`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**);

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

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

konkrete Zeichen;

häufig auch unendliche Alphabete:

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

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;

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

Σ_5 ersetzen durch endliches Alphabet, etwa durch

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

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

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

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:

$$m \in M \qquad\qquad \frac{}{m}$$

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) $\frac{}{\lambda}$

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

$axei \in M$:

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:

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

Erweitern auf alle aussagenlogische Ausdrücke durch Vorschriften:

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

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

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

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

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

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

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:

für alle $\beta \in$ AA: x ist kein Anfangsstück von β
und β 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 $w = \lambda$.