Implementierung der Regularität in PL

Problem:

Enthält ein Ast

- $L = p(s_1, \dots, s_n)$ und
- $L' = p(t_1, \dots, t_n)$,

dann kann spätere Instantiierung der Variablen die Literal L, L' unifizieren und so Regularität verletzen.

Lösung Letz et al. (1992):

Erzeuge **Constraint** der Form

$\mathcal{C} = (s_1 \neq t_1 \vee \cdots \vee s_n \neq t_n)$

„$=$“ ist syntaktische Identität.

Fortan wende alle Substitutionen auch auf $\mathcal{C}$ an.

Verwende nur Substitutionen σ,
die $\mathcal{C}\sigma$ für alle Constraints $\mathcal{C}$ erfüllen.

Erzeuge `fail`, falls ein $\mathcal{C}\sigma$ unerfüllbar.

Satz. Vollständigkeit mit Regularität
Für jede unerfüllbare PL Klauselmenge existiert ein geschlossenes *reguläres* Konnektionstableau. ■

Lifting wird von Regularität nicht beeinträchtigt, also genügt der Beweis der Vollständigkeit im aussagenlogischen Fall.

Zunächst aber Beweis eines Lemmas ...

Lemma. Sei S eine minimal unerfüllbare (mU) AL Klauselmenge. Ferner sei

- $C \in S$ eine Klausel in S,
- $D \subseteq C$ eine Teilklausel von C,
- S'' eine Teilmenge von $S' = (S - \{C\}) \cup \{D\}$.

Ist S'' mU, dann gilt:

1. $D \in S''$,
2. $D \not\subseteq D''$ für alle $D \neq D'' \in S''$.

■

Beweis:

1. Angenommen, D ist nicht in S''.
   Dann gilt $S'' \subseteq S' - \{D\} = S - \{C\} \subsetneq S$. Also ist S nicht mU. Widerspruch.

2. Angenommen $D \subseteq D'' \in S''$, $D \neq D''$.
   Da S'' mU, hat $S'' - \{D''\}$ ein Modell. Dieses ist auch Modell von D, damit aber auch von D'' und also von S''. Widerspruch.

■

Beweis: Vollständigkeit aussagenlogischer Konnektionstableaus mit Regularität.

S ist o.B.d.A. minimal unerfüllbar.

Wir zeigen per Induktion über die Anzahl n der Literal*auftauchen* in S:

> Für jede Nicht-Einerklausel $C \in S$ gibt es ein geschlossenes reguläres Konnektionstableau für S, in dem der erste Erweiterungsschritt mit C erfolgt.

Dies genügt, da Fälle, in denen es keine Nicht-Einerklauseln gibt, trivial sind (s.u.).

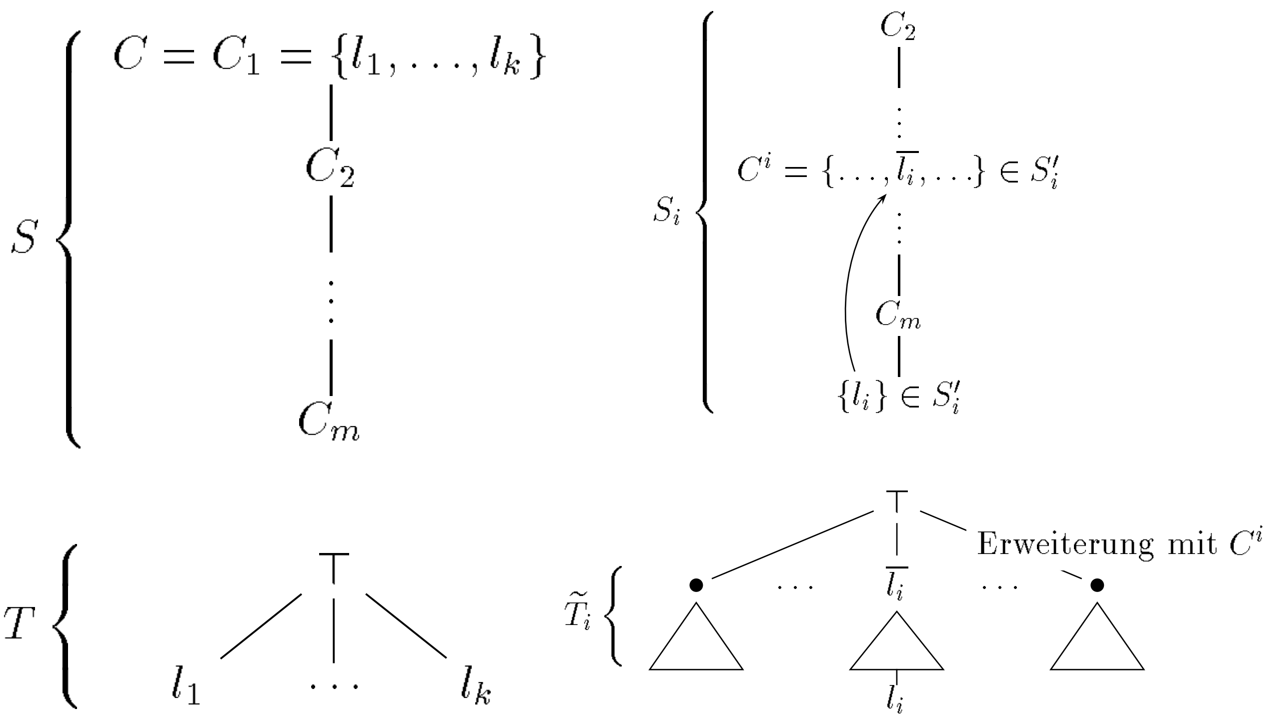
$\mathbf{n = 1}$:
Tritt nicht auf, da S mU.

$\mathbf{n = 2}$:
Wegen mU ist S von der Form $\{\{p\}, \{\neg p\}\}$. Trivial.

$\mathbf{n > 2}$:
Sei $S = \{C_1, \ldots, C_m\}$.
Wegen mU muß es eine Nicht-Einerklausel geben.
O.B.d.A. sei $C = C_1 = \{l_1, \ldots, l_k\} \in S$ eine solche.

Sei T das Tableau, das nach dem ersten Erweiterungsschritt mit $C = C_1$ entstanden ist.

T is offensichtlich regulär und konnektiert.



Sei $S_i = \{\{l_i\}, C_2, \ldots, C_m\}$ für $1 \leq i \leq k$.

Aus dem Lemma folgt:
$\{l_i\}$ kommt in einer mU Teilmenge S'_i von S_i vor.

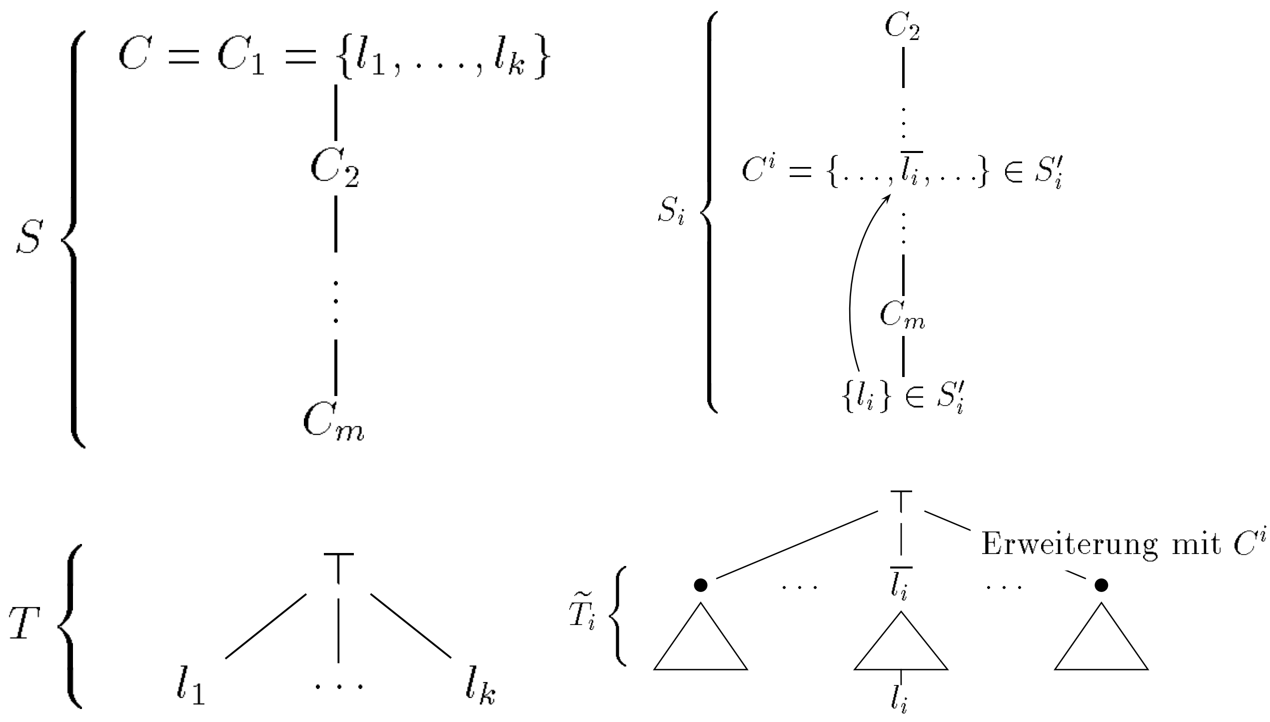
Wegen mU von S'_i hat $\{l_i\}$ Link mit $C^i \in S'_i$.

Ist C^i Einerklausel, wird der i-te Ast von T mit $C^i \in S$ erweitert und geschlossen.

Andernfalls hat S'_i weniger Literalvorkommen als S und die Induktionshypothese liefert ein reguläres Konnektionstableau T_i für $S_i \supseteq S'_i$, in dem zuerst mit C^i erweitert wird.

Der Wald $\widetilde{T}_i$ entstehe aus den T_i durch Löschung der Wurzeln $\top$.

Erweitere jeden noch offenen Ast in T mit Blatt l_i durch „Ankleben“ von $\widetilde{T}_i$.



Neues Tableau T' ist geschlossen, da jedes der $\widetilde{T}_i$ geschlossen ist.

T' ist ein Konnektionstableau, da jedes $\widetilde{T}_i$ eines ist und durch Wahl der Start-Klauseln C^i.

Jedes der $\widetilde{T}_i$ ist regulär.

Aus dem Lemma folgt, daß l_i nur in der Einerklausel in S_i' vorkommt, und also höchstens als Blatt in $\widetilde{T}_i$.

Ersetze alle Erweiterungsschritte mit $\{l_i\}$ in $\widetilde{T}_i$ durch einen Abschluß mit dem obenstehenden l_i in T.

Ergebnis: reguläres Konnektionstableau. ∎

Geordnete Tableaus
Tableaus mit Selektionsfunktion

Ziele:

– Umgehung der Problematik, daß Startklausel in mU Menge sein muß (welche i.a. unbekannt ist).

– Stärkere Einschränkung der Auswahlregel als bei schwachen Konntektionstableaus.

– Beibehaltung der Beweiskonfluenz.

Lösung:

– Verschärfe die Linkbedingung schwacher Konnektionstableaus.

– Erlaube unter gewissen Umständen Erweiterung mit Klauseln ohne Link.

A-Ordnungen

Definition. Eine A-**Ordnung** ist eine irreflexive, transitive Relation $< \subseteq \mathrm{At}_\Sigma \times \mathrm{At}_\Sigma$ mit:

Für alle $p, q \in \mathrm{At}_\Sigma$ und Substitutionen σ:
Aus $p < q$ folgt $p\sigma < q\sigma$.

(Substitutivität)

■

Definition. Seien L, L' Literale und eine C Klausel.

$L < L'$ gelte genau dann, wenn $\mathrm{atom}(L) < \mathrm{atom}(L')$.

L heiße $<$-**maximal** in C, falls es kein $L' \in C$ mit $L' > L$ gibt. ■

A-Ordnungen sind partiell. Insbesondere gilt:
$L \not< L'$ und $L' \not< L$ falls $\{L, L'\}$ unifizierbar.

Beispiel A-Ordnung

Termtiefe $\tau(t)$ für $t \in \mathsf{Term}_\Sigma$:
maximale Differenz zwischen öffnenden und schließenden Klammern in zusammenhängendem Teilwort von t plus 1.

Tiefe $\tau_{\max}(s,t)$ **eines Unterterms** s in t:
entsprechend, beschränkt auf Teilwörter, die direkt links von s enden.

Proposition. Für $p, q \in \mathsf{At}_\Sigma$ sei $p \prec q$, falls

– $\tau(p) < \tau(q)$ und

– $\mathsf{Var}(p) \subseteq \mathsf{Var}(q)$

– $\tau_{\max}(x,p) < \tau_{\max}(x,q)$ für alle $x \in \mathsf{Var}(p)$.

$\prec$ ist eine A-Ordnung. ■

Beispiele.

$$p(x,x) \prec q(f(x),y) \qquad p(x,f(a)) \not\prec q(x,f(x))$$
$$p(x,y) \prec r(g(x,y)) \qquad p(x,a) \not\prec p(f(a),x)$$

Extraktion von Ordnungen

Geeignete Ordnungen können zum Teil aus konkreten Problemen extrahiert werden.

Für SW-Verifikation werden i.a. ADT der Objektprogramme mittels Gleichungen oder Äquivalenzen definiert, z.B.:

$$\begin{array}{l} \mathsf{append(cons(a,x),y)} = \mathsf{cons(a,append(x,y))} \\ \mathsf{x} \neq \mathsf{nil} \rightarrow \\ \quad \mathsf{cons(car(x),append(cdr(x),y))} = \mathsf{append(x,y)} \end{array}$$

Definiere $f > g$ für oberste Funktions- bzw. Prädikatensymbole.

Vermeide Regeln der Form $\phi \rightarrow \sigma = \tau$, falls $\tau\nu$ mit Unterterm von σ unifizierbar.

Im Beispiel also: append $>$ cons

Erweitere $<$ auf Term_Σ, At_Σ mittels:

$s = f(t_1, \ldots, t_n) < g(s_1, \ldots, s_m) = t$ gdw

1. $f < g$, oder $f = g$, $n = m$ und $t_i < s_i$ für $i = 1, \ldots, n$;
2. $\mathsf{Var}(s) \subseteq \mathsf{Var}(t)$.

Geordnete Tableaus, 1. Versuch

Idee:

Schwache Konnektionstableaus, wobei das Link-Literal $<$-maximal in der erweiternden Klausel sein muß.

Aber: **Unvollständig!**

Beispiel für Unvollständigkeit:

$S = \{\{A, \boxed{B}\},\ \{\neg A, \boxed{B}\},\ \{\boxed{\neg B}\}\}$.

$A < B$ und Start mit einer der ersten beiden Klauseln.

S ist minimal unerfüllbar.

Es gibt Beispiele, die unabhängig von der Wahl der Startklausel sind.

Geordnete Tableaus, 2. Versuch

Definition. Ein **schwaches Konnektionstableau mit Neustart** für eine endliche Klauselmenge S ist ein endlichverzweigender, mit Literalen markierter Baum, konstruiert mittels:

1. ... initiales Tableau ...

2. T sei ein Klauseltableau für S, B ein Ast von T, $C = \{L_1, \ldots, L_n\}$ eine Klausel in S und σ eine Substitution, so daß es

   (i) ein $L \in B$ oder
   (ii) ein $L \in C' \in S$

   gibt und $\langle L\sigma, L_i\sigma \rangle$ für ein $1 \leq i \leq n$ ein komplementäres Paar ist.

   Ein neues Klauseltableau für S entsteht aus $T\sigma$, indem B durch n neue Nachfolger mit Markierungen $L_1\sigma$, ... ,$L_n\sigma$ erweitert wird.

3. ... Reduktionsschritt ...

■

Im Fall (ii) heißt C **Neustartklausel**.

Schwache Konnektionstableaus mit Neustart sind Basis für geordnete Tableaus:

Definition. Ein **geordnetes Tableau** für eine endliche Klauselmenge S ist ein schwaches Konnektionstableau mit Neustart, wobei zusätzlich gilt:

1. Bei Erweiterung mit $C\sigma = \{L_1\sigma, \ldots, L_n\sigma\}$ muß das Link-Literal $L_i\sigma$ $<$-maximal in $C\sigma$ sein.

2. Bei einem Neustart muß zudem das andere Link-Literal $L\sigma$ $<$-maximal in $C'\sigma$ sein (wobei $C' \in S$).

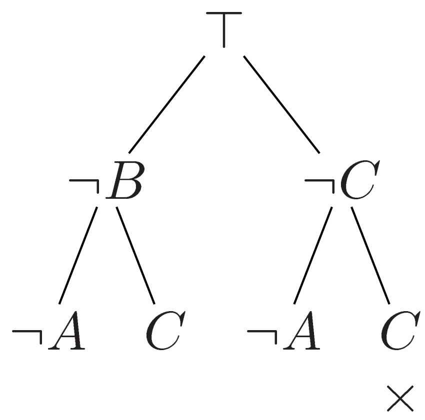
■

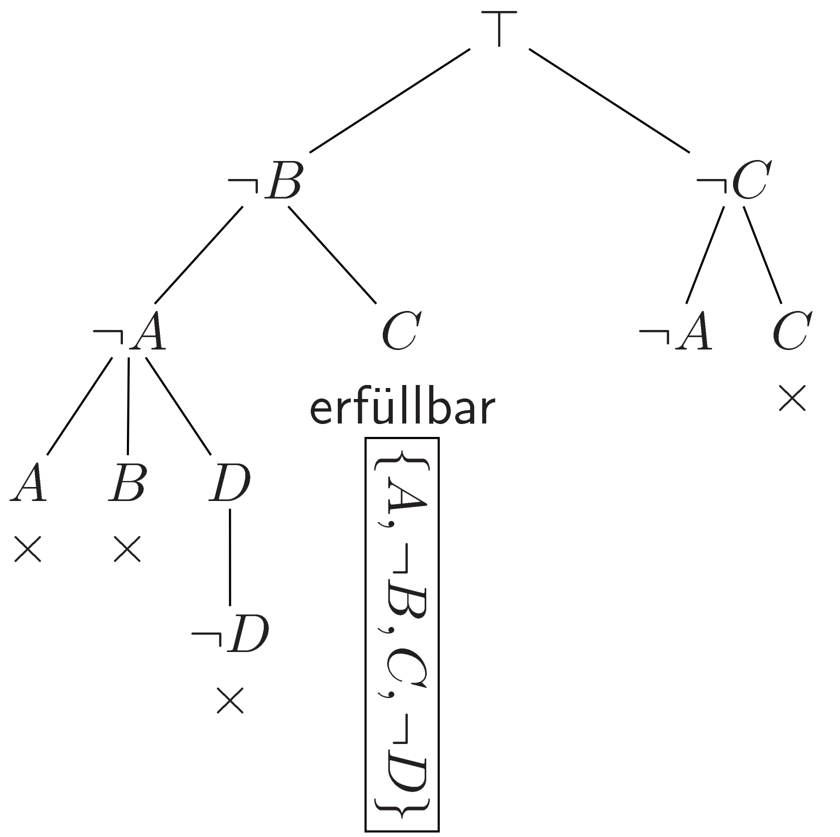
Die Einschränkung gilt auch für ersten Erweiterungsschritt.

Beispiel.

Sei $D < B < A < C$:

$$S = \{\{\neg B,\ \boxed{\neg C}\},\ \{\boxed{A},\ B,\ D\},\ \{\neg A,\ \boxed{C}\},\ \{\boxed{\neg D}\}\}$$





Satz. Vollständigkeit
Sei S eine unerfüllbare Menge von Klauseln;
sei $<$ eine beliebige A-Ordnung.

Dann gibt es ein geschlossenes reguläres $<$-geordnetes Klauseltableau für S.

Geordnete Klauseltableaus sind beweiskonfluent. ■

Beweis: Lifting wird von wegen der Substitutivität von A-Ordnungen nicht beeinträchtigt. Daher genügt es den Satz für den aussagenlogischen Fall zu zeigen.

Ein Ast B heiße **saturiert**, falls er offen ist und für alle $C \in S$:

a. C wurde auf B verwendet oder

b. Erweiterung von B mit C verletzt Bedingungen der Erweiterungsregel

c. Erweiterung mit C verletzt die Regularität.

Gibt es für S kein geschlossenes geordnetes Klauseltableau, dann gibt es offenbar eines mit saturiertem Zweig B.

I sei die durch Literale auf B definierte partielle Interpretation von S:

$$I(p) = \begin{cases} W & \text{falls } p \text{ auf } B \\ F & \text{falls } \neg p \text{ auf } B \end{cases}$$

I ist wohldefiniert, da B offen.

$S' \subseteq S$ sei $\{C \in S \mid I \not\models C\}$.

Auf Klauseln in S' trifft nach Definition von S' und Regularität genau (b) zu.

Sei I' Menge der $<$-maximalen Literale in S'.

I' ist wohldefiniert, sonst Neustart möglich und alsoäre Saturiertheit von B verletzt.

$I \cup I'$ ist wohldefiniert, sonst wäre Erweiterung von B mit C möglich.

Also $I' \models S'$ und damit $I \cup I' \models S$. Widerspruch! ■

Tableaus mit Selektionsfunktion

Jede A-Ordnung $<$ induziert **Selektionsfunktion** $f_<$ auf Klauseln:

$$f_<(C) = \{L \in C \mid L\ <\text{-maximal in } C\}$$

Alle Resultate gelten immer noch falls

- „L $<$-maximal in C“ ersetzt durch „$L \in f(C)$“, wobei
- f jeder Klausel eine beliebige nichtleere Teilmenge ihrer Literale zuweist.

Echte Verallgemeinerung, denn:
$f(\{A, B\}) = A,\ f(\{B, C\}) = B,\ f(\{A, C\}) = C$
nur von zyklischer „Ordnung“ induziert.

Implementierung:

Problematik und Lösung wie bei Regularität.

Verfeinerungen: Pro und Contra

Tableauverfeinerungen schränken Suchraum ein

Aber sie haben auch Nachteile

1. Falls nicht beweiskonfluent:
   Implementierung erfordert Backtracking, keine Gegenbeispiele.

2. Kombination von für sich genommen vollständigen Verfeinerungen kann unvollständig sein.

3. Es gibt Formelklassen Φ_n, deren kürzeste Beweise mit verfeinerten Tableaus exponentiell länger sind als ihre kürzesten Beweise mit Klauseltableaus.