`http://home.mathematik.uni-freiburg.de/flum/ss04li`

Was ist Logik?

Welche Rolle spielt die Logik in der Informatik?

- Überblick über die Regeln des Schließens
  Was ist ein logischer Schluß?

- Was ist ein Beweis?
  (Regeln des Schließens)

  “daraus folgt”
  “somit”
  “daher”
  “unmittelbar ergibt sich”

Aristoteles (384 - 322 v. Chr.)

- Schule der Sophisten

Achilles und die Schildkröte

Achilles und die Schildkröte laufen ein Wettrennen. Achilles gewährt der Schildkröte einen Vorsprung. Dann kann Achilles die Schildkröte niemals einholen.

Zenon von Elea (490 - 425 v. Chr.) gibt folgende Begründung: Zu dem Zeitpunkt, an dem Achilles den Startpunkt der Schildkröte erreicht, ist die Schildkröte schon ein Stück weiter. Etwas später erreicht Achilles diesen Punkt, aber die Schildkröte ist schon etwas weiter. Wenn Achilles diesen Punkte erreicht, ist die Schildkröte wieder etwas weiter. So kann Achilles zwar immer näher an die Schildkröte herankommen, sie aber nie erreichen.

Der Barbier

In einem Städtchen wohnt ein Barbier, der genau diejenigen männlichen Einwohner rasiert, die sich nicht selbst rasieren.

Rasiert nun der Barbier sich selbst?

Antinomie des Lügners

Epimenides (Kreter, 600 v. Chr.)

Brief des Paulus an Titus 1:12-13:

> *Einer von ihren eigenen Landsleuten war ein Prophet, als er sagte: "Die Kreter lügen immer. Sie sind Raubtiere, liegen auf der faulen Haut und denken nur ans Fressen"*. Er hat die Wahrheit gesagt.

Aus Don Quijote de la Mancha von Miguel de Cervantes (1517–1616)

> *Um eine gewisse Brücke zu überqueren, müssen alle Reisenden zunächst angeben, was ihr Ziel ist. Antworten sie wahrheitsgemäß, so dürfen sie die Brücke überqueren. Sonst werden sie gnadenlos an einem Galgen am Fuß der Brücke erhängt.*
>
> *Eines Tages kommt ein Reisender, der angibt, sein Ziel sei es, am Galgen am Fuß der Brücke erhängt zu werden.*

Aristoteles: Bemühen Überblick über die Rgeln des Schließens (Syllogismen).

Prämisse:	Alle *Menschen* sind *sterblich*.
Prämisse:	*Sokrates* ist ein *Mensch*.
Konklusion:	*Sokrates* ist *sterblich*.

Prämisse:	Alle *Sura* sind *derung*.
Prämisse:	*Plarq* ist ein *Sura*.
Konklusion:	*Plarq* ist *derung*.

Prämisse:	Alle p sind q.
Prämisse:	a ist ein p.
Konklusion:	a ist q.

Ziel: Alle Schlußregeln.

- R. Llullus (1235–1315), G. W. Leibniz (1646–1716)
- G. Boole (1815–1864), G. Frege (1848–1943)
- D. Hilbert (1862–1925), B. Russell (1872–1970), K. Gödel (1906–1978)

Peter ist ein Lebewesen.
$f : \mathbb{N} \to \mathbb{N}$ ist eine Funktion.

Ein Chinese hat das Pulver entdeckt.
Ein Chinese ist ein Asiat.

Eine differenzierbare Funktion ist Lösung der Gleichung

$$f'' + f = 0.$$

Eine differenzierbare Funktion ist stetig.

- *Programmverifkation:* Man möchte wissen, dass ein Programm das “Richtige” tut oder dass es zumindest gewisse Eigenschaften hat.

- *Typechecking:* Der Compiler überprüft, dass eine Funktion immer einen Wert vom richtigen Typ zurückgibt.

- *Schaltkreisverifikation:* Man möchte beweisen, dass ein Chip richtig funktioniert.

- *Protokollverifikation:* Man möchte beweisen, dass die Komunikation zwischen zwei “Agenten”, die nach einem gewissen “Protokoll” abläuft sicher ist.

Logic is “the calculus of computer science”.

Logic permeates through computer science much more than it does through mathematics.

Diverse uses of logic in computer science:

- To model computer hardware
- As a database query language
- As a tool for representing and reasoning
- As a tool for specification and verification
- To produce problems that are complete for complexity classes

Σ **Alphabet**: Σ nich-leere Menge von **Zeichen** (**Buchstaben**);

$\Sigma_1 = \{0, 1, \ldots, 9\}$; $\quad \Sigma_2 = \{0, 1\}$;

$\Sigma_3 = \{a, b, \ldots, x, y, z\}$; $\quad \Sigma_4 = \{a, d, f, x, \int,), (\}$.

konkrete Zeichen;

häufig auch unendliche Alphabete:

$\Sigma_5 = \{c_0, c_1, \ldots\}$; $\quad \Sigma_6 = \{c_r \mid r \in \mathbb{R}\}$.

Alphabete: Σ, Π,...

Wort (Zeichenreihe) über Σ:
endliche Aneinanderreihung von Buchstaben aus Σ

Wörter: u, v, w,... leere Wort: λ;

Σ^* Menge der Wörter über dem Alphabet Σ;

$|w|$ **Länge** von w;

$\int f(x)dx, \;\; a \int \int dxd \in \Sigma_4^*$; $\quad |a \int \int dxd| = 6, \quad |\lambda| = 0$.

Σ_5 ersetzen durch endliches Alphabet, etwa durch

$$\Sigma_7 := \{c, {}_0, {}_1, \ldots, {}_9\}.$$

Bei Identifikation von c_{25} mit $c\,{}_2\,{}_5$:

$$\Sigma_5 \subseteq \Sigma_7^* \;\; \text{und} \;\; \Sigma_5^* \subseteq \Sigma_7^*.$$

X: Die Sonne scheint.

Y: Die Logikvorlesung ist langweilig.

Z: Das Softwarepraktikum ist langweilig.

Y und Z: Die Logikvorlesung und das Softwarepraktikum sind langweilig.

Wenn nicht X, so Y: Wenn die Sonne nicht scheint, dann ist die Logikvorlesung langweilig.

Aussagenlogische Ausdrücke oder **aussagenlogische Formeln** sind die Wörter über Σ_a, die mit den folgenden Regeln ableitbar sind:

(A1) Jede aussagenlogische Variable ist ein Ausdruck.

(A2) Ist α ein Ausdruck, so auch $\neg\alpha$.

(A3) Sind α und β Ausdrücke, so auch $(\alpha \wedge \beta)$ und $(\alpha \vee \beta)$.

Beispiel: $(\neg X_5 \vee (X_7 \wedge X_5))$ ist ein Ausdruck.

Begründung: Angabe einer Ableitung:

1	X_5	(A1)
2	X_7	(A1)
3	$(X_7 \wedge X_5)$	(A3) auf 2 und 1
4	$\neg X_5$	(A2) auf 1
5	$(\neg X_5 \vee (X_7 \wedge X_5))$	(A3) auf 4 und 3

Ableitung nicht eindeutig:

1	X_5	(A1)
2	$\neg X_5$	(A2) auf 1
3	X_7	(A1)
4	$(X_7 \wedge X_5)$	(A3) auf 3 und 1
5	$(\neg X_5 \vee (X_7 \wedge X_5))$	(A3) auf 2 und 4

Eine rekursive Definition einer Menge M wird durch einen Kalkül bestehend aus **rekursiven Regeln** gegeben, d.h. Regeln der Gestalt:

Wenn $m_1, \ldots, m_r \in M$, so auch $m \in M$

kurz:

$$\frac{m_1, \ldots, m_r}{m}$$

Falls $r = 0$, so spricht man auch von einer **Basisregel** oder **Ausgangsregel**. Sie hat also die Gestalt:

$m \in M$ $\qquad\qquad \dfrac{\quad}{m}$

M ist dann die Menge aller Objekte, deren Zugehörigkeit zu M durch endlichmalige Anwendung der Regeln des Kalküls gezeigt werden kann.

Beispiel: Sei $\Sigma = \{a, b, \ldots, y, z\}$ und M gegeben durch Kalkül:

(R0) $\dfrac{\quad}{\lambda}$

(R1) $\dfrac{w}{w\xi\eta}$, $\xi \in \{a, e, i, o, u\}$, $\eta \in \Sigma$.

$axei \in M$:

1	λ	(R0)
2	ax	(R1) auf 1 mit $\xi = a$ und $\eta = b$
3	$axei$	(R1) auf 2 mit $\xi = e$ und $\eta = i$

Wozu Klammern?

$$\frac{}{X} \qquad \frac{\alpha}{\neg\alpha} \qquad \frac{\alpha, \beta}{\alpha \wedge \beta} \qquad \frac{\alpha, \beta}{\alpha \vee \beta}$$

Aussagenlogische Belegung:

$$b : \text{AV} \to \{0, 1\}.$$

Erweitern auf alle aussagenlogische Ausdrücke durch Vorschriften:

$$\text{(F1)} \qquad b(\neg\alpha) := \begin{cases} 1 & \text{wenn } b(\alpha) = 0 \\ 0 & \text{wenn } b(\alpha) = 1 \end{cases}$$

$$\text{(F2)} \qquad b(\alpha \wedge \beta) := \begin{cases} 1 & \text{wenn } b(\alpha) = 1 \text{ und } b(\beta) = 1 \\ 0 & \text{sonst} \end{cases}$$

$$\text{(F3)} \qquad b(\alpha \vee \beta) := \begin{cases} 0 & \text{wenn } b(\alpha) = 0 \text{ und } b(\beta) = 0 \\ 1 & \text{sonst.} \end{cases}$$

Sei $b(X) = b(Y) = 0$ und $b(Z) = 1$. Was ist $b(X \wedge Y \vee Z)$?

$$b(X \wedge Y) \overset{\text{(F2)}}{=} 0 \qquad\qquad b(Y \vee Z) \overset{\text{(F3)}}{=} 1$$

$$b(X \wedge Y \vee Z) \overset{\text{(F3)}}{=} 1 \qquad\qquad b(X \wedge Y \vee Z) \overset{\text{(F2)}}{=} 0$$

Satz über die eindeutige Zerlegbarkeit

Jeder Ausdruck $\alpha \in$ AA ist **entweder** ein Ausdruck der Gestalt

(1) X_i **oder**

(2) $\neg\beta$ **oder**

(3) $(\beta \wedge \gamma)$ **oder**

(4) $(\beta \vee \gamma)$.

Dabei sind eindeutig bestimmt

β in (2) und β und γ in (3),(4).

Fall (2): α die **Negation** von β

Fall (3): α die **Konjunktion** von β und γ

Fall (4): α die **Disjunktion** von β und γ

Induktionsprinzip für rekursiv definierte Mengen:

Will man zeigen, daß alle Elemente einer Menge M, die durch einen Kalkül K definiert ist, eine Eigenschaft E haben, so genügt hierzu der Nachweis, daß

> für jede Regel
>
> $$\frac{m_1, \ldots, m_r}{m}$$
>
> von K gilt: Wenn $m_1, \ldots, m_r$ in K ableitbar sind und die Eigenschaft E haben (*Induktionsvoraussetzung*), so hat auch m die Eigenschaft E.

Falls $r = 0$ müssen wir also zeigen, daß m die Eigenschaft E hat (*Induktionsanfang*).

(**Induktion über den Kalkül K**)

Beweis durch Induktion über den Ausdruckskalkül (über den Aufbau der Ausdrücke):

Um nachzuweisen, daß alle aussagenlogischen Ausdrücke eine Eigenschaft E haben, reicht es, zu zeigen:

(I1): Jede Aussagenvariable hat die Eigenschaft E.

(I2): Hat der Ausdruck α die Eigenschaft E, so auch $\neg\alpha$.

(I3): Haben die Ausdrücke α und β die Eigenschaft E, so auch $(\alpha \wedge \beta)$ und $(\alpha \vee \beta)$.

E trifft auf $x \in \Sigma_a^*$ zu:

$$\text{für alle } \beta \in \text{AA: } x \text{ ist kein Anfangsstück von } \beta \\ \text{und} \quad \beta \text{ ist kein Anfangsstück von } x.$$

Wir zeigen

$$\text{für alle } \alpha \in \text{AA:} \quad E\alpha$$

durch Induktion im Ausdruckskalkül:

(I1) $\alpha = X_i$: Sei $\beta \in$ AA. α ist kein Anfangsstück von β, da jeder von X_i verschiedene Ausdruck nicht mit X_i beginnt. β ist kein Anfangsstück von α, da $|\alpha| = 1$ und $|\beta| \geq 1$ für jedes $\beta \in$ AA.

(I2) $\alpha = \neg\alpha'$ und E trifft auf α' zu: Sei $\beta \in$ AA und etwa

$$\alpha = \beta w.$$

Zu zeigen $w = \lambda$. Es gibt x mit $\beta = \neg x$. Somit β mit (A2) gewonnen, also gibt es $\gamma \in$ AA mit $\beta = \neg\gamma$. Somit $\neg\alpha' = \neg\gamma w$; daher $\alpha' = \gamma w$. Wegen $E\alpha'$: $w = \lambda$.

(I3) $\alpha = (\alpha_1 \vee \alpha_2)$ und E trifft auf α_1 und α_2 zu: Sei $\beta \in$ AA und etwa

$$\alpha = \beta w.$$

Zu zeigen $w = \lambda$. β beginnt mit (; somit existieren $\beta_1, \beta_2 \in$ AA und $\circ \in \{\wedge, \vee\}$ mit $\beta = (\beta_1 \circ \beta_2)$. Dann

$$\alpha_1 \vee \alpha_2) = \beta_1 \circ \beta_2)w$$

Wegen $E\alpha_1$: $\alpha_1 = \beta_1$ und somit $\circ = \vee$ und

$$\alpha_2) = \beta_2)w$$

Wegen $E\alpha_2$: $\alpha_2 = \beta_2$ und daher $w = \lambda$.

Bemerkung 3 *Wegen Bemerkung 2 ist es möglich,* **induktive Definitionen über den Aufbau der Ausdrücke** *durchzuführen. Um in eindeutiger Weise eine Funktion für alle Ausdrücke zu definieren, genügt es,*

(D1): jeder Aussagenvariable einen Wert zuzuordnen;

(D2): jedem Ausdruck $\neg\alpha$ einen Wert zuzuordnen unter der Annahme, daß dem Ausdruck α bereits ein Wert zugeordnet ist;

(D3): a) jedem Ausdruck $(\alpha_1 \wedge \alpha_2)$ einen Wert zuzuordnen unter der Annahme, daß den Ausdücken α_1 und α_2 bereits je ein Wert zugeordnet ist;

b) jedem Ausdruck $(\alpha_1 \vee \alpha_2)$ einen Wert zuzuordnen unter der Annahme, daß den Ausdücken α_1 und α_2 bereits je ein Wert zugeordnet ist.

Beispiele: 1) rg : AA $\to \mathbb{N}$ (rg(α) der **Rang** von α):

$$\begin{array}{rcl} \mathrm{rg}(X) & = & 0 \\ \mathrm{rg}(\neg\alpha) & = & 1 + \mathrm{rg}(\alpha) \\ \mathrm{rg}((\alpha \wedge \beta)) & = & 1 + \max\{\mathrm{rg}(\alpha), \mathrm{rg}(\beta)\} \\ \mathrm{rg}((\alpha \vee \beta)) & = & 1 + \max\{\mathrm{rg}(\alpha), \mathrm{rg}(\beta)\} \end{array}$$

2) TA : AA $\to$ Pot(AA) (TA(α) die Menge der **Teilausdrücke** oder **Subformeln** von α):

$$\begin{array}{rcl} \mathrm{TA}(X) & = & \{X\} \\ \mathrm{TA}(\neg\alpha) & = & \mathrm{TA}(\alpha) \cup \{\neg\alpha\} \\ \mathrm{TA}((\alpha \wedge \beta)) & = & \mathrm{TA}(\alpha) \cup \mathrm{TA}(\beta) \cup \{(\alpha \wedge \beta)\} \\ \mathrm{TA}((\alpha \vee \beta)) & = & \mathrm{TA}(\alpha) \cup \mathrm{TA}(\beta) \cup \{(\alpha \vee \beta)\}. \end{array}$$

Koinzidenzlemma Seien b, b' Belegungen für α, also

$$\mathsf{var}(\alpha) \subseteq \mathsf{df}(b) \cap \mathsf{df}(b'),$$

und gelte

$$\text{für alle } X \in \mathsf{var}(\alpha)\text{:} \quad b(X) = b'(X).$$

Dann

$$b(\alpha) = b'(\alpha).$$

Beweis: Zeige durch Induktion über den Aufbau der Ausdrücke β:

$$\text{wenn } \mathsf{var}(\beta) \subseteq \mathsf{df}(b) \cap \mathsf{df}(b')\text{, so } b(\beta) = b'(\beta).$$

$$n \geq 1 \qquad \mathsf{AA}_n := \{\alpha \mid \mathsf{var}(\alpha) \subseteq \{X_1, \ldots, X_n\}\}.$$

Konvention: Ist $\alpha \in \mathsf{AA}_n$ und sind $b_1, \ldots, b_n \in \{0, 1\}$, so steht

$$\alpha[b_1, \ldots, b_n]$$

für den Wert $b(\alpha)$, wobei b irgendeine Belegung ist mit

$$b(X_1) = b_1, \ldots, b(X_n) = b_n.$$

α	β	$\neg\alpha$	$(\neg\alpha \vee \beta)$
1	1	0	1
1	0	0	0
0	1	1	1
0	0	1	1

Somit gilt für jede Belegung b für $(\neg\alpha \vee \beta)$:

$$b((\neg\alpha \vee \beta)) = \dot{\rightarrow}(b(\alpha), b(\beta)).$$

Wir fassen $(\alpha \rightarrow \beta)$ als Abkürzung für $(\neg\alpha \vee \beta)$ auf.

α	β	$(\neg\alpha \vee \beta)$	$(\neg\beta \vee \alpha)$	$((\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha))$
1	1	1	1	1
1	0	0	1	0
0	1	1	0	0
0	0	1	1	1

Somit gilt für jede Belegung b für $((\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha))$:

$$b(((\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha))) = \dot{\leftrightarrow}(b(\alpha), b(\beta)).$$

Wir fassen $(\alpha \leftrightarrow \beta)$ als Abkürzung für $((\neg\alpha\vee\beta)\wedge(\neg\beta\vee\alpha))$ auf.

Definitionen (Hier sei mit Belegung stets Belegungen b mit $\mathrm{df}(b) = \mathrm{AV}$ gemeint)

1. α ist **allgemeingültig** (ist eine **Tautologie**), $\models \alpha$, gdw α gilt bei allen Belegungen.

2. α ist **erfüllbar**, Erf α, gdw es gibt eine Belegung, die α erfüllt.

3. α und β sind **logisch äquivalent** gdw $\models (\alpha \leftrightarrow \beta)$
   gdw für alle Belegungen b: $b(\alpha) = b(\beta)$.

4. Sei $\Gamma \subseteq \mathrm{AA}$ und b eine Belegung.
   $b(\Gamma) = 1$ bedeutet: $b(\alpha) = 1$ für alle $\alpha \in \Gamma$.

5. Γ ist **erfüllbar**, Erf Γ, gdw es gibt b mit $b(\Gamma) = 1$.

6. α **folgt aus** Γ, $\Gamma \models \alpha$, gdw
   für alle Belegungen b: wenn $b(\Gamma) = 1$, so $b(\alpha) = 1$.

Als er ein Kaninchen verfolgte, merkte der Hund, dass der Weg sich in drei Richtungen gabelte. Er beschnüffelte den 1. Weg und fand keine Spur. Dann beschnüffelte er den 2. Weg und fand keine Spur. Dann rannte er den 3. Weg (ohne ihn zu beschnüffeln).

X_i Das Kaninchen wählte den i-ten Weg.

Frage:

$$\{(X_1 \vee X_2 \vee X_3), \neg X_1, \neg X_2\} \models X_3?$$

X_1	X_2	X_3	$(X_1 \vee X_2 \vee X_3)$	$\neg X_1$	$\neg X_2$	X_3
1	1	1	1	0	0	1
1	1	0	1	0	0	0
1	0	1	1	0	1	1
0	1	1	1	1	0	1
1	0	0	1	0	1	0
0	1	0	1	1	0	0
0	0	1	1	1	1	1
0	0	0	0	1	1	0

α und β sind **logisch äquivalent**

gdw für alle totalen b: $b(\alpha) = b(\beta)$

gdw für alle b mit $\mathsf{var}(\alpha) \cup \mathsf{var}(\beta) \subseteq \mathsf{df}(b)$: $b(\alpha) = b(\beta)$.

$\alpha \equiv \beta$: α und β sind logisch äquivalent

Sind

$((\neg\neg\neg X \vee Y) \wedge (Z \vee \neg\neg X))$ und $((\neg X \vee Y) \wedge (Z \vee \neg\neg X))$

logisch äquivalent?

7) **Ersetzungslemma:** (Intuitiv: Ersetzt man in α einen Teilausdruck β durch einen zu β logisch äquivalenten Ausdruck, so erhält man einen zu α logisch äquivalenten Ausdruck.)

Gelte $\alpha_1 \equiv \beta_1$ und $\alpha_2 \equiv \beta_2$; dann

$\neg\alpha_1 \equiv \neg\beta_1, \quad (\alpha_1 \wedge \alpha_2) \equiv (\beta_1 \wedge \beta_2) \quad (\alpha_1 \vee \alpha_2) \equiv (\beta_1 \vee \beta_2).$

8) $(\alpha \wedge \beta) \equiv \neg(\neg\alpha \vee \neg\beta)$.

$$\mathrm{AA}(\neg, \vee) := \{\alpha \mid \text{in } \alpha \text{ kommt } \wedge \text{ nicht vor}\}.$$

9) Für $^* : \mathrm{AA} \to \mathrm{AA}(\neg, \vee)$ und jedes $\alpha \in \mathrm{AA}$ gilt

$$\alpha \equiv \alpha^* \quad \text{und} \quad \mathrm{var}(\alpha) = \mathrm{var}(\alpha^*).$$

* ist induktiv definiert:

$$\begin{array}{lcl} X & := & X \\ \neg\alpha\ ^* & := & \neg\ \alpha^* \\ (\alpha \wedge \beta)^* & := & \neg(\neg\alpha^* \vee \neg\beta^*) \\ (\alpha \vee \beta)^* & := & (\alpha^* \vee \beta^*). \end{array}$$

Kann man aus

$$(X \wedge Y) \equiv \neg(\neg X \vee \neg Y)$$

schließen, dass

$$(\alpha \wedge \beta) \equiv \neg(\neg\alpha \vee \neg\beta)$$

für alle $\alpha, \beta \in$ AA?

Substitutionslemma (intuitiv) Ersetzt man in einer Äquivalenz überall $Y_1, \ldots, Y_n$ durch Ausdrücke $\gamma_1, \ldots, \gamma_n$, so bleibt die Äquivalenz erhalten.

$Y_1, \ldots, Y_n$ paarweise verschieden und $\gamma_1, \ldots, \gamma_n \in$ AA:

$\alpha \in$ AA definieren wir durch Induktion über $\alpha \in$ AA:

$$\alpha\frac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n}$$

- $X\dfrac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n} := \begin{cases} \gamma_i & \text{falls } X = Y_i \text{ und } i \in \{1, \ldots, n\} \\ X & \text{sonst} \end{cases}$

- $\neg\alpha\ \dfrac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n} := \neg\ \alpha\dfrac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n}$

- für $\circ \in \{\wedge, \vee\}$: $(\alpha\circ\beta)\dfrac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n} := (\alpha\dfrac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n} \circ \beta\dfrac{\gamma_1 \cdots \gamma_n}{Y_1 \ldots Y_n})$

Substitutionslemma. Wenn $\alpha \equiv \beta$, so

$$\alpha\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n} \equiv \beta\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n}.$$

Beweis: Für eine totale Belegung b sei b_{sub} die Belegung

$$b_{\text{sub}}(X) := \begin{cases} b(\gamma_i) & \text{falls } X = Y_i \text{ und } i \in \{1, \ldots, n\} \\ b(X) & \text{sonst} \end{cases}$$

Wir zeigen:

$$\text{für alle } \delta \in \text{AA}: \quad b(\delta\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n}) = b_{\text{sub}}(\delta). \tag{1}$$

Aus (1) ergibt sich das Substitutionslemma: Für totales b gilt nämlich:

$$b(\alpha\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n}) \overset{(1)}{=} b_{\text{sub}}(\alpha) \overset{\alpha\equiv\beta}{=} b_{\text{sub}}(\beta)) \overset{(1)}{=} b(\beta\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n}).$$

Der Nachweis von (1) erfolgt durch Induktion über γ:

Basisregel: $\delta = Y_i$ mit $1 \leq i \leq n$: Dann $Y_i\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n} = \gamma_i$ und $b_{\text{sub}}(Y_i) = b(\gamma_i)$; daher

$$b(Y_i\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n}) = b(\gamma_i) = b_{\text{sub}}(Y_i).$$

Ist $\delta = X$ und $X \notin \{Y_1, \ldots, Y_n\}$, dann

$$b(X\frac{\gamma_1 \ldots \gamma_n}{Y_1 \ldots Y_n}) = b(X) = b_{\text{sub}}(X).$$

Seien $n \geq 1$, $\alpha \in \mathsf{AA}_n$.

$$h_\alpha : \{1,0\}^n \to \{1,0\}$$

die **durch α definierte n-stellige Wahrheitswertfunktion** ist gegeben durch:

für alle $b_1, \ldots, b_n \in \{1,0\}$

$$h_\alpha(b_1, \ldots, b_n) := \alpha[b_1, \ldots, b_n]$$

Beispiele: $h_{(X_1 \wedge X_2)} = \dot{\wedge}$, $\quad h_{(X_1 \vee X_2)} = \dot{\vee}$, $\quad h_{(\neg X_1 \vee X_2)} = \dot{\to}$, $h_{\neg X_1} = \dot{\neg}$.

Bemerkung: Für $\alpha, \beta \in \mathsf{AA}_n$:

α und β sind logisch äquivalent gdw $h_\alpha = h_\beta$

Satz: $n \geq 1$. Zu jedem $h : \{1,0\}^n \to \{1,0\}$ gibt es ein $\alpha \in \mathsf{AA}_n$ mit

$$h_\alpha = h.$$

α kann in KNF oder in DNF gewählt werden.

Folgerung 1. Jeder Ausdruck ist zu einem Ausdruck in KNF und zu einem Ausdruck in DNF logisch äquivalent.

Definition: Ausdrücke der Gestalt

$$(\lambda_1 \wedge \ldots \wedge \lambda_n) \quad \text{mit } \lambda_i \in \{X_i, \neg X_i\} \text{ für } i = 1, \ldots, n$$

sind n-**Atome**.

Folgerung 2. Jedes erfüllbare $\alpha \in \mathrm{AA}_n$ ist zu einer Disjunktion von n-Atomen logisch äquivalent.

Folgerung 3. Für $n \geq 1$ gibt es genau $2^{(2^n)}$ paarweise nicht logisch äquivalente Ausdrücke in AA_n.

Beispiele: 1) $\{\dot\neg, \dot\vee\}$ und damit $\{\dot\neg, \dot\wedge, \dot\vee\}$ sind funktional vollständig.

2) $\{\dot|\}$ mit

		$\dot\vert$
1	1	0
1	0	1
0	1	1
0	0	1

ist funktional vollständig.

AA(|): $\qquad \dfrac{}{X} \qquad \dfrac{\alpha, \beta}{(\alpha \mid \beta)}$

Bei n Aussagenvariablen hat Wahrheitstafel 2^n Zeilen. Verfahren mit Wahrheitstafeln sehr ineffizient, da

Variable	Zeilen		
10	1.024	$\approx$	10^3
20	1.048.576	$\approx$	10^6
40	1.099.511.627.776	$\approx$	10^{12}
60	1.152.921.504.606.846.976	$\approx$	10^{18}

Bemerkung. Seien $Y_1, \ldots, Y_n, Z_1, \ldots, Z_n$ paarweise verschiedene Variable. Jede zu

$$((Y_1 \leftrightarrow Z_1) \wedge (Y_2 \leftrightarrow Z_2) \wedge \ldots \wedge (Y_n \leftrightarrow Z_n))$$

logisch äquivalente Formel in DNF ist eine Disjunktion von mindestens 2^n iterierten Konjunktionen ist.

Definition. Ein Ausdruck ist in **Negationsnormalform**, **NNF**, wenn in ihm Negationszeichen höchstens unmittelbar vor Variablen auftreten.

Bemerkung. Für die folgende induktiv definierte Abbildung * : AA $\to$ AA gilt:

1. für $\alpha \in$ AA: $\alpha \equiv \alpha^*$ und α^* in NNF.

2. * ist in polynomieller Zeit berechenbar.

$X^* := X$

$$\neg\alpha\ ^* := \begin{cases} \neg Y & \text{wenn } \alpha = Y \\ \beta^* & \text{wenn } \alpha = \neg\beta \\ (\neg\beta\ ^* \vee \neg\gamma\ ^*) & \text{wenn } \alpha = (\beta \wedge \gamma) \\ (\neg\beta\ ^* \wedge \neg\gamma\ ^*) & \text{wenn } \alpha = (\beta \vee \gamma) \end{cases}$$

$(\beta \wedge \gamma)^* := (\beta^* \wedge \gamma^*)$

$(\beta \vee \gamma)^* := (\beta^* \vee \gamma^*)$.

$$\begin{aligned}
\beta_S &:= (X \wedge Y \wedge U) \vee \\
&\quad\; (X \wedge \neg Y \wedge \neg U) \vee (\neg X \wedge Y \wedge \neg U) \vee (\neg X \wedge \neg Y \wedge U) \\
\beta_N &:= (X \wedge Y) \vee (X \wedge U) \vee (Y \wedge U).
\end{aligned}$$

		$\dot{\oplus}$
1	1	0
1	0	1
0	1	1
0	0	0

$(\alpha \oplus \beta)$ Abkürzung für $((\alpha \wedge \neg\beta) \vee (\neg\alpha \wedge \beta))$

Beschreibung der Schaltung:

$$\begin{aligned}
\alpha_S &:= ((X \oplus Y) \oplus U) \\
\alpha_N &:= ((U \wedge (X \oplus Y)) \vee (X \wedge Y))
\end{aligned}$$

Verifikationsproblem:

Gilt $\alpha_S \equiv \beta_S$ und $\alpha_N \equiv \beta_N$?

Schaltelement S:

Eingangsvariable: X_1, X_2; Ausgangsvariable: Y_1, Y_2;

Beschreibung des Verhaltens:

$$(Y_1 \leftrightarrow \neg(X_1 \wedge X_2)) \qquad (Y_2 \leftrightarrow (X_1 \wedge X_2))$$

Schaltelement K: Variable für Eingänge und Ausgänge von K:

$$X_1, X_2, \qquad Y_1, Y_2, Y_3, Y_4.$$

Variable für Eingänge und Ausgänge jedes Schaltelements:

$$X_1^u, X_2^u, Y_1^u, Y_2^u,\ \ X_1^m, X_2^m, Y_1^m, Y_2^m,\ \ X_1^o, X_2^o, Y_1^o, Y_2^o$$

Formelmenge Γ, die Verhalten beschreibt:

$$\begin{array}{rl}
(Y_1^u \leftrightarrow \neg(X_1^u \wedge X_2^u)) & (Y_2^u \leftrightarrow (X_1^u \wedge X_2^u)) \\
(Y_1^m \leftrightarrow \neg(X_1^m \wedge X_2^m)) & (Y_2^m \leftrightarrow (X_1^m \wedge X_2^m)) \\
(Y_1^o \leftrightarrow \neg(X_1^o \wedge X_2^o)) & (Y_2^o \leftrightarrow (X_1^o \wedge X_2^o)) \\
(X_1^u \leftrightarrow X_1), (X_2^u \leftrightarrow X_2) & (X_1^m \leftrightarrow X_1), (X_2^m \leftrightarrow Y_1^u) \\
(X_1^o \leftrightarrow X_2), (X_2^o \leftrightarrow Y_1^m) & \\
(Y_1 \leftrightarrow Y_1^o), (Y_2 \leftrightarrow Y_2^o) & (Y_3 \leftrightarrow Y_2^m), (Y_4 \leftrightarrow Y_2^u).
\end{array}$$

Für $\alpha \in$ AA$(\neg, \leftrightarrow)$ und $X \in$ AV sei:

$$
\begin{array}{rcl}
\neg_\alpha \in \{0,1\} & := & \text{Anzahl der Vorkommen von } \neg \text{ in } \alpha \text{ mod } 2\\
\leftrightarrow_\alpha \in \{0,1\} & := & \text{Anzahl der Vorkommen von } \leftrightarrow \text{ in } \alpha \text{ mod } 2\\
j_\alpha \in \{0,1\} & := & \text{Anz. der Vorkom. von Junkt. in } \alpha \text{ mod } 2\\
X_\alpha \in \{0,1\} & := & \text{Anzahl der Vorkommen von } X \text{ in } \alpha \text{ mod } 2\\
U(\alpha) & := & \{Y \in \text{AV} \mid Y_\alpha = 1\}
\end{array}
$$

Lemma 1. Für $\alpha \in$ AA$(\neg, \leftrightarrow)$ und jede totale Beleg. b:

$$(*) \qquad b(\alpha) = j_\alpha + \sum_{X \in U(\alpha)} b(X) \mod 2.$$

Folgerung 1. Für $\alpha, \beta \in$ AA$(\neg, \leftrightarrow)$ mit var$(\alpha)\cup$var$(\beta) \subseteq \{X_1, \ldots, X_n\}$ gilt:

1. Wenn $U(\alpha) \neq \emptyset$, so wird α von genau der Hälfte der Tupel in $\{0,1\}^n$ erfüllt.
2. Wenn nicht $\alpha \equiv \beta$, so gibt es genau 2^{n-1} Tupel $(b_1, \ldots, b_n)$ in $\{0,1\}^n$ mit: $\alpha[b_1, \ldots, b_n] \neq \beta[b_1, \ldots, b_n]$.
3. Wenn $U(\alpha) = \emptyset$, so ist

   α allgemeingültig oder nicht erfüllbar.

Beweis von 1: Wähle i mit $1 \leq i \leq n$ und $X_i \in U(\alpha)$. Dann

$$\alpha[b_1, \ldots, b_i, \ldots, b_n] = 1 \iff \alpha[b_1, \ldots, 1 - b_i, \ldots, b_n] = 0.$$

Folgerung 2. $\neg, \leftrightarrow$ ist nicht funktional vollständig.

Beweis: Es gibt kein α mit $h_\alpha = \dot{\rightarrow}$ wegen Folgerung 1.

$$b(\alpha) \;=\; j_\alpha + \sum_{X\in U(\alpha)} b(X) \mod 2$$

Beweis: Induktion über α: (alle Gleichungen sind mod 2 zu lesen)

$\alpha = X$: $b(X) = 0 + b(X)$;

$\alpha = \neg\beta$:

$$b(\neg\beta) = 1 + b(\beta) \stackrel{\text{I.V.}}{=} \underbrace{1 + j_\beta}_{=j_\alpha} + \sum_{X\in \underbrace{U(\beta)}_{=U(\alpha)}} b(X)$$

$\alpha = (\beta \leftrightarrow \gamma)$: Beachte $U((\beta \leftrightarrow \gamma)) = U(\beta) \triangle U(\gamma)$. Es gilt:

$$\begin{aligned}
b(\alpha) &= 1 + b(\beta) + b(\gamma) \qquad \text{(vgl. Def. von } \dot{\leftrightarrow}\text{)} \\
&\stackrel{\text{I.V.}}{=} 1 + j_\beta + j_\gamma + \sum_{X\in U(\beta)} b(X) + \sum_{X\in U(\gamma)} b(X) \\
&= j_\alpha + 2 \cdot \sum_{X\in U(\beta)\cap U(\gamma)} b(X) + \sum_{X\in U(\beta)\triangle U(\gamma)} b(X) \\
&= j_\alpha + 0 + \sum_{X\in U((\beta\leftrightarrow\gamma))} b(X).
\end{aligned}$$

Sei $n \geq 2$

$$\Gamma_n := \{\alpha \in \mathsf{AA}(\neg, \leftrightarrow) \mid \mathsf{var}(\alpha) \subseteq X_1, \ldots, X_{n-1}\}\}.$$

Lemma 2. Für $\alpha \in \Gamma_n$

$$\leftrightarrow_\alpha = 1 \iff X_{1\alpha} + X_{2\alpha} + \cdots + X_{n-1\alpha} = 0 \quad \text{mod } 2.$$

Beweis: Induktion über α (leicht).

Für $\alpha \in \Gamma_n$ sei

$$w(\alpha) := (X_{1\alpha}, X_{2\alpha}, \ldots, X_{n-1\alpha}, \neg_\alpha).$$

Lemma 3. Für $\alpha, \beta \in \Gamma_n$

$$w(\alpha) = (0, \ldots, 0) \iff \alpha \text{ ist allgemeingültig}$$

und damit für $\alpha, \beta \in \Gamma_n$

$$w(\alpha) = w(\beta) \iff \alpha \equiv \beta.$$

Beweis: Nach Folgerung 1: Wenn α allgemeingültig, so:

$$w(\alpha) = (0, \ldots, 0, 0) \quad \text{oder} \quad w(\alpha) = (0, \ldots, 0, 1)$$

Dann wegen Lemma 2 $\leftrightarrow_\alpha = 1$ und somit

$$\begin{aligned} \alpha \text{ allgemeingültig} \quad & \overset{\text{Lemma 1}}{\iff} \quad j_\alpha = \neg_\alpha + \leftrightarrow_\alpha = 1 \\ & \iff \quad \neg_\alpha = 0. \end{aligned}$$

Lemma 4. Zu jedem $x = (x_1, \ldots, x_n) \in \{0, 1\}^n$ gibt es ein $\alpha_x \in \Gamma_n$ mit $w(\alpha_x) = (x_1, \ldots, x_n)$.

$G = (V, E)$ ist ℓ-**färbbar** gdw ex. $V_1, \ldots, V_\ell$ mit

- $V = V_1 \dot\cup \ldots \dot\cup V_\ell$ "$V_1, \ldots, V_\ell$ bilden eine **Partition** von V".
- wenn $\{a, b\} \in E$, so liegen a und b in verschiedenen V_is.

Beachte: Wir können $V = V_1 \dot\cup \ldots \dot\cup V_\ell$ durch

$$V = V_1 \cup \ldots \cup V_\ell$$

ersetzen.

$G = (V, E)$ Graph, $W \subseteq V$. Der **von G auf W induzierte Subgraph** ist der Graph

$$(W, E') \quad \text{mit } E' = E \cap [W]^2.$$

Wir bezeichnen ihn mit: $[W]^G$.

$G = (V, E)$ Graph, $W \subseteq V$.

$$\begin{aligned} \Gamma(W) \quad := \quad & \{(X_{a,1} \vee \ldots \vee X_{a,\ell}) \mid a \in W\} \cup \\ & \{(\neg X_{a,i} \vee \neg X_{b,i}) \mid \{a, b\} \in E \cap [W]^2,\, i \in \{1, \ldots, \ell\}\} \end{aligned}$$

Bemerkung. Erf $\Gamma(W)$ gdw $[W]^G$ ist ℓ-färbbbar.

Insbesondere: Erf $\Gamma(V)$ gdw G ist ℓ-färbbbar.

Satz. Ist jeder durch eine endliche Teilmenge von V induzierter Subgraph von $G = (V E)$ ℓ-färbbbar, so ist auch G ℓ-färbbbar.

$G = (V, E)$ Graph. $D \subseteq V$ ist eine **dominierende Menge** (in G) gdw

zu jedem $b \notin D$ gibt es ein $a \in D$ mit $\{a, b\} \in E$.

Seien $\alpha \in$ AA und $k \in \mathbb{N}$. α ist k-**erfüllbar** gdw es gibt eine Belebung b für α mit:

$$b(\alpha) = 1 \text{ und } |\{X \mid X \in \mathsf{var}(\alpha) \text{ und } b(X) = 1\}| = k.$$

Sei $G = (V, E)$ ein endlicher Graph. Wir setzen:

$$\alpha := \bigwedge_{b \in V} \bigvee_{\substack{a \in V, \\ a=b \text{ oder } \{a,b\} \in E}} X_a$$

Lemma. Sei b eine Belebung für α und

$$D := \{a \mid b(X_a) = 1\}.$$

Dann: D ist dominierende Menge gdw $b(\alpha) = 1$.

Somit für $k \in \mathbb{N}$:

G hat domi. Menge der Größe $k \iff \alpha$ ist k-erfüllbar.

$G = (V, E)$ Graph und $W \subseteq V$.

W ist **unabhängig** (in G) gdw für alle $a, b \in W$: $\{a, b\} \notin E$.

I(ndependent) S(et) ist das folgende Problem:

IS	
Eingabe:	Graph $G = (V, E)$ und $k \in \mathbb{N}$.
Problem:	Gibt es in G unabhängige Menge der Größe k.

Satz. IS ist NP-vollständig.

Beweis: IS $\in$ NP: Errate Teilmenge und verifiziere.

IS ist NP-hart: Wir zeigen

$$\text{3-SAT} \leq_{\text{poly}} \text{IS}.$$

Sei α in 3-KNF. O.B.d.A. bestehe jede Disjunktion aus genau 3 Literalen, die wiederum verschiedene Aussagenvariable enthalten:

Ersetze $(\neg X \vee Y)$ durch $(\neg X \vee Y \vee Z) \wedge (\neg X \vee Y \vee \neg Z)$

Streiche $(\neg X \vee Y \vee \neg Y)$.

Sei

$$\alpha = (\beta_1 \wedge \ldots \wedge \beta_s)$$

und seien die Variablen in α

$$Y_1, \ldots, Y_\ell.$$

Etwa

$$\alpha = (X \vee \neg Y \vee Z) \wedge (\neg X \vee U \vee \neg Z) \wedge (Y \vee \neg Z \vee U).$$

$\alpha = (\beta_1 \wedge \ldots \wedge \beta_s)$ Variable: $Y_1, \ldots, Y_\ell$.

$$\alpha = (X \vee \neg Y \vee Z) \wedge (\neg X \vee U \vee \neg Z) \wedge (Y \vee \neg Z \vee U).$$

Graph $G = (V, E)$:

(K1) Für $j = 1, \ldots, \ell$ enthält G:
$$\begin{tikzcd} Y_j \arrow[d, dash] \\ \neg Y_j \end{tikzcd}$$

(K2) Für $i = 1, \ldots, s$ sei $\beta_i = (\lambda_{i,1} \vee \lambda_{i,2} \vee \lambda_{i,3})$. G enthält:

$$\begin{tikzcd} & (i, \lambda_{i,1}) \arrow[dl, dash] \arrow[dr, dash] & \\ (i, \lambda_{i,2}) \arrow[rr, dash] & & (i, \lambda_{i,3}) \end{tikzcd}$$

(K3) Für $i = 1, \ldots, s$ und $j = 1, 2, 3$:
- wenn $\lambda_{i,j} = X$, so verbinde $(i, \lambda_{i,j})$ mit $\neg X$;
- wenn $\lambda_{i,j} = \neg X$, so verbinde $(i, \lambda_{i,j})$ mit X.

Dann gilt

1. Jede unabhängige Menge in G enthält höchstens $\ell + s$ Punkte (höchstens einen Punkt aus $\{Y_j, \neg Y_j\}$ wegen (K1) und einen Punkt aus $\{\lambda_{i,1}, \lambda_{i,2}, \lambda_{i,3}\}$ wegen (K2)).

2. Sei $M_0 = \{\lambda_1, \ldots, \lambda_\ell\}$ mit $\lambda_j \in \{Y_j, \neg Y_j\}$ für $j = 1, \ldots, \ell$ und b^{M_0} die Belegung mit $b^{M_0}(\lambda_j) = 1$ für $j = 1, \ldots, \ell$. Dann
$$b^{M_0}(\alpha) = 1 \iff \text{es gibt } M \subseteq V \text{ mit } M_0 \subseteq M, \; |M| = \ell + s \text{ und } M \text{ ist unabhängig.}$$

Beweisidee: Sei

$$\alpha = (\underbrace{\underbrace{\neg X}_{\beta_1} \vee Y)}_{\beta_2} \vee \underbrace{(\underbrace{(X \wedge U)}_{\beta_3} \vee Z)}_{\beta_4}$$

1. Schritt: Führe für jede nichtatomare Subformel β eine neue Variable X_β ein.

Für

$$\begin{array}{rll} \alpha' = & (X_{\beta_1} \leftrightarrow \neg X) \wedge & (\text{da } \beta_1 = \neg X) \\ & (X_{\beta_2} \leftrightarrow (X_{\beta_1} \vee Y)) \wedge & (\text{da } \beta_2 = (\beta_1 \vee Y)) \\ & (X_{\beta_3} \leftrightarrow (X \wedge U)) \wedge & (\text{da } \beta_3 = (X \wedge U)) \\ & (X_{\beta_4} \leftrightarrow (X_{\beta_3} \vee Z)) \wedge & (\text{da } \beta_4 = (\beta_3 \vee Z)) \\ & (X_\alpha \leftrightarrow (X_{\beta_2} \vee X_{\beta_4})) \wedge & (\text{da } \alpha = (\beta_2 \vee \beta_4)) \\ & X_\alpha & \end{array}$$

Dann

$$\text{Erf } \alpha \text{ gdw Erf } \alpha'.$$

2. Schritt: α' ist Konjunktionen von Formeln mit höchstens drei Variablen. Man wandle diese in KNF um und erhält damit α^*.

$$\begin{array}{rl} \alpha^* := & (X_{\beta_1} \vee X) \wedge (\neg X_{\beta_1} \vee \neg X) \wedge \\ & (X_{\beta_2} \vee \neg X_{\beta_1}) \wedge (X_{\beta_2} \vee \neg Y) \wedge (\neg X_{\beta_2} \vee X_{\beta_1} \vee Y) \wedge \\ & (X_{\beta_3} \vee \neg X \vee \neg U) \wedge (\neg X_{\beta_3} \vee X) \wedge (\neg X_{\beta_3} \vee U) \wedge \\ & (X_{\beta_4} \vee \neg X_{\beta_3}) \wedge (X_{\beta_4} \vee \neg Z) \wedge (\neg X_{\beta_4} \vee X_{\beta_3} \vee Z) \wedge \\ & (X_\alpha \vee \neg X_{\beta_2}) \wedge (X_\alpha \vee \neg X_{\beta_4}) \wedge (\neg X_\alpha \vee X_{\beta_2} \vee X_{\beta_4}) \wedge \\ & X_\alpha. \end{array}$$

$$\alpha_0 = (\neg X \vee Y \vee Z) \wedge \neg U \wedge (U \vee \neg Y) \wedge (X \vee Z) \wedge \neg Z$$

$\mathfrak{K}_{\alpha_0} := \{K_{\alpha_1}, K_{\alpha_2}, K_{\alpha_3}, K_{\alpha_4}, K_{\alpha_5}\}$ mit $K_{\alpha_1} = \{\neg X, , Y, Z\}, \ldots$

Definition.

1. Eine **Klausel** ist eine endliche Menge von Literalen.

2. b Belegung, K Klausel

   b **erfüllt** K, $b(K) = 1 \iff$ ex. $\lambda \in K : \; b(\lambda) = 1$.

   ACHTUNG!

   $K = \emptyset$ (K "leere Disjunktion"): K nicht erfüllbar.

3. Sei $\mathfrak{K}$ eine Menge von Klauseln, b Belegung

   b **erfüllt** $\mathfrak{K}$, $b(\mathfrak{K}) = 1 \iff$ für alle $K \in \mathfrak{K} : \; b(K) = 1$.

   ACHTUNG: $b(\emptyset) =?$; $\emptyset$ Klausel oder Klauselmenge?

4. $\mathfrak{K}$ Klauselmenge

   $\mathfrak{K}$ **erfüllbar**, $\mathbf{Erf}\ \mathfrak{K} \iff$ ex. b mit $b(\mathfrak{K}) = 1$.

var($\mathfrak{K}$), var(K): Variablen in Literalen von $\mathfrak{K}$ bzw. K.

Sei λ ein Literal. Dann sei $\bar{\lambda}$ gegeben durch:

$$\bar{\lambda} := \begin{cases} \neg X & \text{falls } \lambda = X \\ X & \text{falls } \lambda = \neg X \end{cases}$$

Resolutionsregel: Seien K und L Klauseln und λ ein Literal.

$$\text{(R)} \qquad \frac{K \dot{\cup} \{\lambda\},\ L \dot{\cup} \{\bar{\lambda}\}}{K \cup L}$$

“$K \cup L$ entsteht aus $K \cup \{\lambda\}$ und $L \cup \{\bar{\lambda}\}$ durch Resolution entlang λ”

“$K \cup L$ ist eine **Resolvente** von $K \cup \{\lambda\}$ und $L \cup \{\bar{\lambda}\}$”

Resolutionslemma. Jede Belegung erfüllt mit zwei Klauseln auch jede ihrer Resolventen, d.h.: Seien b eine Belegung, K, L Klauseln und λ ein Literal:

> Wenn $b(K \cup \{\lambda\}) = 1$ und $b(L \cup \{\bar{\lambda}\}) = 1$, so $b(K \cup L) = 1$.

Beweis. Wir wissen: $b(\lambda) = 1$ oder $b(\lambda) = 0$.

Wenn $b(\lambda) = 1$, so $b(L) = 1$, somit $b(K \cup L) = 1$.

Wenn $b(\lambda) = 0$, so $b(K) = 1$, somit $b(K \cup L) = 1$.

Definition. $\mathfrak{K}$ Menge von Klauseln.

Ein Resolutionsbeweis einer Klausel L aus $\mathfrak{K}$ ist ein Tupel $(K_1, \ldots, K_m)$ von Klauseln, so dass $K_m = L$ und für $i = 1, \ldots, m$ gilt

> $K_i \in \mathfrak{K}$ oder
> es gibt $j, k \in \{1, \ldots, i-1\}$, so dass K_i Resolvente von K_j und K_k ist.

Eine Klausel L ist resolutionsbeweisbar aus $\mathfrak{K}$, $\mathfrak{K} \vdash_{\mathrm{R}} L$, gdw es gibt einen Resolutionsbeweis von L aus $\mathfrak{K}$.

Beachte: $\mathfrak{K} \vdash_{\mathrm{R}} L$ gdw L kann man durch endlichmalige Anwendung der folgenden Regeln gewinnen:

$$\frac{}{K} \text{ mit } K \in \mathfrak{K} \qquad \text{(R)}$$

Bemerkung 1.

1. Wenn $\mathfrak{K} \vdash_{\mathrm{R}} L$ und b erfüllt $\mathfrak{K}$, so $b(L) = 1$ (wegen Resolutionslemma).
2. Wenn $\mathfrak{K} \vdash_{\mathrm{R}} \emptyset$, so nicht Erf $\mathfrak{K}$ (wegen 1).

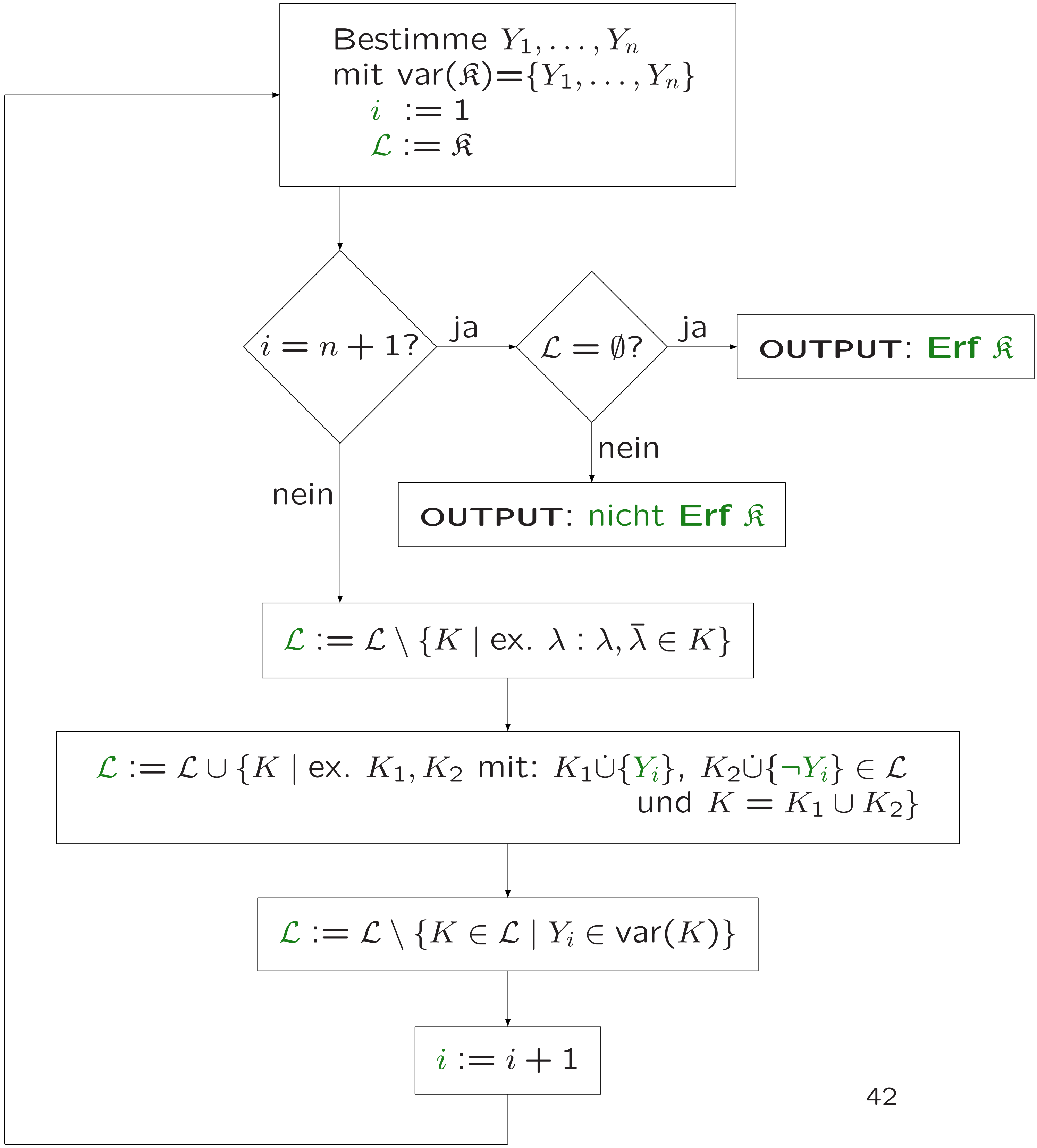
Resolutionssatz. Sei $\mathfrak{K}$ eine Menge von Klauseln. Dann:

$$\text{Erf } \mathfrak{K} \quad \text{gdw} \quad \text{nicht } \mathfrak{K} \vdash_{\mathrm{R}} \emptyset$$

d.h.:

$$\text{nicht Erf } \mathfrak{K} \quad \text{gdw} \quad \mathfrak{K} \vdash_{\mathrm{R}} \emptyset.$$

$\mathrm{DPP}(\mathfrak{K})$ $\quad$ $\mathfrak{K}$ endliche Klauselmenge



Satz. Sei $\mathfrak{K}$ eine endliche Klauselmenge. DPP($\mathfrak{K}$), d.h. DPP bei Eingabe $\mathfrak{K}$, liefert die richtige Antwort auf die Frage “Ist $\mathfrak{K}$ erfüllbar?”

Beweis: Sei var($\mathfrak{K}$) $= \{Y_1, \ldots, Y_n\}$. Für $i = 1, \ldots, n+1$ sei $\mathfrak{L}_i$ der Wert von $\mathfrak{L}$ zu Beginn des i-ten Schleifendurchlaufs.

1. $\mathfrak{L}_1 = \mathfrak{K}$.

2. Für $i = 1, \ldots, n+1$:
$$\text{var}(\mathfrak{L}_i) \subseteq \{Y_i, \ldots, Y_n\};$$
somit
$$\mathfrak{L}_{n+1} = \{\emptyset\} \quad \text{oder} \quad \mathfrak{L}_{n+1} = \emptyset.$$

3. Für $i = 1, \ldots, n+1$:
$$\mathfrak{L}_i \subseteq \{L \mid \mathfrak{K} \vdash_{\mathsf{R}} L\}.$$

4. $$\text{nicht Erf } \mathfrak{K} \text{ gdw } \mathfrak{L}_{n+1} = \{\emptyset\}$$
und somit
$$\text{Erf } \mathfrak{K} \text{ gdw } \mathfrak{L}_{n+1} = \emptyset$$
d.h. DPP($\mathfrak{K}$) liefert die richtige Antwort.

Beispiel. $\mathfrak{K}$: $\{X, Y\}$, $\{\neg X\}$, $\{\neg X, \neg Y\}$

$n = 2$, $\quad X, Y$

(A1) $\{X, Y\}$, $\{\neg X\}$, $\{\neg X, \neg Y\}$

(B1) $\{X, Y\}$, $\{\neg X\}$, $\{\neg X, \neg Y\}$, $\{Y\}$, $\{Y, \neg Y\}$

(C1) $\{Y\}$, $\{Y, \neg Y\}$

(A2) $\{Y\}$

(B2) $\{Y\}$

(C2)

Somit: $\mathfrak{L}_3 = \emptyset$, d.h.: Erf $\mathfrak{K}$.

Beispiel. $\mathfrak{K}$: $\{\neg X, Y\}$, $\{\neg Y, \neg Z, U\}$, $\{X\}$, $\{Z\}$, $\{\neg U, \neg Z\}$

$n = 4$, $\quad X, Y, Z, U$

(A1) $\{\neg X, Y\}$, $\{\neg Y, \neg Z, U\}$, $\{X\}$, $\{Z\}$, $\{\neg U, \neg Z\}$

(B1) $\{\neg X, Y\}$, $\{\neg Y, \neg Z, U\}$, $\{X\}$, $\{Z\}$, $\{\neg U, \neg Z\}$, $\{Y\}$

(C1) $\{\neg Y, \neg Z, U\}$, $\{Z\}$, $\{\neg U, \neg Z\}$, $\{Y\}$

(A2) $\{\neg Y, \neg Z, U\}$, $\{Z\}$, $\{\neg U, \neg Z\}$, $\{Y\}$

(B2) $\{\neg Y, \neg Z, U\}$, $\{Z\}$, $\{\neg U, \neg Z\}$, $\{Y\}$, $\{\neg Z, U\}$

(C2) $\{Z\}$, $\{\neg U, \neg Z\}$, $\{\neg Z, U\}$

(A3) $\{Z\}$, $\{\neg U, \neg Z\}$, $\{\neg Z, U\}$

(B3) $\{Z\}$, $\{\neg U, \neg Z\}$, $\{\neg Z, U\}$, $\{\neg U\}$, $\{U\}$

(C3) $\{\neg U\}$, $\{U\}$

(A4) $\{\neg U\}$, $\{U\}$

(B4) $\{\neg U\}$, $\{U\}$, $\emptyset$

(C4) $\emptyset$. Somit nicht Erf $\mathfrak{K}$.

Schubfachprinzip: Werden $n+1$ Objekte auf n Schubfächer verteilt, so enthält mindestens ein Schubfach mindestens zwei Objekte.

Für $i = 1, \ldots, n+1$ und $s = 1, \ldots, n$ Variable

$$X_{i,s} \qquad \text{“}i\text{-tes Objekt im }s\text{-ten Schubfach”}$$

$\mathfrak{K}_n$:

$$\{X_{i,1}, \ldots, X_{i,n}\} \text{ für } 1 \leq i \leq n+1$$

$$\{\neg X_{i,s}, \neg X_{j,s}\} \text{ für } 1 \leq i < j \leq n+1, \quad 1 \leq s \leq n.$$

Nach Schubfachprinzip:

$$\text{nicht Erf } \mathfrak{K}_n \text{ und somit } \mathfrak{K}_n \vdash_{\mathrm{R}} \emptyset.$$

Satz. Es gibt ein $c > 0$, so dass jeder Resolutionsbeweis von $\emptyset$ aus $\mathfrak{K}_n$ eine Länge $\geq 2^{c \cdot n}$ besitzt.

Eine Hornklausel ist eine Klausel, die höchestens ein positives Literal enthält.

Einheitsresolutionsregel: Sei K eine Klausel und X eine Variable.

$$\text{(ER)} \qquad \frac{K \mathbin{\dot\cup} \{\neg X\},\ \{X\}}{K}$$

Ein Einheitsresolutionsbeweis einer Klausel L aus $\mathfrak{K}$ ist ein Tupel $(K_1, \ldots, K_m)$ von Klauseln, so dass $K_m = L$ und für $i = 1, \ldots, m$ gilt

$K_i \in \mathfrak{K}$ oder
es gibt $j, k \in \{1, \ldots, i-1\}$, so dass K_i aus K_j und K_k durch (ER) entsteht.

$\mathfrak{K} \vdash_{\mathsf{ER}} L$ gdw es gibt einen Einheitsresolutionsbeweis von L aus $\mathfrak{K}$.

$$((\neg X \vee \neg Y \vee \neg Z) \wedge \neg U \wedge (V \to X) \wedge V \wedge Y \wedge (W \to Z) \wedge W)$$

$$((\neg X \vee \neg Y \vee \neg Z) \wedge \neg U \wedge (V \to X) \wedge V \wedge Y \wedge (W \to Z) \wedge W)$$

$$((\neg X \vee \neg Y \vee \neg Z) \wedge \neg U \wedge (V \to X) \wedge V \wedge Y \wedge (W \to Z) \wedge W)$$

$$((\neg X \vee \neg Y \vee \neg Z) \wedge \neg U \wedge (V \to X) \wedge V \wedge Y \wedge (W \to Z) \wedge W)$$

$$((\neg X \vee \neg Y \vee \neg Z) \wedge \neg U \wedge (V \to X) \wedge V \wedge Y \wedge (W \to Z) \wedge W)$$

Unterstreichungsalgorithmus: Eingabe: Hornausdruck α

(U1) Man unterstreiche in α alle Vorkommen einer Variable, die selber Konjunktionsglied von α ist.

(U2) Sind in einem Konjunktionsglied $((Y_1 \wedge \ldots \wedge Y_r) \to Y)$ von α die Variablen $Y_1, \ldots, Y_r$ bereits unterstrichen, so unterstreiche alle Vorkommen von Y in α.

Bemerkung. α is erfüllbar gdw in keinem Konjunktionsglied $(\neg Y_1 \vee \ldots \vee \neg Y_s)$ sind "am Ende" alle Variable unterstrichen. Dann ist b mit

$$b(Y) := \begin{cases} 1 & \text{wenn } Y \text{ unterstrichen} \\ 0 & \text{sonst} \end{cases}$$

eine α erfüllende Belegung.

Vor.: (1) $(X_A \to X_B)$

(2) $(\neg X_B \vee \neg X_C)$

Beh.: (3) $(\neg X_A \vee \neg X_C)$

Zunächst Ziel:

$$\{(X_A \to X_B), (\neg X_B \vee \neg X_C)\} \models (\neg X_A \vee \neg X_C)$$

Dann neues Ziel:

$$\{(X_A \to X_B), (\neg X_B \vee \neg X_C), \neg(\neg X_A \vee \neg X_C)\} \models \perp$$

oder

$\{(X_A \to X_B), (\neg X_B \vee \neg X_C), \neg(\neg X_A \vee \neg X_C)\} \models (X_A \wedge \neg X_A)$.

Eine Sequenz

$$\alpha_1, \ldots, \alpha_k, \beta$$

ist korrekt, wenn $\{\alpha_1, \ldots, \alpha_k\} \models \beta$.

Eine Sequenzenregel

$$\frac{\begin{array}{c}\Gamma_1, \beta_1 \\ \vdots \\ \Gamma_s, \beta_s\end{array}}{\Gamma, \beta}$$

ist korrekt, wenn sie bei Anwendung auf korrekte Sequenzen eine korrekte Sequenz liefert.

Ein Sequenzenkalkül $\mathfrak{S}$ ist eine Menge von Sequenzenregeln.

Eine Sequenz Γ, β ist in $\mathfrak{S}$ ableitbar oder in $\mathfrak{S}$ formal beweisbar, $\vdash_{\mathfrak{S}} \Gamma, \beta$, wenn sie durch endlichmalige Anwendung der Regeln in $\mathfrak{S}$ gewonnen werden kann.

$\mathfrak{S}$ ist korrekt: alle Regeln in $\mathfrak{S}$ sind korrekt.

$\mathfrak{S}$ ist vollständig: jede korrekte Sequenz ist in $\mathfrak{S}$ ableitbar.

Bemerkung. Ist $\mathfrak{S}$ korrekt, so ist jede in $\mathfrak{S}$ ableitbare Sequenz korrekt.

Ein korrekter und vollständiger Sequenzenkalkül $\mathfrak{S}_0$

Für AA$(\neg, \vee)$

(Vor) $\dfrac{}{\Gamma, \alpha}$ falls α in Γ

(Ant) $\dfrac{\Gamma, \alpha}{\Gamma', \alpha}$ falls jeder Ausdruck in Γ auch in Γ' vorkommt

(FU) $\dfrac{\begin{matrix}\Gamma, \alpha, \beta \\ \Gamma, \neg\alpha, \beta\end{matrix}}{\Gamma, \beta}$ (Wid) $\dfrac{\begin{matrix}\Gamma, \neg\alpha, \beta \\ \Gamma, \neg\alpha, \neg\beta\end{matrix}}{\Gamma, \alpha}$

($\vee$A) $\dfrac{\begin{matrix}\Gamma, \alpha, \beta \\ \Gamma, \delta, \beta\end{matrix}}{\Gamma, (\alpha \vee \delta), \beta}$

($\vee$S$_1$) $\dfrac{\Gamma, \alpha}{\Gamma, (\alpha \vee \beta)}$ ($\vee$S$_2$) $\dfrac{\Gamma, \alpha}{\Gamma, (\beta \vee \alpha)}$

Beispiel 3. Die Regel

$$\frac{\begin{matrix}\Gamma, (\alpha \vee \beta) \\ \Gamma, \neg\alpha\end{matrix}}{\Gamma, \beta} \quad \text{ist ableibar.}$$

Rechtfertigung:

1	$\Gamma, (\alpha \vee \beta)$	Prämisse
2	$\Gamma, \neg\alpha$	Prämisse
3	$\Gamma, \alpha, \neg\alpha$	(Ant) auf 2
4	Γ, α, α	(Vor)
5	Γ, α, β	(Wid') auf 4 und 3
6	Γ, β, β	(Vor)
7	$\Gamma, (\alpha \vee \beta), \beta$	($\vee$A) auf 5 und 6
8	$\Gamma, \neg(\alpha \vee \beta), (\alpha \vee \beta)$	(Ant) auf 1
9	$\Gamma, \neg(\alpha \vee \beta), \neg(\alpha \vee \beta)$	(Vor)
10	$\Gamma, \neg(\alpha \vee \beta), \beta$	(Wid') auf 8 und 9
11	Γ, β	(FU) auf 7 und 10

Sei $\Gamma \subseteq \mathrm{AA}(\neg, \vee)$ und $\beta \in \mathrm{AA}(\neg, \vee)$.

β ist aus Γ $\mathfrak{S}_0$-ableitbar, $\Gamma \vdash_{\mathfrak{S}_0} \beta$,

gdw

es gibt endlich viele $\alpha_1, \ldots, \alpha_r \in \Gamma$ mit: $\vdash_{\mathfrak{S}_0} \alpha_1, \ldots, \alpha_r, \beta$

Ziel:

$$\Gamma \vdash_{\mathfrak{S}_0} \beta \iff \Gamma \models \beta$$

$\Rightarrow$= Korrektheit von $\mathfrak{S}_0$; $\Leftarrow$= Vollständigkeit von $\mathfrak{S}_0$

$\vdash$ statt $\vdash_{\mathfrak{S}_0}$; ableitbar statt $\mathfrak{S}_0$-ableitbar

Γ ist ($\mathfrak{S}_0$-)widerspruchsfrei, Wf Γ,

gdw

es gibt keinen Ausdruck α mit: $\Gamma \vdash \alpha$ und $\Gamma \vdash \neg\alpha$.

HILBERTs System $\mathfrak{H}_0$:

(A1) $$\frac{}{(X \to (Y \to X))}$$

(A2) $$\frac{}{((X \to (Y \to Z)) \to ((X \to Y) \to (X \to Z)))}$$

(A3) $$\frac{}{((\neg X \to Y) \to ((\neg X \to \neg Y) \to X))}$$

(MP) $$\frac{\begin{array}{c} X \\ (X \to Y) \end{array}}{Y}$$

(SUB) $$\frac{\alpha}{\alpha\frac{\beta_1,\ldots,\beta_n}{X_1,\ldots,X_n}}$$ $X_1, \ldots, X_n$ paarw. verschieden

MEREDITHs System: (MP), (SUB), (A).

(A) $$\frac{}{\begin{array}{l}(((((X \to Y) \to (\neg Z \to \neg U)) \to Z) \to V) \\ \quad \to ((V \to X) \to (U \to X)))\end{array}}$$

$$\mathsf{SAT}_0 = \{\alpha \in \mathsf{AA} \mid \mathsf{Erf}\ \alpha\}; \qquad \mathsf{SAT} = \{\alpha \in \mathsf{KNF} \mid \mathsf{Erf}\ \alpha\}$$

$$\mathsf{TAUT} := \{\alpha \in \mathsf{AA} \mid \alpha \text{ allgemeingültig}\}$$

$$\alpha \text{ allgemeingültig} \iff \text{nicht Erf } \neg\alpha \qquad (2)$$

Σ Alphabet, $W \subseteq \Sigma^*$:

$$W \in \text{co-NP} \iff \Sigma^* \setminus W \in \mathsf{NP}.$$

$\mathsf{TAUT} \subseteq \Sigma_a^*$:

Satz 1. TAUT $\in$ co-NP.

Beweis. Für $w \in \Sigma_a^*$

$$w \in \Sigma_a^* \setminus \mathsf{TAUT} \overset{(2)}{\iff} w \notin \mathsf{AA} \text{ oder } (w \in \mathsf{AA} \text{ und } \neg w \in \mathsf{SAT}).$$

Da SAT $\in$ NP, somit TAUT $\in$ co-NP.

Ein Beweissystem für TAUT ist eine in polynomieller Zeit berechenbare surjektive Funktion $f : \Sigma^* \to \mathsf{TAUT}$ für ein geeignetes Alphabet Σ.

Ein Beweissystem $f : \Sigma^* \to$ TAUT ist polynomiell beschränkt, wenn ein Polynom $q \in \mathbb{N}[x]$ existiert, so dass für alle $\beta \in$ TAUT ein $w \in \Sigma^*$ existiert mit

$$f(w) = \beta \quad \text{und} \quad |w| \le q(|\beta|).$$

Satz 2. Die folgenden Aussagen sind äquivalent:

1. Es gibt ein polynomiell beschränktes Beweissystem für TAUT.
2. TAUT $\in$ NP.
3. NP = co-NP.

Beweis. (1) $\Rightarrow$ (2): Seien Σ, f, q wie oben. Dann

$$\beta \in \text{TAUT} \quad \Longleftrightarrow \quad \text{ex. } w \in \Sigma^* : (|w| \le q(|\beta|) \text{ und } f(w) = \beta).$$

Somit TAUT $\in$ NP: Bei gegebenem β errate w und prüfe $f(w) = \beta$.

(2) $\Rightarrow$ (3): Sei $L \subseteq \Sigma^*$ und $L \in$ co-NP. Dann $\Sigma^* \setminus L \in$ NP. Da SAT NP-vollständig ist, gibt es eine in polynomieller Zeit berechenbare Funktion $g : \Sigma^* \to$ AA (!) mit

$$\begin{aligned} x \in \Sigma^* \setminus L \quad &\Longleftrightarrow \quad g(x) \in \text{SAT} \\ &\Longleftrightarrow \quad \neg g(x) \notin \text{TAUT} \end{aligned}$$

also

$$x \in L \quad \Longleftrightarrow \quad \neg g(x) \in \text{TAUT}.$$

Somit zeigt $h : \Sigma^* \to \Sigma_a^*$ mit $h(x) = \neg g(x)$, dass $L \le_{\text{pol}}$ TAUT; somit $L \in$ NP.

Somit co-NP $\subseteq$ NP. Damit NP = co-(co-NP) $\subseteq$ co-NP, also NP = co-NP.

$$\frac{}{\top} \qquad \frac{}{\bot} \qquad \frac{}{X} \qquad \frac{\alpha}{\neg\alpha} \qquad \frac{\alpha, \beta}{(\alpha \wedge \beta)} \qquad \frac{\alpha, \beta}{(\alpha \vee \beta)}$$

$$\frac{\alpha}{\forall X \alpha} \qquad \frac{\alpha}{\exists X \alpha}$$

Satz über die eindeutige Zerlegbarkeit. Jeder Ausdruck $\alpha \in$ QAA ist entweder ein Ausdruck der Gestalt

(1) $\top$ oder

(2) $\bot$ oder

(3) X_i oder

(4) $\neg\beta$ oder

(5) $(\beta \wedge \gamma)$ oder

(6) $(\beta \vee \gamma)$ oder

(7) $\forall X \beta$ oder

(8) $\exists X \beta$.

Dabei sind eindeutig bestimmt

β in (4), β und γ in (5),(6) und X und β in (7),(8).

$b : \mathsf{AV} \to \{0,1\}$ totale Belegung, $X \in \mathsf{AV}$ und $b_0 \in \{0,1\}$. Dann ist $b[X \to b_0]$ die totale Belebung mit

$$b(Y) := \begin{cases} b_0 & \text{wenn } Y = X \\ b(Y) & \text{sonst} \end{cases}$$

Für $\alpha \in \mathsf{QAA}$ sei $\mathsf{fr}(\alpha)$, die Menge der in α frei vorkommenden Variablen, durch Induktion über α definiert:

$$\begin{array}{ll} \mathsf{fr}(\top) = \emptyset; & \mathsf{fr}(\bot) = \emptyset; \\ \mathsf{fr}(X) = \{X\}; & \mathsf{fr}(\neg\alpha) = \mathsf{fr}(\alpha); \\ \mathsf{fr}((\alpha \wedge \beta)) = \mathsf{fr}(\alpha) \cup \mathsf{fr}(\beta); & \mathsf{fr}((\alpha \vee \beta)) = \mathsf{fr}(\alpha) \cup \mathsf{fr}(\beta); \\ \mathsf{fr}(\forall X \alpha) = \mathsf{fr}(\alpha) \setminus \{X\}; & \mathsf{fr}(\exists X \alpha) = \mathsf{fr}(\alpha) \setminus \{X\}. \end{array}$$

$$\begin{array}{rc} & \mathsf{fr}((\exists X(X \vee Z) \wedge \forall Y(\neg Y \vee X))) \\ = & \mathsf{fr}(\exists X(X \vee Z)) \cup \mathsf{fr}(\forall Y(\neg Y \vee X)) \\ = & (\mathsf{fr}((X \vee Z)) \setminus \{X\}) \cup (\mathsf{fr}((\neg Y \vee X)) \setminus \{Y\}) \\ = & (\{X, Z\} \setminus \{X\}) \cup (\{Y, X\} \setminus \{Y\}) \\ = & \{Z, X\}. \end{array}$$

Koinzidenzlemma. Ist $\alpha \in \mathsf{QAA}$ und sind b, b' totale Belegungen mit

$$b(X) = b'(X) \quad \text{für alle } X \in \mathsf{fr}(\alpha),$$

so

$$b(\alpha) = b'(\alpha).$$

Für $\alpha \in$ AA$(\top, \bot, \neg, \wedge, \vee)$ sei $\alpha\frac{\top}{X}$ die Zeichenreihe, die aus α durch Ersetzung aller Vorkommen von X durch $\top$ entsteht. Entsprechend sei $\alpha\frac{\bot}{X}$ definiert.

Es gilt

$$\alpha\frac{\top}{X}, \alpha\frac{\bot}{X} \in \text{AA}(\top, \bot, \neg, \wedge, \vee).$$

Satz 1. $\tilde{\ } : \text{QAA} \to \text{AA}(\top, \bot, \neg, \wedge, \vee)$ sei wie folgt definiert:

$$\begin{array}{ll}
\tilde{\top} = \top; & \tilde{\bot} = \bot; \\
\tilde{X} = X; & \widetilde{\neg\alpha} = \neg\widetilde{\alpha}; \\
\widetilde{(\alpha \wedge \beta)} = (\widetilde{\alpha} \wedge \widetilde{\beta}); & \widetilde{(\alpha \vee \beta)} = (\widetilde{\alpha} \vee \widetilde{\beta}); \\
\widetilde{\forall X\alpha} = (\widetilde{\alpha}\frac{\top}{X} \wedge \widetilde{\alpha}\frac{\bot}{X}); & \widetilde{\exists X\alpha} = (\widetilde{\alpha}\frac{\top}{X} \vee \widetilde{\alpha}\frac{\bot}{X}).
\end{array}$$

Dann gilt für alle $\alpha \in$ QAA:

1. $\widetilde{\alpha} \equiv \alpha$;
2. var$(\widetilde{\alpha}) =$ fr(α).