1.8 Resolutionskalkül

Der Resolutionskalkül ist ein Widerlegungskalkül, d.h. damit versucht man, die Unerfüllbarkeit einer Formel zu beweisen. Der Kalkül hat zwei Besonderheiten:

(a) er arbeitet nicht mit Formeln, sondern mit *Klauselmengen*, einer besonderen Schreibweise von Formeln in konjunktiver Normalform, bei der von der Reihenfolge der Konjunktions- und Disjunktionsglieder abstrahiert wird und Wiederholungen gleicher Glieder vermieden werden,

(b) er hat nur eine Schlußregel, weshalb er sich besonders für das automatische Beweisen eignet.

Definition 1.9 Eine *Klausel* ist eine endliche Menge von Literalen, eine *Klauselmenge* eine endliche Menge von Klauseln.

Die Klausel K *repräsentiert* die[5] Formel $\bigvee K$, die Disjunktion aller Literale aus K. (Die leere Klausel wird meist mit $\Box$ bezeichnet; sie repräsentiert $\bot$.) Die Klauselmenge M *repräsentiert* die[6] Formel $\bigwedge\{ \bigvee K \mid K \in M \}$, die Konjunktion aller Formeln $\bigvee K$ mit $K \in M$.

Die von M repräsentierte Formel α_M ist in konjunktiver Normalform. Umgekehrt können wir aus jeder Formel

$$\alpha = (L_{1,1} \vee \ldots \vee L_{1,n_1}) \wedge \ldots \wedge (L_{m,1} \vee \ldots \vee L_{m,n_m})$$

in konjunktiver Normalform die *zugehörige* Klauselmenge

$$M_\alpha = \{ \{ L_{i,j} \mid j = 1, \ldots, n_i \} \mid i = 1, \ldots, m \}$$

bilden; die von ihr repräsentierte Formel α_{M_α} ist zu α äquivalent.

Definition 1.10 Eine Klauselmenge M heißt *erfüllbar*, wenn die von ihr repräsentierte Formel $\bigwedge\{ \bigvee K \mid K \in M \}$ erfüllbar ist.

Definition 1.11 Die einzige Regel des Resolutionskalküls ist die *Resolutionsregel* zur Bildung von Klauseln:

$$\frac{K_1 \dot{\cup} \{L\} \qquad K_2 \dot{\cup} \{\overline{L}\}}{K_1 \cup K_2},$$

wobei L und $\overline{L}$ komplementäre Literale sind. Die untere Klausel ist eine *Resolvente* der beiden oberen Klauseln.

[5] Genau genommen muß man festlegen, in welcher Reihenfolge die Literale von K zu einer Disjunktion zusammengefaßt werden (z.B. das nicht negierte Literal A_i mit kleinstem i Index zuerst, dann $\neg A_i$, usw.).

[6] Genau genommen muß man festlegen, in welcher Reihenfolge die Menge der $\bigvee K$ zu einer Konjunktion zusammengefaßt wird.

Sei M eine Menge von Klauseln. Wir setzen[7]

$$\begin{aligned} Res^0(M) &:= M, \\ Res^{n+1}(M) &:= Res^n(M) \\ &\quad \cup \{ R \mid R \text{ ist Resolvente zweier Klauseln aus } Res^n(M) \}, \\ Res^*(M) &:= \bigcup \{ Res^n(M) \mid n \geq 0 \}. \end{aligned}$$

Die Klausel K *ist aus M herleitbar*, geschrieben $M \vdash K$, falls $K \in Res^*(M)$ ist.

Wenn M endlich ist, ist auch $Res^*(M)$ endlich, da die neuen Klauseln ja nur Literale enthalten, die in einer Klausel aus M vorkommen. Davon gibt es aber nur endlich viele. Also kann man $Res^*(M)$ berechnen.

Beispiel 1.12 Aus $M = \{\{A_0, A_1\}, \{\neg A_1\}, \{\neg A_0, A_2\}, \{\neg A_2\}\}$ ist die leere Klausel $\Box$ herleitbar:

$$\dfrac{\dfrac{\dfrac{\{A_0, A_1\} \qquad \{\neg A_1\}}{\{A_0\}} \qquad \{\neg A_0, A_2\}}{\{A_2\}} \qquad \{\neg A_2\}}{\Box}$$

Der Resolutionskalkül ist korrekt:

Lemma 1.13 Falls $M \vdash K$, so ist $\bigwedge\{ \bigvee \tilde{K} \mid \tilde{K} \in M \} \models \bigvee K$

Beweis: Wir zeigen für jedes n, daß für alle $K \in Res^n(M)$ die von K repräsentierte Formel aus der von M repräsentierten Formel folgt.

$n = 0$: Dann ist $K \in M$, und jede Belegung, die M erfüllt, erfüllt auch $\bigvee K$.

$n+1$: Falls $K \in Res^n(M)$ ist, gilt die Behauptung nach Induktionsannahme. Im anderen Fall gibt es Klauseln $K_1 \dot\cup \{L\}, K_2 \dot\cup \{\overline{L}\} \in Res^n(M)$, und $K = K_1 \cup K_2$. Sei g eine Belegung, die M erfüllt. Nach Induktionsannahme erfüllt g dann auch

$$L \vee \bigvee K_1 \qquad \text{und} \qquad \overline{L} \vee \bigvee K_2.$$

Falls $[\![L]\!]g = 0$ ist, so ist $[\![\bigvee K_1]\!]g = 1$ und daher $[\![\bigvee K]\!]g = [\![\bigvee(K_1 \cup K_2)]\!]g = 1$.

Falls $[\![L]\!]g = 1$ ist, so ist $[\![\overline{L}]\!]g = 0$ und daher $[\![\bigvee K_2]\!]g = 1$; folglich ist auch $[\![\bigvee K]\!]g = [\![\bigvee(K_1 \cup K_2)]\!]g = 1$. $\Box$

[7] In der Übungsstunde haben wir $M \vdash K$ etwas anders definiert: $M \vdash K$ genau dann, wenn es einen *Baum t (für einen Beweis von K aus M)* gibt mit: (i) an der Wurzel von t steht die Klausel K, (ii) an den Blättern von t stehen Klauseln aus M, und (iii) an jedem inneren Knoten von t steht eine Resolvente der Klauseln, die an seinen beiden direkten Nachfolgerknoten stehen. $Res^n(M)$ enthält die Klauseln, die an der Wurzel der Beweisbäume von K aus M mit Tiefe $\leq n$ stehen. Ich habe jetzt keine Zeit, das hier umzuschreiben.

Korollar 1.14 Sei $M \vdash K$. Die Klauselmenge M ist genau dann erfüllbar, wenn $M \cup \{K\}$ erfüllbar ist.

Korollar 1.15 Wenn $M \vdash \Box$, so ist M unerfüllbar.

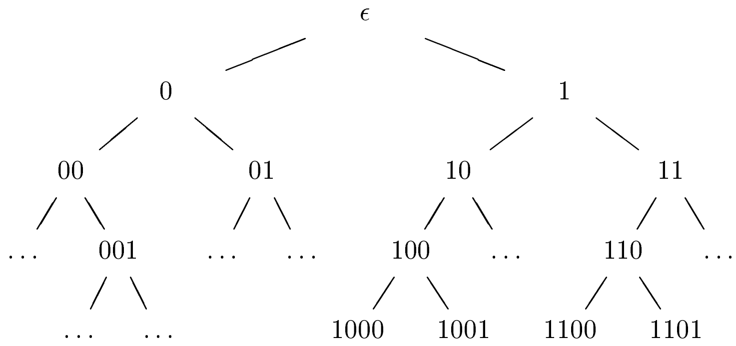
Beweis: Da die von $\Box$ repräsentierte Formel $\bot$ unerfüllbar ist, ist $M \cup \{\Box\}$ und dann nach Korollar 1.14 auch M unerfüllbar. $\Box$

Bleibt zu zeigen, daß der Resolutionskalkül vollständig ist. Statt aus $\bigwedge\{\bigvee \tilde{K} \mid \tilde{K} \in M\} \models \bigvee K$ zu folgern, daß $M \vdash K$ gilt, zeigen wir: wenn $M \cup \{\overline{L} \mid L \in K\}$ unerfüllbar ist, ist $M \cup \{\overline{L} \mid L \in K\} \vdash \Box$.

Der Resolutionskalkül ist (widerlegungs-)vollständig:

Lemma 1.16 Wenn eine Klauselmenge M unerfüllbar ist, so ist $M \vdash \Box$.

Beweis: Sei T der Baum aller Belegungen $g : Var \to \{0,1\}$ wie folgt: die Knoten des Baums sind die endlichen Folgen aus 0 und 1, wobei die Wurzel die leere Folge ist. Jeder Knoten k hat eine *Tiefe* $|k|$, die Länge der Folge k, und zwei *direkte Nachfolger*, einen linken Nachfolger $k1$ und einen rechten Nachfolger $k0$. Jedem unendlichen Pfad π des Baums entspricht die Folge seiner Knoten von der Wurzel ab, was eine wachsende $0,1$-Folge ergibt, z.B. ϵ, 1, 10, 100, 1001 usw. Jeder Pfad definiert eine Belegung g durch $g(A_n) = i$ genau dann, wenn die $n+1$-te Ziffer dieser $0,1$-Folge i ist.



D.h. die letzte Ziffer des Knotens auf dem Pfad, der Tiefe $n+1$ hat, gibt den Wert $g(A_n)$ an. Umgekehrt entspricht jeder Belegung g ein Pfad in T. Daher sehen wir einen Pfad in T und die entsprechende Belegung als gleich an.

Ein Knoten k von T *widerlegt die Klausel* K, falls bei jeder Belegung g, die durch k läuft, $[\![\bigvee K]\!]g = 0$ ist. Ein Knoten k von T ist ein *Fehlerknoten für die Klauselmenge* M, wenn er eine Klausel aus M widerlegt und keiner seiner Vorgängerknoten eine Formel aus M widerlegt. (Die Vorgängerknoten von k sind die auf dem Weg von der Wurzel bis zu k, außer k selbst.)

Das *Gewicht von (T bezüglich) M* ist die Anzahl aller Knoten von T, die weder Fehlerknoten noch Nachfolger eines Fehlerknotens von M sind.

Beh.1 Für jede Klauselmenge M gilt:

(a) Das Gewicht von M ist genau dann endlich, wenn M unerfüllbar ist.

(b) Das Gewicht von M ist genau dann 0, wenn $\Box \in M$.

Beweis:

(a) $\Rightarrow$: Das Gewicht von M sei endlich, und g sei eine Belegung. Auf g liegt ein Fehlerknoten, denn sonst sind die unendlich vielen Knoten auf g Anteile des Gewichts, das also unendlich wäre. Also widerlegt g mindestens eine Klausel von M. Es gibt also keine Belegung, die M erfüllt.

$\Leftarrow$: Sei M unerfüllbar. Betrachte die Menge $T(M)$ der Knoten von T, die weder Fehlerknoten bezüglich M noch Nachfolger von solchen sind. Wir müssen zeigen, daß das Gewicht von M, also $|T(M)|$, endlich ist. Angenommen, $T(M)$ wäre unendlich. Sei k ein Knoten von T, z.B. die Wurzel, sodaß unendlich viele Knoten von $T(M)$ Nachfolger von k sind. Da k nur zwei direkte Nachfolger hat, müssen unendlich viele Knoten aus $T(M)$ Nachfolger von $k0$ oder von $k1$ sein. Angenommen, das gelte für $k0$. Da auch $k0$ nur zwei direkte Nachfolger hat, müssen von den unendlich vielen Nachfolgern von $k0$, die in $T(M)$ liegen, wieder unendlich viele Nachfolger von $k00$ oder von $k01$ sein. Auf diese Weise erhalten wir einen unendlichen Pfad g von T, dessen Knoten alle aus $T(M)$ sind.[8] Da auf g kein Fehlerknoten liegt, gibt es keine Klausel $K \in M$ mit $[\![\bigvee K]\!]g = 0$. Daher wird M von g erfüllt, im Widerspruch zur Voraussetzung. Also muß die Annahme, $|T(M)|$ sei unendlich, falsch sein.

(b) $\Rightarrow$: In diesem Fall ist die Wurzel von T ein Fehlerknoten für M. Daher gibt es ein $K \in M$, das von der Wurzel von T widerlegt wird. Da jede Belegung g durch die Wurzel läuft, ist $[\![\bigvee K]\!]g = 0$ für alle g, und da K eine Menge von Literalen ist, muß $K = \Box$ sein.

$\Leftarrow$: Offenbar ist die durch $\Box$ repräsentierte Formel $\bot$ nicht erfüllbar. Nach Korollar 1.14 ist mit $M \cup \{\Box\}$ auch M nicht erfüllbar.

Damit ist die Behauptung 1 bewiesen.

Sei nun, wie in der Behauptung $\Rightarrow$ des Lemmas, M eine unerfüllbare Klauselmenge. Das Gewicht von M ist nach Beh.1 (a) endlich, etwa n. Falls $n = 0$ ist, ist nach Beh. 1 (b) sogar $\Box \in M$, also insbesondere $M \vdash \Box$. Falls $n > 0$ ist, muß es einen Knoten $k \in T(M)$ geben, dessen direkte Nachfolger $k0$ und $k1$ Fehlerknoten sind; sonst könnte man statt k den direkten Nachfolger betrachten, der kein Fehlerknoten ist; und das geht höchstens $n = |T(M)|$ mal. Seien

[8] Das ist eine Anwendung des Lemmas von König. Die Existenz eines solchen unendlichen Pfades wird gezeigt, aber man kann ihn nicht effektiv angeben.

$K_2', K_1' \in M$ Klauseln, die von $k0$ bzw. $k1$ widerlegt werden. Da diese nicht von k widerlegt werden, muß es „an der Variablen A_i mit $i = |k|$ liegen“, d.h. es muß $K_1' = K_1 \dot\cup \{\neg A_i\}$ und $K_2' = K_2 \dot\cup \{A_i\}$ sein, für gewisse K_1, K_2.

Wegen $K_1', K_2' \in M$ ist $M \vdash K_1'$ und $M \vdash K_2'$. Durch Anwenden der Resolutionsregel erhalten wir

$$\frac{K_1 \dot\cup \{\neg A_i\} \qquad K_2 \dot\cup \{A_i\}}{K_1 \cup K_2},$$

also auch $M \vdash K$ für die Resolvente $K := K_1 \cup K_2$. Da die Belegung an der Variablen A_i keine Rolle spielt, wird K schon durch k widerlegt, und das Gewicht von $M \cup \{K\}$ ist $< n$. Nach Induktion gilt schon

$$M \cup \{K\} \vdash \Box.$$

Also ist $M \vdash \Box$, denn $\Box \in \mathit{Res}^*(M \cup \{K\}) = \mathit{Res}^*(M)$, wegen $M \vdash K$. $\Box$

Duch Korollar 1.14 und Lemma 1.16 haben wir gezeigt:

Satz 1.17 Der Resolutionskalkül ist korrekt und (wiederlegungs-)vollständig: Eine Klauselmenge M ist genau dann unerfüllbar, wenn $M \vdash \Box$.

Bemerkung 1.18 Die Resolvente zweier Hornformeln ist eine Hornformel: enthalten $K_1 \dot\cup \{L\}$ und $K_2 \dot\cup \{\overline{L}\}$ jeweils höchstens ein positives Literal, so enthält auch die Resolvente $K_1 \cup K_2$ höchstens ein positives Literal.

Bemerkung 1.19 Die Hornformel $B_0 \wedge \ldots \wedge B_n \to B$ entspricht einerseits der Klausel $\{\neg B_0, \ldots, \neg B_n, B\}$ und andererseits der PROLOG-Klausel

$$B :- B_1, \ldots, B_n. \tag{17}$$

Die Resolutionsregel können wir also auch so lesen: Anstatt etwas mit den beiden PROLOG-Klauseln

$$A :- A_1, \ldots, A_k, B, C_1, \ldots, C_n. \qquad \text{und} \qquad B :- B_1, \ldots, B_m.$$

zu beweisen (bzw. zu widerlegen), kann man es mit der Klausel

$$A :- A_1, \ldots, A_k, B_1, \ldots, B_m, C_1, \ldots, C_n.$$

beweisen, die der Resolvente der beiden PROLOG-Klauseln entspricht.