Formale Grundlagen der Informatik 1
Kapitel 17
Ableitungen und Resolution

Frank Heitmann
heitmann@informatik.uni-hamburg.de

15. & 16. Juni 2015

Motivation

Der Sinn von **Ableitungen**:

- Aufgrund **syntaktischer Eigenschaften** von Formeln/Formelmengen auf **semantische Eigenschaften schließen** (statt Wahrheitswerteverläufe zu erstellen und zu prüfen).

Dies ist vor allem auch deswegen wichtig, da für komplexere Logiken (wie die Prädikatenlogik) i.A. die Tabellen nicht mehr komplett aufgebaut werden können!

Beispiel

Unabhängig von F ist

- $F \vee \neg F$ eine Tautolgoie
- $F \wedge \neg F$ eine Kontradiktion

Dies kann man allein am **syntaktischen Muster** erkennen!

Ähnlich kann man schlussfolgern (besser: ableiten):

- Wenn F und $F \Rightarrow G$ als wahr angenommen werden
- dann muss auch G wahr sein

(Man kann sich das semantisch klar machen und dann immer wenn das Muster F und $F \Rightarrow G$ vorliegt G **ableiten**.)

Substitutionen und Inferenzregeln

Um dies formal zu definieren brauchen wir nun

1. Inferenzregeln wie
$$\frac{F, F \Rightarrow G}{G}$$
2. Substitutionen, um formal auszudrücken wie in Formelmengen das durch eine Regel vorgegebene Muster gefunden werden kann.

Bemerkung

In
$$\{(A \vee B) \Rightarrow (C \vee D), A \vee B\}$$
tritt das Muster
$$F, F \Rightarrow G$$
auf!

Substitution

Definition (Substitution)

Eine (Formel-)**Substitution** ist eine nach dem Prinzip der strukturellen Rekursion definierte Funktion $sub : \mathcal{L}_{AL} \to \mathcal{L}_{AL}$.

- Aussagensymbole A_i werden auf $sub(A_i)$ abgebildet.
- Für eine nicht-atomare Formel H ergibt sich daraus das Bild $sub(H)$ mittels:
  - Für $H = \neg F$: $sub(\neg F) = \neg sub(F)$.
  - Für $H = F \circ G$: $sub(F \circ G) = sub(F) \circ sub(G)$, wobei $\circ \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$.

Für eine Formelmenge M ist $sub(M) = \{sub(F) \mid F \in M\}$.

Substitution: Beispiel

Durch eine Substitution wird eine Formel F auf $sub(F)$ abgebildet. Dabei wird einfach jedes Vorkommen eines Aussagensymbols A_i durch die Formel $sub(A_i)$ ersetzt.

Ist z.B. $sub(A) = B$ und $sub(B) = A$, dann ist $sub(A \wedge B) = B \wedge A$. Ist z.B. $sub(A) = A \wedge B$, $sub(B) = D \Rightarrow E$ und $sub(C) = C$, dann ist

$$sub(A \wedge (B \vee C)) = (A \wedge B) \wedge ((D \Rightarrow E) \vee C)$$

Wichtige Anmerkung

Wir benutzen Klammerersparnisregeln, aber keine Äquivalenzumformungen!

Ein Satz

Satz

Wenn $\models F$ gilt, dann gilt auch $\models sub(F)$.

Beweis.

Seien $A_1, \dots, A_n$ die in F vorkommenden Aussagensymbole und sei $\mathcal{A}$ eine Belegung. Wir definieren eine neue Belegung $\mathcal{A}'$ durch

$$\mathcal{A}'(A_i) := \mathcal{A}(sub(A_i)).$$

Dies ist möglich, da die A_i kontingent sind.
Es gilt nun $\mathcal{A}'(F) = \mathcal{A}(sub(F))$ (zu zeigen mittels struktureller Induktion) und somit folgt aus $\models F$ dann $\mathcal{A}'(F) = 1 = \mathcal{A}(sub(F))$ und damit ist $sub(F)$ ebenfalls eine Tautologie. □

Weitere Sätze

Satz

Es seien F und G Formeln, M eine Formelmenge und sub eine Substitution.

1. *Wenn $F \models$ gilt, dann auch $sub(F) \models$.*
2. *Wenn $F \equiv G$ gilt, dann auch $sub(F) \equiv sub(G)$.*
3. *Wenn M unerfüllbar ist, dann auch $sub(M)$.*
4. *Wenn $M \models F$ gilt, dann auch $sub(M) \models sub(F)$.*

Anmerkung

Im Allgemeinen gilt die Umkehrung *nicht*! Z.B. ist $F := A \vee B$ nicht allgemeingültig, aber mit $sub(A) = A$ und $sub(B) = \neg A$ ist $sub(F) = A \vee \neg A$ allgemeingültig.

Fragen

Sei $F = A \vee \neg B$ und $G = A \vee B$. Ist $sub(F) = G$ möglich?

1. Ja, mit $sub(A) = A \vee B$ und $sub(B) = \top$.
2. Ja, mit $sub(A) = A$ und $sub(\neg B) = B$.
3. Nein, nicht möglich.
4. Weiß nicht ...

Fragen

Sei $F = A \Rightarrow (B \vee A)$ und $G = B \Rightarrow (C \vee D \vee B)$ Ist $sub(F) = G$ möglich?

1. Ja!
2. Ja, mit ...
3. Nein!
4. Weiß ich nicht ...

Fragen

Sei $M = \{A, A \Rightarrow B\}$. Mit welcher Substitution gilt $sub(M) \subseteq \{B \Rightarrow C, (C \vee D) \Rightarrow D, C, C \vee D\}$?

1. Mit $sub(A) = B$, $sub(B) = C$
2. Mit $sub(A) = C \vee D$, $sub(B) = D$
3. Mit $sub(A) = C \vee D$, $sub(B) = C$
4. Mit $sub(A) = B \Rightarrow C$, $sub(B) = (C \vee D) \Rightarrow D$
5. Weiß ich nicht ...

Zur Nachbereitung

Zur Nachbereitung

1. Nein, nicht möglich, da man die durch die Junktoren vorgegebene Struktur nicht entfernen kann, d.h. das $\neg$ muss bleiben. Bei 2 muss also zunächst $sub(\neg B) = \neg sub(B)$ gelten und dass $\neg$ kriegt man dann nicht weg. Durch 1 erreicht man nur eine Formel mit $sub(F) \equiv G$.
2. Ja, mit $sub(A) = B$ und $sub(B) = C \vee D$
3. Mit 2.

Inferenzregeln

Definition (Inferenzregel)

Sind $F_1, \ldots, F_n$ und G Formeln, so stellt

$$R = \frac{F_1, \ldots, F_n}{G}$$

eine **Inferenzregel** dar. Die F_i werden als *Prämissen*, G als *Konklusion* der Regel bezeichnet.

Inferenzregeln sind keine Formeln, sondern spezifizieren **Muster** in Formelmengen.

Motivation

Hat man nun z.B. die Regel

$$\frac{F, F \Rightarrow G}{G}$$

so finden wir das in der Prämisse gegebene *Muster* in der Menge

$$\{A \wedge B, B \vee C, (B \vee C) \Rightarrow (D \Rightarrow A)\}$$

wieder (zweite und dritte Formel).

Ersetzen wir in der Regel F durch $B \vee C$ und G durch $D \Rightarrow A$ so erhalten wir genau Formeln in der Menge!

Formal ...

Inferenzregeln anwenden

Definition (Inferenzregeln anwenden)

Es sei $R = \frac{F_1,\ldots,F_n}{G}$ eine Inferenzregel.
Das **Muster** $F_1, \ldots, F_n$ **liegt in einer Formelmenge** M genau dann vor, wenn es eine Substitution *sub* gibt mit $sub(\{F_1, \ldots, F_n\}) \subseteq M$. (Andere Sprechweise: R kann auf M angewendet werden.)
In diesem Fall, kann $sub(G)$ **in einem Schritt aus** M **abgeleitet werden**. (Andere Sprechweise: $sub(G)$ ist mit R direkt aus M ableitbar.)
Notiert wird dies mit: $M \vdash_R sub(G)$ oder $M \vdash sub(G)$, wenn R klar ist oder anders erwähnt wird.

Inferenzregeln anweden (informal)

Bemerkung

Um eine Inferenzregel $R = \frac{F_1,\ldots,F_n}{G}$ auf eine Menge M anzuwenden,

- substituieren wir also so in $F_1, \ldots, F_n$, dass Elemente aus M entstehen ($sub(\{F_1, \ldots, F_n\}) \subseteq M$) und
- leiten dann die selbe Substitution auf G angewendet ab ($M \vdash_R sub(G)$).

Beispiel

Sei als Inferenzregel

$$MP = \frac{F, F \Rightarrow G}{G}$$

gegeben und als Menge

$$M = \{A \wedge B, B \vee C, (B \vee C) \Rightarrow (D \Rightarrow A)\}$$

so gilt mit $sub(F) = B \vee C$ und $sub(G) = D \Rightarrow A$

$$sub(\{F, F \Rightarrow G\}) \subseteq M$$

und wir dürfen $sub(G)$ ableiten. Haben also insgesamt:

$$M \vdash_{MP} D \Rightarrow A$$

Inferenzregeln

Konjunktionseinführung (KE):	$\frac{F,G}{F \wedge G}$	
Konjunktionslöschung (KL):	$\frac{F \wedge G}{F}$	$\frac{F \wedge G}{G}$
Disjunktionseinführung (DE):	$\frac{F}{F \vee G}$	$\frac{G}{F \vee G}$
Disjunktiver Syllogismus (DS):	$\frac{\neg G, F \vee G}{F}$	$\frac{\neg F, F \vee G}{G}$
Modus Ponens (MP):	$\frac{F, F \Rightarrow G}{G}$	
Modus Tollens (MT):	$\frac{\neg G, F \Rightarrow G}{\neg F}$	
Hypothetischer Syllogismus (HS):	$\frac{F \Rightarrow G, G \Rightarrow H}{F \Rightarrow H}$	
Konstruktives Dilemma (KD):	$\frac{F \Rightarrow G, H \Rightarrow I, F \vee H}{G \vee I}$	

Ausblick: Korrekte Inferenzregeln

Anmerkung

Die Regeln eben waren alle *korrekt* (kommt später). Die Prämissen und die Konklusion hängen offensichtlich semantisch zusammen. Zunächst wären auch Regeln wie $\frac{F}{F \wedge G}$ oder auch $\frac{F}{G}$ möglich. Die sind aber nur wenig hilfreich.
Wir kommen später darauf zurück ...

Mehrschrittige Ableitungen

Statt die Inferenzregel nur einmal anzuwenden, kann man sie auch wiederholt anwenden und insb. auch bereits abgeleitete Formeln mit in die Menge, aus der man ableitet, aufnehmen. Sei $\mathcal{R}$ eine Menge von Inferenzregeln, M eine Formelmenge. Wir setzen

$$\begin{aligned}
Abl^0_{\mathcal{R}}(M) &:= M \\
Abl^n_{\mathcal{R}}(M) &:= Abl^{n-1}_{\mathcal{R}}(M) \cup \\
&\quad \{F \in \mathcal{L}_{AL} \mid Abl^{n-1}_{\mathcal{R}}(M) \vdash_R F \text{ mit } R \in \mathcal{R}\} \\
Abl_{\mathcal{R}}(M) &:= \cup_{i \geq 0} Abl^i_{\mathcal{R}}(M)
\end{aligned}$$

Beispiel

Als Regeln haben wir

$$R_1 = \frac{F, F \Rightarrow G}{G} \text{ und } R_2 = \frac{F \wedge G}{G}$$

Sei $M = \{C \Rightarrow (A \Rightarrow B), A \wedge C\}$ und wir wollen $A \Rightarrow B$ ableiten, dann:

$$\begin{aligned} M &\vdash A \wedge C \text{ [aus } M] \\ &\vdash C \text{ [mit (1) und } R_2 \text{ und } sub(F) = A, sub(G) = C] \\ &\vdash C \Rightarrow (A \Rightarrow B) \text{ [aus } M] \\ &\vdash A \Rightarrow B \text{ [mit (2), (3), } R_1 \text{ und } sub(F) = C, sub(G) = A \Rightarrow B] \end{aligned}$$

Man beachte, dass man nicht an das B herankommt. Wir müssten aus $A \wedge C$ das A ableiten, aber mit R_1 und R_2 gelingt das nicht (und wir dürfen keine Äquivalenzumformungen machen!)

Logik-Kalküle - Motivation

Wir haben eben $\vdash$ als Symbol dafür benutzt aus dem vorherigen abzuleiten (also inkl. der schon abgeleiteten Formeln).

Dies kann man in Logik-Kalkülen genauer fassen (und noch mit Axiomen und mehreren Regeln anreichern, so wie dies oben bereits geschehen ist).

Logik-Kalküle

Definition

Kalkül Ein Kalkül $\mathcal{C}$ der Aussagenlogik wird gebildet durch

1. Die Logik-Sprache $\mathcal{L}_{AL}$.
2. Eine Teilmenge $Ax \subseteq \mathcal{L}_{AL}$, die Axiome.
3. Eine endliche Menge $\mathcal{R}$ von Inferenzregeln.

Beispiel

Ein Kalkül ist z.B. $\mathcal{C} = (\mathcal{L}_{AL}, \{A \vee \neg A, A \Rightarrow (B \Rightarrow A)\}, MP)$.

Definition (Ableitung im Kalkül)

Sei $\mathcal{C}$ ein Kalkül der Aussagenlogik, M eine Formelmenge und G eine Formel. Eine endliche Folge von Formeln $F_1, \ldots, F_n$ heißt genau dann eine Ableitung bzgl. $\mathcal{C}$ von G aus M, wenn $G = F_n$ gilt und für jedes k (mit $1 \leq k \leq n$) wenigstens eine der folgenden Bedingungen gilt:

1. $F_k \in M$,
2. $F_k = sub(H)$, wobei H ein Axiom aus $\mathcal{C}$ und sub eine Substitution ist,
3. $\{F_1, \ldots, F_{k-1}\} \vdash_R F_k$, wobei R eine Inferenzregel aus $\mathcal{C}$ ist.

Wir sagen dann G ist in $\mathcal{C}$ ableitbar aus M und notieren kurz $M \vdash_{\mathcal{C}} G$ oder $M \vdash G$, sollte $\mathcal{C}$ klar sein. Mit $Abl_{\mathcal{C}}(M)$ werden alle in $\mathcal{C}$ aus M ableitbaren Formeln bezeichnet.

Beispiel

Sei $M = \{(B \vee \neg B) \Rightarrow (A \Rightarrow C), A \wedge \neg C\}$ und $\mathcal{C} = (\mathcal{L}_{AL}, Ax, \mathcal{R})$ mit $Ax = \{F \vee \neg F\}$ und $\mathcal{R} = \{\frac{F \wedge G}{F}, \frac{F, F \Rightarrow G}{G}\}$ und wir wollen C ableiten. Dann haben wir:

$$
\begin{array}{lll}
M & \vdash & B \vee \neg B \text{ [mit Axiom } F \vee \neg F \text{ und } sub(F) = B] \\
 & \vdash & (B \vee \neg B) \Rightarrow (A \Rightarrow C) \text{ [aus } M] \\
 & \vdash & A \Rightarrow C \text{ [mit (1), (2), MP und} \\
 & & \qquad sub(F) = B \vee \neg B, sub(G) = A \Rightarrow C] \\
 & \vdash & A \wedge \neg C \text{ [aus } M] \\
 & \vdash & A \text{ [mit (4), KL1 und } sub(F) = A, sub(G) = \neg C] \\
 & \vdash & C \text{ [mit (5), (3), MP und } sub(F) = A, sub(G) = C]
\end{array}
$$

Fragen

Sei $F = (A \Rightarrow B) \vee A$ und $G = C \vee A$ Ist $sub(F) = G$ möglich?

1. Ja!
2. Ja, mit ...
3. Nein!
4. Weiß ich nicht ...

Fragen

Kann aus $\{B \Rightarrow (C \wedge D), B \wedge C\}$ und $\mathcal{R} = \{\frac{F \wedge G}{F}, \frac{F, F \Rightarrow G}{G}\}$ das C abgeleitet werden?

1. Ja, in ... Schritten
2. Nein
3. Weiß ich nicht ...
4. Ich habe das noch nicht verstanden ...

Fragen

Kann aus $\{A \wedge B, (A \vee B) \Rightarrow C\}$ und $\mathcal{R} = \{\frac{F, G}{F \vee G}, \frac{F \wedge G}{F, G}, \frac{F, F \Rightarrow G}{G}\}$ das C abgeleitet werden?

1. Ja, in ... Schritten
2. Nein
3. Weiß ich nicht ...
4. Ich habe das noch nicht verstanden ...

Zur Nachbereitung

Zur Nachbereitung

1. Nein, $sub(G) = F$ ist möglich, aber nicht $sub(F) = G$, da man die durch die Junktoren in F vorgegebene Struktur nicht entfernen kann (nur erweitern).
2. Ja, in 5 Schritten (wenn man das aus der Menge nehmen mitzählt).
3. Nein, da $\frac{F \land G}{F,G}$ als Regel nicht geht (immer nur eine Formel in der Konklusion). Wenn man stattdessen die zwei Regeln $\frac{F \land G}{G}$ und $\frac{F \land G}{F}$ hätte, dann ginge es. Alternativ kann man die Regel erlauben und so wie gedacht verfahren.

Ableitung und Folgerbarkeit

Bisher fehlt ein Zusammenhang zwischen Ableitungen (syntaktische Muster finden) und semantischen Eigenschaften der Formeln. Man erreicht dies, indem man die

- Inferenzregeln einschränkt!

So ist bisher viel zu viel möglich. Z.B. auch $\frac{F}{G}$ ...

Korrekte Inferenzregeln

Definition (Korrektheit einer Inferenzregel)

Eine Inferenzregel $R = \frac{F_1,\dots,F_n}{G}$ heißt genau dann **korrekt**, wenn für alle Formelmengen M und alle Formeln H gilt: Wenn $M \vdash_R H$, dann auch $M \models H$.

Was mit einer korrekten Inferenzregel aus M ableitbar ist, ist auch aus M folgerbar.

Satz

Eine Inferenzregel $R = \frac{F_1,\dots,F_n}{G}$ ist genau dann korrekt, wenn $\{F_1, \dots, F_n\} \models G$ gilt.

Diesen Satz benutzt man zum Test, ob eine Inferenzregel korrekt ist! (Beweis als Übung.)

Korrekte Inferenzregeln

Zwei Beispiele:

- Modus Ponens (MP): $\frac{F, F \Rightarrow G}{G}$

F	G	$F \Rightarrow G$
0	0	1
0	1	1
1	0	0
1	1	1

- Hypothetischer Syllogismus (HS): $\frac{A \Rightarrow B, B \Rightarrow C}{A \Rightarrow C}$
  Sei $\mathcal{A}$ eine Belegung mit $\mathcal{A}(A \Rightarrow B) = \mathcal{A}(B \Rightarrow C) = 1$ und ferner mit $\mathcal{A}(A) = 1$. Wegen $\mathcal{A}(A \Rightarrow B) = 1$ folgt dann auch $\mathcal{A}(B) = 1$ und damit folgt wegen $\mathcal{A}(B \Rightarrow C) = 1$ auch $\mathcal{A}(C) = 1$ woraus mit $\mathcal{A}(A) = 1$ auch $\mathcal{A}(A \Rightarrow C) = 1$ folgt.

Korrektheit und Vollständigkeit

Definition

Sei $\mathcal{C}$ ein aussagenlogischer Kalkül.

1. $\mathcal{C}$ heißt **korrekt**, wenn für alle Formelmengen M und alle Formeln H gilt: Wenn $M \vdash_{\mathcal{C}} H$, dann $M \models H$.
2. $\mathcal{C}$ heißt **vollständig**, wenn für alle Formelmengen M und alle Formeln H gilt: Wenn $M \models H$, dann $M \vdash_{\mathcal{C}} H$.

Anmerkung

Gilt $\emptyset \vdash_{\mathcal{C}} H$ für eine Formel H, so sagt man H ist beweisbar in $\mathcal{C}$ und nennt H ein Theorem. Ist der Kalkül korrekt, dann ist H eine Tautologie!

Der Hilbert-Kalkül

Letzteres geht nur mit Axiomen oder wenn wir weitere Regeln einführen.

Anmerkung

Im **Hilbert-Kalkül** nimmt man als Regel nur den Modus Ponens und einige wenige Axiome wie $F \Rightarrow (G \Rightarrow F)$, $F \Rightarrow (\neg F \Rightarrow G)$, ... Der Hilbert-Kalkül kann als korrekt und vollständig nachgewiesen werden. In ihm sind insb. alle aussagenlogischen Tautologien aus wenigen Axiomen und mit nur einer Regel ableitbar!

Zusammenfassung

Die Begriffe bisher:

- Substitution (um Inferenzregeln benutzen zu können)
- Inferenzregel
- Ableitung, mehrschrittige Ableitung
- Kalkül
- Korrekte Inferenzregeln (um einen Zusammenhang zwischen Ableitung und Folgerbarkeit herstellen zu können)
- Korrekte und vollständige Kalküle

Motivation

Wir wollen nun die **Resolution** betrachten, ein **spezielles Ableitungsverfahren**, das mit KNFs arbeitet.

Die Resolution ist ein **Widerlegungsverfahren**, d.h. es ist möglich eine Formel auf Unerfüllbarkeit zu testen.

Auf die Idee zur Resolution kann man kommen, wenn man einige der bisherigen Regeln betrachtet ...

Motivation

- Disjunktiver Syllogismus 1: $\frac{\neg G, F \vee G}{F}$
- Disjunktiver Syllogismus 2: $\frac{\neg F, F \vee G}{G}$
- Modus Ponens: $\frac{F, F \Rightarrow G}{G} \ldots \frac{F, \neg F \vee G}{G}$
- Modus Tollens: $\frac{\neg G, F \Rightarrow G}{\neg F} \ldots \frac{\neg G, \neg F \vee G}{\neg F}$
- Hypothetischer Syllogismus: $\frac{F \Rightarrow G, G \Rightarrow H}{F \Rightarrow H} \ldots \frac{\neg F \vee G, \neg G \vee H}{\neg F \vee H}$

Es werden Pärchen komplementäre Literale entfernt. Dies kann man verallgemeinern um zu einem korrekten Ableitungsverfahren zu gelangen.

Mengendarstellung

Resolution arbeitet mit Formeln in KNF und benutzt eine **Mengendarstellung**

- Ist $K = \vee_{i=1}^{m} L_i$ eine Klausel, dann ist $\mathbf{K} = \{L_1, \ldots, L_m\}$ die Mengendarstellung von K.
- Ist $F = (\wedge_{i=1}^{n} (\vee_{j=1}^{m_i} L_{i,j}))$ eine Formel in KNF, dann ist $\mathbf{F} = \{\{L_{1,1}, \ldots, L_{1,m_1}\}, \ldots, \{L_{n,1}, \ldots, L_{n,m_n}\}\}$ die Mengendarstellung von F.
- Die leere Klausel (Mengendarstellung zu $\perp$) wird mit $\Box$ bezeichnet.
- Die Wahrheitswerteberechnung wird angepasst:
  - $\mathcal{A}(\mathbf{K}) = max(\{\mathcal{A}(L) \mid L \in \mathbf{K}\})$
  - $\mathcal{A}(\mathbf{F}) = min(\{\mathcal{A}(\mathbf{K}) \mid \mathbf{K} \in \mathbf{F}\})$
  - $\mathcal{A}(\Box) = 0$

Mengendarstellung - Beispiel

$$F = (\neg A \vee B) \wedge E \wedge (\neg G \vee \neg C)$$

Dann ist

- $K_1 = \neg A \vee B$ und $\mathbf{K_1} = \{\neg A, B\}$
- $K_2 = E$ und $\mathbf{K_2} = \{E\}$
- $K_3 = \neg G \vee \neg C$ und $\mathbf{K_3} = \{\neg G, \neg C\}$
- $\mathbf{F} = \{\{\neg A, B\}, \{E\}, \{\neg G, \neg C\}\}$

Anmerkung

In der Mengendarstellung sind die Junktoren nicht mehr explizit zu sehen.

Die Resolutionsregel

Definition (Resolvente)

Seien K_1 und K_2 Klauseln (in Mengendarstellung) und L ein Literal mit $L \in K_1$ und $\overline{L} \in K_2$. Dann heißt die (Literal-)Menge $R = (K_1 - \{L\}) \cup (K_2 - \{\overline{L}\})$ **Resolvente** von K_1 und K_2 (bzgl. L).

Dabei ist $\overline{L} = A$, falls $L = \neg A$ und $\overline{L} = \neg A$, falls $L = A$.

Im Falle $K_1 = \{L\}$ und $K_2 = \{\neg L\}$ ist $R = \emptyset$ und wird durch $\Box$ symbolisiert.

Die Resolutionsregel

Definition (Resolvente)

Seien K_1 und K_2 Klauseln (in Mengendarstellung) und L ein Literal mit $L \in K_1$ und $\overline{L} \in K_2$. Dann heißt die (Literal-)Menge $R = (K_1 - \{L\}) \cup (K_2 - \{\overline{L}\})$ **Resolvente** von K_1 und K_2 (bzgl. L).

- Resolventenbildung als Ableitung: $\{K_1, K_2\} \vdash_{res} R$
- Darstellung als Diagramm:

$$\begin{tikzcd} K_1 \arrow[dr] & & K_2 \arrow[dl] \\ & R & \end{tikzcd}$$

Beispiele

- $$\begin{tikzcd} \{\neg B, C\} \arrow[d] & \{\neg C\} \arrow[dl] \\ \{\neg B\} & \end{tikzcd}$$
- $$\begin{tikzcd} \{\neg B, C, A\} \arrow[d] & \{A, D, B\} \arrow[dl] \\ \{C, A, D\} & \end{tikzcd}$$
- $$\begin{tikzcd} \{C\} \arrow[d] & \{\neg C\} \arrow[dl] \\ \square & \end{tikzcd}$$

Beispiele

Wichtige Anmerkung

Das unten stehende auf keinen Fall!

$$\begin{tikzcd} \{\neg B, C\} \arrow[d] & \{B, \neg C\} \arrow[dl] \\ \square & \end{tikzcd}$$

Wichtige Anmerkung

Wirklich nicht! Nein, nein, nein! Es wird immer nur genau ein Literal aus der einen Mengen und ein (komplementäres) Literal aus der anderen Menge entfernt!

Beispiele

Wichtige Anmerkung

Das unten stehende auch nicht!

$$\begin{tikzcd} \{\neg B, B\} \arrow[d] \\ \square \end{tikzcd}$$

Wichtige Anmerkung

Zur Resolventenbildung werden zwei Klauseln benötigt!

Resolventenmengen

Ähnlich wie bei den Ableitungen, führen wir auch hier mehrschrittige Resolventenbildungen ein:

Definition

Sei F eine Formel in KNF dargestellt als Klauselmenge.

$$\begin{aligned}
Res(F) &:= F \cup \{R \mid R \text{ ist Resolvente zweier Klauseln aus } F\} \\
Res^0(F) &:= F \\
Res^{n+1}(F) &:= Res(Res^n(F)) \\
Res^*(F) &:= \bigcup_{i \geq 0} Res^i(F)
\end{aligned}$$

Resolutionssatz (Vorschau)

Später zeigen wir:

Satz (Resolutionssatz)

Eine Klauselmenge F ist unerfüllbar genau dann, wenn $\square \in Res^*(F)$ gilt.

Da dieser Satz gilt, werden die ganzen Dinge oben überhaupt nur eingeführt!

Beispiel

Beispiel

Wir wollen die folgende Formel auf Erfüllbarkeit testen:

$$(\neg A \vee B) \wedge (\neg B \vee C) \wedge A \wedge \neg C$$

Als Klauselmenge:

$$\{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$$

$$\begin{tikzcd}
\{A\} \arrow[dr] & \{\neg A, B\} \arrow[d] & \{\neg B, C\} \arrow[d] & \{\neg C\} \arrow[dl] \\
 & \{B\} \arrow[d] & \{\neg B\} \arrow[dl] & \\
 & \square & &
\end{tikzcd}$$

Ausblick

Nächstes Mal

- zeigen wir noch den Resolutionssatz und
- leiten daraus einen Algorithmus zum Test auf Unerfüllbarkeit ab.