



Sonderforschungsbereich 378
Ressourcenadaptive
Kognitive Prozesse



Automatisches Beweisen in Logik höherer Stufe

Christoph Benz Müller

`chris@ags.uni-sb.de`

The Ω MEGA Group

`http://www.ags.uni-sb.de/~chris`

FB Informatik, Universität des Saarlandes, Saarbrücken, Germany

Berlin, 8. Mai 1999

Motivation:

Formalisierung math. Schließens

Logik erster Stufe

- Vorteil: Semi-Entscheidbarkeit des Folgerungsbegriffs
- Nachteil: **Ausdrucksschwäche**

Ausweg

1. Mögl.: Axiomatisierung der Mengentheorie, z.B. ZF
⇒ unnatürlich; entgegen der mathematischen Praxis
2. Mögl.: **Logik höherer Stufe**



Motivation: Formalisierung math. Schließens

Logik höherer Stufe

- Vorteil: Ausdruckstärke; natürliche Formalisierungen
- Nachteil: **Unentscheidbarkeit des Folgerungsbegriffs**

Ausweg

Abschwächung des Semantikbegriffs:

Standardsemantik \implies Henkin-Semantik

Ziel ist nun

Entwicklung und Realisierung **Henkin-vollständiger** Beweiskalküle



Übersicht zum Vortrag

1. Klassische Typtheorie & Standard- bzw. Henkin-Semantik
2. Traditionelle Beweisverfahren (basierend auf Resolution)
3. Probleme mit der Henkin-Vollständigkeit
4. Extensionale Resolution höherer Stufe
(evtl. Paramodulation & RUE-Resolution)
5. Beweisprinzip der abstrakten Konsistenz



Klassische Typtheorie

- **Typen:** (i) $\{i, o\} \in T$ (ii) $\alpha, \beta \in T$, dann $\alpha \rightarrow \beta \in T$

- **Terme:**

(i) $V_\alpha \subseteq \Lambda$; V_α Menge von Variablen ($\alpha \in T$)

(ii) $C_\alpha \subseteq \Lambda$; C_α Menge von Konstanten ($\alpha \in T$)

Bedingungen: $\neg_{o \rightarrow o} \in C_{o \rightarrow o}$, $\forall_{o \rightarrow (o \rightarrow o)} \in C_{o \rightarrow (o \rightarrow o)}$,
 $\Pi_{(\alpha \rightarrow o) \rightarrow o} \in C_{(\alpha \rightarrow o) \rightarrow o}$ ($\alpha \in T$)

(iii) Applikationen: $\mathbf{A}_{\alpha \rightarrow \beta}$, $\mathbf{B}_\alpha \in \Lambda$, dann $(\mathbf{A} \mathbf{B})_\beta \in \Lambda$

(iii) Abstraktionen: $X_\alpha \in V_\alpha$, $\mathbf{A}_\beta \in \Lambda$, dann $(\lambda X. \mathbf{A})_{\alpha \rightarrow \beta} \in \Lambda$

- **λ -Konversion / β -Normalform / $\beta\eta$ -(Kopf-)Normalform:**

$$\lambda X_\gamma. \mathbf{A} \leftrightarrow^\alpha \lambda Y_\gamma. \mathbf{A}[Y/X]$$

$$(\lambda X_\gamma. \mathbf{A}) \mathbf{B}_\gamma \rightarrow^\beta \mathbf{A}[\mathbf{B}/X] \quad \lambda X. \mathbf{A} X \rightarrow^\eta \mathbf{A}, \text{ falls } X \notin \text{Free}(\mathbf{A})$$

Standardsemantik

- **Universum:** Wähle: D_ι
Festgelegt: $D_o = \{\perp, \top\}$, $D_{\alpha \rightarrow \beta} = \text{Funcs}(D_\alpha, D_\beta)$
- **Interpretation:** Wähle: $I_\alpha : C_\alpha \longrightarrow D_\alpha$
Festgelegt: $I(\neg_{o \rightarrow o})$ und $I(\vee_{o \rightarrow (o \rightarrow o)})$ wie üblich

$I(\Pi_{(\alpha \rightarrow o) \rightarrow o})$ ist Prädikat $p \in D_{(\alpha \rightarrow o) \rightarrow o}$, so daß für jedes $q_{\alpha \rightarrow o} \in D_{\alpha \rightarrow o} : p q_{\alpha \rightarrow o} = \top$ gdw. q gilt für alle $a \in D_\alpha$
 $\Rightarrow \forall X_\alpha. \mathbf{A}_o$ wird kodiert als $\Pi (\lambda X_\alpha. \mathbf{A}_o)$

- **Variablenbelegung:** $\varphi_\alpha : V_\alpha \longrightarrow D_\alpha$
- **Interpretation von Termen:** $I_\varphi : \Lambda_\alpha \longrightarrow D_\alpha$
 $I_\varphi(X) = \varphi(X)$, $I_\varphi(c) = I(c)$, $I_\varphi(\mathbf{A} \mathbf{B}) = I_\varphi(\mathbf{A}) I_\varphi(\mathbf{B})$,
 $I_\varphi(\lambda X_\alpha. \mathbf{B}_\beta) = f \in D_{\alpha \rightarrow \beta}$, so daß $f a = I_{\varphi[a/X]}(\mathbf{B})$ für alle $a \in D_\alpha$
- **Modell:** $\mathcal{M} = (\mathcal{D} : \{D_\alpha\}, \mathcal{I} : \{I_\alpha\})$, Erfüllbarkeit und Gültigkeit wie üblich

Henkin-Semantik

- wie Standardsemantik, außer: $D_{\alpha \rightarrow \beta} \subseteq \text{Functions}(D_\alpha, D_\beta)$
 - Bedingung aber: I_Φ is total (d.h., jeder Term hat eine Denotation)
 - Es gilt:
 - Jedes Standardmodell ist ein Henkin-Modell
 - Es gibt weniger Henkin-Modelle als Standardmodelle
 - Gültigkeit in Henkin-Sem. \Rightarrow Gültigkeit in Standardsem.
 - Erfüllbarkeit in Henkin-Sem. \Leftarrow Erfüllbarkeit in Standardsem.
- \Rightarrow Gödel 1931: Es kann keine vollständigen Kalküle für die Standardsemantik geben
- \Rightarrow Henkin 1950: Henkin-Semantik erlaubt vollständige Kalküle



Eigenschaften der klassischen Typtheorie

- **Komprehensionsprinzip** ist eingebaut $(\exists F_{\alpha \rightarrow \beta} \cdot \forall X_{\alpha} \cdot (F X) = \mathbf{A}_{\beta})$
- Optional: **Auswahlaxiom** $(\exists F_{(\alpha \rightarrow o) \rightarrow \alpha} \cdot \forall M_{\alpha \rightarrow o} \cdot (\exists X_{\alpha} \cdot M X) \Rightarrow M (F M))$ und
“Descriptionoperator” ι
- **Leibniz-Gleichheit** denotiert intendierte Gleichheitsrelation (d.h. eine funktionale Kongruenzrelation)

$$\doteq^{\alpha} := \lambda X_{\alpha} \cdot \lambda Y_{\alpha} \cdot \forall P_{\alpha \rightarrow o} \cdot P X \Rightarrow P Y$$

$$\text{d.h.: } a_{\alpha} \doteq^{\alpha} b_{\alpha} \quad \text{expandiert zu} \quad \forall P_{\alpha \rightarrow o} \cdot P a \Rightarrow P b$$

\Rightarrow Gleichheit ist **fest eingebaut** (bei Standard- oder Henkin-Semantik)

aber ... Mechanisierung ist sehr aufwendig

Resolution erster Stufe

- **Initialisierung:** Klauselnormalisierung
- **Beweissuche:** Resolution & Faktorisierung

$$\frac{[\mathbf{A}]^\alpha \vee \mathbf{C} \quad [\mathbf{B}]^\beta \vee \mathbf{D} \quad \sigma(\mathbf{A}) = \sigma(\mathbf{B}) \quad \alpha \neq \beta, \alpha, \beta \in \{T, F\}}{\sigma(\mathbf{C} \vee \mathbf{D})} \text{Res}$$

$$\frac{[\mathbf{A}]^\alpha \vee [\mathbf{B}]^\alpha \vee \mathbf{C} \quad \sigma(\mathbf{A}) = \sigma(\mathbf{B}) \quad \alpha \in \{T, F\}}{\sigma([\mathbf{A}]^\alpha \vee \mathbf{C})} \text{Fac}$$

- **Nebenrechnungen:** Unifikation erster Stufe (entscheidbar, unitär)

Klauselnormalisierung CNF

$$\frac{C \vee [A \vee B]^T}{C \vee [A]^T \vee [B]^T} \vee^T \quad \frac{C \vee [A \wedge B]^F}{C \vee [A]^F} \vee_l^F \quad \frac{C \vee [A \wedge B]^F}{C \vee [B]^F} \vee_r^F$$

$$\frac{C \vee [\neg A]^T}{C \vee [A]^F} \neg^T \quad \frac{C \vee [\neg A]^F}{C \vee [A]^T} \neg^F \quad \frac{C \vee [\Pi^\alpha A]^T \quad X_\alpha \text{ neue Variable}}{C \vee [A \ X]^T} \Pi^T$$

$$\frac{C \vee [\Pi^\alpha A]^F \quad s_\alpha \text{ Skolem-Term}}{C \vee [A \ s_\alpha]^F} \Pi^F$$



Andrews' Resolution höherer Stufe (1971)

- **Initialisierung:** keine
- **Neu:** Kalkülregeln für λ -Konversion & zusätzliche Disjunktions- und Simplifikationsregeln
- **Neu:** Klauselnormalisierung als Bestandteil des Kalküls
- **Beweissuche:** Resolution (Cut), Simplifikation (Faktorisierung identischer Literale)
- **Rückschritt:** Substitutionsregel (beliebige Instantiierung freier Variablen, d.h. Aufzählung des Herbrand-Universums)

Wichtigster Beitrag: Adaptation des Beweisprinzips der abstrakten Konsistenz



Ansatz von Jensen/Pietrowski (1972)

- **Initialisierung:** Skolemisierung, keine Normalisierung
- **Axiome:** Reduktion (Normalisierung) & Expansion
z.B. $[P \Rightarrow Q]^T \vee [P]^T$ $[P \Rightarrow Q]^T \vee [Q]^F$...
- **Beweissuche:** (Hyper-)Resolution
- **Nebenrechnungen:** Unifikation bis Ordnung k

Wichtigster Beitrag: Unifikation höherer Stufe (bis Ordnung k)



Huet's Constraint Resolution (1972)

- **Initial & nach vorzeitiger Unifikation:** Klauselnormalisierung
- **Beweissuche:** Constraint Resolution/Faktorisierung

$$\frac{[A]^\alpha \vee C \quad [B]^\beta \vee D \quad \alpha \neq \beta, \alpha \in \{T, F\}}{C \vee D \vee [A \neq? B]} \text{ Res} \quad \frac{[A]^\alpha \vee [B]^\alpha \vee C \quad \alpha \in \{T, F\}}{[A]^\alpha \vee C \vee [A \neq? B]} \text{ Fac}$$

- **Final:** Unifikation/Prä-Unifikation (aber erlaubt: vorzeitige Unifikation)
- **Zusätzlich:** Splitting Regeln

$$\frac{[P \overline{T^n}]^T \vee C \quad \alpha \neq \beta, \alpha \in \{T, F\}}{\text{z.B. } [X_o]^F C \vee [(P \overline{T^n}) \neq? (\neg X_o)]} \text{ Split}_{\neg}^T \quad \frac{[P \overline{T^n}]^\alpha \vee C \quad \alpha \neq \beta, \alpha \in \{T, F\}}{[X_o]^T \vee [Y_o]^T C \vee [(P \overline{T^n}) \neq? (X_o \vee Y_o)]} \text{ Split}_{\vee}^T$$

Wichtigster Beitrag: Constraint Idee, Prä-Unifikation

Andrews' Konnektionsmethode (1989)

- **Initialisierung:** keine
- **Deshalb:** Schrittweise Normalisierung im Kalkül
- **Beweissuche:** Bildung von Konnektionen in Matrix
- **Nebenrechnungen:** Prä-Unifikation nach Huet, Multiple "Matingsearch Prozessoren"
- **Verbesserung:** Huet's Splitting Regeln \implies Primitive Substitution

$$\frac{[Q_\gamma \overline{U^k}]^\alpha \vee \mathbf{C} \quad \mathbf{P} \in \mathcal{GB}_\gamma^{\{\neg, \vee\} \cup \{\Pi^\beta \mid \beta \in \mathcal{T}^k\}}}{[Q_\gamma \overline{U^k}]^\alpha \vee \mathbf{C} \vee [Q = \mathbf{P}]^F} \quad Prim$$

Beispiel:

$$P := \lambda \overline{X^n} \cdot \neg(H \overline{X^n})$$

$$P := \lambda \overline{X^n} \cdot (H^1 \overline{X^n}) \vee (H^2 \overline{X^n})$$

Wichtigster Beitrag: Primitive Substitution, Matrix-Kalkül, Multiple Strategien



Weitere Ansätze

- Snyder's *E*-Unifikation (1990) in bisherigen Ansätzen
- Wolfram's Theorie-Resolution (1993)
- Kohlhase's sortierte Constraint Resolution (1994)
- Higher-Order Rewriting (sehr aktiv seit ca. 10 Jahren; z.B. Nipkow, Prehofer)
- Extensionale Resolution (Benzmüller & Kohlhase; 1997)
- Extensionale Paramodulation/RUE-Resolution höherer Stufe (Benzmüller; 1998)



Probleme

- **Extensionalitätsaxiome** werden benötigt in: Andrews' Resolution höherer Stufe (1971), Huet's Constraint Resolution (1972), Jensen & Pietrowski (1972), Wolfram (1993), Kohlhase (1994), TPS-System, HOL-System, ...

– **EXT-Func**[≐]: $\forall F_{\alpha \rightarrow \beta} \cdot \forall G_{\alpha \rightarrow \beta} (\forall X_{\beta} \cdot F X \doteq G X) \Rightarrow F \doteq G$

expandiert: $\forall F_{\alpha \rightarrow \beta} \cdot \forall G_{\alpha \rightarrow \beta} (\forall X_{\beta} \cdot \forall P_{\beta \rightarrow o} \cdot P (F X) \Rightarrow P (G X) \Rightarrow \forall Q_{(\alpha \rightarrow \beta) \rightarrow o} \cdot Q F \Rightarrow Q G$

Klauseln: $\mathcal{C}_1 : [p_{\beta \rightarrow o} (F s_{\beta})]^T \vee [Q F]^F \vee [Q G]^T$, $\mathcal{C}_2 : [p_{\beta \rightarrow o} (G s_{\beta})]^T \vee [Q F]^F \vee [Q G]^T$

– **EXT-Bool**[≐]: $\forall A_o \cdot \forall B_o \cdot (A \Leftrightarrow B) \Leftrightarrow A \doteq^o B$

expandiert: $\forall A_o \cdot \forall B_o \cdot (A \Leftrightarrow B) \Leftrightarrow (\forall Q_{o \rightarrow o} \cdot Q A \Rightarrow Q B)$

Klauseln: $\mathcal{C}_1 : [A]^F \vee [B]^F \vee [P A]^F \vee [P B]^T$, $\mathcal{C}_2 : [A]^T \vee [B]^T \vee [P A]^F \vee [P B]^T$, $\mathcal{C}_3 :$

$[A]^F \vee [B]^T \vee [p A]^T$, $\mathcal{C}_4 : [A]^F \vee [B]^T \vee [p B]^F$, $\mathcal{C}_5 : [A]^T \vee [B]^F \vee [p A]^T$, $\mathcal{C}_6 : [A]^T \vee [B]^F \vee [p B]^F$

Extensionale Resolution \mathcal{ER}

Constraint Resolution

$$\frac{[A]^\alpha \vee C \quad [B]^\beta \vee D \quad \alpha \neq \beta}{C \vee D \vee [A = B]^F} \text{Res} \qquad \frac{[A]^\alpha \vee [B]^\alpha \vee C \quad \alpha \in \{T, F\}}{[A]^\alpha \vee C \vee [A = B]^F} \text{Fac}$$

$$\frac{[Q_\gamma \overline{U^k}]^\alpha \vee C \quad \mathbf{P} \in \mathcal{GB}_\gamma^{\{\neg, \vee\} \cup \{\Pi^\beta \mid \beta \in \mathcal{T}^k\}}}{[Q_\gamma \overline{U^k}]^\alpha \vee C \vee [Q = \mathbf{P}]^F} \text{Prim}$$

Achtung: Resolution/Faktorisierung auf Unifikations-Constraints nicht erlaubt

Primitive Substitution: $\exists P_{\alpha \rightarrow o} \cdot P \ a_\alpha \xrightarrow{CNF} C_1 : [P \ a]^F$

$\text{Prim}(C_1, [\lambda X_\alpha \cdot \neg(P' X) / P]) : C_2 : [P' a]^T$



Extensionale Resolution \mathcal{ER} – Forts.

Prä-Unifikation höherer Stufe

$$\frac{\mathbf{C} \vee [\text{red}\mathbf{A}_{\alpha \rightarrow \beta} \ \mathbf{C}_{\alpha} = \text{green}\mathbf{B}_{\alpha \rightarrow \beta} \ \mathbf{D}_{\alpha}]^F}{\mathbf{C} \vee [\mathbf{A} = \mathbf{B}]^F \vee [\mathbf{C} = \mathbf{D}]^F} \text{Dec}$$

$$\frac{\mathbf{C} \vee [\mathbf{A} = \mathbf{A}]^F}{\mathbf{C}} \text{Triv}$$

$$\frac{\mathbf{C} \vee [\mathbf{F}_{\gamma}] \overline{\mathbf{U}^n} = h \overline{\mathbf{V}^m}]^F \quad \mathbf{G} \in \mathcal{GB}_{\gamma}^h}{\mathbf{C} \vee [\mathbf{F} = \mathbf{G}]^F \vee [\mathbf{F} \overline{\mathbf{U}^n} = h \overline{\mathbf{V}^m}]^F} \text{FlexRigid}$$

$$\frac{\mathbf{C} \vee [(\lambda X_{\alpha} \cdot \mathbf{M}_{\beta}) = \mathbf{N}_{\alpha \rightarrow \beta}]^F}{\mathbf{C} \vee [(\lambda X_{\alpha} \cdot \mathbf{M}) \ \mathbf{s} = \mathbf{N} \ \mathbf{s}]^F} \text{Func}_1 \quad \frac{\mathbf{C} \vee [(\lambda X_{\alpha} \cdot \mathbf{M}_{\beta}) = (\lambda Y_{\alpha} \cdot \mathbf{N}_{\beta})]^F}{\mathbf{C} \vee [(\lambda X_{\alpha} \cdot \mathbf{M}) \ \mathbf{s} = (\lambda X_{\alpha} \cdot \mathbf{N}) \ \mathbf{s}]^F} \text{Func}_2$$

$$\frac{\mathbf{C} \vee [\mathbf{X} = \mathbf{A}]^F \quad \mathbf{X} \notin \text{Free}(\mathbf{A})}{(\mathbf{C}[\mathbf{A}/\mathbf{X}])} \text{Subst}$$

$$\frac{\mathbf{D} \quad \mathbf{C} \in \mathcal{CNF}(\mathbf{D})}{\mathbf{C}} \text{Cnf}$$

Extensionale Resolution \mathcal{ER} – Forts.

Extensionalität: **Rekursive Aufrufe an die Beweissuche aus der Unifikation**

$$\frac{C \vee [M_o = N_o]^F}{C \vee [M_o \Leftrightarrow N_o]^F} \textit{Equiv} \qquad \frac{C \vee [M_\alpha = N_\alpha]^F}{C \vee [\forall P_{\alpha \rightarrow o}. P \ M \Rightarrow P \ N]^F} \textit{Leib}$$

$$\frac{C \vee [M_{\alpha \rightarrow \beta} = N_{\alpha \rightarrow \beta}]^F \quad s_\alpha \text{ Skolem term for this clause}}{C \vee [M \ s = N \ s]^F} \textit{Func}$$

- **Vermutung:** Regel *Leib* kann auf Typ ι beschränkt werden
- ⇒ Erster **Henkin-vollständiger** Kalkül der zusätzliche axiome im Suchraum vermeidet (CADE-15)
- ⇒ Unterschied zu Huet (1972): **frühzeitige Unifikation ist essentiell**

Beispiel: $(\lambda X_{\alpha} \blacksquare auto_{\alpha \rightarrow o} X \wedge klein_{\alpha \rightarrow o} X) = (\lambda X_{\alpha} \blacksquare klein X \wedge auto X)$

$$\forall P_{(\alpha \rightarrow o) \rightarrow o} \blacksquare P (\lambda X_{\alpha} \blacksquare auto_{\alpha \rightarrow o} X \wedge klein_{\alpha \rightarrow o} X) \Rightarrow P (\lambda X_{\alpha} \blacksquare klein X \wedge auto X)$$

$$c1: [p (\lambda X \blacksquare auto X \wedge klein X)]^T$$

$$c2: [p (\lambda X \blacksquare klein X \wedge auto X)]^F$$

$$c3: [(p (\lambda X \blacksquare auto X \wedge klein X)) = (p (\lambda X \blacksquare klein X \wedge auto X))]^F$$

$$c4: [(\lambda X \blacksquare auto X \wedge klein X) = (\lambda X \blacksquare klein X \wedge auto X)]^F$$

$$c5: [(auto s \wedge klein s) = (klein s \wedge auto s)]^F$$

$$c6: [(auto s \wedge klein s) \equiv (klein s \wedge auto s)]^F$$

$$c7: [auto s]^T \vee [klein s]^T$$

$$c8: [auto s]^T$$

$$c9: [klein s]^T$$

$$c10: [auto s]^F \vee [klein s]^F$$



Mechanisierung primitiver Gleichheit

- **Warum:** Leibniz Gleichheit führt viele **flexible Köpfe** in Suchraum ein (Primitive Substitution)

⇒ Evtl. verbessert primitive Gleichheit die Möglichkeiten zur **Mechanisierung**

- Definition basierend auf Reflexivitätsprinzip:

$$\doteq^\alpha := \lambda X_\alpha. \lambda Y_\alpha. \forall Q_{\alpha \rightarrow \alpha \rightarrow o}. (\forall Z_\alpha. (Q Z Z)) \Rightarrow (Q X Y)$$

- Modifizierte Leibniz Gleichheit:

$$\doteq^\alpha := \lambda X_\alpha. \lambda Y_\alpha. \forall P_{\alpha \rightarrow o}. ((a_o \vee \neg a_o) \wedge P X) \Rightarrow ((b_o \vee \neg b_o) \wedge P Y)$$

⇒ Es ist **nicht entscheidbar**, ob Problem definierte Gleichungen enthält

⇒ Ein Henkin-vollständiger Kalkül muß **stets** auch die definierte Gleichheit behandeln, unabhängig von einer primitiven Gleichheitsbehandlung

Extensionale Paramodulation \mathbb{P}

$$\frac{[\mathbf{A}[\mathbf{T}_\beta]]^\alpha \vee C \quad [\mathbf{L} =^\beta \mathbf{R}]^T \vee D}{[\mathbf{A}[\mathbf{R}]]^\alpha \vee C \vee D \vee [\mathbf{T} =^\beta \mathbf{L}]^F} \text{ Para}$$

$$\frac{[\mathbf{A}]^\alpha \vee C \quad [\mathbf{L} =^\beta \mathbf{R}]^T \vee D}{[P_{\alpha \rightarrow o} \mathbf{R}]^\alpha \vee C \vee D \vee [\mathbf{A} =^o P_{\beta \rightarrow o} \mathbf{L}]^F} \text{ Para}'$$

- Negative Gleichungsliterale repräsentieren Unifikations-Constraints
- Resolution auf Unifikations-Constraints ist nicht erlaubt

$\frac{[p(f(f a))]^T \quad [f = g]^T}{[p(f(g a))]^T} \text{ Para, Uni}$	$\frac{[p(f(f a))]^T \quad [f = g]^T}{[P g]^T \vee [(P f) = (p(f(f a)))]^F} \text{ Para}'$
$\frac{[p(f(f a))]^T \quad [f = g]^T}{[p(g(f a))]^T} \text{ Para, Uni}$	$\frac{[p(f(f a))]^T \text{ with } [\lambda \mathbf{X} \cdot (p(f(f a)))/P]}{[p(f(g a))]^T \text{ with } [\lambda \mathbf{X} \cdot (p(f(\mathbf{X} a)))/P]} \text{ UNI}$ $\frac{[p(f(f a))]^T \text{ with } [\lambda \mathbf{X} \cdot (p(\mathbf{X}(f a)))/P]}{[p(g(f a))]^T \text{ with } [\lambda \mathbf{X} \cdot (p(\mathbf{X}(\mathbf{X} a)))/P]} \text{ UNI}$

Extensionale Paramodulation EP – Forts.

- In erster Stufe **Reflexivitätsregel** notwendig \rightarrow hier **eingebaut** in UNI

$$\frac{[(fX) = (fa)]^F}{\square} \text{Ref} \qquad \frac{[(fX) = (fa)]^F}{\square} \text{UNI}$$

- Beispiel:

$$C_1 : \underbrace{[\text{nicht-leer} (\lambda X_{\iota} \bullet ((\text{auto } X \wedge \text{klein } X) \wedge \text{kippt } X))]}^{\{X \mid \text{auto } X \wedge \text{klein } X \wedge \text{kippt } X\} \in \text{nicht-leer}_{(\iota \rightarrow o) \rightarrow o}}]^T \quad C_2 : [\underbrace{\text{auto } X \wedge \text{klein } X = \text{klw } X}_{\forall X_{\iota} \bullet (\text{auto } X \wedge \text{klein } X) = \text{klw } X}]^T$$

$$\text{To show: } C_3 : \underbrace{[\text{nicht-leer} (\lambda X_{\iota} \bullet \text{klw } X \wedge \text{kippt } X)]^F}_{\{X \mid \text{klw } X \wedge \text{kippt } X\} \in \text{nicht-leer}}$$

- Typische Widerlegung basierend auf Paramodulation/Termersetzung:

$$\text{Para}(C_1, C_2), \text{UNI} : \quad C_4 : [\text{nicht-leer} (\lambda X_{\iota} \bullet (\text{klw } X \wedge \text{kippt } X))]^T$$

$$\text{Res}(C_4, C_3), \text{UNI} : \quad \square$$

Problem mit positiven Gleichheitsliteralsen

- Einzelne positive Gleichheitsliteralsen können **widersprüchlich** sein

$$\begin{array}{c}
 \{X \mid \textit{klein } X\} = \overline{\{X \mid \textit{klein } X\}} \\
 \hline
 [\mathbf{A}_o = \neg \mathbf{A}_o]^T \quad \overbrace{[(\lambda X. \textit{klein } X) = (\lambda X. \neg(\textit{klein } X))]}^{}]^T
 \end{array}$$

- **Zusätzliche Extensionalitätsregeln** benötigt

$$\frac{\mathbf{C} \vee [\mathbf{M}_o = \mathbf{N}_o]^T}{\mathbf{C} \vee [\mathbf{M}_o \Leftrightarrow \mathbf{N}_o]^T} \textit{Equiv}' \quad \frac{\mathbf{C} \vee [\mathbf{M}_{\alpha \rightarrow \beta} = \mathbf{N}_{\alpha \rightarrow \beta}]^T \quad X \textit{ new}}{\mathbf{C} \vee [\mathbf{M } X = \mathbf{N } X]^T} \textit{Func}'$$

- Neue Regeln verstärken den **differenzreduzierenden Charakter** des Kalküls
- **Henkin-Vollständigkeit** ohne zusätzliche Axiome
(bewiesen bisher nur mit zusätzlicher FlexFlex-Regel)

Extensionale Paramodulation EP– Forts.

- Geringfügig modifiziertes Problem: keine Termersetzung möglich!

$$C'_1 : [nicht-leer(\lambda X_l. \blacksquare((auto\ X \wedge kippt\ X) \wedge klein\ X))]^T \quad C2_2 : [(auto\ X \wedge klein\ X) = klw\ X]^T$$

$$\text{Zu Zeigen: } C_3 : [nicht-leer(\lambda X_l. \blacksquare klw\ X \wedge kippt\ X)]^F$$

$$Para(C_1, C_2) : \quad C_4 : [nicht-leer(\lambda X. \blacksquare(klw\ X \wedge klein\ X))]^T \vee [(auto\ X \wedge klein\ X) = (auto\ X \wedge kippt\ X)]^F$$

...

Anstelle von Termersetzung verwende Differenzreduktion

$$Res(C'_1, C_3) : \quad C_4 : [(nicht-leer(\lambda X_l. \blacksquare((auto\ X \wedge kippt\ X) \wedge klein\ X))) = (nicht-leer(\lambda X_l. \blacksquare klw\ X \wedge kippt\ X))]^F$$

$$Dec(C_4), Func, Equiv : \quad C_5 : [((auto\ s \wedge kippt\ s) \wedge klein\ s) \equiv (klw\ s \wedge kippt\ s)]^F$$

$$Equiv'(C_2) : \quad C_6 : [(auto\ X \wedge klein\ X) \equiv klw\ X]^T$$

$$CNF(C_5, C_6) : \quad \dots$$



⇒ Unvermeidbarer Mix von Termersetzung & Differenzreduktion

Extensionale RUE-Resolution ERUE

- Motivation: Kalkül für **reine** Differenzreduktion
- Extensionale RUE-Resolution:
 - Ersetze Paramodulationsregel ...
 - durch **Resolution und Faktorisierung auf Unifikations-Constraints**

• $C_1 : [\textit{nicht-leer} (\lambda X. \blacksquare ((\textit{auto} X \wedge \textit{klein} X) \wedge \textit{kippt} X))]^T$ $C_2 : [(\textit{auto} X \wedge \textit{klein} X) = \textit{klw} X]^T$

$C_3 : [\textit{nicht-leer} (\lambda X. \blacksquare \textit{klw} X \wedge \textit{kippt} X)]^F$

$\textit{Res}(C_1, C_3), \textit{Dec}, \textit{Func} :$ $C_4 : [((\textit{auto} s \wedge \textit{klein} s) \wedge \textit{kippt} s) = (\textit{klw} s \wedge \textit{kippt} s)]^F$

$\textit{Dec}(C_4), \textit{Triv} :$ $C_5 : [(\textit{auto} s \wedge \textit{klein} s) = \textit{klw} s]^F$

$\textit{Res}(C_5, C_2), \textit{UNI} :$... \square

Extensionale RUE-Resolution ERUE

- Geringfügig modifiziertes Beispiel

- $C_1 : [\textit{nicht-leer} (\lambda X. \blacksquare ((\textit{auto } X \wedge \textit{kippt } X) \wedge \textit{klein } X))]^T$ $C_2 : [(\textit{auto } X \wedge \textit{klein } X) = \textit{klw } X]^T$

$$C_3 : [\textit{nicht-leer} (\lambda X. \blacksquare \textit{klw } X \wedge \textit{kippt } X)]^F$$

$$\textit{Res}(C_1, C_3), \textit{Dec}, \textit{Func} : C_4 : [((\textit{auto } s \wedge \textit{kippt } s) \wedge \textit{klein } s) = (\textit{klw } s \wedge \textit{kippt } s)]^F$$

$$\textit{Equiv}(C_4) : C_5 : [((\textit{auto } s \wedge \textit{kippt } s) \wedge \textit{klein } s) \equiv (\textit{klw } s \wedge \textit{kippt } s)]^F$$

$$\textit{Equiv}'(C_2) : C_6 : [(\textit{auto } X \wedge \textit{klein } X) \equiv \textit{klw } X]^T$$

$$\textit{CNF}(C_5, C_6) : \dots \quad \square$$

⇒ Reine Differenzreduktion **besser handhabbar** als gemischter Ansatz?

- **Henkin-Vollständigkeit** ohne zusätzliche Axiome
(bewiesen bisher nur mit zusätzlicher FlexFlex-Regel)



Zusammenfassung

- Übersicht zur Entwicklung des automatischen Beweisens in Logik höherer Stufe; insbesondere eigene Kalküle ER , EP und $ER\cup E$
- Implementierung LEO
- Vielversprechende Experimente
- Adaptation von Smullyan's / Andrews' Beweisprinzip der abstrakten Konsistenz hinsichtlich der Henkin-Semantik



Higher-Order Abstract Consistency

Definition 0.1 (Properties for Abstract Consistency Classes). Let \mathcal{I}_Σ be a class of sets of Σ -sentences.

∇_c If \mathbf{A} is atomic, then $\mathbf{A} \notin \Phi$ or $\neg\mathbf{A} \notin \Phi$.

∇_{\neg} If $\neg\neg\mathbf{A} \in \Phi$, then $\Phi * \mathbf{A} \in \mathcal{I}_\Sigma$.

∇_β If $\mathbf{A} \in \Phi$ and \mathbf{B} is the β -normal form of \mathbf{A} , then $\mathbf{B} * \Phi \in \mathcal{I}_\Sigma$.

∇_f If $\mathbf{A} \in \Phi$ and \mathbf{B} is the $\beta\eta$ -normal form of \mathbf{A} , then $\mathbf{B} * \Phi \in \mathcal{I}_\Sigma$.

∇_{\vee} If $\mathbf{A} \vee \mathbf{B} \in \Phi$, then $\Phi * \mathbf{A} \in \mathcal{I}_\Sigma$ or $\Phi * \mathbf{B} \in \mathcal{I}_\Sigma$.

∇_{\wedge} If $\neg(\mathbf{A} \vee \mathbf{B}) \in \Phi$, then $\Phi \cup \{\neg\mathbf{A}, \neg\mathbf{B}\} \in \mathcal{I}_\Sigma$.

∇_{\forall} If $\Pi^\alpha \mathbf{F} \in \Phi$, then $\Phi * \mathbf{F}\mathbf{W} \in \mathcal{I}_\Sigma$ for each $\mathbf{W} \in \text{cwff}_\alpha(\Sigma)$.

∇_{\exists} If $\neg\Pi^\alpha \mathbf{F} \in \Phi$, then $\Phi * \neg(\mathbf{F}w) \in \mathcal{I}_\Sigma$ for any constant $w \in \Sigma_\alpha$, which does not occur in Φ .

∇_b If $\neg(\mathbf{A} \doteq^o \mathbf{B}) \in \Phi$, then $\Phi \cup \{\mathbf{A}, \neg\mathbf{B}\} \in \mathcal{I}_\Sigma$ or $\Phi \cup \{\neg\mathbf{A}, \mathbf{B}\} \in \mathcal{I}_\Sigma$.

∇_q If $\neg(\mathbf{F} \doteq^{\alpha \rightarrow \beta} \mathbf{G}) \in \Phi$, then $\Phi * \neg(\mathbf{F}w \doteq^\beta \mathbf{G}w) \in \mathcal{I}_\Sigma$ for any constant $w \in \Sigma_\alpha$, which does not occur in Φ .

∇_e (r) $\neg(\mathbf{A} =^\alpha \mathbf{A}) \notin \Phi$

(s) if $\mathbf{F}[\mathbf{A}]_p \in \Phi$ and $\mathbf{A} = \mathbf{B} \in \Phi$, then $\Phi * \mathbf{F}[\mathbf{B}]_p \in \mathcal{I}_\Sigma$



Higher-Order Abstract Consistency



Christoph Benz Müller, Ω MEGA-Group, Universität des Saarlandes

