

Aussagenlogik

- ▶ **Syntax und Semantik**
- ▶ **Boolesche Algebra**
- ▶ **Erfüllbarkeit**
- ▶ **SAT-Solver**
- ▶ **Kompaktheit**
- ▶ **Beweiskalküle**

Einführendes Beispiel

Martin sagt “Markus sagt die Wahrheit”.

Markus sagt “Matthias lügt”.

Matthias sagt “Martin und Markus sagen entweder beide die Wahrheit oder lügen beide”.

Wer lügt, und wer sagt die Wahrheit?

Syntax der Aussagenlogik

Wir setzen eine Menge $\mathcal{V} = \{A, B, C, \dots\}$ von **Aussagenvariablen** voraus.

Formeln der **Aussagenlogik** (über $\mathcal{V}$) sind induktiv definiert durch:

- Jeder Aussagenvariable A ist eine Formel.
- Die **Konstanten** $\top$ und $\perp$ sind Formeln.
- Sind φ und ψ Formeln, so sind auch
 - $\varphi \wedge \psi$ (“und”)
 - $\varphi \vee \psi$ (“oder”)
 - $\neg \varphi$ (“nicht”)
 - $\varphi \rightarrow \psi$ (“wenn-dann”)
 - $\varphi \leftrightarrow \psi$ (“genau-dann-wenn”)

Formeln.

Präzedenzregeln

Bindungskraft der Operatoren (auch Junktoren genannt) in absteigender Reihenfolge:

$$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$$

soll heissen:

$$A \vee \neg B \wedge \neg C \leftrightarrow C \rightarrow A$$

ist zu lesen als

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

Interpretationen

Def.: Sei $\mathbb{B} = \{\text{tt}, \text{ff}\}$ die Menge der **Booleschen Werte** *wahr* und *falsch*.

Def.: Eine **Interpretation** (Variablenbelegung) ist eine Abbildung $\mathcal{I} : \mathcal{A} \rightarrow \mathbb{B}$.

Interpretationen können **Modelle** einer Formel sein; diese Beziehung ist induktiv definiert:

$$\mathcal{I} \models \top$$

$$\mathcal{I} \not\models \perp$$

$$\mathcal{I} \models A \quad \text{gdw.} \quad \mathcal{I}(A) = \text{tt}$$

$$\mathcal{I} \models \varphi \wedge \psi \quad \text{gdw.} \quad \mathcal{I} \models \varphi \text{ und } \mathcal{I} \models \psi$$

$$\mathcal{I} \models \varphi \vee \psi \quad \text{gdw.} \quad \mathcal{I} \models \varphi \text{ oder } \mathcal{I} \models \psi$$

$$\mathcal{I} \models \neg \varphi \quad \text{gdw.} \quad \mathcal{I} \not\models \varphi$$

$$\mathcal{I} \models \varphi \rightarrow \psi \quad \text{gdw.} \quad \text{wenn } \mathcal{I} \models \varphi \text{ dann } \mathcal{I} \models \psi$$

$$\mathcal{I} \models \varphi \leftrightarrow \psi \quad \text{gdw.} \quad \mathcal{I} \models \varphi \text{ genau dann, wenn } \mathcal{I} \models \psi$$

Beispiele

Bsp.: $\mathcal{I} = \{A \mapsto \text{tt}, B \mapsto \text{ff}, C \mapsto \text{tt}, D \mapsto \text{ff}\}$

- $\mathcal{I} \models (A \vee B) \wedge (C \vee D)$
- $\mathcal{I} \not\models \neg A \vee B \vee (\neg C \wedge D)$
- $\mathcal{I} \models A \rightarrow \neg B$
- $\mathcal{I} \models \neg A \rightarrow B$
- $\mathcal{I} \not\models A \rightarrow B$
- $\mathcal{I} \models \neg A \rightarrow \neg B$
- $\mathcal{I} \models (A \leftrightarrow B) \leftrightarrow \neg(C \leftrightarrow \neg D)$

Beispiel

beachte: wir benutzen anonyme Aussagenvariablen, um eine Logik zu haben, die für **beliebige** Aussagen gilt; Formeln lassen sich aber mit konkreten Aussagen instanziiieren

Bsp. (weitergef.):

- Martin sagt “Markus sagt die Wahrheit”.
- Markus sagt “Matthias lügt”.
- Matthias sagt “Martin und Markus sagen entweder beide die Wahrheit oder lügen beide”.

Lösung mithilfe der Aussagenlogik erfordert Formalisierung; drei Aussagenvariablen A, B, C mit intendierter Bedeutung: *Martin sagt die Wahrheit* (A), *Markus sagt ...*

obiger Sachverhalt wird beschrieben durch die Formel

$$(A \rightarrow B) \wedge (\neg A \rightarrow \neg B) \wedge (B \rightarrow \neg C) \wedge (\neg B \rightarrow C) \wedge (C \rightarrow (A \leftrightarrow B)) \wedge (\neg C \rightarrow \neg(A \leftrightarrow B))$$

Formeln und Boolesche Funktionen

eine Formel φ mit n vorkommenden Aussagenvariablen $A_1, \dots, A_n$ stellt eine **Funktion** vom Typ

$$\mathbb{B}^n \rightarrow \mathbb{B}$$

dar

beachte: es gibt nur 2^n viele Interpretationen, die sich in $A_1, \dots, A_n$ unterscheiden; also gibt es nur 2^n viele verschiedene “Eingaben” an φ

Funktionswert $\models$ besagt, dass durch Argumente gegebene Interpretation ein Modell ist

Funktionen mit endlichem Domain können durch **Tabellierung** aller Argumente repräsentiert werden

Wahrheitstafeln

... für die Junktoren und Konstanten der Aussagenlogik

φ	ψ	$\varphi \wedge \psi$
ff	ff	ff
ff	tt	ff
tt	ff	ff
tt	tt	tt

φ	ψ	$\varphi \vee \psi$
ff	ff	ff
ff	tt	tt
tt	ff	tt
tt	tt	tt

φ	$\neg \varphi$
ff	tt
tt	ff

φ	ψ	$\varphi \rightarrow \psi$
ff	ff	tt
ff	tt	tt
tt	ff	ff
tt	tt	tt

φ	ψ	$\varphi \leftrightarrow \psi$
ff	ff	tt
ff	tt	ff
tt	ff	ff
tt	tt	tt

$\top$
tt

$\perp$
ff

Wahrheitstafeln

... für komplexere Formeln

A	B	C	$A \wedge B$	$A \wedge B \rightarrow \perp$	$\neg B$	$\neg B \rightarrow C$	$(A \wedge B \rightarrow \perp) \wedge (\neg B \rightarrow C)$
ff	ff	ff	ff	tt	tt	ff	ff
ff	ff	tt	ff	tt	tt	tt	tt
ff	tt	ff	ff	tt	ff	tt	tt
ff	tt	tt	ff	tt	ff	tt	tt
tt	ff	ff	ff	tt	tt	ff	ff
tt	ff	tt	ff	tt	tt	tt	tt
tt	tt	ff	tt	ff	ff	tt	ff
tt	tt	tt	tt	ff	ff	tt	ff

Funktionale Vollständigkeit

Def.: eine Menge J von Junktoren heißt **funktional vollständig**, wenn es für jedes $n \in \mathbb{N}$ und jede Funktion $f : \mathbb{B}^n \rightarrow \mathbb{B}$ eine Formel φ_f über n Variablen gibt, die nur Junktoren aus J benutzt und f repräsentiert

Thm.: $\{\wedge, \vee, \neg\}$ ist funktional vollständig

Bsp.: Sei f gegeben durch

A	B	C	$f(A, B, C)$
ff	ff	ff	ff
ff	ff	tt	tt
ff	tt	ff	tt
ff	tt	tt	ff
tt	ff	ff	ff
tt	ff	tt	ff
tt	tt	ff	tt
tt	tt	tt	ff

Dann wird f realisiert durch

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

Funktionale Vollständigkeit

somit müssen sich insbesondere die anderen Junktoren durch $\neg, \vee, \wedge$ ausdrücken lassen

- $\varphi \rightarrow \psi$ ist dasselbe wie $\neg\varphi \vee \psi$
- $\varphi \leftrightarrow \psi$ ist dasselbe wie $(\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$

Thm.: Die folgenden Mengen von Junktoren sind funktional vollständig:

$$\{\neg, \vee\} \quad , \quad \{\neg, \wedge\} \quad , \quad \{\rightarrow\} \quad , \quad \dots$$

BEWEIS: (Übung)

Funktionale Unvollständigkeit

nicht jede Menge von Junktoren ist funktional vollständig, z.B. $\emptyset$ sicherlich nicht, $\{\neg\}$ auch nicht (aber wieso?)

Thm.: $\{\wedge, \vee\}$ ist nicht funktional vollständig

Def.: Definiere partielle Ordnung auf $\mathbb{B}$ durch $\text{ff} < \text{tt}$. Ein $f : \mathbb{B}^n \rightarrow \mathbb{B}$ heißt **monoton** im i -ten Argument, wenn für alle $x, y, x_1, \dots, x_n \in \mathbb{B}$ gilt: wenn $x \leq y$, dann

$$f(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n) \leq f(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n)$$

Funktionale Unvollständigkeit von $\{\vee, \wedge\}$

Lemma: Sei φ aufgebaut aus n Variablen, Konstanten und den Junktoren $\vee, \wedge$. Dann ist die durch φ definierte Funktion $f_\varphi : \mathbb{B}^n \rightarrow \mathbb{B}$ monoton in allen Argumenten.

BEWEIS: durch Induktion über den Aufbau von φ

BEWEIS (der funktionalen Unvollständigkeit von $\{\vee, \wedge\}$):
Die Funktion $f = \{\text{ff} \mapsto \text{tt}, \text{tt} \mapsto \text{ff}\}$ ist nicht monoton im ersten Argument, kann daher nicht durch ein solches φ definiert werden.



Äquivalenzen

Def.: φ und ψ heißen **äquivalent**, geschrieben $\varphi \Longleftrightarrow \psi$, gdw. für alle Interpretationen $\mathcal{I}$ gilt: $\mathcal{I} \models \varphi$ gdw. $\mathcal{I} \models \psi$

Lemma: $\varphi \Longleftrightarrow \psi$ gdw. $\mathcal{I} \models \varphi \leftrightarrow \psi$ für alle $\mathcal{I}$

Äquivalenzen können z.B. ausgenutzt werden, um kleinere Formeln, die dasselbe ausdrücken, zu erhalten

Bsp.: $B \leftrightarrow (A \rightarrow \neg B) \Longleftrightarrow A \leftrightarrow \neg B$

Beweis z.B. durch Wahrheitstafeln

A	B	$B \leftrightarrow (A \rightarrow \neg B)$	$A \leftrightarrow \neg B$
ff	ff	ff	ff
ff	tt	tt	tt
tt	ff	tt	tt
tt	tt	ff	ff

Beispiel (weiterg.)

- Martin sagt “Markus sagt die Wahrheit”.
- Markus sagt “Matthias lügt”.
- Matthias sagt “Martin und Markus sagen entweder beide die Wahrheit oder lügen beide”.

formalisiert als $\varphi :=$

$$(A \rightarrow B) \wedge (\neg A \rightarrow \neg B) \wedge (B \rightarrow \neg C) \wedge (\neg B \rightarrow C) \wedge (C \rightarrow (A \leftrightarrow B)) \wedge (\neg C \rightarrow \neg(A \leftrightarrow B))$$

A	B	C	φ
ff	ff	ff	ff
ff	ff	tt	tt
ff	tt	ff	ff
ff	tt	tt	ff
tt	ff	ff	ff
tt	ff	tt	ff
tt	tt	ff	ff
tt	tt	tt	ff

einzigste mögliche Lösung: Martin und Markus lügen, Matthias sagt die Wahrheit

Boolesche Algebra

Def.: eine **Boolesche Algebra** ist eine Menge M mit zwei Konstanten $\top, \perp \in M$ und drei Funktionen $\cap, \cup : M \times M \rightarrow M$ und $\bar{\cdot} : M \rightarrow M$, sodass für alle $x, y, z \in M$ gilt:

- $x \cap y = y \cap x$ und $x \cup y = y \cup x$ (Kommutativität)
- $(x \cap y) \cap z = x \cap (y \cap z)$ und $(x \cup y) \cup z = x \cup (y \cup z)$ (Assoziativität)
- $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$ und $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$ (Distributivität)
- $x \cup (x \cap y) = x$ und $x \cap (x \cup y) = x$ (Absorption)
- $x \cup \bar{x} = \top$ und $x \cap \bar{x} = \perp$ (Komplemente)
- $x \cup x = x$ und $x \cap x = x$ (Idempotenz)
- $x \cup \perp = x$ und $x \cap \top = x$ (Neutralität)
- $x \cap \perp = \perp$ und $x \cup \top = \top$ (Extremalität)

Boolesche Algebren

Lemma: $(\mathbb{B}, \text{tt}, \text{ff}, \wedge, \vee, \neg)$ ist eine Boolesche Algebra

Gültigkeit der Gesetze lässt sich z.B. durch Wahrheitstafeln ausrechnen

andere Beispiele für Boolesche Algebren:

- **Potenzmengenverband** einer endlichen Menge M :
 $(2^M, M, \emptyset, \cap, \cup, \bar{\cdot})$
- **Singleton**-Menge (wieso?)
- ...

Redundanz und Herleitung

Beachte: nicht alle Gesetze für Boolesche Algebren sind unabhängig

Z.B. folgt Neutralität aus Absorption und Komplementen

$$x \sqcup \perp = x \sqcup (x \sqcap \bar{x}) = x$$

In ähnlicher Weise lassen sich auch weitere Gesetze finden, die in jeder Booleschen Algebra gelten müssen; diese sind aus den obigen Gesetzen **herleitbar**, z.B. die **de Morgan-Gesetze**:

a) $\overline{x \sqcup y} = \bar{x} \sqcap \bar{y}$

b) $\overline{x \sqcap y} = \bar{x} \sqcup \bar{y}$

Erfüllbarkeit und Allgemeingültigkeit

Def.: eine Formel φ heißt **erfüllbar**, wenn es **ein** $\mathcal{I}$ gibt, so dass $\mathcal{I} \models \varphi$

Def.: eine Formel φ heißt **allgemeingültig** (oder **Tautologie**), wenn für **alle** $\mathcal{I}$ gilt: $\mathcal{I} \models \varphi$

Lemma.: φ is erfüllbar gdw. $\neg\varphi$ nicht allgemeingültig ist

BEWEIS:

“ $\Rightarrow$ ” Sei φ erfüllbar. Dann ex. $\mathcal{I}$ mit $\mathcal{I} \models \varphi$ und daher $\mathcal{I} \not\models \neg\varphi$.
Somit ist $\neg\varphi$ nicht allgemeingültig.

“ $\Leftarrow$ ” Genauso.



Zusammenhänge

Beachte: aus obigem Lemma folgt z.B. sofort, dass φ unerfüllbar ist gdw. $\neg\varphi$ allgemeingültig ist; dies liegt daran, dass die folgende Formel der Aussagenlogik allgemeingültig ist

$$(A \rightarrow \neg B) \rightarrow (B \rightarrow \neg A)$$

Thm.:

- a) $\varphi \wedge \psi$ ist **allgemeingültig** gdw. φ und ψ **allgemeingültig** sind
- b) $\varphi \vee \psi$ is **erfüllbar** gdw. φ oder ψ **erfüllbar** ist
- c) $\varphi \iff \psi$ gdw. $\varphi \leftrightarrow \psi$ **allgemeingültig**
- d) φ **allgemeingültig** gdw. $\varphi \iff \top$
- e) φ **unerfüllbar** gdw. $\varphi \iff \perp$

BEWEIS: (Übung)

Beispiele

die folgenden Formeln sind **erfüllbar**

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

die folgenden Formeln sind **unerfüllbar**

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

die folgenden Formeln sind **Tautologien**

$$A \vee \neg A, (A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow (A \rightarrow C), \neg\neg A \leftrightarrow A$$

Fallstricke

Vorsicht! Folgendes gilt **nicht**:

- $\varphi \vee \psi$ allgemeingültig gdw. φ oder ψ allgemeingültig
- $\varphi \wedge \psi$ erfüllbar gdw. φ und ψ erfüllbar

der Grund dafür ist jeweils die implizite existentielle (Erfüllbarkeit) oder universelle (Allgemeingültigkeit) Quantifizierung über Interpretation

existentielle Quantifizierung kommutiert mit Dis- aber nicht mit Konjunktionen; universelle kommutiert mit Kon- aber nicht mit Disjunktionen

aber es gelten jeweils eine der beiden Richtungen, welche?

Substitutionen

Def.: $\varphi[\psi/A]$ bezeichne die **simultane Ersetzung** von jedem Vorkommen der Variable A in φ durch ψ

Thm.: Wenn $\psi \iff \theta$ dann $\varphi[\psi/A] \iff \varphi[\theta/A]$

BEWEIS (durch Induktion über den Aufbau von φ)

Frage: macht es einen Unterschied, wenn man **nicht simultan** ersetzt?

Mehrstellige Junktoren

aufgrund der Kommutativ- und Assoziativgesetze können wir mehrstellige Dis- und Konjunktionen einführen:

$$\bigwedge_{i=1}^n \varphi_i := \varphi_1 \wedge \dots \wedge \varphi_n \qquad \bigvee_{i=1}^n \varphi_i := \varphi_1 \vee \dots \vee \varphi_n$$

genauso für endliche Indexmengen I : $\bigwedge_{i \in I} \varphi_i$ bzw. $\bigvee_{i \in I} \varphi_i$

beachte: falls $n = 0$, dann $\bigwedge_{i=1}^n \varphi_i := \top$ und $\bigvee_{i=1}^n \varphi_i := \perp$;
ebenfalls für $I = \emptyset$

Normalformen

Def.:

- Ein **Literal** ist eine Variable A oder ihre Negation $\neg A$.
- Eine **Klausel** ist eine Disjunktion von Literalen, $\bigvee_{i=1}^n l_i$.
- Ein **Minterm** ist eine Konjunktion von Literalen, $\bigwedge_{i=1}^n l_i$.
- Eine Formel ist in **konjunktiver Normalform** (KNF), falls sie eine Konjunktion von Klauseln ist, $\bigwedge_{i=1}^n \bigvee_{j=1}^{m_i} l_{i,j}$.
- Eine Formel ist in **disjunktiver Normalform** (DNF), falls sie eine Disjunktion von Mintermen ist, $\bigvee_{i=1}^n \bigwedge_{j=1}^{m_i} l_{i,j}$.

Bsp. $(A \vee \neg B) \wedge (B \vee \neg C \vee \neg A)$ ist in KNF

wir schreiben Formeln in KNF (oder DNF) wegen Assoziativität, Kommutativität und Absorption auch als **Mengen von Mengen von Literalen**

Existenz von Normalformen

Thm.: Für jedes φ existiert ein ψ in KNF / DNF, sodass $\varphi \iff \psi$.

BEWEIS: Durch schrittweises Umbauen von φ :

- 1 Elimination von $\rightarrow, \leftrightarrow$ mittels

$$\varphi_1 \leftrightarrow \varphi_2 \iff (\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1) \quad , \quad \varphi_1 \rightarrow \varphi_2 \iff \neg\varphi_1 \vee \varphi_2$$

- 2 Anwenden der de Morgan-Gesetze und $\neg\neg\theta \iff \theta$ liefert Formel, die nur aus Literalen mit $\wedge, \vee$ gebaut ist.
- 3 Anwenden der Distributivgesetze liefert KNF oder DNF. □

Ein naiver Erfüllbarkeitstest

Def.: Das **Erfüllbarkeitsproblem der Aussagenlogik** (SAT) ist das folgende: Geg. φ , entscheide, ob φ erfüllbar ist oder nicht.

Thm.: SAT ist in Zeit $\mathcal{O}(2^n)$ entscheidbar. ($n = \text{Grösse der Eingabe} = |\varphi|$)

BEWEIS: Beachte:

- in Zeit $\mathcal{O}(|\varphi|)$ lässt sich für gegebenes $\mathcal{I}$ entscheiden, ob $\mathcal{I} \models \varphi$ gilt oder nicht (Übung).
- es gibt höchstens $\lceil |\varphi|/2 \rceil$ viele Variablen in φ

Durch Aufzählung aller relevanten Interpretationen und sukzessives Testen kann man Erfüllbarkeit in Zeit $2^{\lceil |\varphi|/2 \rceil} \cdot \mathcal{O}(|\varphi|) = \mathcal{O}(2^n)$ entscheiden. □

Das Erfüllbarkeitsproblem für DNF

Thm.: DNF-SAT (SAT für Formeln in DNF) lässt sich in Zeit $\mathcal{O}(n)$ entscheiden.

BEWEIS:

- Ein Minterm $\bigwedge_{i=1}^n l_i$ ist erfüllbar gdw. es kein A gibt, so dass $l_i = A$ und $l_j = \neg A$ für $1 \leq i, j \leq n$.
- Eine Disjunktion $\bigvee_{i=1}^n \varphi_i$ ist erfüllbar gdw. es ein i gibt, so dass φ_i erfüllbar ist.

Somit kann Erfüllbarkeit einer DNF in einem Durchlauf durch die Formel entschieden werden. □

Warum dann nicht Erfüllbarkeitstest für allgemeine Formel φ :

- 1 Wandle φ in äquivalente DNF ψ um.
- 2 Teste Erfüllbarkeit von ψ .

Laufzeit?

Erfüllbarkeitsäquivalenz

neben dem starken Äquivalenzbegriff $\iff$ führen wir noch einen schwächeren ein

Def.: φ und ψ sind **erfüllbarkeitsäquivalent**, $\varphi \equiv_{sat} \psi$, falls gilt: φ erfüllbar gdw. ψ erfüllbar

beachte: $\equiv_{sat}$ ist Äquivalenzrelation mit nur zwei Äquivalenzklassen; kanonische Vertreter sind $\top, \perp$

Wofür kann das dann überhaupt gut sein?

Ist man an Erfüllbarkeit von φ interessiert, so reicht es aus, Erfüllbarkeit von ψ zu testen, falls $\varphi \equiv_{sat} \psi$ (aber evtl. **nicht** $\varphi \iff \psi$).

Erfüllbarkeitsäquivalente KNF

Thm.: Für jedes φ gibt es ein ψ in KNF, so dass $\varphi \equiv_{sat} \psi$ und $|\psi| = \mathcal{O}(|\varphi|)$.

BEWEIS: Für jede nicht-atomare Subformel θ von φ führen wir eine Variable X_θ ein. Dann wird φ sukzessive nach folgender Vorschrift “von unten nach oben” umgebaut.

Solange es noch eine nicht-atomare Subformel θ gibt, ersetze diese durch X_θ und definiere eine KNF ψ_θ je nach Junktor in θ , z.B.

Falls $\theta = Y \wedge Z$, dann

$$\psi_\theta := (\neg X_\theta \vee Y) \wedge (\neg X_\theta \vee Z) \wedge (X_\theta \vee \neg Y \vee \neg Z)$$

Definiere schlussendlich $\psi := X_\varphi \wedge \bigwedge \{\psi_\theta \mid \theta \text{ Subformel von } \varphi\}$ □

Erfüllbarkeitsäquivalente KNF

Mit $\text{Var}(\varphi)$ bezeichnen wir die in φ **vorkommenden** Variablen.

Beachte: Es gilt in obiger Konstruktion nicht nur $\varphi \equiv_{\text{sat}} \psi$, sondern noch etwas stärkeres:

- $\text{Var}(\varphi) \subseteq \text{Var}(\psi)$
- Ist $\mathcal{I} \models \psi$, so auch $\mathcal{I} \models \varphi$ (aber nicht unbedingt umgekehrt).

Soll heissen: ψ ist **nicht nur erfüllbarkeitsäquivalent** zu φ , sondern jeder erfüllende Variablenbelegung für ψ ist auch eine für φ .

Beachte: Linearzeiterfüllbarkeitstest war für DNF, nicht KNF!
Umwandlung in erfüllbarkeitsäquivalente DNF ist wohl nicht mit nur polynomiellern Aufwand möglich.

Beispiel

Gesucht ist Formel über Variablen $A_1, \dots, A_n$ die besagt “genau eine der Aussagen $A_1, \dots, A_n$ ist wahr”.

Leicht möglich mit Formel der Größe $\mathcal{O}(n^2)$: $\bigvee_{i=1}^n (A_i \wedge \bigwedge_{j \neq i} \neg A_j)$

Geht es auch mit Formel der Größe $\mathcal{O}(n)$? Ja, wenn man sich mehr Variablen spendiert: $\varphi_1 \wedge \varphi_2$, wobei

- $\varphi_1 := \bigvee_{i=1}^n A_i$, “Mindestens eine der $A_1, \dots, A_n$ ist wahr”
- zusätzliche Variablen B_i , $i = 1, \dots, n$, mit intuitiver Bedeutung: “eine der $A_1, \dots, A_i$ ist wahr”

$$\varphi_2 := (A_1 \leftrightarrow B_1) \wedge \bigwedge_{i=2}^n ((\neg B_{i-1} \leftrightarrow A_i) \rightarrow B_i) \wedge \neg(B_{i-1} \wedge A_i)$$

Horn-Formeln

Def.: Eine **Horn-Formel** ist ein φ in **KNF**, so dass in jeder Klausel höchstens ein positives Literal vorkommt.

Beachte:

$$\neg A_1 \vee \dots \vee \neg A_n \vee B \iff A_1 \wedge \dots \wedge A_n \rightarrow B$$

$$\neg A_1 \vee \dots \vee \neg A_n \iff A_1 \wedge \dots \wedge A_n \rightarrow \perp$$

Thm.: Das Erfüllbarkeitsproblem für Horn-Formeln ist in Zeit $\mathcal{O}(n^2)$ lösbar.

BEWEIS: (Übung)

Beachte: mit etwas Cleverness lässt es sich sogar in $\mathcal{O}(n)$ lösen

SAT-Solver

Ein SAT-Solver ist eine Implementierung eines Algorithmus für das SAT-Problem.

Obwohl dies i.A. exponentielle (in $|Var(\varphi)|$) Laufzeit braucht, gibt es mittlerweile einige SAT-Solver, die in der Praxis erstaunlich gut funktionieren.

- ZCHAFF <http://www.princeton.edu/~chaff/zchaff.html>
- MINISAT <http://minisat.se/>
- PICOSAT <http://fmv.jku.at/picosat/>
- BERKMIN <http://eigold.tripod.com/BerkMin.html>
- RSAT <http://reasoning.cs.ucla.edu/rsat/>
- ...

siehe auch SATLive-Webseite <http://www.satlive.org/>

Das DIMACS-Format

SAT-Solver verlangen typischerweise eine Eingabe in KNF.

Standardisiertes Format: DIMACS

- Variablen sind natürliche Zahlen ≥ 1
- Literale werden durch Integer bezeichnet, z.B. $A_7 = 7$, $\neg A_4 = -4$
- Klausel ist Liste von Integern, 0 markiert Klauselende
- KNF ist Liste von Klauseln
- Kommentare im Header (c ...)
- spezielle Headerzeile (p cnf ...) gibt Anzahl verwendeter Klauseln und Variablen an

Beispiel

Die KNF

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

kann im DIMACS-Format so repräsentiert werden:

c Beispielformel aus der Vorlesung

c Autor: Martin Lange

p cnf 4 5

-1 2 3 0

2 -3 0

-4 0

1 4 0

-2 -3 -4 0

SAT-Solver im Einsatz

Cleverer Heuristiken und jahrelanges Tuning haben dazu geführt, dass moderne SAT-Solver typischerweise Instanzen der Größenordnung

- $\sim 10^5$ Variablen
- $\sim 10^6$ Klauseln

lösen können.

Vorsicht! Es gibt natürlich auch (im Vergleich dazu) sehr kleine Instanzen, an denen sie sich die Zähne ausbeissen.

typischer Einsatz von SAT-Solvern (nicht annähernd vollständig):

- Hardware-Verifikation
- Planungsprobleme in der KI
- Constraint-Solving
- Puzzle (z.B. Sudoku leicht als SAT-Problem zu kodieren)
- ...

Ersetzung von Literalen

Def.: Sei $\mathcal{C}$ Klauselmenge (= Menge von Mengen von Literalen). Mit $\mathcal{C}[\top/A]$ bezeichnen wir die Menge von Klauseln, die dadurch entsteht, dass man

- ① jede Klausel, die das Literal A enthält, aus $\mathcal{C}$ entfernt, und
- ② das Literal $\neg A$ aus jeder Klausel in $\mathcal{C}$ entfernt.

Für $\mathcal{C}[\perp/A]$ gilt das entsprechend duale.

Bsp.:

$$\begin{aligned}\mathcal{C} &= \{\{A, \neg B\}, \{\neg A, \neg B\}, \{\neg A, B\}\} \\ \mathcal{C}[\top/A] &= \{\{\neg B\}, \{B\}\}\end{aligned}$$

Lemma: Sei $\mathcal{C}$ Klauselmenge (als KNF aufgefasst) und A darin vorkommende Variable. Dann ist $\mathcal{C}$ erfüllbar gdw. $\mathcal{C}[\top/A]$ oder $\mathcal{C}[\perp/A]$ erfüllbar ist.

BEWEIS: (Übung)

Unit-Propagation

Lemma: Sei $\mathcal{C}$ Klauselmenge, A Variable, so dass $\{A\} \in \mathcal{C}$. Dann ist $\mathcal{C}$ erfüllbar gdw. $\mathcal{C}[\top/A]$ erfüllbar ist.

BEWEIS: ($\Leftarrow$) folgt sofort aus Lemma davor.

($\Rightarrow$) Sei $\mathcal{C}$ erfüllbar. Wegen Lemma davor müssen wir lediglich zeigen, dass $\mathcal{C}[\perp/A]$ unerfüllbar ist. Dies ist der Fall, denn da $\{A\} \in \mathcal{C}$ gilt $\emptyset \in \mathcal{C}[\perp/A]$, und wegen KNF steht $\emptyset$ für $\perp$, und $\perp \wedge \phi \iff \perp$, was unerfüllbar ist.

$\rightsquigarrow$ Algorithmus Unit-Propagation($\mathcal{C}$) führt **sukzessive** diese Ersetzungsschritte durch, solange noch Singleton-Klauseln in $\mathcal{C}$ vorhanden sind.

Der DPLL-Algorithmus

Alle modernen SAT-Solver basieren auf dem DPLL-Algorithmus (nach Davis, Putnam, Logemann, Loveland).

```
DPLL( $\mathcal{C}$ ) =  
  Unit-Propagation( $\mathcal{C}$ )  
  if  $\mathcal{C} = \emptyset$  then return erfüllbar  
  if  $\emptyset \in \mathcal{C}$  then return unerfüllbar  
  wähle Variable  $A$ , die noch in  $\mathcal{C}$  vorkommt  
   $\mathcal{C}' = \mathcal{C}[\top/A]$   
  if DPLL( $\mathcal{C}'$ ) = erfüllbar then return erfüllbar  
  return DPLL( $\mathcal{C}[\perp/A]$ )
```

Bem.: Algorithmus DPLL **terminiert** immer, ist **korrekt** (wenn er “erfüllbar” sagt, dann war die Eingabe auch erfüllbar) und **vollständig** (wenn die Eingabe erfüllbar ist, dann sagt er auch “erfüllbar”), aber wieso?

Erfüllbarkeit und Konsistenz

Def.: Eine Menge Φ von Formeln heißt **erfüllbar**, wenn es eine Interpretation $\mathcal{I}$ gibt, so dass $\mathcal{I} \models \varphi$ für alle $\varphi \in \Phi$ gilt. Notation: $\mathcal{I} \models \Phi$.

Bem.: Für endliche Φ ist also die **Menge** Φ erfüllbar gdw. die **Formel** $\bigwedge \Phi$ erfüllbar ist. Aber unendliche Formeln gibt es (hier) nicht.

Bsp.: $\{A_i \rightarrow A_{i+1} \mid i \in \mathbb{N}\}$ ist erfüllbar

Im folgenden nehmen wir an, dass $\mathcal{V}$ nur **abzählbar unendlich viele** Variablen enthält, also o.B.d.A. $\mathcal{V} = \{A_0, A_1, \dots\}$.

Def.: Eine Menge Φ von Formeln heißt **konsistent**, wenn Ψ für alle $\Psi \subseteq \Phi$ mit $|\Psi| < \infty$ erfüllbar ist.

Der Kompaktheitssatz

Kompaktheit bedeutet:

- Unerfüllbarkeit kann sich nicht erst im Unendlichen einstellen, oder
- Erfüllbarkeit im Endlichen setzt sich ins Unendliche fort.

Thm.: Wenn Φ konsistent ist, dann ist Φ erfüllbar.

Bem.:

- Trivial, falls $|\Phi| < \infty$.
- Anders gesagt: Ist jede endliche Teilmenge einer Menge Φ erfüllbar, so ist auch Φ erfüllbar.

Notation: $\Psi \subseteq_{fin} \Phi$ gdw. $\Psi \subseteq \Phi$ und $|\Psi| < \infty$

Beweis des Kompaktheitssatzes

Lemma 1: Sei $\mathcal{I}(A) = \mathcal{I}'(A)$ für alle $A \in \text{Var}(\varphi)$. Dann gilt $\mathcal{I} \models \varphi$ gdw. $\mathcal{I}' \models \varphi$.

BEWEIS Einfach per Induktion über Aufbau von φ .

Lemma 2: Ist Φ konsistent, so ist $\Phi \cup \{A\}$ oder $\Phi \cup \{\neg A\}$ konsistent.

BEWEIS: Durch Widerspruch. Angenommen, sowohl $\Phi \cup \{A\}$ als auch $\Phi \cup \{\neg A\}$ seien inkonsistent. Dann ex. unerfüllbare $\Psi \subseteq_{fin} \Phi \cup \{A\}$ und $\Psi' \subseteq_{fin} \Phi \cup \{\neg A\}$.

Somit ist auch $\Theta := \Psi \cup \Psi'$ unerfüllbar, und damit auch $\Theta \cup \{A\}$ und $\Theta \cup \{\neg A\}$.

Dann muss aber bereits $\Theta \setminus \{\{A\}, \{\neg A\}\}$ unerfüllbar sein.

Da $\Theta \setminus \{\{A\}, \{\neg A\}\} \subseteq_{fin} \Phi$, ist Φ also dann inkonsistent. □

Beweis des Kompaktheitssatzes

Thm.: Wenn Φ konsistent ist, dann ist Φ erfüllbar.

BEWEIS: Def. simultan $\Phi_0 := \Phi$, $\Phi_{i+1} := \Phi_i \cup \{l_i\}$ und

$$l_i := \begin{cases} A_i & , \text{ falls } \Phi_i \cup \{A_i\} \text{ konsistent} \\ \neg A_i & , \text{ sonst} \end{cases}$$

Mit Lemma 2 und Induktion sind alle Φ_i konsistent. Definiere $\mathcal{I}$ über

$$\mathcal{I}(A_i) := \begin{cases} \text{tt} & , \text{ falls } l_i = A_i \\ \text{ff} & , \text{ falls } l_i = \neg A_i \end{cases}$$

Behauptung: $\mathcal{I} \models \varphi$ für alle $\varphi \in \Phi$

Beweis der Behauptung

Sei $\varphi \in \Phi$.

Wähle $k := \max\{i \mid A_i \in \text{Var}(\varphi)\}$.

Da $\Phi = \Phi_0 \subseteq \Phi_1 \subseteq \dots$ gilt also $\varphi \in \Phi_{k+1}$ und somit

$$\Psi := \{\varphi, l_0, \dots, l_k\} \subseteq_{fin} \Phi_{k+1}$$

Wegen Konsistenz von Φ_{k+1} ist Ψ erfüllbar. Also ex. $\mathcal{I}'$, so dass $\mathcal{I}' \models \Psi$.

Beachte: $\mathcal{I}(A) = \mathcal{I}'(A)$ für alle $A \in \text{Var}(\varphi)$ und außerdem $\mathcal{I}' \models \varphi$.

Wegen Lemma 1 gilt dann $\mathcal{I} \models \varphi$. □

Eine Anwendung des Kompaktheitssatzes

Kacheln sind Einheitsquadrate mit gefärbten Kanten:



Sei K eine endliche Menge von Kacheln. Dies induziert zwei Relationen H und V , die besagen, ob zwei Kacheln **horizontal** bzw. **vertikal** aneinanderpassen.

Eine K -**Kachelung** der $n \times n$ -Ebene ist eine Funktion $k : \{0, \dots, n-1\}^2 \rightarrow K$, so dass für alle $i = 0, \dots, n-2$, $j = 0, \dots, n-1$ gilt:

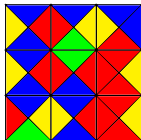
- $(k(i, j), k(i+1, j)) \in H$ “horizontal passt alles”
- $(k(j, i), k(j, i+1)) \in V$ “vertikal passt alles”

analog K -Kachelung der unendlichen $\mathbb{N} \times \mathbb{N}$ -Ebene definiert

Beispiel

Bsp.: $K =$ 

K -Kachelung der 3×3 -Ebene:



Anwendung des Kompaktheitssatzes

Thm.: Sei K eine Menge von Kacheln. Wenn jede $n \times n$ -Ebene K -kachelbar ist, so ist auch die $\mathbb{N} \times \mathbb{N}$ -Ebene K -kachelbar.

BEWEIS: Benutze Aussagenvariablen $A_{i,j,t}$, $i, j \in \mathbb{N}$, $t \in K$ mit Bedeutung “das Feld (i, j) ist mit Kachel t belegt”

drücke K -Kachelbarkeit der $n \times n$ -Ebene aus:

$$\begin{aligned} \varphi_n := & \bigwedge_{i=0}^{n-1} \bigwedge_{j=0}^{n-1} \left(\bigvee_{t \in K} A_{i,j,t} \wedge \bigwedge_{t' \neq t} \neg A_{i,j,t'} \right) \\ & \wedge \bigwedge_{i=0}^{n-2} \bigwedge_{j=0}^{n-1} \left(\bigwedge_{(t,t') \notin H} \neg (A_{i,j,t} \wedge A_{i+1,j,t'}) \right) \wedge \left(\bigwedge_{(t,t') \notin V} \neg (A_{j,i,t} \wedge A_{j,i+1,t'}) \right) \end{aligned}$$

Anwendung des Kompaktheitssatzes

Beachte:

- Erfüllende Belegung für φ_n induziert Kachelung der $n \times n$ -Ebene.
- Wenn $m \leq n$, dann ist $\varphi_n \rightarrow \varphi_m$ allgemeingültig. Intuitiv: $n \times n$ -Kachelung liefert auch immer eine $m \times m$ -Kachelung.

Sei $\Phi := \{\varphi_n \mid n \in \mathbb{N}\}$.

“Jede $n \times n$ -Ebene ist K -kachelbar” bedeutet: Für alle $n \in \mathbb{N}$ ist φ_n erfüllbar.

Sei $\Psi \subseteq_{fin} \Phi$. Dann ist $\Psi = \{\varphi_{i_1}, \dots, \varphi_{i_k}\}$ für ein $k \in \mathbb{N}$ und $i_1 < i_2 < \dots < i_k$. Da φ_{i_k} erfüllbar ist, ist mit obiger Bemerkung auch Ψ erfüllbar.

Aus dem Kompaktheitssatz folgt, dass auch Φ erfüllbar ist; erfüllende Belegung induziert K -Kachelung der $\mathbb{N} \times \mathbb{N}$ -Ebene. □

Beweiskalküle

DPLL-Algorithmus in gewisser Weise **semantisches** Verfahren zum Erkennen von Erfüllbarkeit. (Konstruiert Modell für Formel)

Im folgenden zwei **syntaktische** Verfahren zum Erkennen von (Un-)Erfüllbarkeit / Allgemeingültigkeit.

- ① Resolution (für Unerfüllbarkeit)
- ② Sequenzenkalkül (für Folgerungsbeziehung und damit insbesondere Allgemeingültigkeit)

Beachte Zusammenhang zwischen Erfüllbarkeit und Allgemeingültigkeit (und auch Folgerungsbeziehung, wie wir noch sehen werden): diese Verfahren sind somit auch in der Lage, die jeweils anderen Fragestellungen zu lösen.

Resolventen

Wir erweitern den Begriff der Äquivalenz. Sei C Klausel, $\mathcal{K}, \mathcal{K}'$ Klauselmengen:

$$\mathcal{I} \models C \quad \text{gdw.} \quad \mathcal{I} \models \bigvee_{\ell \in C} \ell$$

$$\mathcal{I} \models \mathcal{K} \quad \text{gdw.} \quad \text{für alle } C \in \mathcal{K} : \mathcal{I} \models C$$

$$\mathcal{K} \iff \mathcal{K}' \quad \text{gdw.} \quad \text{für alle } \mathcal{I} : \mathcal{I} \models \mathcal{K} \text{ gdw. } \mathcal{I} \models \mathcal{K}'$$

Def.: Sei ℓ Literal. $\bar{\ell} := \begin{cases} \neg A & , \text{ falls } \ell = A, \\ A & , \text{ falls } \ell = \neg A \end{cases}$

Def.: Seien C_1, C_2 Klauseln, ℓ Literal, so dass $\ell \in C_1, \bar{\ell} \in C_2$.
Dann heisst

$$C := (C_1 \setminus \{\ell\}) \cup (C_2 \setminus \{\bar{\ell}\})$$

Resolvente von C_1 und C_2 .

Das Resolutionslemma

Lemma: Sei $\mathcal{K}$ Klauselmenge, $C_1, C_2 \in \mathcal{K}$, C Resolvente von C_1 und C_2 . Dann gilt: $\mathcal{K} \Longleftrightarrow \mathcal{K} \cup \{C\}$.

BEWEIS: “ $\Leftarrow$ ” Sei $\mathcal{I} \models \mathcal{K} \cup \{C\}$. Da $\mathcal{K} \subseteq \mathcal{K} \cup \{C\}$ gilt dann auch $\mathcal{I} \models \mathcal{K}$.

“ $\Rightarrow$ ” Sei $\mathcal{I} \models \mathcal{K}$. Es reicht aus zu zeigen, dass $\mathcal{I} \models C$ gilt.

Da $C_1, C_2 \in \mathcal{K}$ gilt also insbesondere $\mathcal{I} \models C_1$ und $\mathcal{I} \models C_2$. D.h. es gibt Literale $\ell_1 \in C_1$, $\ell_2 \in C_2$, so dass $\mathcal{I} \models \ell_1$ und $\mathcal{I} \models \ell_2$. Somit gilt $\ell_1 \neq \bar{\ell}_2$. Da $C = (C_1 \setminus \{\ell\}) \cup (C_2 \setminus \{\bar{\ell}\})$ für ein $\ell \in C_1$ muss $\ell_1 \in C$ oder $\ell_2 \in C$ sein. Dann gilt aber $\mathcal{I} \models C$. □

Resolution

Def.: Ein **Resolutionsbeweis** für (Unerfüllbarkeit von) $\mathcal{K}$ ist ein endlicher, binär verzweigender Baum, dessen Knoten mit Klauseln beschriftet sind und für den gilt:

- Die **Wurzel** ist mit $\emptyset$ beschriftet.
- An den **Blättern** stehen nur Klauseln aus $\mathcal{K}$.
- Die Beschriftung eines **inneren Knoten** ist Resolvente der Beschriftungen seiner beiden Söhne.

Bsp.: $\mathcal{K} = \{\{A, B\}, \{A, \neg B\}, \{\neg A, B\}, \{\neg A, \neg B\}\}$

$$\begin{array}{c}
 \begin{array}{cc}
 A, B & \neg A, B
 \end{array} \\
 \hline
 B
 \end{array}
 \quad
 \begin{array}{cc}
 A, \neg B & \neg A, \neg B
 \end{array} \\
 \hline
 \neg B
 \end{array}
 \\
 \hline
 \emptyset$$

Bsp.: $\mathcal{K} = \{\{A, B\}, \{A, \neg B\}, \{\neg A, B\}\}$ hat keinen Resolutionsbeweis, aber wieso?

Korrektheit der Resolution

Thm.: Sei $\mathcal{K}$ Klauselmenge. $\mathcal{K}$ ist unerfüllbar gdw. es einen Resolutionsbeweis für $\mathcal{K}$ gibt.

BEWEIS: “ $\Leftarrow$ ” Angenommen, es existiert Resolutionsbeweis T für $\mathcal{K}$. Für $i \geq 0$ definiere induktiv $\mathcal{W}_i = \mathcal{W}_{i-1} \cup \{C \mid C \text{ ist Knoten der Tiefe } i \text{ in } T\}$. Beachte: Blätter haben Tiefe 0.

Es reicht aus zu zeigen, dass $\mathcal{W}_0$ unerfüllbar ist, denn $\mathcal{W}_0 \subseteq \mathcal{K}$.

Für alle $i > 0$ gilt: $\mathcal{W}_i \setminus \mathcal{W}_{i-1}$ besteht nur aus Resolventen von Klauseln in $\mathcal{W}_{i-1}$. Also gilt nach (evtl.) mehrfacher Anwendung des Resolutionslemmas jeweils für $i > 0$:

$$\mathcal{W}_i \iff \mathcal{W}_{i-1}$$

Da T endliche Tiefe t hat, gilt $\emptyset \in \mathcal{W}_t$. Somit ist $\mathcal{W}_t$ unerfüllbar und daher auch $\mathcal{W}_0$ und somit auch $\mathcal{K}$.

Vollständigkeit der Resolution

“ $\implies$ ” Angenommen $\mathcal{K}$ ist unerfüllbar. Nach dem Kompaktheitssatz existiert $\mathcal{K}_0 \subseteq_{fin} \mathcal{K}$, welches bereits unerfüllbar ist. Offensichtlich gilt: Ein Resolutionsbeweis für $\mathcal{K}_0$ ist auch einer für $\mathcal{K}$. Sei $Var(\mathcal{K}_0) = \{A_1, \dots, A_n\}$. Wir zeigen die Existenz eines Resolutionsbeweises für $\mathcal{K}_0$ durch Induktion über n .

Induktionsanfang, $n = 0$. Dann ist $Var(\mathcal{K}_0) = \emptyset$. Es gibt nur zwei Klauselmengen über der leeren Variablenmenge: $\emptyset$ und $\{\emptyset\}$. Da $\emptyset$ aber trivialerweise erfüllbar ist, muss $\mathcal{K}_0 = \{\emptyset\}$ gelten.

Offensichtlich lässt sich dafür ein Resolutionsbeweis bauen.

Induktionsschritt, $n > 0$. Die Induktionshypothese besagt, dass es für unerfüllbare Klauselmengen über den Variablen $A_1, \dots, A_{n-1}$ Resolutionsbeweise gibt. Konstruiere nun

$$\mathcal{K}_0^+ := \{C \setminus \{\neg A_n\} \mid C \in \mathcal{K}_0\}$$

$$\mathcal{K}_0^- := \{C \setminus \{A_n\} \mid C \in \mathcal{K}_0\}$$

Vollständigkeit der Resolution

Beachte: sowohl $\mathcal{K}_0^+$ als auch $\mathcal{K}_0^-$ sind unerfüllbar (Übung), denn sonst wäre $\mathcal{K}_0$ erfüllbar.

Die Induktionshypothese liefert nun also zwei Resolutionsbeweise T^+ und T^- . Durch Einfügen von $\neg A_n$ in T^+ und A_n in T^- lassen sich Klauseln darin zu Klauseln in $\mathcal{K}_0$ und deren Resolventen erweitern. Seien T'^+ und T'^- die jeweils entstehenden Bäume.

Jetzt gibt es zwei Fälle:

- 1 In T^+ oder T^- wurde nicht das Literal $\neg A_n$ bzw. A_n an der Wurzel eingefügt. Dann ist T'^+ bzw. T'^- auch ein Resolutionsbeweis für $\mathcal{K}_0$.
- 2 Sowohl in T^+ als auch T^- wurde jeweils das Literal $\neg A_n$ bzw. A_n eingefügt. Dann sind die Wurzeln von T'^+ und T'^- jeweils $\{\neg A_n\}$ und $\{A_n\}$. Diese haben als Resolvente $\emptyset$, und so kann ein Resolutionsbeweis T' für $\mathcal{K}_0$ mit Wurzel $\emptyset$ und den zwei Teilbäumen T'^+ und T'^- gebaut werden. □

Resolution verwenden

Unerfüllbarkeit ist eine **universelle** Eigenschaft: **alle** Interpretationen sind kein Modell. Resolution charakterisiert dies **existentiell**: statt alle Interpretationen für eine Formel zu testen, reicht es aus, einen Resolutionsbeweis anzugeben.

Aber: Resolutionsbeweise können **exponentielle Größe** haben (Übung). Im Vergleich: Zeugen für **Erfüllbarkeit** (Modelle) haben höchstens **lineare** Größe.

Beweissuche im Resolutionskalkül für Klauselmengen $\mathcal{K}$:

$$\begin{aligned}\mathcal{K}^0 &:= \mathcal{K} \\ \mathcal{K}^{n+1} &:= \mathcal{K}^n \cup \{C \mid \text{es gibt } C_1, C_2 \in \mathcal{K}^n \text{ so dass} \\ &\quad C \text{ Resolvente von } C_1 \text{ und } C_2 \text{ ist} \}\end{aligned}$$

Iteration bis $\emptyset$ als Resolvente auftritt oder $\mathcal{K}^{n+1} = \mathcal{K}^n$ für ein n gilt.

Sequenzen

Zum Abschluss des Kapitels über Aussagenlogik behandeln wir noch Gentzens **Sequenzenkalkül**.

Charakterisiert logische **Folgerungsbeziehung** syntaktisch.

Def.: Seien φ, ψ Formeln. ψ **folgt aus** φ , geschrieben $\varphi \models \psi$, falls für alle $\mathcal{I}$ gilt: wenn $\mathcal{I} \models \varphi$ dann $\mathcal{I} \models \psi$.

Beachte: $\varphi \models \psi$ gdw. $\varphi \rightarrow \psi$ allgemeingültig

Def.: Eine **Sequenz** ist ein Paar $\Gamma \Longrightarrow \Delta$ von Formelmengen. Γ heißt Antezedens, Δ Sukzedens. Vereinfachte Schreibweise ohne Mengenklammern, etc.: $\varphi_1, \dots, \varphi_n \Longrightarrow \psi_1, \dots, \psi_m$

Def.: $\Gamma \Longrightarrow \Delta$ ist **gültig**, falls $\bigwedge \Gamma \models \bigvee \Delta$.

Beispiele

Bsp.: welche der folgenden Sequenzen sind gültig?

① $A, A \rightarrow B \Longrightarrow B$

② $\neg A, \neg B \Longrightarrow A, B$

③ $A, A \rightarrow B \Longrightarrow \emptyset$

④ $A, \neg A \Longrightarrow B$

⑤ $A \rightarrow B, B \rightarrow C, A \Longrightarrow C$

⑥ $A \wedge B \rightarrow C, A \Longrightarrow B \rightarrow C$

Folgerung und Allgemeingültigkeit

Bereits oben gesehen: Folgerung kann mithilfe von Allgemeingültigkeit ausgedrückt werden:

$$\Gamma \implies \Delta \text{ gültig } \text{ gdw. } \bigwedge \Gamma \rightarrow \bigvee \Delta \text{ allgemeingültig}$$

Umkehrung gilt ebenfalls:

Lemma: φ ist allgemeingültig gdw. die Sequenz $\emptyset \implies \varphi$ gültig ist.

BEWEIS: “ $\implies$ ” Angenommen, $\emptyset \implies \varphi$ ist nicht gültig. Dann existiert $\mathcal{I}$, so dass $\mathcal{I} \models \bigwedge \emptyset$ und $\mathcal{I} \not\models \bigvee \{\varphi\}$. Beachte: $\bigvee \{\varphi\} \iff \varphi$, also ist φ nicht allgemeingültig.

“ $\impliedby$ ” Angenommen, $\emptyset \implies \varphi$ ist gültig, d.h. für alle $\mathcal{I}$ gilt: $\mathcal{I} \not\models \bigwedge \emptyset$ oder $\mathcal{I} \models \bigvee \{\varphi\}$. Da $\bigwedge \emptyset \iff \perp$ muss also $\mathcal{I} \models \varphi$ für alle $\mathcal{I}$ gelten. Somit ist φ allgemeingültig. $\square$

Also auch: $\varphi \implies \emptyset$ gdw. φ unerfüllbar.

Beweise im Sequenzenkalkül

Sequenzenkalkül charakterisiert genau die gültigen Sequenzen, d.h. eine Sequenz ist gültig gdw. sie im Sequenzenkalkül beweisbar ist.

Def.: Ein **Beweis** im Sequenzenkalkül für eine Sequenz $\Gamma \Longrightarrow \Delta$ ist ein endlicher Baum, dessen

- **Wurzel** mit $\Gamma \Longrightarrow \Delta$ beschriftet ist,
- **Blätter** mit **Axiomen** beschriftet sind,
- **innere Knoten** mit ihren Söhnen Instanzen von **Beweisregeln** sind.

Beweisregeln haben die Form

$$\frac{\Gamma_1 \Longrightarrow \Delta_1 \quad \dots \quad \Gamma_n \Longrightarrow \Delta_n}{\Gamma \Longrightarrow \Delta} \text{ (Name)}$$

$\Gamma_i \Longrightarrow \Delta_i$ heißen **Prämissen**, $\Gamma \Longrightarrow \Delta$ **Konklusion**

Axiom = Beweisregel ohne Prämissen

Axiome und Regeln des Sequenzenkalküls

Axiome:

$$\frac{}{\Gamma, \perp \Longrightarrow \Delta} (\perp_L) \quad \frac{}{\Gamma \Longrightarrow \Delta, \top} (\top_R) \quad \frac{}{\Gamma, \varphi \Longrightarrow \Delta, \varphi} (\text{Ax})$$

Beweisregeln:

$$\frac{\Gamma, \varphi, \psi \Longrightarrow \Delta}{\Gamma, \varphi \wedge \psi \Longrightarrow \Delta} (\wedge_L) \quad \frac{\Gamma \Longrightarrow \Delta, \varphi \quad \Gamma \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \varphi \wedge \psi} (\wedge_R)$$

$$\frac{\Gamma, \varphi \Longrightarrow \Delta \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \varphi \vee \psi \Longrightarrow \Delta} (\vee_L) \quad \frac{\Gamma \Longrightarrow \Delta, \varphi, \psi}{\Gamma \Longrightarrow \Delta, \varphi \vee \psi} (\vee_R)$$

Beweisregeln des Sequenzenkalküls

$$\frac{\Gamma \Longrightarrow \Delta, \varphi}{\Gamma, \neg \varphi \Longrightarrow \Delta} (\neg_L) \qquad \frac{\Gamma, \varphi \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \neg \varphi} (\neg_R)$$

$$\frac{\Gamma \Longrightarrow \Delta, \varphi \quad \Gamma, \psi \Longrightarrow \Delta}{\Gamma, \varphi \rightarrow \psi \Longrightarrow \Delta} (\rightarrow_L) \qquad \frac{\Gamma, \varphi \Longrightarrow \Delta, \psi}{\Gamma \Longrightarrow \Delta, \varphi \rightarrow \psi} (\rightarrow_R)$$

$$\frac{\Gamma \Longrightarrow \Delta}{\Gamma, \top \Longrightarrow \Delta} (\top_L) \qquad \frac{\Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \perp} (\perp_R)$$

Es fehlen noch 2 Regeln für $\leftrightarrow$ (Übung)

Beispiel

$$\begin{array}{c}
 \frac{}{\psi_1, \psi_2 \Rightarrow \varphi, \psi_1} (\text{Ax}) \quad \frac{}{\psi_1, \psi_2 \Rightarrow \varphi, \psi_2} (\text{Ax}) \\
 \frac{}{\psi_1, \psi_2 \Rightarrow \varphi \vee \psi_1} (\vee_R) \quad \frac{}{\psi_1, \psi_2 \Rightarrow \varphi \vee \psi_2} (\vee_R) \\
 \frac{}{\psi_1, \psi_2 \Rightarrow (\varphi \vee \psi_1) \wedge (\varphi \vee \psi_2)} (\wedge_L) \quad \frac{}{\varphi \Rightarrow \varphi, \psi_1} (\text{Ax}) \quad \frac{}{\varphi \Rightarrow \varphi, \psi_2} (\text{Ax}) \\
 \frac{}{\psi_1 \wedge \psi_2 \Rightarrow (\varphi \vee \psi_1) \wedge (\varphi \vee \psi_2)} (\wedge_R) \quad \frac{}{\varphi \Rightarrow \varphi \vee \psi_1} (\vee_R) \quad \frac{}{\varphi \Rightarrow \varphi \vee \psi_2} (\vee_R) \\
 \frac{}{\varphi \Rightarrow (\varphi \vee \psi_1) \wedge (\varphi \vee \psi_2)} (\wedge_R) \\
 \frac{}{\varphi \vee (\psi_1 \wedge \psi_2) \Rightarrow (\varphi \vee \psi_1) \wedge (\varphi \vee \psi_2)} (\vee_L) \\
 \frac{}{\emptyset \Rightarrow \varphi \vee (\psi_1 \wedge \psi_2) \rightarrow (\varphi \vee \psi_1) \wedge (\varphi \vee \psi_2)} (\rightarrow_R)
 \end{array}$$

Axiomen- und Ableitungslemma

Ziel: zeige, dass im Sequenzenkalkül **genau** die gültigen Sequenzen beweisbar sind

dazu brauchen wir lediglich drei Lemmas

Lemma: (Axiomenlemma I) Jede Sequenz $\Gamma \Longrightarrow \Delta$, die ein Axiom ist, ist gültig.

BEWEIS: Leicht zu sehen für Axiome $(\perp_L)$ und $(\top_R)$. Betrachte noch Axiom (Ax) mit $\Gamma, \varphi \Longrightarrow \Delta, \varphi$. Sei $\mathcal{I}$ Interpretation. Zu zg.: Wenn $\mathcal{I} \models \bigwedge \Gamma \cup \{\varphi\}$ dann $\mathcal{I} \models \bigvee \Delta \cup \{\varphi\}$.

Angenommen, $\mathcal{I} \models \bigwedge \Gamma \cup \{\varphi\}$. Dann gilt insbesondere $\mathcal{I} \models \varphi$ und somit auch $\mathcal{I} \models \varphi \vee \bigvee \Delta$ bzw. $\mathcal{I} \models \bigvee \Delta \cup \{\varphi\}$. □

Lemma: (Ableitungslemma) Für alle Regeln des Sequenzenkalküls gilt: Die Konklusion ist gültig gdw. alle Prämissen gültig sind.

Beweis des Ableitungslemmas

BEWEIS Wir zeigen dies exemplarisch für die Regeln $(\wedge_L)$ und $(\wedge_R)$.

Fall $(\wedge_L)$. Dies ist trivial, da $\bigwedge \Gamma \cup \{\varphi \wedge \psi\} \iff \bigwedge \Gamma \cup \{\varphi, \psi\}$.

Fall $(\wedge_R)$. Zur Erinnerung: Konklusion $K = \Gamma \implies \Delta, \varphi \wedge \psi$,
Prämissen sind $P_1 = \Gamma \implies \Delta, \varphi$ und $P_2 = \Gamma \implies \Delta, \psi$.

“ $\implies$ ” Angenommen, eine der beiden Prämissen ist ungültig. Sei dies P_1 . Der Fall mit P_2 ist analog. Dann ex. $\mathcal{I}$, so dass $\mathcal{I} \models \bigwedge \Gamma$ und $\mathcal{I} \not\models \bigvee \Delta \cup \{\varphi\}$. Daraus folgt insbesondere, dass $\mathcal{I} \not\models \bigvee \Delta$ und $\mathcal{I} \not\models \varphi$. Somit gilt dann aber auch $\mathcal{I} \not\models \varphi \wedge \psi$. Zusammengefasst: $\mathcal{I} \models \bigwedge \Gamma$ und $\mathcal{I} \not\models \bigvee \Delta \cup \{\varphi \wedge \psi\}$. Also ist K nicht gültig.

“ $\Leftarrow$ ” Angenommen, die Konklusion ist ungültig. Also gibt es $\mathcal{I}$, so dass $\mathcal{I} \models \bigwedge \Gamma$ und $\mathcal{I} \not\models \bigvee \Delta \cup \{\varphi \wedge \psi\}$. Insbesondere gilt $\mathcal{I} \not\models \varphi \wedge \psi$, also $\mathcal{I} \not\models \varphi$ oder $\mathcal{I} \not\models \psi$. Dann gilt auch $\mathcal{I} \not\models \bigvee \Delta \cup \{\varphi\}$ oder $\mathcal{I} \not\models \bigvee \Delta \cup \{\psi\}$. Also ist entweder P_1 ungültig oder P_2 ungültig. □

Korrektheit des Sequenzenkalküls

Thm.: Jede im Sequenzenkalkül beweisbare Sequenz ist gültig.

BEWEIS: Angenommen es ex. Beweis für $\Gamma \Longrightarrow \Delta$. Wir zeigen per Induktion über die Höhe h des Beweisbaums, dass $\Gamma \Longrightarrow \Delta$ gültig ist.

Induktionsanfang $h = 1$. Dann ist $\Gamma \Longrightarrow \Delta$ ein Axiom und laut Axiomenlemma I gültig.

Induktionsschritt. Sei $h > 1$. Dann gibt es eine Beweisregel mit Prämissen $P_1, \dots, P_n$, zu denen $\Gamma \Longrightarrow \Delta$ Konklusion ist. Beachte: Jedes P_i ist beweisbar im Sequenzenkalkül mit einem Beweis der Höhe $< h$. Nach Induktionsvoraussetzung sind alle P_i somit gültig. Mit dem Ableitungslemma folgt dann, dass auch $\Gamma \Longrightarrow \Delta$ gültig sein muss.

Vorbereitung auf die Vollständigkeit

Lemma: (Axiomenlemma II) Angenommen $\Gamma, \Delta \subseteq \mathcal{V}$. Dann ist $\Gamma \implies \Delta$ gültig gdw. $\Gamma \cap \Delta \neq \emptyset$.

BEWEIS: (nur “ $\implies$ ”) Angenommen, $\Gamma \cap \Delta = \emptyset$. Wir zeigen, dass $\Gamma \implies \Delta$ ungültig ist, indem wir eine falsifizierende Interpretation angeben.

$$\mathcal{I}(A) := \begin{cases} \text{tt} & , \text{ falls } A \in \Gamma \\ \text{ff} & , \text{ sonst} \end{cases}$$

Aufgrund der Voraussetzung gilt $\mathcal{I}(B) = \text{ff}$ für alle $B \in \Delta$. Also gilt

$$\mathcal{I} \models \bigwedge \Gamma \quad \text{und} \quad \mathcal{I} \not\models \bigvee \Delta$$

und somit ist $\Gamma \implies \Delta$ nicht gültig. □

Vollständigkeit des Sequenzenkalküls

Thm.: Jede gültige Sequenz $\Gamma \Longrightarrow \Delta$ ist im Sequenzenkalkül herleitbar.

BEWEIS: Sei $\Gamma \Longrightarrow \Delta$ gültig. Wir zeigen, dass es auch beweisbar ist durch Induktion über die Anzahl j der Vorkommen der Konstanten $\perp$ und $\top$ und der Junktoren $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ in $\Gamma \cup \Delta$.

Induktionsanfang, $j = 0$. Dann besteht $\Gamma \cup \Delta$ nur aus Variablen. Nach dem Axiomenlemma II gilt dann $\Gamma \cap \Delta \neq \emptyset$. Dann ist $\Gamma \Longrightarrow \Delta$ Instanz von (Ax) und somit beweisbar.

Induktionsschritt, $j > 0$. Also existiert noch mindestens ein Junktor oder eine Konstante in $\Gamma \cup \Delta$. Wir unterscheiden zwei Fälle.

Vollständigkeit des Sequenzenkalküls

- ① $\perp \in \Gamma$ oder $\top \in \Delta$. Dann ist $\Gamma \Longrightarrow \Delta$ Instanz von $(\perp_L)$ oder $(\top_R)$ und somit beweisbar.
- ② Sonst. Da $j > 0$ muss mindestens eine Beweisregel anwendbar sein. Nach dem Ableitungslemma sind alle entstehenden Prämissen gültig. Diese haben jedoch jeweils $< j$ Junktoren. Nach Induktionshypothese sind diese beweisbar. Durch Verknüpfung derer Beweisbäume erhält man einen Beweis für $\Gamma \Longrightarrow \Delta$. □

Beweissuche

Der Sequenzenkalkül ermöglicht es, **automatisch festzustellen**, ob eine gegebene Formel allgemeingültig ist. **Systematisch** wendet man Regel auf die Sequenz $\emptyset \Longrightarrow \varphi$ an um einen Beweisbaum zu konstruieren.

Alle Pfade enden in Axiomen $\rightsquigarrow$ Beweis gefunden. Ein Pfad endet in Sequenz, die kein Axiom ist und auf die keine Regel angewandt werden kann $\rightsquigarrow$ kein Beweis möglich.

Beachte: Die Regel selbst verlangen zwar keine Auswahl seitens des Benutzers, auf eine Sequenz können jedoch i.A. **mehrere Regeln angewandt** werden. Es ist so (hier kein Beweis), dass die **Reihenfolge** der Regelanwendungen nicht die Tatsache beeinflusst, ob ein Beweis letztendlich gefunden wird oder nicht.

Sie kann aber die **Größe** des gefundenen Beweises beeinflussen.

Beispiel

$$\begin{array}{c}
 \frac{A \Rightarrow A, B, C \quad \frac{B \Rightarrow A, B, C \quad C \Rightarrow A, B, C}{(B \vee C) \Rightarrow A, B, C} (\vee_L)}{A \vee (B \vee C) \Rightarrow A, B, C} (\vee_L) \\
 \frac{A \vee (B \vee C) \Rightarrow A, B, C}{A \vee (B \vee C) \Rightarrow A \vee B, C} (\vee_R) \\
 \frac{A \vee (B \vee C) \Rightarrow A \vee B, C}{A \vee (B \vee C) \Rightarrow (A \vee B) \vee C} (\vee_R)
 \end{array}$$

$$\begin{array}{c}
 \frac{A \Rightarrow A, B, C}{A \Rightarrow A \vee B, C} (\vee_R) \quad \frac{\frac{B \Rightarrow A, B, C}{B \Rightarrow A \vee B, C} (\vee_R) \quad \frac{C \Rightarrow A, B, C}{C \Rightarrow A \vee B, C} (\vee_R)}{B \vee C \Rightarrow (A \vee B) \vee C} (\vee_L) \\
 \frac{A \Rightarrow (A \vee B) \vee C}{A \vee (B \vee C) \Rightarrow (A \vee B) \vee C} (\vee_L)
 \end{array}$$

Herleitbarkeit

Def.: Eine Regel mit Prämissen $P_1, \dots, P_n$ und Konklusion K heißt **herleitbar**, wenn es einen Beweis für K gibt, der $P_1, \dots, P_n$ als Axiome benutzt.

Bsp.: Die folgenden Regeln sind z.B. im Sequenzenkalkül herleitbar.

$$\frac{\Gamma \Rightarrow \Delta, \varphi_1 \quad \dots \quad \Gamma \Rightarrow \Delta, \varphi_n}{\Gamma \Rightarrow \Delta, \varphi_1 \wedge \dots \wedge \varphi_n} (\wedge_R^*) \quad \frac{\Gamma, \varphi, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg(\varphi \wedge \psi)} (\text{NAND}_R)$$

Herleitbare Regeln können die Beweissuche vereinfachen.
Außerdem sollte folgendes offensichtlich sein.

Thm.: Sei $\mathcal{S}$ der Sequenzenkalkül mit zusätzlichen, herleitbaren Regeln. Dann ist eine Sequenz $\Gamma \Rightarrow \Delta$ in $\mathcal{S}$ beweisbar, gdw. sie gültig ist.

Zulässigkeit

Def.: Eine Regel heißt **zulässig**, wenn sich im Sequenzenkalkül **mit** dieser Regel dieselben Sequenzen beweisen lassen wie **ohne** diese Regel.

Bsp.: Die folgenden Regeln sind z.B. zulässig aber nicht herleitbar!

$$\begin{array}{c}
 \frac{\Gamma \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta} \text{ (Weak}_L\text{)} \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi} \text{ (Weak}_R\text{)} \\
 \\
 \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \text{ (Cut)}
 \end{array}$$

Beachte: Regel (Cut) zusammen mit $(\neg_L)$ drückt **Fallunterscheidung** aus.

Thm.: Jede herleitbare Regel ist zulässig. Nicht jede zulässige Regel ist herleitbar.

Cut-Elimination

Betrachte Verallgemeinerung von (Cut):

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \text{ (Cut)} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Theta, \varphi \Rightarrow \Psi}{\Gamma, \Theta \Rightarrow \Delta, \Psi} \text{ (Cut*)}$$

Lemma: (Cut/Axiomen-Lemma) Sind die Prämissen der Regel (Cut*) Axiome, so ist die Konklusion auch bereits ein Axiom.

BEWEIS: Durch mehrere Fallunterscheidungen.

- Ist $\perp \in \Gamma$, so ist auch $\perp \in \Gamma \cup \Theta$.
- Ist $\perp \in \Theta \cup \{\varphi\}$, dann gilt: Ist $\perp \in \Theta$, so auch $\perp \in \Gamma \cup \Theta$. Ist $\varphi = \perp$, dann benutzen wir die Tatsache, dass $\Gamma \Rightarrow \Delta, \varphi$ auch Axiom ist. Dann kann nur noch $\top \in \Delta$ oder $\Gamma \cap \Delta \neq \emptyset$ gelten. In beiden Fällen ist die Konklusion ebenfalls Axiom.
- ...



Cut-Elimination

Thm.: Die Regel (Cut) ist zulässig.

BEWEIS: Wir zeigen ein stärkeres Resultat, nämlich dass sogar die Regel zulässig ist. (Beachte: (Cut) ist Vereinfachung von (Cut*).)

Angenommen, es gibt einen Beweis für eine Sequenz, der (Cut*) benutzt. Dieser lässt sich zu einem Beweis umbauen, der (Cut*) nur an den Blättern benutzt. Dazu **vertauschen** wir die Anwendung von (Cut*) mit der Anwendung einer Regel darüber, hier exemplarisch gezeigt für ($\vee_R$) und ($\vee_L$).

$$\begin{array}{c}
 \vdots \\
 \hline
 \Gamma \Rightarrow \Delta, \varphi \quad \frac{\frac{\vdots}{\Theta, \varphi \Rightarrow \Psi, \psi_1, \psi_2} (\vee_R) \quad \Theta, \varphi \Rightarrow \Psi, \psi_1 \vee \psi_2}{} (\text{Cut}^*) \\
 \hline
 \Gamma, \Theta \Rightarrow \Delta, \Psi, \psi_1 \vee \psi_2 \\
 \vdots
 \end{array}
 \rightsquigarrow
 \begin{array}{c}
 \vdots \quad \vdots \\
 \hline
 \frac{\Gamma \Rightarrow \Delta, \varphi \quad \frac{\frac{\vdots}{\Theta, \varphi \Rightarrow \Psi, \psi_1, \psi_2} (\text{Cut}^*) \quad \Theta, \varphi \Rightarrow \Psi, \psi_1, \psi_2}{} (\vee_R)}{\Gamma, \Theta \Rightarrow \Delta, \Psi, \psi_1 \vee \psi_2} (\text{Cut}^*) \\
 \vdots
 \end{array}$$

Beweis der Cut-Elimination

$$\begin{array}{c}
 \vdots \qquad \qquad \vdots \\
 \hline
 \Gamma, \gamma_1 \Rightarrow \Delta, \varphi \quad \Gamma, \gamma_2 \Rightarrow \Delta, \varphi \\
 \hline
 \Gamma, \gamma_1 \vee \gamma_2 \Rightarrow \Delta, \varphi \quad (V_L) \quad \vdots \\
 \hline
 \Theta, \varphi \Rightarrow \Psi \\
 \hline
 \Gamma, \gamma_1 \vee \gamma_2, \Theta \Rightarrow \Delta, \Psi \quad (Cut^*) \\
 \hline
 \vdots \\
 \rightsquigarrow \\
 \vdots \qquad \qquad \vdots \qquad \qquad \vdots \qquad \qquad \vdots \\
 \hline
 \Gamma, \gamma_1 \Rightarrow \Delta, \varphi \quad \Theta, \varphi \Rightarrow \Psi \quad (Cut^*) \quad \Gamma, \gamma_2 \Rightarrow \Delta, \varphi \quad \Theta, \varphi \Rightarrow \Psi \quad (Cut^*) \\
 \hline
 \Gamma, \gamma_1, \Theta \Rightarrow \Delta, \Psi \quad \Gamma, \gamma_2, \Theta \Rightarrow \Delta, \Psi \\
 \hline
 \Gamma, \gamma_1 \vee \gamma_2, \Theta \Rightarrow \Delta, \Psi \quad (V_L) \\
 \hline
 \vdots
 \end{array}$$

So entsteht also ein Beweis, in dem Regel (Cut*) nur unter Axiomen (und wiederum darunter) vorkommt. Aus dem Cut/Axiomen-Lemma folgt dann, dass diese auch alle weggelassen werden können. □

PVS

PVS ist ein **Theorembeweiser**, in dem der Sequenzenkalkül implementiert ist.

frei erhältlich von <http://pvs.csl.sri.com/>

Zum manuellen Beweisen von aussagenlogischen Sequenzen reichen die Befehle

- `(flatten)`, wendet Regeln mit einer Prämisse an, z.B. $(\vee_R), (\wedge_L)$, etc.
- `(split  $n$ )`, wendet Regel mit zwei Prämissen auf n -te Formel in der Sequenz an, z.B. $(\vee_L), (\wedge_R)$, etc.