leadsto$	$\{t^+ = \varepsilon \vert \varepsilon\}, \sigma$
R_3	$\{Xs = \varepsilon \vert Xt\}, \sigma$	$\leadsto$	$\{s = \varepsilon \vert t\}, \sigma$
R_4	$\{Cs = \varepsilon \vert Vt\}, \sigma$	$\leadsto$	$\{Vt = \varepsilon \vert Cs\}, \sigma$
R_5	$\{Vs = z \vert \varepsilon\}, \sigma$	$\leadsto$	$\{s = \varepsilon \vert \varepsilon\}, [z/V] \cup \sigma$
R_6	$\{Vs = \varepsilon \vert C_1 t\}, \sigma$	$\leadsto$	$\{s = \varepsilon \vert C_1 t\}, [\varepsilon/V] \cup \sigma$
R_7	$\{Vs = z \vert C_1 C_2 t\}, \sigma$	$\leadsto$	$\{s = \varepsilon \vert C_2 t\}, [zC_1/V] \cup \sigma$
R_8	$\{Vs^+ = \varepsilon \vert V_1 t\}, \sigma$	$\leadsto$	$\{V_1 t = V \vert s^+\}, \sigma$
R_9	$\{Vs^+ = z^+ \vert V_1 t\}, \sigma$	$\leadsto$	$\{V_1 t = V' \vert s^+\}, [z^+V'/V] \cup \sigma$
R_{10}	$\{Vs = z \vert Xt\}, \sigma$	$\leadsto$	$\{Vs = zX \vert t\}, \sigma$ ($V{\neq}X$, und $s{=}\varepsilon$, $t{\neq}\varepsilon$, oder X Konstante)

– $\mathcal{V}$: Variablenmenge, $\mathcal{C}$: Konstantenmenge, $\mathcal{V}^*$: Menge von Hilfsvariablen
– s, t, z: Strings, s^+, t^+, z^+: nichtleere Strings
– X Einzelsymbol, $V{\neq}V_1$ Variablen, C, C_1, C_2 Konstante (Einzelsymbole)
– V' neue Variable, die bisher nicht in σ vorkam

UNIFIKATION VON $a_0 a_{11} A_{12} a_{15} A_{16}$ UND $a_0 a_{11} a_{22} A_{23} a_{24}$ – (1)

$$
\begin{array}{lll}
 & \{a_0 a_{11} A_{12} a_{15} A_{16} = \varepsilon | a_0 a_{11} a_{22} A_{23} a_{24}\}, & [\,] \\
\xrightarrow{R_3} & \{a_{11} A_{12} a_{15} A_{16} = \varepsilon | a_{11} a_{22} A_{23} a_{24}\}, & [\,] \\
\xrightarrow{R_3} & \{A_{12} a_{15} A_{16} = \varepsilon | a_{22} A_{23} a_{24}\}, & [\,] \\
1. \xrightarrow{R_6} & \boldsymbol{\{a_{15} A_{16} = \varepsilon | a_{22} A_{23} a_{24}\}}, & [\varepsilon / A_{12}] \quad \diamond \\
2. \xrightarrow{R_{10}} & \{A_{12} a_{15} A_{16} = a_{22} | A_{23} a_{24}\}, & [\,] \\
2.1. \xrightarrow{R_9} & \{A_{23} a_{24} = A' | a_{15} A_{16}\}, & [a_{22} A' / A_{12}] \\
\xrightarrow{R_{10}} & \{A_{23} a_{24} = A' a_{15} | A_{16}\}, & [a_{22} A' / A_{12}] \\
\xrightarrow{R_9} & \{A_{16} = A'' | a_{24}\}, & [a_{22} A' / A_{12}, A' a_{15} A'' / A_{23}] \\
\xrightarrow{R_{10}} & \{A_{16} = A'' a_{24} | \varepsilon\}, & [a_{22} A' / A_{12}, A' a_{15} A'' / A_{23}] \\
\xrightarrow{R_5} & \{\varepsilon = \varepsilon | \varepsilon\}, & [a_{22} A' / A_{12}, A' a_{15} A'' / A_{23}, A'' a_{24} / A_{16}] \\
\xrightarrow{R_1} & \{\}, & \boldsymbol{[a_{22} A' / A_{12}, A' a_{15} A'' / A_{23}, A'' a_{24} / A_{16}]} \quad \square \\
2.2. \xrightarrow{R_{10}} & \{A_{12} a_{15} A_{16} = a_{22} A_{23} | a_{24}\}, & [\,] \\
\xrightarrow{R_{10}} & \{A_{12} a_{15} A_{16} = a_{22} A_{23} a_{24} | \varepsilon\}, & [\,] \\
\xrightarrow{R_5} & \boldsymbol{\{a_{15} A_{16} = \varepsilon | \varepsilon\}}, & [a_{22} A_{23} a_{24} / A_{12}] \quad \diamond
\end{array}
$$

Einzige erfolgreiche Folge von Transformationen ergibt nur einen mgu

Konstruktive Logik im Rückblick

- **Aussagekräftigere Beweise mit algorithmischen Anteilen**
  – Klassische Syntax aber konstruktives Verständnis von $\vee$, $\Rightarrow$, $\exists$
  – Beweise, die dieses Verständnis nicht widerspiegeln, sind nicht erlaubt
- **Erweiterung des Matrixkalküls erforderlich**
  – Pfade müssen weiterhin komplementäre Konnektionen enthalten
  – Komplementarität verlangt zusätzlich Unifizierbarkeit der Präfixe
- **Erweiterung des Extensionsverfahrens entsprechend**
  – Pfadüberprüfungsverfahren bleibt unverändert
  – Komplementaritätstest wird um Präfix-Unifikation erweitert
- **Es gibt auch Beweiser in Klauselform**
  – Mitführen von Präfixen ermöglicht Normalformbildung
  – ileanCop basiert auf Normalformkalkül (§4) und Präfix-Unifikation
  – Nicht-Normalformbeweiser JProver langsamer aber “rückübersetzbar”