Inferenzmethoden

Teil III

Behandlung spezifischer Fragestellungen

Spezialisierte Beweistechniken

1. Verarbeitung mathematischer Theorien
2. Gleichheitsbehandlung
3. Termersetzung und -auswertung
4. Zahlen und Induktion

Steigerung der Effizienz von Beweisverfahren

- **Reale Problemstellungen liefern komplexe Formeln**
  - Formeln enthalten große Mengen von Fakten und Zusammenhängen
  - Formeln enthalten Bezüge zu verschiedenen mathematischen Theorien
    - Zahlen, Gleichheit, Relationen, Funktionen mit "Bedeutung" (Wert)
  - Wie kann man derartige Formeln effizient genug verarbeiten?
- **Verdichtung allgemeiner Beweisverfahren**
  - Spezialanalyse liefert gleiche Informationen wie explizite Beweisschritte
    - Kompakte Verarbeitung von Klauselkopien durch Faktorisierung
    - Verdichtung wiederholter Argumenteketten durch Zyklenanalyse
    - Datenbanktechniken und Indizierung für große Faktenmengen
  - Verfahren sind sehr technisch und liefern wenig methodische Erkentnisse
- **Theoriespezifische Spezialverfahren**
  - Entscheidungsprozeduren für Gleichheit, Arithmetik, etc.
  - Rewrite-Verfahren zur Auswertung von Termen
  - Präfixbehandlung für Verarbeitung nichtklassischer Logiken
  - Verfahren können in den Unifikationsalgorithmus integriert werden

Inferenzmethoden

Einheit 11

Theorie- und Gleichheitsbehandlung

1. Theoriekonnektionen & Unifikationstheorie
2. Axiomatische Gleichheitsbehandlung
3. Gleichheitskonnektionen
4. Resolution und Gleichheit

Separate Verarbeitung spezieller Inferenzen

- **Theorien sind gekennzeichnet durch Axiome**
  - z.B. Reflexivität, Symmetrie, Transitivität, Substitutivität für Gleichheit
    Assoziativität, Identität, Inverse für Gruppen
    Peano-Axiome für natürliche Zahlen
  - Axiome sind die "Grundwahrheiten" der Theorie, aus denen alles folgt
- **Viele Theorien benutzen spezielle Inferenzketten**
  - Standardargumente um Axiome effizient in Schlußfolgerungen einzusetzen
  - z.B. gezieltes Einsetzen von Substitutivität beim Gleichheitsschließen
- **Allgemeine Beweiser unterstützen dies nicht**
  - Theoriespezifische Inferenzen passen nicht zum allgemeinen Verfahren
  - Beweiser müssen die Axiome als zusätzliche Klauseln hinzunehmen

Einbettung von Theorien in Beweisverfahren

Beweise $Pa \wedge a{=}b \;\Rightarrow\; Pb$ aus Gleichheitsaxiomen

- **Konventioneller Matrixbeweis mit Axiomen**

$$\begin{bmatrix} Pa^T & a{=}b^T & x{=}y^F & x{=}y^F & x{=}x^T & x{=}y^F & Pb^F \\ & & y{=}z^F & y{=}x^T & & Px^F & \\ & & x{=}z^T & & & Py^T & \end{bmatrix}$$

  – Gleichheitsaxiome sind in die Matrix integriert

  – Viele Schritte bei der Beweissuche nötig

- **Integriere Theorie durch spezielle Konnektionen**

$$\begin{array}{c} \boxed{EQ} \\ 1 \quad 2 \quad 3 \\ \begin{bmatrix} Pa^T & a{=}b^T & Pb^F \end{bmatrix} \end{array} \qquad \text{wobei } \boxed{EQ} \equiv \begin{bmatrix} x{=}y^F & x{=}y^F & x{=}x^T & x{=}y^F \\ y{=}z^F & y{=}x^T & & Px^F \\ x{=}z^T & & & Py^T \end{bmatrix}$$

  – Theoriekonnektion beinhaltet Inferenzschritte der Theorie EQ

Theoriekonnektionen

- **Erweiterter Komplementaritätsbegriff für Theorien**
  - $P\,t_1{}^T$ und $P\,t_2{}^F$ sind komplementär in der Theorie $\mathcal{T}$, wenn $\sigma(t_1)$ und $\sigma(t_2)$ in $\mathcal{T}$ gleich sind (σ zulässige Substitution)
  - Erlaubt Verarbeitung theoriespezifischer Inferenzketten
- **Unifikation ist mehr als syntaktisches Gleichmachen**

$$\begin{bmatrix} & & P(1)^F \\ \text{Arith} & & \\ P((x{+}x){-}1)^T & & \end{bmatrix} \quad \sigma{=}[1/x]$$

  - Konnektion benutzt Unifikation für einfache Arithmetik

$$\begin{bmatrix} & R(z{\cdot}(\overline{c}{\cdot}c), z{\cdot}(\overline{z}{\cdot}b))^F \\ \text{Group} & \\ R(c,b)^T & \end{bmatrix} \quad \sigma{=}[c/z]$$

  - Konnektion benutzt Unifikation für Gruppentheorie
- **Allgemeiner Mechanismus noch unerforscht**
  - Meist Integration von Theorie-Unifikation in konventionellen Beweiser

Unifikationstheorie

$$\left[\begin{array}{ccc} & \boxed{\mathcal{A}} & \\ 1 & 2 & 3 \\ a<b^T & b=c+1^T & a\leq c^F \end{array}\right]$$

- **$\{a<b^T, b=c+1^T, a\leq c^F\}$ komplementär in Theorie $\mathcal{A}$**
  - Konnektionen können auch unär oder ternär sein
  - Konnektionen auch zwischen verschiedenartigen Literalen möglich
    z.B. bei Verwendung der Axiome $x<y \Rightarrow x+1\leq y$ und $x+1\leq y+1 \Rightarrow x\leq y$
  - Unifikationsmechanismus muß ganze Literale wie Terme behandeln
- **Es gibt noch viele offene Fragen**
  - Wie genau Unifizierbarkeit modulo Theorie $\mathcal{T}$ definieren?
  - Gibt es mgu's und, wenn ja, wieviele?
  - Gibt es Unifikationsalgorithmen (als Entscheidungsprozeduren)?
  - Was ist die Komplexität des Unifikationsverfahrens?
- **Bisher gibt es nur wenig allgemeine Lösungen**
  - Erfolgreich nur für spezielle Theorien (Gleichheit, Gruppen, ...)

Typen von Unifikationstheorien

- **unitäre:**
  - Es gibt (bei Unifizierbarkeit) genau einen allgemeinsten Unifikator
  - z.B. Standard-Unifikation
- **finitäre:**
  - Es gibt bei endlich viele allgemeinste Unifikatoren
  - z.B. AC-Unifikation, Präfix-Unifikation
- **infinitäre:**
  - Es gibt unendlich viele allgemeinste Unifikatoren
  - z.B. Unifikation modulo Assoziativität
- **leere:**
  - Es gibt i.a. keine allgemeinsten Unifikatoren
  - Wenig erwünscht

Die Theorie der Gleichheit

- **Wichtigste Grundbeziehung zwischen Objekten**
  - Spezialbehandlung sehr lohnenswert
  - Dargestellt als zweistelliges Prädikat zwischen Termen
  - Prädikatszeichen $\doteq$ in Infix-Notation
- **Charakterisiert durch 5 Grundeigenschaften**
  - $x \doteq x$ Reflexivität
  - $x \doteq y \;\Rightarrow\; y \doteq x$ Symmetrie
  - $x \doteq y \wedge y \doteq z \;\Rightarrow\; x \doteq z$ Transitivität
  - $x_i \doteq y \;\Rightarrow\; f(x_1, .., x_i, .., x_n) \doteq f(x_1, .., y, .., x_n)$
    Substitutivität auf Funktionen (Schema)
  - $x_i \doteq y \;\Rightarrow\; [P(x_1, .., x_i, .., x_n) \Leftrightarrow P(x_1, .., y, .., x_n)]$
    Substitutivität auf Prädikaten (Schema)
- **Symmetrie und Transitivität sind ableitbar**

Gleichheitsbeweisen ohne Verdichtung

- **Erweitere Formel um Axiome der Gleichheit**
- **Verwende minimale Axiomenmenge**
  - $x \doteq x$
  - $x_i \doteq y \;\Rightarrow\; f(x_1,..,x_i,..,x_n) \doteq f(x_1,..,y,..,x_n)$
  - $x_i \doteq y \;\Rightarrow\; [P(x_1,..,x_i,..,x_n) \Rightarrow P(x_1,..,y,..,x_n)]$

  Das Schema der Substitutivität muß für jedes vorkommende Funktions- und Prädikatssymbol instantiiert werden
- **Erhebliche Vergrößerung des Suchraums**
  - Unbrauchbar für komplexe Formeln

- **Axiomatische Gleichheitsbehandlung ist aufwendig**
  – Einfache Beweise wie $Pf(a,b) \wedge a \doteq c \;\Rightarrow\; Pf(c,b)$ werden umständlich

$$\begin{bmatrix} x\doteq y^F & x\doteq y^F & & & \\ f(x,z)\doteq f(y,z)^F & Px^F & Pf(a,b)^T & a\doteq c^T & Pf(c,b)^F \\ & Py^T & & & \end{bmatrix} \longrightarrow \begin{bmatrix} Pf(a,b)^T & a\doteq c^T & Pf(c,b)^F \end{bmatrix}$$

  – Menschen gehen direkter mit Gleichheiten um
- **Verdichte Beweisführung durch eq-Konnektion**
  – Konnektion verbindet Literalpaar und ein oder mehrere Gleichungen
  – Unifikation darf konnektierte Gleichheiten berücksichtigen
- **Strategische Steuerung wird aufwendiger**
  – Welche Gleichheiten sind geeignet? (i.a. unentscheidbares Problem)
  – Sehr kompliziert, wenn gleichzeitig Substitutionen zu bestimmen sind

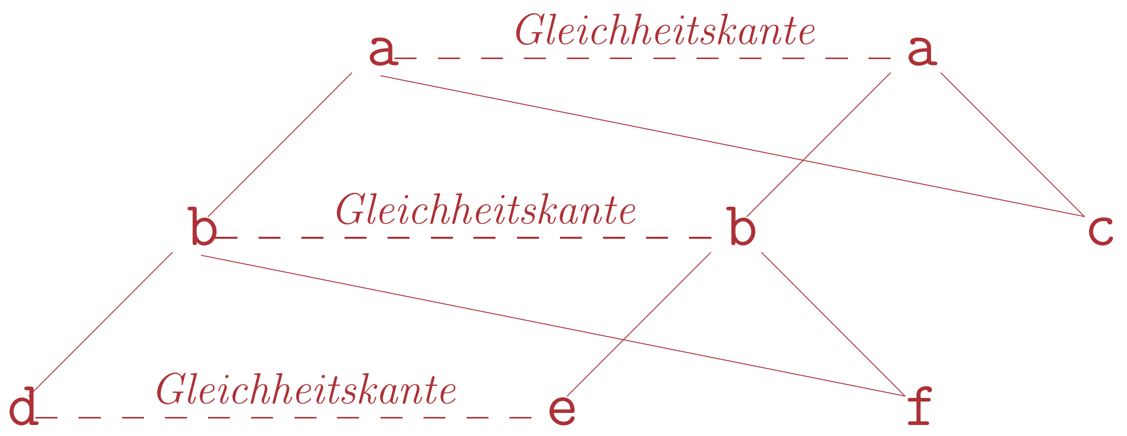
Entscheidungsprozedur für einfache Gleichheit

Folgt eine Gleichheit aus anderen Gleichheiten?

- **Wichtig für praktische Beweisführung**
  - z.B.: $f(f(a,b),b) \doteq a$ folgt aus $f(a,b) \doteq a$
    $g(a) \doteq a$ folgt aus $g(g(g(a))) \doteq a$ und $g(g(g(g(g(a))))) \doteq a$
  - Intuitiver Beweis (gezieltes Einsetzen) einfach
- **Quantorenfreie Gleichheit ist entscheidbar**
  - Einfache Theorie: Gleichheiten mit uninterpretierten Symbolen
  - Semantik: Reflexivität, Symmetrie, Transitivität, Substitution
- **Effiziente Verfahren verfügbar**
  - Berechnung der transitiven Hülle einer Äquivalenzrelation
  - Technisch: Kongruenzabschluß des Relationsgraphen
- **Entscheidungsprozedur ist keine Unifikation**
  - Verfahren überprüft Gleichheiten, aber instantiiert keine Variablen

Gleichheitsschliessen am Beispiel

Zeige: $\texttt{a(b(d,f),c)} \doteq \texttt{a(b(e,f),c)}$ **folgt aus** $\texttt{d} \doteq \texttt{e}$



1. Verschmelze identische Knoten
2. Verbinde gleiche Knoten durch Gleichheitskante
3. Verbinde Wurzeln von Teilbäumen, die in allen Knoten gleich sind

Gleichheit $\hat{=}$ Wurzeln der Termbäume sind verbunden

Wichtige graphentheoretische Konzepte

- **Notationen für gerichtete Graphen $G = (V, E)$**
  - $\boldsymbol{l(v)}$: Markierung des Knoten v in G
  - $\boldsymbol{\delta(v)}$: Anzahl der von v ausgehenden Kanten
  - $\boldsymbol{v[i]}$: i-ter Nachfolgerknoten von v
  - u **Vorgänger** von v, wenn $v = u[i]$ für ein i
- **Begriffe für Äquivalenzrelationen R auf V**
  - **u und v kongruent unter R** ($\boldsymbol{u \sim_R v}$):
    $l(u) = l(v),\ \ \delta(u) = \delta(v)$ und für alle i $(u[i], v[i]) \in R$
  - **R abgeschlossen unter Kongruenzen**: $u \sim_R v \ \Rightarrow\ (u, v) \in R$
  - **Kongruenzabschluß R^***: eindeutige minimale Erweiterung von R, die abgeschlossen unter Kongruenzen und Äquivalenzrelation ist
    $\hat{=}$ Menge aller Äquivalenzen, die logisch aus R folgen

Gleichheitsschliessen als Kongruenzabschluss

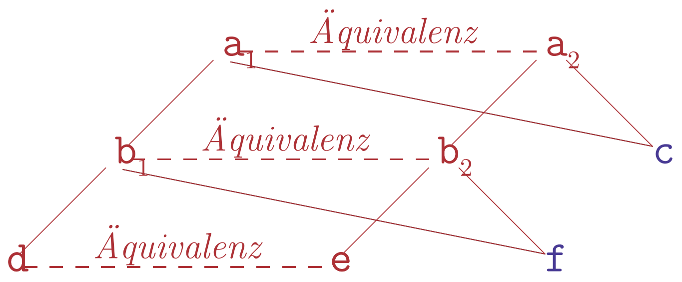
Folgt $s \doteq t$ aus $s_1 \doteq t_1, \ldots, s_n \doteq t_n$?

- **Konstruiere Graph G von $s, s_1, .., s_n,\ t, t_1, .., t_n$**
  - G besteht aus Termbäumen von $s, s_1, .., s_n,\ t, t_1, .., t_n$
  - Identische Teilausdrücke werden durch denselben Teilbaum dargestellt
- **Bestimme Kongruenzabschluß der $s_i \doteq t_i$ iterativ**
  - Start: Wähle R als Identitätsrelation auf den Knoten von G ($R^* = R$)
  - Im Schritt i bestimme Kongruenzabschluß von $R^* \cup \{(\tau(s_i), \tau(t_i))\}$

    ($\tau(u)$: Wurzelknoten des Termbaums von u)
  - Repräsentiere R^* als Menge von Äquivalenzklassen $\{\, [u]_R \mid u \in V \,\}$

    ($[u]_R \ \equiv\ \{x \in V \mid (x, u) \in R\}$)
- **Teste Äquivalenz von s und t**
  - $s \doteq t$ gilt genau dann, wenn $(\tau(s), \tau(t)) \in R^*$

Kongruenzabschluss: $d \doteq e \;\Rightarrow\; a(b(d,f),c) \doteq a(b(e,f),c)$



- **Graph ist Termbaum von $a(b(d,f),c)$ und $a(b(e,f),c)$**
  - Identische Teilausdrücke benutzen denselben Teilbaum
  - Initiale Relation: $R := \{\,\{a_1\},\{a_2\},\{b_1\},\{b_2\},\{c\},\{d\},\{e\},\{f\}\,\}$

- **Hinzunahme von $d \doteq e$**

  Bestimme Vorgänger von $[d]_R$ ($\{b_1\}$) und $[e]_R$ ($\{b_2\}$)
  - Vereinige $[d]_R$ und $[e]_R$: $R := \{\,\{a_1\},\{a_2\},\{b_1\},\{b_2\},\{c\},\{d,e\},\{f\}\,\}$

  Bestimme Vorgänger von $[b_1]_R$ ($\{a_1\}$) und $[b_2]_R$ ($\{a_2\}$)
  - Vereinige $[b_1]_R$ und $[b_2]_R$: $R := \{\,\{a_1\},\{a_2\},\{b_1,b_2\},\{c\},\{d,e\},\{f\}\,\}$

  Bestimme Vorgänger von $[a_1]_R$ ($\emptyset$) und $[a_2]_R$ ($\emptyset$)
  - Vereinige $[a_1]_R$ und $[a_2]_R$: $R := \{\,\{a_1,a_2\},\{b_1,b_2\},\{c\},\{d,e\},\{f\}\,\}$

  Wurzelknoten der beiden Terme sind äquivalent

BERECHNE KONGRUENZABSCHLUSS VON $R \cup \{(u,v)\}$

- **Algorithmus** MERGE(R,u,v)
  – Eingabe: gerichteter Graph $G = (V, E)$, u, $v \in V$
  Äquivalenzrelation R (abgeschlossen unter Kongruenzen)
- **Falls $u \sim_R v$, dann halte mit Ergebnis R**
  – Es gilt $(R \cup \{(u, v)\})^* = R$
- **Andernfalls modifiziere R durch Verschmelzung**
  – Setze $P_u := \{x \in V \mid \exists w \in [u]_R.\ x \text{ Vorgänger von } w\}$
  – Setze $P_v := \{x \in V \mid \exists w \in [v]_R.\ x \text{ Vorgänger von } w\}$
  – Vereinige Äquivalenzklassen $[u]_R$ und $[v]_R$ in R
  – Wiederhole für $x \in P_u$ und $y \in P_v$
  Falls $x \sim_R y$ und $[x]_R \neq [y]_R$ dann setze R:=MERGE(R,x,y)

  Halte mit der modifizierten Relation R als Ergebnis

Kongruenzabschluss: $g(g(g(a)))\doteq a, \quad g(g(g(g(g(a)))))\doteq a$

- **Graph ist Termbaum von $g(g(g(g(g(a)))))$**
  - Initiale Relation: $R := \{\, \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\}, \{v_6\}\, \}$
- **Hinzunahme von $g(g(g(g(g(a)))))\doteq a$**
  - $R := \{\, \{v_1, v_6\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_5\}\, \}$ ist abgeschlossen
- **Hinzunahme von $g(g(g(a)))\doteq a$**

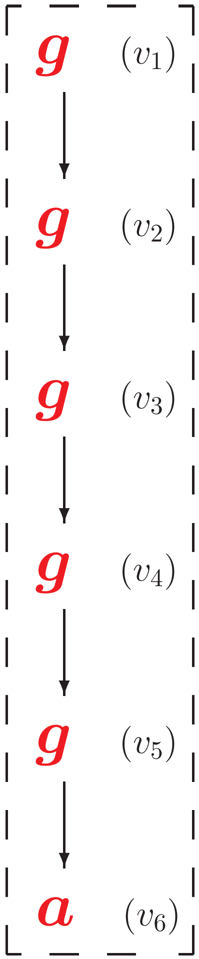
  MERGE(R,v_3,v_6):
  - $P_{v_3} := \{v_2\}, \quad P_{v_6} := \{v_5\}, \quad R := \{\, \{v_1, v_6, v_3\}, \{v_2\}, \{v_4\}, \{v_5\}\, \}$
  - Wegen $(v_3, v_6) \in R$ gilt $v_2 \sim_R v_5$ aber $[v_2]_R \neq [v_5]_R$

  MERGE(R,v_2,v_5):
  - $P_{v_2} := \{v_1\}, \quad P_{v_5} := \{v_4\}, \quad R := \{\, \{v_1, v_6, v_3\}, \{v_4\}, \{v_2, v_5\}\, \}$
  - Wegen $(v_2, v_5) \in R$ gilt $v_1 \sim_R v_4$ aber $[v_1]_R \neq [v_4]_R$

  MERGE(R,v_1,v_4):
  - $P_{v_1} := \{v_2, v_5\}, \quad P_{v_4} := \{v_3\}, \quad R := \{\, \{v_1, v_6, v_3, v_4\}, \{v_2, v_5\}\, \}$
  - Wegen $(v_6, v_4) \in R$ gilt $v_5 \sim_R v_3$ aber $[v_5]_R \neq [v_3]_R$

  MERGE(R,v_5,v_3):
  - $P_{v_5} := \{v_1, v_4\}, \quad P_{v_3} := \{v_2, v_5, v_3\}, \quad R := \{\, \{v_1, v_6, v_3, v_4, v_2, v_5\}\, \}$

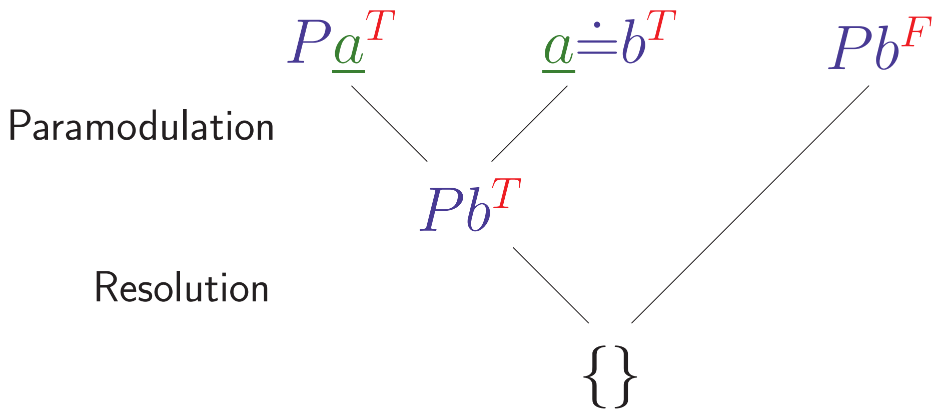
  Alle Knoten sind äquivalent: $R = R^*$



Gleichheitsbehandlung in Resolutionsbeweisern

- **Resolutionsähnliche Kalkülregel Paramodulation**
  - Wähle zwei Elternklauseln $\{L\}\cup C_1$ und $\{r \doteq s\}\cup C_2$ und kennzeichne einen Teilterm t von L
  - Bestimme allgemeinsten Unifikator σ von r und t
  - Generiere Paramodulant $\sigma(\{L'\}\cup C_1 \cup C_2)$, wobei $L' =$ "$L[s/t]$"

  Zusammen mit Resolution vollständig für Prädikatenlogik mit Gleichheit



- **Alternative Sicht als bedingte Termersetzungsregel**
  - C_2 ist Bedingung für die Ersetzung von r durch s in einem Literal L

Probleme der Paramodulation mit Unifikation

- **Welche Richtung einer Gleichheit wird gewählt?**

$$Qb \lor P\underline{x}^T \qquad \underline{a} \doteq b \lor Rb^T$$

$$Qb \lor Pb \lor Rb^T$$

$$\sigma = [a/x]$$

$$Qb \lor P\underline{x}^T \qquad a \doteq \underline{b} \lor Rb^T$$

$$Qb \lor Pa \lor Rb^T$$

$$\sigma = [b/x]$$

- **Welches Variablenvorkommen wird ersetzt?**

$$P\underline{x}x \lor Qb^T \qquad \underline{a} \doteq b \lor Rb^T$$

$$Pba \lor Qb \lor Rb^T$$

$$\sigma = [a/x]$$

$$Px\underline{x} \lor Qb^T \qquad \underline{a} \doteq b \lor Rb^T$$

$$Pab \lor Qb \lor Rb^T$$

$$\sigma = [a/x]$$

Resolution und Gleichheit

- **Koppelung von Resolution + Paramodulation**
  - Vollständig und konsistent für Prädikatenlogik mit Gleichheit
  - Benötigt Reflexivitätsaxiom
- **Lokale Sicht bedeutet großen Suchraum**
  - Viele Paramodulanten möglich
  - Effiziente Suchstrategien erforderlich
- **Strategien für Resolution mit Gleichheit**
  - Demodulation: gerichtete Anwendung von Gleichheiten $\longmapsto$ Rewriting
  - E–Resolution: komplexes Äquivalent zu eq-Konnektionen und eq-Literalen
  - RUE–Resolution: Erzeugung von Paramodulationsgleichungen bei Bedarf

E–Resolution

Resolution nach Einsetzung assoziierter Gleichungen

$$\{Qgy^{T},\ P(c,h(f(a,y),b))^{T}\} \qquad \{P(a,h(gc,d))^{F}\}$$

$$\{Ra^{T},\ a\doteq c^{T}\} \qquad \{b\doteq d^{T}\} \qquad \{f(x,e)\doteq gz^{T},\ Qx^{T}\}$$

$$\{Ra^{T},\ Qge^{T},\ Qa^{T}\}$$

- **Bedingungsliterale der Gleichungen bleiben in Resolvente**
- **Vollständig und korrekt**
- **Durchführung aufwendig**
  – Suche nach geeigneten Gleichungen unentscheidbar

RUE–Resolution

Unterteilung von E-Resolution in Teilschritte

- **Resolution anwendbar auch ohne Unifizierbarkeit der Literale**
  - Verbleibende Gleichheitsbedingungen erscheinen in Resolvente
  - Gleichheitsbedingungen werden später verarbeitet

$$\{Qgy^T,\ P(c,h(f(a,y),b))^T\} \qquad \{P(a,h(gc,d))^F\}$$

$$\{Qgy^T,\ c\doteq a^F,\ fay\doteq gc^F,\ b\doteq d^F\}$$

- **Paramodulation wird nur bei Bedarf ausgeführt**
  - Bessere Steuerung bei Suche nach geeigneten E-Resolventen