Kapitel 4
Formale Logik

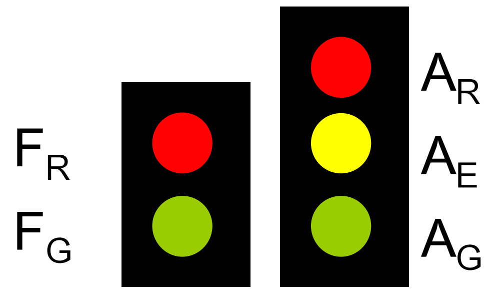
4 Ziele

- Präzise Beschreibung von Sachverhalten so, daß
  - mit mechanisch durchführbaren, syntaktischen Schlüssen inhaltliche, semantische Eigenschaften festgestellt und Schlußfolgerungen gezogen werden können
  - Konsistenz/Widersprüchlichkeit bzw. Vollständigkeit von Aussagen festgestellt werden kann
  - nachgeprüft werden kann, ob das logische Gedanken-Gebäude ein Modell in der realen Welt besitzt
- Formale Logik ist
  - das allgemeinste und genaueste Verfahren zur Spezifikation von Aufgaben und den Eigenschaften von Lösungen, insbesondere der Korrektheit von Programmen
  - **Beispiel**: Zustände vor/nach einem Zustandsübergang durch Vor-/Nachbedingungen (prädikatenlogische Formel) charakterisieren
  - formale Logik ist Grundlage des logischen Programmierens, des automatischen Theorem-Beweisens und anderer Zweige der KI
- digitaler Entwurf von Schaltkreisen ist eine Anwendung der Aussagenlogik

Mathematische und formale Logik sind Synonyme, philosophische und andere Logiken unterscheiden sich davon

Beispiel:

Eine Fußgänger-Ampel darf nur ganz bestimmte Kombinationen an Lichtzeichen zeigen. Die Funktionsweise kann mittels formaler Logik beschrieben werden.



Die Fußgängerampel zeigt genau dann grün (F_G), wenn die Verkehrsampel nicht grün ($\neg A_G$) zeigt:

$$F_G = \neg A_G$$

$$F_R = A_G \vee A_E$$

Die Verkehrsampel zeigt genau dann grün, wenn sie weder rot oder gelb zeigt:

$$A_G = \neg A_E \wedge \neg A_R \qquad \text{usw.}$$

☛ Spezifikation mittels formaler Logik

Beispiel: Bauernregeln

- Gibt es Eis und Schnee im Januar, so beginnt sehr kalt das Jahr
- Es gibt Eis und Schnee im Januar
- Also beginnt das Jahr sehr kalt.

Beispiel:

- Wenn es schneit, dann sind die Straßen glatt.
- Es schneit.
- Also sind die Straßen glatt.

4.1 Beobachtungen

- Wir verknüpfen Aussagen:
  - es gibt Eis und Schnee im Januar $\rightarrow$ das Jahr beginnt sehr kalt
  - es gibt Eis und Schnee im Januar
  - wir haben die Aussage „das Jahr beginnt sehr kalt“ gefolgert.
  - es schneit $\rightarrow$ die Straßen sind glatt
  - es schneit
  - wir haben die Aussage „die Straßen sind glatt“ gefolgert
- die Art des Schlusses ist dieselbe.
  - aus $(a \rightarrow b)$ und a wurde b gefolgert.
  - insbesondere ist der Schluß unabhängig von konkreten Inhalten.
  - konkrete Inhalte sind Interpretationen.
    - ☛ Schlußfolgern heißt Formeln syntaktisch herleiten (Kalkül)
    - ☛ trotzdem ist das auch semantisch richtig! (Korrektheit)
  - können wir auch alles Richtige folgern? (Vollständigkeit)

4.1 Aussagenlogische Formeln

<u>aussagenlogische Formel</u>: Term mit Variablen in der initialen Termalgebra $\mathcal{J} = (\Sigma, V)$ zur Signatur $\Sigma = \{ O/0, L/0, \neg/1, \vee/2, \wedge/2 \}$

- die Signatur entspricht der booleschen Algebra $\mathscr{B}$:
  $O \mapsto \bot \quad L \mapsto \top \quad \neg \mapsto \complement \quad \vee \mapsto \vee \quad \wedge \mapsto \wedge$
  - lies: O als ‚falsch'
    L als ‚wahr'
    ¬ als ‚nicht'
    ∧ als ‚und'
    ∨ als ‚oder'
- aber: wir wissen noch nicht, ob auch die Gesetze V1-V10 gelten!
- <u>atomare Aussage</u>: O, L, $p \in V$, <u>Literal</u>: O, L, p, ¬O, ¬L, ¬p
- syntaktisch korrekt aufgebaute Terme heißen <u>(syntaktisch) korrekt</u>
  - hat nichts damit zu tun, ob sie semantisch wahr sind

Beispiele:
- ¬(es gibt Eis und Schnee im Januar) ∨ (das Jahr beginnt sehr kalt)
- $x \wedge (y \vee z)$
- $O \vee x$

Abkürzungen: $p \to q \;\triangleq\; \neg p \lor q$

impliziert (auch: wenn…, dann…, aus ... folgt ...)

$p \equiv q$ oder $p \leftrightarrow q \;\triangleq\; (p \to q) \land (q \to p)$

äquivalent (auch: genau dann…, wenn…)

$$\bigvee_{i=1..n} p_i \;\triangleq\; p_1 \lor \ldots \lor p_n \quad \text{(auch bei abzählbar vielen } p_i\text{)}$$

$$\bigwedge_{i=1..n} p_i \;\triangleq\; p_1 \land \ldots \land p_n \quad \text{(auch bei abzählbar vielen } p_i\text{)}$$

$$\bigvee_{i=1..0} p_i \;\triangleq\; O$$

$$\bigwedge_{i=1..0} p_i \;\triangleq\; L$$

- $\neg$, $\lor$, $\land$, $\to$, $\equiv$ heißen Junktoren

4.1 Klammern

Konventionen zum Weglassen von Klammern:

	$\neg$
bindet stärker als	$\wedge$
bindet stärker als	$\vee$
bindet stärker als	$\rightarrow$
bindet stärker als	$\leftrightarrow$

Klammerung von $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$ ist linksassoziativ, z.B.

$$x \wedge y \wedge z = (x \wedge y) \wedge z$$

Beispiel:

$$\begin{aligned} & p \wedge q \rightarrow r \\ = \; & (p \wedge q) \rightarrow r \\ = \; & \neg(p \wedge q) \vee r \\ = \; & (\neg(p \wedge q)) \vee r \end{aligned}$$

4.1 Interpretation von Formeln (I)

Ziel: Formeln inhaltlich betrachten, prüfen, ob

- Formeln immer wahr sind (allgemeingültig, Tautologie)
- Formeln wahr sein können (erfüllbar)
- Formeln nie wahr sein können (unerfüllbar)

dazu müssen Formeln interpretiert werden.

Grundidee:
Interpretation von Formeln durch Abbildung $\mathcal{I}$ in eine boolesche Algebra mit Signatur $\Sigma = \{ f/0, w/0, \neg/1, \vee/2, \wedge/2 \}$

- Abbildung durch Umbenennung der Signatur :
  $O \mapsto f \quad L \mapsto w \quad \neg \mapsto \complement \quad \vee \mapsto \vee \quad \wedge \mapsto \wedge$
- Trägermenge B = {f, w}, f ist „falsch“, w ist „wahr“, $f \leq w$
- Belegung: Variablenabbildung durch Substitution $\sigma = [w/v]$ bzw. $\sigma = [f/v]$
- immer nur endlich viele Variable abbilden!
  - in endlich vielen Formeln kommen nur endlich viele Variable vor

Beispiel:

- **p ∧ q** ist erfüllbar:

  die Variablen (Elementaroperanden) p und q werden jeweils durch w interpretiert: σ = [w/p, w/q] anwenden

- **p ∨ ¬p** ist allgemeingültig:
  unabhängig von der Interpretation des Elementaroperanden p ergibt sich w nach Definition des Komplements

- **p ∧ ¬p** ist unerfüllbar:
  unabhängig von der Interpretation des Elementaroperanden p ergibt sich f nach der Definition des Komplements

Belegung: Substitution σ: $V' \to \{w, f\}$,
endliche Teilmenge $V' \subseteq V$ wird abgebildet

Interpretation $\mathcal{I}_\sigma$: Abbildung von Formeln nach {f, w} unter Belegung σ:

$$\mathcal{I}_\sigma(O) = f \qquad \mathcal{I}_\sigma(L) = w$$

$$\mathcal{I}_\sigma(a) = \sigma(a) \text{ für } a \in V \qquad \mathcal{I}_\sigma(\neg F) = \begin{cases} w & \text{wenn } \mathcal{I}_\sigma(F) = f \\ f & \text{wenn } \mathcal{I}_\sigma(F) = w \end{cases}$$

$$\mathcal{I}_\sigma(F \wedge G) = \begin{cases} w & \text{wenn } \mathcal{I}_\sigma(F) = w \text{ \underline{und} } \mathcal{I}_\sigma(G) = w \\ f & \text{sonst} \end{cases}$$

$$\mathcal{I}_\sigma(F \vee G) = \begin{cases} w & \text{wenn } \mathcal{I}_\sigma(F) = w \text{ \underline{oder} } \mathcal{I}_\sigma(G) = w \\ f & \text{sonst} \end{cases}$$

Beachte: und und oder werden jetzt inhaltlich (semantisch) interpretiert!
☛ Die Regel für ¬F interpretiert „¬" als „es gilt nicht"

4.1 Modell

Eine Interpretation $\mathcal{I}_\sigma$ heißt Modell für eine Formel F, wenn $\mathcal{I}_\sigma(F) = w$ gilt.
$\mathcal{I}_\sigma$ heißt **Modell** für die Formelmenge $\mathcal{F}$, wenn $\mathcal{I}_\sigma$ Modell für alle $F \in \mathcal{F}$ ist.

erfüllbare Formel F:
es gibt eine Belegung σ, so daß $\mathcal{I}_\sigma(F) = w$ oder:
es gibt ein Modell $\mathcal{I}_\sigma$ für die Formel F.

allgemeingültige Formel F:
für alle Belegungen σ ist $\mathcal{I}_\sigma(F) = w$ oder:
alle Interpretationen $\mathcal{I}_\sigma$ sind Modelle für F.

unerfüllbare Formel F:
für alle Belegungen σ ist $\mathcal{I}_\sigma(F) = f$ oder:
es gibt kein Modell für F.

Eigenschaft: Eine Formel F ist genau dann allgemeingültig, wenn $\neg F$ unerfüllbar ist.

4.1 Wahrheitstafeln: Beispiel

- Formel $\varphi = \neg(\neg p \lor q) \lor \neg(\neg q \lor r) \lor \neg p \lor r$

Belegungen			Interpretationen						
p	q	r	$\neg p$	$\neg q$	$\neg p \lor q$	$\neg(\neg p \lor q)$	$\neg p \lor r$	$\neg(\neg p \lor r)$	φ
f	f	f	w	w	w	f	w	f	w
f	f	w	w	w	w	f	w	f	w
f	w	f	w	f	w	f	w	f	w
f	w	w	w	f	w	f	w	f	w
w	f	f	f	w	f	w	f	w	w
w	f	w	f	w	f	w	w	f	w
w	w	f	f	f	w	f	f	w	w
w	w	w	f	f	w	f	w	f	w

- **Beachte:** A v B v C ist wahr, wenn mindestens eine Formel A, B, C wahr ist.
  ☛ φ ist allgemeingültig, weil φ unter allen möglichen Belegungen w ist.
- $\neg(\neg p \lor q)$ ist erfüllbar: es gibt Belegungen, unter denen sie wahr wird.

- $\Psi = \neg(\neg(p \land (\neg p \lor q)) \lor p)$

Zur Abkürzung definieren wir:

$$A = \neg p \lor q$$
$$B = p \land (\neg p \lor q)$$
$$C = \neg B \lor p = \neg(p \land (\neg p \lor q)) \lor p$$

Belegungen		Interpretationen					
p	q	$\neg p$	A	B	$\neg B$	C	Ψ
f	f	w	w	f	w	w	f
f	w	w	w	f	w	w	f
w	f	f	f	f	w	w	f
w	w	f	w	w	f	w	f

☛ Ψ unerfüllbar, weil die Interpretation unter allen Belegungen f ergibt.

4.1 Wahrheitstafeln, Aufwand

- Wahrheitstafel für eine Formel F mit n Variablen: Tabelle mit 2^n Zeilen
  - alle Kombinationen von Belegungen der Variablen mit w/f auflisten
  - dazu in einer Spalte das Ergebnis e(F) von F angeben
    (eventuell auch Ergebnisse von Teilformeln (nur zur Erleichterung))
- **F besitzt Modell (F erfüllbar):** mindestens einmal e(F) = w
- **F unerfüllbar:** immer e(F) = f
- **F allgemeingültig:** immer e(F) = w

- Aufwand dieser Prüfungen: Größenordnung 2^n, n = Anzahl Variable
  ☛ Aufwand also exponentiell!

- Aufwandsklassifikation:
  - **P (polynomiell):** Aufwand ≤ n^k für festes k
  - **NP (nicht-deterministisch polynomiell):** Aufwand in jedem Einzelfall polynomiell, aber mindestens exponentiell viele Fälle (liegt hier vor)
  - **EXP (exponentiell):** Aufwand immer mindestens proportional zu 2^n

Folgerung einer Formel φ aus einer Formelmenge $\mathcal{F}$:

Jede Belegung von Variablen, die alle Formeln aus $\mathcal{F}$ erfüllt, ist auch eine erfüllende Belegung für φ.

$\mathcal{I}_\sigma(\varphi) = w$ für alle Interpretationen $\mathcal{I}_\sigma$, die Modell für $\mathcal{F}$ sind.

Notation: $\mathcal{F} \vDash \varphi$ steht für die semantische Folgerung einer Formel φ aus einer Formelmenge $\mathcal{F}$

Beispiel: $\{p, p \rightarrow q\} \vDash q$

Belegungen		Interpretation		Folgerung	
p	q	$p \rightarrow q$	$\mathcal{F}$	q	-
f	f	w	f	-	-
f	w	w	f	-	-
w	f	f	f	-	-
w	w	w	w	✓	w

also $\{p, p \rightarrow q\} \vDash q$

4.1 Kalküle

Ziel:

Nachweis von Folgerungen ohne Ausrechnen aller Belegungen

- es gibt Eis und Schnee im Januar → das Jahr beginnt sehr kalt
- es gibt Eis und Schnee im Januar
- Wir haben die Aussage „das Jahr beginnt sehr kalt“ gefolgert.
- es schneit → die Straßen sind glatt
- es schneit
- Wir haben die Aussage „die Straßen sind glatt“ gefolgert.

Beobachtung:

Die Art des Schlusses ist derselbe.

- Aus Formeln der Form $F \rightarrow G$ und der Formel F wurde die Formel G gefolgert.
- Offenbar ist die Folgerung richtig, egal was die Formeln F und G sind

Ziel: syntaktische Herleitung von Folgerungen

Notation: $\mathcal{F} \vdash \varphi$ bezeichnet die syntaktische Herleitung einer Folgerung $\mathcal{F} \models \varphi$

Beispiel einer Schlußregel: Modus Ponens

$$\left.\begin{array}{lll} \mathcal{F} & \vdash & F \\ \mathcal{F} & \vdash & F \rightarrow G \end{array}\right\} \text{Prämisse}$$

$$\frac{}{\mathcal{F} \quad \vdash \quad G} \quad \text{Konklusion}$$

Beobachtung: Das war genau die Art von Argumentation in den bisherigen Beispielen.

Anwendung einer Schlußregel:

- Wenn die Folgerungen in den Voraussetzungen (über dem Strich) gelten (durch Einsetzen der entsprechenden Formelmengen und Formeln),
- dann gilt auch die Folgerung in der Konsequenz (unter dem Strich, mit den entsprechend eingesetzten Formelmengen)

Beispiel:

$$\frac{}{\mathcal{F} \quad \vdash \quad F} \text{ für } F \text{ in } \mathcal{F}$$

$$\frac{\begin{array}{lcl} \mathcal{F} \cup \{\neg F\} & \vdash & G \\ \mathcal{F} \cup \{\neg F\} & \vdash & \neg G \end{array}}{\begin{array}{lcl} \mathcal{F} & \vdash & F \end{array}}$$

$$\{p, \neg p, \neg q, \neg r\} \vdash p$$

$$\{p, \neg p, \neg q, \neg r\} \vdash \neg p$$

$$\{p, \neg p, \neg q\} \vdash r$$

Herleitung von $\mathcal{F} \vdash \varphi$: Liste von Folgerungen $\mathcal{F}_i \vdash \varphi_i$, wobei jedes $\mathcal{F}_i \vdash \varphi_i$ aus vorherigen Folgerungen durch Anwenden einer Schlußregel entsteht.

4.1 Diskussion

Beobachtung: Herleitungen sind ausschließlich syntaktisch

☛ kann im Rechner ablaufen (z.B. in Expertensystemen)

Was hat dies mit der Folgerung $\mathcal{F} \vDash \varphi$ zu tun?

korrekter Kalkül $\vdash$: Wenn $\mathcal{F} \vdash \varphi$ hergeleitet werden kann, dann gilt auch $\mathcal{F} \vDash \varphi$.

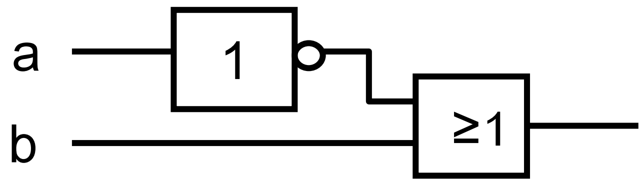
vollständiger Kalkül $\vdash$: Wenn $\mathcal{F} \vDash \varphi$ gilt, dann kann auch $\mathcal{F} \vdash \varphi$ hergeleitet werden

Vollständige Regelmenge für aussagenlogischen Kalkül siehe Buch 4.1.3, sowie Vorlesungen Informatik III und Formale Systeme

4.1 Vergleich: ⊢ und →

$F \rightarrow G$	$\mathcal{F} \vdash_K G$
Implikation	**Ableitung**
▪ Aussagenlogische Abkürzung für den Ausdruck $\neg F \vee G$ ▪ kann in einem **Programm** berechnet werden ▪ logische Aussage, die **wahr oder falsch** sein kann	▪ Es gilt das Theorem G unter der Annahme (Axiomenmenge) $\mathcal{F}$. ▪ Diese Ableitung wird durch syntaktische Ersetzungen realisiert. ▪ G ist aus $\mathcal{F}$ ableitbar

Beispiel:

$a \rightarrow b$ steht für die einfache Boolesche Funktion $\neg a \vee b$: 	Wenn $\mathcal{F} \vdash (a \rightarrow b)$ gilt, kann man schließen, daß $(\mathcal{F} \wedge a) \vdash b$ gilt: man kann b folgern, wenn man a zur Formelmenge $\mathcal{F}$ hinzunimmt.

4.1 Vergleich: ⊨ und ⊢

$\mathcal{F} \models G$	$\mathcal{F} \vdash_K G$
Schluß	**Ableitung**
▪ G (Folgerung) folgt **semantisch** aus $\mathcal{F}$ (Annahme) ▪ Die Annahme kann auch leer sein (☛ Tautologien) ▪ Voraussetzung: $\mathcal{I}_\sigma(G) = w$ für alle Interpretationen $\mathcal{I}_\sigma$, die Modell für $\mathcal{F}$ sind.	▪ G (Ableitung) ist in endlich vielen Schritten aus $\mathcal{F}$ **mittels des Kalküls K** („Regelwerk") ableitbar. ▪ Auch hier kann die Formelmenge $\mathcal{F}$ leer sein.

- **korrekter Kalkül K:** Was man mittels dem Regelwerk K ableiten kann, kann auch semantisch aus $\mathcal{F}$ gefolgert werden.
- **vollständiger Kalkül K:** Alles, was semantisch gefolgert werden kann, kann man auch mittels einer endlichen Zahl von Regelanwendungen aus K ableiten.

Beispiel: Betrachte $\{p, \neg p, \neg q, \neg r\} \vdash p$

$$\{p, \neg p, \neg q, \neg r\} \vdash \neg p$$

$$\{p, \neg p, \neg q\} \vdash r$$

Beobachtung:

analog kann man für beliebige Formeln F zeigen, daß $\{p, \neg p, \neg q\} \vdash F$

☛ neue Schlußregel

$$\frac{\mathcal{F} \vdash F \qquad \mathcal{F} \vdash \neg F}{\mathcal{F} \vdash G}$$

ex falso quod libet

- Aus Widersprüchen folgt beliebiges.
- Eine solche Formelmenge $\mathcal{F}$ heißt inkonsistent.
- Eine Formelmenge $\mathcal{F}$, die nicht inkonsistent ist, heißt konsistent.

4.1 Anwendung

- Im Eingangsbeispiel „Ampel“ haben wir das Problem durch Formelmengen definiert.
- Solche Spezifikationen müssen **konsistent** sein.
- Eine inkonsistente Spezifikation kann beliebig implementiert werden.

4.1 Normalformen

Disjunktive Normalform: $\varphi = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} L_{ij}$

wobei L_{ij} = p oder L_{ij} = ¬p für eine aussagenlogische Variable p ist.
L_{ij} heißt Literal.
Konjunktive Normalform: $\varphi = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m} L_{ij}$

Satz: Jede aussagenlogische Formel kann in disjunktiver und in konjunktiver Normalform geschrieben werden.

Beweis: strukturelle Induktion über den Aufbau von Formeln:

- Literale p, ¬p bereits in DNF
- ¬F, F bereits in DNF: Anwendung von V10 (De Morgan) liefert einfachere Formel F', danach eventuell V8,V9
- $F = F_1 \vee F_2$, F_1, F_2 bereits in DNF: F in DNF (nach Identifikation sowohl in F_1 als auch in F_2 vorkommender Teilformeln)
- $F = F_1 \wedge F_2$, F_1, F_2 bereits in DNF: fortgesetzte Anwendung von V5 (Distributivgesetz) (und V8, V9) liefert DNF
- Für KNF analog

Aufwand NP! Grund: aus DNF kann Erfüllbarkeit direkt abgelesen werden

4.1 Disjunktive Normalform: Beispiel

Disjunktive Normalform von $F = \neg(\neg(p \wedge (\neg p \vee q)) \vee p)$:

$F = \neg\neg(p \wedge (\neg p \vee q)) \wedge \neg p$	V10
$= ((p \wedge \neg p) \vee (p \wedge q)) \wedge \neg p$	V5
$= p \wedge q \wedge \neg p$	V8: $p \wedge \neg p = O$, O weglassen
$= O$	V8

- Alternatives Verfahren: Aufstellung Wahrheitstafel vgl. Folie 14
- **Beispiel**: $F = \neg(\neg p \vee q) \vee \neg(\neg q \vee r) \vee \neg p \vee r$ (vgl. Folie 12)
  $F = p \wedge q \wedge r \vee p \wedge q \wedge \neg r \vee p \wedge \neg q \wedge r \vee p \wedge \neg q \wedge \neg r \vee$
  $\neg p \wedge q \wedge r \vee \neg p \wedge q \wedge \neg r \vee \neg p \wedge \neg q \wedge r \vee \neg p \wedge \neg q \wedge \neg r$
- Prinzip: für jede Zeile mit Ergebnis e(F) = w bilde konjunktiven Term, in dem mit w belegte Variable positiv, mit f belegte Variable negiert sind
  - Belegung (w,f,w): Term $p \wedge \neg q \wedge r$
- Im Beispiel kommen alle $2^3=8$ konjunktiven Terme vor, da F allgemeingültig

4.1 Junktoren

- Wieviele Operationen τp bzw. p τ q von k aussagenlogischen Variablen p, q mit potentiell unterschiedlichem Ergebnis gibt es?
- Antwort: die Wahrheitstafel hat 2^k Zeilen, die alternativ O oder L ergeben können, also $2^{2\text{^}k}$ Möglichkeiten
- k = 1: Operationen p, ¬p, O, L (identisch wahr/falsch)
- k = 2: $2^{2\text{^}k} = 16$:

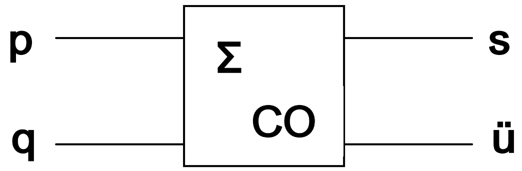
O	O	L	L	p	Kommentar
O	L	O	L	q	
O	O	O	O	O	identisch O
O	O	O	L	p ∧ q	
O	O	L	O	¬(p→ q)	p ∧ ¬q
O	O	L	L	p	
O	L	O	O	¬(q→ p)	¬p ∧ q
O	L	O	L	q	
O	L	L	O	¬(p ≡ q)	p xor q, exklusiv. oder
O	L	L	L	p ∨ q	

L	O	O	O	¬(p ∨ q)	p nor q, p/q, Sheffer-Strich
L	O	O	L	p ≡ q	p ↔ q
L	O	L	O	¬q	
L	O	L	L	¬q ∨ p	q → p
L	L	O	O	¬p	
L	L	O	L	¬p ∨ q	p → q
L	L	L	O	¬(p ∧ q)	p nand q, Peirce Fkt.
L	L	L	L	L	identisch L

4.1 Einsichten und Anwendungen

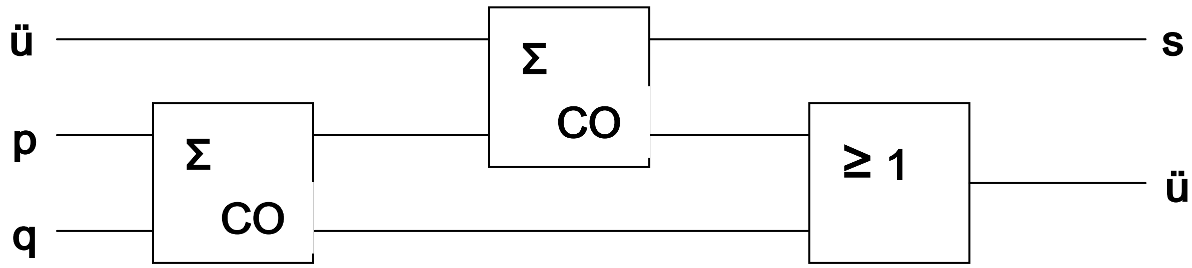
- Der Sheffersche Strich, die Peirce-Funktion, sowie die Paare ¬, ∧ und ¬, ∨ genügen jeweils für sich, um alle Junktoren auszudrücken

- Halbaddierer: p, q als Ziffern 0/1,
  Ergebnis ist Summe und Übertrag (CO), p + q = (s,ü) = (p xor q, p ∧ q)



CO: carry out
CI: carry in

- Volladdierer: p + q + ü = (s,ü)
  = (p xor q xor ü, ((p xor q) ∧ ü) nor (p ∧ q))



4.1 Zusammenfassung

- Aussagenlogik dient der Formalisierung von Aussagen
- Syntax von Formeln basiert auf aussagenlogischen Variablen und den Operatoren ¬(nicht), ∧ (und), ∨ (oder); Variable ≙ Aussage
- Die boolesche Algebra ist Grundlage der Interpretation von Formeln.
- Den Wahrheitsgehalt von Formeln kann man mit Wahrheitstafeln ausrechnen.
- Allgemeingültige Formeln sind immer wahr, erfüllbare Formeln können wahr werden, unerfüllbare Formeln sind nie wahr.
- Formeln kann man aus Formelmengen semantisch folgern ($\mathcal{F} \models F$).
- Auch dies kann man syntaktisch mit Wahrheitstafeln nachrechnen.
- Das Nachrechnen mit Wahrheitstafeln ist sehr aufwendig.
- Mit einem korrekten und vollständigen Kalkül kann man syntaktische Folgerungen einfacher nachweisen ($\mathcal{F} \vdash F$).
- DNF und KNF sind aufwendig herzustellen, aber Grundlage vieler Anwendungen
- Die Junktoren spielen in der technischen Informatik eine große Rolle

4.2 Prädikatenlogik

- Problem:
  - in der Aussagenlogik bezeichnen Variable Aussagen
    ☛ keine Möglichkeit Aussagen p(X) über Objekte X zu machen
- Prädikatenlogik:
  - Variable bezeichnen Objekte, nur in Logik höherer Stufe auch Aussagen
    - Objekte werden repräsentiert durch Terme einer Termalgebra
  - Aussagen p(X) über Objekte heißen Prädikate (über X)
  - auch Aussagen q(X,Y,...) über mehrere Objekte möglich: Prädikatssymbole p, q, ... haben Stelligkeit p/1, q/2, ...
  - Prädikate sind atomare Formeln
  - atomare Formeln kann man mit Junktoren verknüpfen
    ☛ Gesetze und Regeln wie in der Aussagenlogik
  - zusätzlich: mit Quantoren ∀,∃ kann man Prädikate über alle Objekte formulieren oder die Existenz eines Objekts mit p(X) postulieren:
    ☛ $\forall$ X: p(X) bzw. $\exists$ X: p(X)

4.2 Prädikatenlogik: Beispiel

Beispiel: Weisheiten

- Von je zwei Politikern einer Versammlung von Politikern ist wenigstens einer bestechlich.
- Ein Politiker der Versammlung ist unbestechlich.
- Also sind alle Politiker bis auf einen bestechlich.

Aus *Smullyan: Dame oder Tiger, Fischer, 1992*

Beobachtungen:

- Diese Weisheiten können nicht in Aussagenlogik formalisiert werden, denn
  - wir wissen nicht, wie viele Politiker an der Versammlung teilnehmen.
  - wir wissen insbesondere nicht, welcher Politiker unbestechlich ist.
  - wir reden von der Eigenschaft, daß Politiker bestechlich sein können
  - wir reden von **allen** Politikern und von der **Existenz** eines unbestechlichen Politikers.

Beispiel: Weisheiten

- Von je zwei Politikern einer Versammlung von Politikern ist wenigstens einer bestechlich.
- Ein Politiker der Versammlung ist unbestechlich.
- Also sind alle Politiker bis auf den einen bestechlich.

Weisheiten als Formeln:

- $\forall p_1 \forall p_2$: $inVersammlung(p_1) \wedge inVersammlung(p_2) \wedge \neg(p_1 = p_2)$
  $\rightarrow istBestechlich(p_1) \vee istBestechlich(p_2)$
- $\exists p$: $inVersammlung(p) \wedge \neg istBestechlich(p)$
- $\exists p_1$: $inVersammlung(p_1) \wedge \neg istBestechlich(p_1)$
  $\rightarrow \forall p_2$: $inVersammlung(p_2) \wedge \neg(p_1 = p_2) \rightarrow istBestechlich(p_2)$

Abkürzungen: $\forall x \in U: p$ statt $\forall x: x \in U \rightarrow p$

$\forall x,y: p$ statt $\forall x \forall y: p$ (U implizit bekannt)

(entsprechend für $\exists$, oft ohne Doppelpunkt oder durch Punkt ersetzt)

4.2 Beispiel: Sortieren

Eingabe: Daten (beliebiger Anzahl) in irgendeiner Reihenfolge

Ausgabe: dieselben Daten wie in der Eingabe, aber sortiert

Probleme:

- Wie sehen diese Daten aus?
- Was heißt *Reihenfolge*?
- Was heißt *sortiert*?
- Was heißt *dieselben* Daten?

Wie sehen die Daten aus?

- Daten stammen aus einem Universum U. ($x \in U$)

Was heißt *Reihenfolge*?

- *Reihenfolge* heißt, daß die Daten in einer Liste (Monoid) angeordnet sind und die Elemente dieser Liste bilden. ($q \in U^*$, $x \in q$)

Was heißt *sortiert*?

- *sortiert* verlangt, daß U total geordnet ist mit einer Ordnung **≤**:

$$\forall x:\ x \in U \rightarrow x \leq x$$

$$\forall x\, \forall y:\ x \in U \wedge y \in U \wedge x \leq y \wedge y \leq x \rightarrow x = y$$

$$\forall x\, \forall y\, \forall z:\ x \in U \wedge y \in U \wedge z \in U \wedge x \leq y \wedge y \leq z \rightarrow x \leq z$$

$$\forall x\, \forall y:\ x \in U \wedge y \in U \rightarrow x \leq y \vee y \leq x$$

- *sortiert* bedeutet, daß die Elemente in einer Liste vorliegen, so daß alle Elemente z, die vor einem beliebigen Element x kommen, ≤ x sind:

$$\mathrm{isSorted}([])$$

$$\forall a{:}a \in U \rightarrow \mathrm{isSorted}([a])$$

$$\forall a\, \forall q{:}a \in U \wedge q \in U^* \wedge \neg(q = []) \wedge (\forall x{:}\ x \in q \rightarrow a \leq x) \wedge \mathrm{isSorted}(q)$$
$$\rightarrow \mathrm{isSorted}(\mathrm{append}([a], q))$$

4.2 Beispiel Sortieren: Antworten

Was heißt *dieselben* Daten ?

- *dieselben* Daten heißt, daß alle Elemente der Eingabeliste auch in der Ausgabeliste vorkommen und umgekehrt, auch mit der selben Vielfachheit anz. Dazu Prädikat „ist Permutation“:

$$\forall x \in U: anz(x, []) = 0$$

$$\forall x \in U: anz(x,[x]) = 1$$

$$\forall x \in U\ \forall y \in U: x \neq y \rightarrow anz(x,[y]) = 0$$

$$\forall x \in U\ \forall q,q',q'' \in U^*: q = append(q',q'') \rightarrow anz(x,q) = anz(x,q') + anz(x,q'')$$

$$\forall q\ \forall q': isPerm(q, q') \leftrightarrow \forall x \in U: anz(x, q) = anz(x, q')$$

Eingabe: $q \in U^*$

Ausgabe: $sort(q) \in U^*$

Ausgabebedingungen: $isPerm(q, sort(q)) \wedge isSorted(sort(q))$

4.2 Formeln der Prädikatenlogik 1. Stufe (I)

Alphabet ist ein Tripel $\mathcal{A} = (V, \Sigma, \Pi)$ mit

- V ist Menge von **Variablen**
- Σ ist Signatur von **Funktionssymbolen**
- $\Pi = \Pi^{(1)} \cup \Pi^{(2)} \cup \ldots$ ist Menge von Prädikats- oder Relationssymbolen
  - $p \in \Pi^{(n)}$ heißt n-stelliges Prädikatsymbol

Terme entstammen der initialen Grundtermalgebra $\mathcal{I}(\Sigma, V)$ über der Signatur Σ mit Variablen V:

- Jede Variable $x \in V$ ist ein Term.
- Wenn $f/n \in \Sigma$, und $t_1, t_2, \ldots, t_n$ Terme sind, dann ist auch $f(t_1, \ldots, t_n)$ ein Term

4.2 Formeln der Prädikatenlogik 1. Stufe (II)

atomare Formeln: Wenn $t_1, \ldots, t_n$ Terme und $p \in \Pi^{(n)}$ n-stelliges Prädikatsymbol ist, dann ist $p(t_1, \ldots, t_n)$ eine atomare Formel

Formeln:

- Jede atomare Formel ist eine Formel
- Wenn F und G Formeln sind, so auch $\neg F$, $F \vee G$ und $F \wedge G$
- Wenn F Formel und $x \in V$ Variable ist, dann ist auch „$\forall x$: F“ und „$\exists x$: F“ eine Formel

Die Quantoren können sich nur auf Termvariable beziehen

Prädikatenlogik 2. Stufe:

es gibt auch Variable für Prädikate und Quantoren können sich auch auf Prädikatsvariable beziehen

- $\forall p: p(X) \rightarrow \ldots$ „für alle Eigenschaften p von X gilt …“

4.2 gebundene und freie Variable (I)

Variable x komme in einer Formel F vor.

- x heißt **gebunden in F**, wenn
  - F hat die Form $\forall x$: F' oder $\exists x$: F'
    (F' heißt Wirkungsbereich des Quantors $\forall x$ bzw. $\exists x$)
  - x kommt nur in einer Teilformel vor, z.B. $F = p(y) \land \forall x: q(x)$
- x heißt **frei in F**, wenn es außerhalb des Wirkungsbereichs eines Quantors $\forall x$ bzw. $\exists x$ vorkommt
- x kann sowohl frei als auch gebunden sein, z.B. in $p(x,y) \land \forall x: q(x)$

$\forall n: \; n \in \mathbb{N} \;\rightarrow\; 0 + n = n$

alle Variablen n sind durch den Quantor $\forall$ n gebunden

$n \in \mathbb{N} \;\land\; \forall n \in \mathbb{N} \;\rightarrow\; \neg succ(n) = n$

Das erste n ist frei. Die anderen n sind gebunden.

$\forall n: (n \in \mathbb{N} \;\rightarrow\; \exists\, n: n = 0)$

Wirkungsbereich des Allquantors: $n \in \mathbb{N} \;\rightarrow\; \exists n: \; n = 0$

Aber nur das erste n ist an den Allquantor gebunden. Für die anderen **verdeckt** der Existenzquantor die Variable des Allquantors.

4.2 Interpretation

- Gegeben sei ein Alphabet $\mathcal{A}$ = (V, Σ, Π) und eine **Struktur** **A** = (U,I)
  - U ist nichtleere Menge, der **Individuenbereich** oder das **Universum** von **A**
  - I ist (partielle) Abbildung, die den $f^{(m)} \in \Sigma$ Abbildungen If: $U^m \to U$ und den Prädikaten $p^{(n)} \in \Pi$ Relationen Ip $\subseteq U^n$ zuordnet
- **Belegung** $\alpha: V \to U$ der Variablenmenge von $\mathcal{A}$ in das Universum U
- **Interpretation** $\mathcal{J}$, gegeben durch (**A**,α), bildet alle Variablen, Terme und Prädikate in das Universum U und Relationen über U ab
  - $\mathcal{J}(\neg F) = \begin{cases} w & \text{wenn } \mathcal{J}(F) = f \\ f & \text{wenn } \mathcal{J}(F) = w \end{cases}$
  - $\mathcal{J}(F \wedge G) = \begin{cases} w & \text{wenn } \mathcal{J}(F) = w \text{ \textbf{und} } \mathcal{J}(G) = w \\ f & \text{sonst} \end{cases}$
  - $\mathcal{J}(F \vee G) = \begin{cases} w & \text{wenn } \mathcal{J}(F) = w \text{ \textbf{oder} } \mathcal{J}(G) = w \\ f & \text{sonst} \end{cases}$
  - $\mathcal{J}(\forall x\colon F) = \begin{cases} w & \text{wenn } \mathcal{J}\,[a/x]\,(F) = w \text{ \textbf{für alle} } a \in U \\ f & \text{sonst} \end{cases}$
  - $\mathcal{J}(\exists x\colon F) = \begin{cases} w & \text{wenn } \mathcal{J}\,[a/x]\,(F) = w \text{ \textbf{für mindestens} ein } a \in U \\ f & \text{sonst} \end{cases}$

$\mathcal{J}$ [a/x] (F): a für alle in F freien x einsetzen, dann $\mathcal{J}$ anwenden

4.2 Modelle, Folgerungsbegriff

- Interpretation $\mathcal{I}$ heißt Modell für Formel (oder Formelmenge) F, $\mathcal{I} \models F$, wenn $\mathcal{I}(F) = w$
- F heißt erfüllbar/unerfüllbar/allgemeingültig, wenn es ein Modell gibt/nicht gibt/für alle Interpretationen $\mathcal{I}(F) = w$ gilt

- Wie für die Aussagenlogik gibt es für die Prädikatenlogik erster Stufe Kalküle K, um aus einer Formelmenge $\mathcal{F}$ eine Formel F in endlich vielen Schritten zu folgern, $\mathcal{F} \vdash F$

- Korrektheit eines Kalküls: Wenn $\mathcal{F} \vdash F$ dann $\mathcal{F} \models F$
- Vollständigkeit eines Kalküls (Gödel 1930): Wenn $\mathcal{F} \models F$ dann $\mathcal{F} \vdash F$

(bis hierher alles wie in der Aussagenlogik)

- **Unentscheidbarkeit der Prädikatenlogik 1. Stufe (Church 1936)**: Es gibt keinen Algorithmus, der in endlich vielen Schritten entscheidet, ob $\mathcal{F} \vdash F$ gilt
- **Unvollständigkeit der Prädikatenlogik 2. Stufe (Gödel)**: Die Menge der semantisch korrekten Formeln der Prädikatenlogik 2. Stufe ist nicht aufzählbar

4.2 Struktur und Modell (I)

Beispiel: Formel F = $\exists x\ \exists y\ \exists z\ \ (P(x, y, z)\ \wedge\ P(x, z, y)\ \wedge\ P(z, y, x))$

Struktur **A** = (U,I) mit:

$U = \mathbb{N} \setminus \{0\}$

$P = \{\ (r, s, t)\ \mid\ r, s, t \in \mathbb{N},\ \ r < s \leq t\ \}$

Ist **A** ein Modell für die Formel F?

$P(x, y, z)$	$P(x, z, y)$	$P(z, y, x)$
ist wahr für:	ist wahr für:	ist wahr für:
$x < y$	$x < z$	$z < y$
$x < z$	$x < y$	$z < x$
$y \leq z$	$z \leq y$	$y \leq x$

Widerspruch

Die Struktur ist also kein Modell für die Formel.

4.2 Struktur und Modell (II)

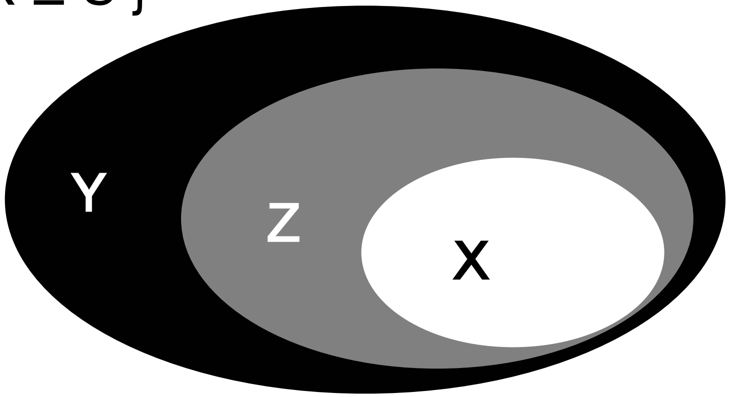
Beispiel: Formel $F = \exists x \exists y \exists z \; (P(x, y) \wedge P(z, y) \wedge P(x, z) \wedge \neg P(z, x))$

Struktur $\mathbf{A} = (U,I)$ mit:

$U = \mathscr{P}(\mathbb{N})$

$P = \{ (R, S) \mid R, S \subseteq \mathbb{N}, \; R \subseteq S \}$

Ist $\mathbf{A}$ ein Modell für die Formel F?



Relationen:

$P(x,y) = \{ (X, Y) \mid X, Y \subseteq \mathbb{N}, \; X \subseteq Y \}$

$P(z,y) = \{ (Z, Y) \mid Z, Y \subseteq \mathbb{N}, \; Z \subseteq Y \}$

$P(x,z) = \{ (X, Z) \mid X, Z \subseteq \mathbb{N}, \; X \subseteq Z \}$

1. Aus $m \in X$ folgt $m \in Z$, damit IP(x,z) wahr ist.
2. Aus $m \in Z$ folgt $m \in Y$, damit IP(z,y) wahr ist.
3. Daher gilt $x \in Y$, wenn $m \in X$; somit gilt IP(x, y).
4. Sei nun $X \neq Z$, $m \in Z \setminus X$, also $m \notin X$, dann ist ¬IP(z, x) erfüllt.

Aus 1.- 4. folgt: Struktur $\mathbf{A}$ ist ein Modell für die Formel: wähle $X \subsetneq Z \subseteq Y$.

4.2 Rechenregeln für Quantoren

Aus der Definition einer Interpretation folgt, daß die folgenden Umformungen bei Formeln mit Quantoren semantisch korrekt sind:

- eine gebundene Variable x darf in einer Formel Qx: F durch eine Variable y ersetzt werden, **wenn y in F nicht frei vorkommt**.
  Neue Form: Qy: F[y/x] (mit $Q \in \{ \forall, \exists \}$)
- es gilt $\neg\exists x: F = \forall x: \neg F$, $\neg\forall x: F = \exists x: \neg F$
- $F_1 \vee Qx: F_2 = Qx: F_1 \vee F_2$, $F_1 \wedge Qx: F_2 = Qx: F_1 \wedge F_2$,
  wenn x in F_1 nicht frei vorkommt
- $\forall x\ \forall y: F = \forall y\ \forall x: F$
- **Achtung:** $(\exists y\ \forall x: F) \rightarrow (\forall x\ \exists y: F)$ **aber nicht umgekehrt**
  - **Beispiel**: Stetigkeitsdefinition in der Analysis
- also: man darf Variable umbenennen, Negation mit Vertauschung $\forall \leftrightarrow \exists$ durchziehen, Quantoren vorziehen und Allquantoren untereinander vertauschen
- **man darf nicht immer Existenz- und Allquantoren vertauschen**

4.2 Normalformen (I)

Eine Folge von Quantoren $P = Qx_1 \ldots Qx_k$, $Q \in \{ \forall, \exists \}$ heißt **Präfix** einer Formel $F = PF' = Qx_1 \ldots Qx_k\, F'$.
F befindet sich in **pränexer Normalform**, wenn F' quantorenfrei ist.

Es gilt der Satz:

Jede prädikatenlogische Formel F kann in eine äquivalente Formel G in pränexer Normalform überführt werden.

Beispiel:

- $F = \forall x \exists y \; (p(x) \land q(x, y)) \lor \neg\forall x \; r(x)$
  Beseitigung der negierten Quantoren und Bereinigung von F:
- $F' = \forall x \exists y \; (p(x) \land q(x, y)) \lor \exists z \neg r(z)$
  Quantoren vorziehen:
- $F'' = \forall x \exists y \exists z \; (p(x) \land q(x, y)) \lor \neg r(z)$
  F''ist in pränexer Normalform.

Eine pränexe Normalform kann leider nicht so standardisiert werden, daß zu Beginn die Allquantoren und dahinter die Existenzquantoren kommen. Es gibt aber eine semantisch äquivalente Normalform, die nur noch die Allquantoren aufweist.

Satz: Zu jeder prädikatenlogischen Formel F gibt es eine Formel G mit

- $G = \forall x_1 \dots \forall x_k\, G'$, $k \geq 0$
- G' quantorenfrei
- F ist genau dann erfüllbar, wenn G erfüllbar ist.

- G heißt Skolemform von F
  Die Skolemform erreicht man, indem man die durch Existenzquantoren gebundenen Variablen nacheinander durch Skolemfunktionen ersetzt, die von den Variablen der vorausgehenden Allquantoren abhängt.

Beispiel: $\forall u\ \exists v\ \forall x\ \exists y\colon p(u,v,x,y)$

wird ersetzt durch die Skolemform $\forall u\ \forall x\colon p\ (u,sk_v(u),x,sk_y(u,x))$

4.2 Satz von Herbrand

Jacques Herbrand, 1908-1935, französischer Logiker

- Gegeben sei eine Formel (oder Formelmenge) F, $\Sigma_F \subseteq \Sigma$ sei die Menge der in F vorkommenden Funktionssymbole
  - enthält Σ_F kein 0-stelliges Funktionssymbol, so nehmen wir noch ein solches hinzu
- Die initiale Grundtermalgebra $G_0(\Sigma_F)$ heißt Herbrand-Universum $\mathcal{H}(F)$ zu F.
- Ist $\mathcal{I} = (\mathbf{A},\alpha)$ ein Modell der Formel F ohne freie Variable (geschlossene Formel), so kann man daraus ein Modell $\mathcal{I}' = (\mathcal{H}(F), \alpha)$ über dem Herbrand-Universum, die Herbrand-Interpretation, herleiten
- Die Herbrand-Interpretation $\mathcal{I}'$ erfüllt ebenfalls F und heißt ein Herbrand-Modell.

Satz von Herbrand: Wenn eine Formel ohne freie Variable kein Herbrand-Modell besitzt, so ist sie unerfüllbar.

4.2 Horn-Klauseln, Resolutionskalkül

Alfred Horn, norwegischer Logiker

- Gegeben seien atomare Formeln $p_1,\ldots,p_m,q$
- Hornklausel: $p_1 \wedge p_2 \wedge \ldots \wedge p_m \rightarrow q = \neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_m \vee q$
  - Implikation: $m \geq 1$
  - Faktum: $m = 0$
  - Anfrage: q fehlt
- Resolution (*Robert Kowalski*): gegeben eine Hornformel $\mathcal{H}$, beweise, daß eine Anfrage G in $\mathcal{H}$ erfüllbar ist. Es gilt $\mathcal{H} \rightarrow G$ mit geeigneter Variablenbelegung, wenn die Negation $\neg(\mathcal{H} \rightarrow G) = \neg(\neg\mathcal{H} \vee G) = \mathcal{H} \wedge \neg G$ unerfüllbar ist
  - wende dazu den Satz von Herbrand an: $\mathcal{H} \wedge \neg G$ ist unerfüllbar, wenn es ein Gegenbeispiel, d.h. ein Modell für $\mathcal{H} \rightarrow G$, gibt
- In der Prädikatenlogik: $p_1,\ldots,p_m,q$, G sind atomare Prädikate über der initialen Grundtermalgebra $\mathcal{I}(\Sigma_F, V)$ mit Variablen
  - alle Variablen sind all-quantifiziert (implizit, Allquantor nicht explizit geschrieben)
  - dem Gegenbeispiel liegt eine Belegung $\alpha: V \rightarrow G_0(\Sigma_F)$ zugrunde
  - ermittle α durch Unifikation: bestimme allgemeinsten Unifikator

Alain Colmerauer, französischer Informatiker

- Idee von Prolog:
  - wende Resolution auf Hornklauseln an
  - mache das Verfahren deterministisch, indem die Klauseln in fester Reihenfolge vorgegeben werden
  - unifiziere die Anfrage G mit dem „Kopf“ q der ersten dazu geeigneten Hornklausel H; lautet diese $p_1 \wedge p_2 \wedge \ldots \wedge p_m \rightarrow q$, so füge $p_1\sigma,\ldots,p_m\sigma$ der Liste zu erfüllender Anfragen hinzu
    - σ: durch die bisherigen Unifikationen definierte Variablensubstitution
    - Immer die zuletzt der Liste zugefügte Anfrage wird als erstes bearbeitet
  - läßt sich G so nicht erfüllen, so suche die in der Reihenfolge nach H nächste passende Hornklausel H'
  - Gibt es keine solche Hornklausel H', so schlägt die Anfrage G fehl: es wird kein Modell für G gefunden

negation by failure: Wird kein Modell gefunden, so heißt das noch nicht, daß das Gegenteil wahr ist!

4.2 Prolog: Schreibweise

- Konventionen:
  - Variablenbezeichner beginnen mit Großbuchstaben, alle anderen Bezeichner mit Kleinbuchstaben
  - _ ist ein Variablenbezeichner wechselnder Identität

- Hornklauseln $p_1 \wedge p_2 \wedge \ldots \wedge p_m \rightarrow q$
  - Implikation: q :- $p_1, \ldots, p_m$. Komma statt $\wedge$, abschließender Punkt
  - Faktum: q . abschließender Punkt
  - Anfrage: ?- G . abschließender Punkt

4.2 Beispiel: formales Differenzieren

Prolog-Programm:

```
diff(X,X,1).
diff(C,X,0)                    :- atomic(C), not(C=X).
diff(U+V,X,DU+DV)              :- diff(U,X,DU), diff(V,X,DV).
diff(U-V,X,DU-DV)              :- diff(U,X,DU), diff(V,X,DV).
diff(U*V,X,U*DV+V*DU)          :- diff(U,X,DU), diff(V,X,DV).
diff(U/V,X,(V*DU-U*DV)/(V*V))  :- diff(U,X,DU), diff(V,X,DV).
```

Anfragen:

```
?- diff(x*x,x,E).
E = x*1 + 1*x
?- diff(a*x+b,x,E).
E = a*1+x*0+0
?- diff(x^2,x,E)
no
```

4.2 Beispiel: formales Differenzieren


```
diff(X,X,1).
diff(C,X,0)                      :- atomic(C), not(C=X).
diff(C+U,X,D)                    :- atomic(C), not(C=X), diff(U,X,D).
diff(U+C,X,D)                    :- atomic(C), not(C=X), diff(U,X,D).
diff(U+V,X,DU+DV)                :- diff(U,X,DU), diff(V,X,DV).
diff(U-V,X,DU-DV)                :- diff(U,X,DU), diff(V,X,DV).
diff(C*X,X,C)                    :- atomic(C), not(C=X).
diff(C*U,X,C*D)                  :- atomic(C), not(C=X), diff(U,X,D).
diff(U*C,X,C*D)                  :- atomic(C), not(C=X), diff(U,X,D).
diff(U*V,X,U*DV+V*DU)            :- diff(U,X,DU), diff(V,X,DV).
diff(U/V,X,(V*DU-U*DV)/(V*V))    :- diff(U,X,DU), diff(V,X,DV).

?- diff(x*x,x,E).
E = x*1 + x*1
?- diff(a*x+b,x,E).
E = a
```

4.2 Beispiel: formales Differenzieren

```
diff(X,X,1).
diff(C,X,0)        :- atomic(C), not(C=X).
diff(U+V,X,E)      :- diff(U,X,DU), diff(V,X,DV), einfach(DU+DV,E).
diff(U-V,X,E)      :- diff(U,X,DU), diff(V,X,DV), einfach(DU-DV,E).
diff(U*V,X,E)      :- diff(U,X,DU), diff(V,X,DV), einfach(U*DV+V*DU,E).
diff(U/V,X,E)      :- diff(U,X,DU), diff(V,X,DV, einfach((V*DU-U*DV)/(V*V),E).
einfach(0+U,E)           :- einfach(U,E).
einfach(U+0,E)           :- einfach(U,E).
einfach(U*1+V,E)         :- einfach(U+V,E).
einfach(1*U+V,E)         :- einfach(U+V,E).
einfach(U*0+V,E)         :- einfach(V,E).
…
einfach(U+V,E)           :- einfach(U,U1), not(U=U1),
                            einfach(V,V1), einfach(U1+V1,E).
…
einfach(U,U).
?- diff(x*x,x,E).
E = x + x
?- diff(a*x+b,x,E).
E = a
```

2.3 Eigenschaften von Halbordnungen – ÄNDERUNG

Gegeben: Halbordnung (U, ≤)

fundierte Ordnung: **jede nichtleere Teilmenge X von U enthält mindestens ein minimales Element $x \in X$**

Beispiel: $(\mathbb{N}, \leq)$, aber $(\mathbb{Z}, \leq)$ ist nicht fundiert

artinsche Ordnung: (*Emil Artin, 1898-1962, dt. Mathematiker*)
jede absteigende Kette $\ldots \leq a_{-i} \leq \ldots \leq a_{-1} \leq a_0$ bricht ab.

Beispiel: $(\mathbb{N}, \leq)$

noethersche Ordnung: (*Emmy Noether, 1882-1935, dt. Mathematikerin*)
jede aufsteigende Kette $a_0 \leq a_1 \leq \ldots \leq a_i \leq \ldots$ bricht ab.

Beispiel: „$\Rightarrow^*$" eines terminierenden Semi-Thue-System

Ausblick: Diese Eigenschaften spielen eine wichtige Rolle bei Korrektheits- und Terminierungsbeweisen

Satz: $(U, \leq)$ ist genau dann fundiert, wenn sie artinsch ist.

Beweis:

„⇒“ Sei $(U, \leq)$ fundiert.

Jede Kette K ist Teilmenge von U

$K \subseteq U \Rightarrow \inf(K) \in K$

„⇐“ Sei $(U, \leq)$ artinsch.

Annahme: Es gibt $X \subseteq U$ ohne minimales Element $x \in X$

Sei $x_0 \in X$

$\Rightarrow$ es gibt $x_1 \in X$, mit $x_1 \leq x_0$ und $x_1 \neq x_0$, also $x_1 < x_0$

$\Rightarrow$ Induktion ergibt nicht abbrechende Kette $x_0 > x_1 > x_2 > \ldots$

$\Rightarrow$ Widerspruch!