

WS 2016/17

Diskrete Strukturen

Kapitel 2: Grundlagen (Prädikatenlogik)

Hans-Joachim Bungartz

Lehrstuhl für wissenschaftliches Rechnen

Fakultät für Informatik

Technische Universität München

[http://www5.in.tum.de/wiki/index.php/Diskrete Strukturen - Winter 16](http://www5.in.tum.de/wiki/index.php/Diskrete_Strukturen_-_Winter_16)

- Prädikatenlogik:

- Die Korrektheit des Arguments

Wenn (alle X sind Y) und (Z ist ein X), dann (Z ist ein Y).

kann mit der Aussagenlogik nicht nachgewiesen werden.

- Intuitiver Grund: Die Aussagenlogik formalisiert nur die Begriffe „und“, „oder“, „nicht“, „wenn...dann“, aber **nicht** die Begriffe „für alle“ oder „ist“. Die Korrektheit des Argumentes hängt aber von den Letzten ab. Vergleiche:

- Wenn A und B, dann C;
- Wenn „alle A sind B“ und „C ist A“ dann „C ist B“.

- Prädikatenlogik: Aussagenlogik + „für alle“, „es gibt“ + „ist“.



- Praktische Anwendungen der Prädikatenlogik:
 - Zur formalen Spezifikation komplexer Systeme.
 - Zum automatischen Beweisen von Theoremen.
 - Zur automatischen Verifikation von Programmen.
 - Zur Spezifikation von Abfragen in Datenbanken.
 - Und viele mehr.



- **Subjekte und Prädikate:**
 - In dem Satz „*Sokrates ist sterblich*“ ist „*Sokrates*“ das **Subjekt** (das Individuum, von dem etwas behauptet wird) und „*ist sterblich*“ das **Prädikat** (die Eigenschaft, die von dem Individuum behauptet wird).
 - In der Prädikatenlogik wird ein Prädikat als eine Abbildung $P(\cdot)$ von **Individuen** auf **Aussagen** aufgefasst, z.B.:
$$P(x) = \text{„}x \text{ ist-sterblich“}.$$
(wobei x eine Variable ist, die mit Individuen instanziiert wird).
 - Aus logischer Sicht ist „*Sokrates ist sterblich*“ eine Abkürzung für „*das Individuum Sokrates hat die Eigenschaft, sterblich zu sein*“.



- Mehrstellige Prädikate:
 - Der Satz „*Anna liebt Bernhard*“ kann aus logischer Sicht als Abkürzung für
 „*Anna hat die Eigenschaft, Bernhard zu lieben*“ betrachtet werden.
 - Dann muss jedoch ein Prädikat für jedes Individuum eingeführt werden: „*Bernhard zu lieben*“, „*Cesar zu lieben*“, „*Daniel zu lieben*“, ...
 - Stattdessen wird „*Anna liebt Bernhard*“ als ein Satz **über das Paar (Anna, Bernhard)** betrachtet. Das Prädikat ist:
 „*das erste Individuum liebt das zweite Individuum*“.



- Mehrstellige Prädikate:
 - In der Prädikatenlogik wird das durch ein zweistelliges Prädikat $P(\cdot, \cdot)$ modelliert.
 - $P(\cdot, \cdot)$ bildet **Paare von Individuen** auf Aussagen ab, z.B.: $P(x, y) = \text{„}x \text{ liebt } y\text{“}$ (wobei x, y Variablen sind, die mit den Individuen instanziiert werden können).
 - Prädikate höherer Arität sind auch möglich.



- Funktionen:

- In dem Satz „*Die Mutter von Sokrates ist sterblich*“ ist „*Mutter von*“ eine Funktion, die jeden Mensch auf seine Mutter abbildet.
- In der Prädikatenlogik wird eine Funktion als eine Abbildung $f(\cdot)$ von **Individuen** auf **Individuen** modelliert, z.B.:

$$m(x) = \text{„Mutter von } x\text{“}$$

(wobei x eine Variable ist, die mit den Individuen instanziiert werden kann).

- Funktionen können höhere Arität haben.
Beispiel: Im Satz „*Die Summe der Zahlen 3 und 5 ist 8*“ ist „*Summe*“ eine Funktion der Arität 2.



- Syntax der Prädikatenlogik:
 - Das Vokabular setzt sich aus folgenden Zeichenklassen zusammen:
 - (Individuen)variablen: x, y, z, \dots
 - Konstanten: a, b, c, \dots (z.B. 13, π)
 - Wahrheitskonstanten: true, false;
 - Prädikatsymbole: P^k, Q^k, R^k, \dots
 - Funktionssymbole: f^k, g^k, h^k, \dots
mit Stelligkeit $k = 0, 1, 2, \dots$
 - Gleichheitssymbol: =
 - Logische Operatoren: $\neg, \wedge, \vee, \rightarrow$
 - Quantoren: \forall („für alle“), \exists („es gibt“)
 - Hilfssymbole: (,)



- Syntax der Prädikatenlogik:
 - Formationsregeln:
 - Regel 0:** Jede Variable und jede Konstante ist ein **Term**.
 - Regel 1:** Sind t_1, \dots, t_n Terme, dann ist $f^n(t_1, \dots, t_n)$ ebenfalls ein **Term**.
 - Regel 2:** Sind t_1, \dots, t_n Terme, dann ist $P^n(t_1, \dots, t_n)$ eine **Formel**.
 - Regel 3:** Sind t und u Terme, dann ist $t = u$ eine **Formel**.



- Syntax der Prädikatenlogik:
 - Formationsregeln:
 - Regel 4:** Ist F eine Formel, dann ist auch $\neg F$ eine Formel.
 - Regel 5:** Sind F und G Formeln, dann sind $(F \wedge G)$, $(F \vee G)$ und $(F \rightarrow G)$ ebenfalls Formeln.
 - Regel 6:** Ist x eine Variable und F eine Formel, dann sind $\forall x F$ und $\exists x F$ ebenfalls Formeln.



- Aufgabe: Formeln oder Nicht-Formeln?

$$P^1(x)$$

x

$$\forall x (f(x) \wedge P^1(x))$$

$$\forall x \exists y (x = y \vee \neg Q^1(y))$$

$$x = P^1(x)$$

$$\forall x P^1(x) = Q^1(f(g(x)))$$

$$\exists x \forall x (P^1(x) \wedge Q^2(x, b))$$

$$\exists x f(x)$$

$$(\forall x P^1(a) \wedge Q^1(x))$$

$$\forall P^1 \exists x P^1(x)$$

$$P^1(x, y)$$

$$\left((P^1(x) \wedge Q^2(a, y)) \vee f(x) = y \right)$$



- Syntax der Prädikatenlogik:

- Die Stelligkeit der Prädikat- und Funktionssymbole lassen wir oft weg. Wir nehmen an, dass alle Vorkommnisse eines Symbols dieselbe Stelligkeit haben.

Beispiel: $\forall x \forall y (P(x, y) \rightarrow P(y, x))$.

Achtung: $\forall x (P(x) \wedge P(x, x))$ ist **keine** Formel!

- Manchmal lassen wir Klammern weg, oder fügen welche hinzu. Dabei nehmen wir an, dass Quantoren stärker als Konjunktion, Disjunktion und Implikation binden:

$\forall x P(x) \wedge Q(y)$ ist die Formel $(\forall x P(x)) \wedge Q(y)$ und nicht $\forall x (P(x) \wedge Q(y))$.



- Syntax der Prädikatenlogik:
 - Der Gültigkeitsbereich eines Vorkommens einer Variablen x in einer Formel F ist die kleinste Unterformel von F der Gestalt $\forall x G$ oder $\exists x G$, welche das Vorkommen enthält.

Wenn es diese Unterformel nicht gibt, dann ist der Gültigkeitsbereich die Formel F selbst.

- Im ersten Fall heißt das Vorkommen **gebunden**, sonst ist das Vorkommen **frei**.
- Eine Formel ohne freie Vorkommnisse von Variablen heißt **geschlossen**.



- Syntax der Prädikatenlogik:
 - Beispiele:

$$\exists x P(x) \wedge Q(x).$$

Erstes Vorkommen von x ist gebunden,
zweites frei.

$$\forall x (P(x) \wedge \exists y (P(y) \vee Q(x, y))).$$

Die Formel ist geschlossen.



- Syntax der Prädikatenlogik:
 - Später werden wir definieren, wann zwei Formeln äquivalent sind.
 - Es wird Folgendes gelten: Jede Formel ist äquivalent zu einer **bereinigten** Formel, in der
 - keine Variable sowohl gebunden als auch frei vorkommt, und
 - hinter allen vorkommenden Quantoren verschiedene Variablen stehen.
 - Meistens werden Formeln in bereinigter Form dargestellt. In diesem Fall kann man von freien und gebundenen Variablen einer Formel sprechen.



- Aufgabe:

	Nicht-Formel	Formel	Bereinigte Formel
$\forall x P(a)$			
$\forall x \exists y (P(x, y) \vee Q(x, y))$			
$\forall x Q(x, x) \rightarrow \exists x Q(x, y)$			
$\forall x P(x) \vee \forall x Q(x, x)$			
$\forall x (P(x) \wedge \forall y P(x))$			
$P(x) \rightarrow \exists x Q(x, P(x))$			
$\forall x \exists x P(x, f(x))$			



- Semantik der Prädikatenlogik – Intuition:
 - Die Semantik einer Formel ist die Funktion, die jeder möglichen „Welt“, die zur Formel „passt“, den Wahrheitswert der Formel (0 oder 1) in dieser „Welt“ zuordnet.
 - Eine Welt, die zu $F = \forall x P(a, x)$ passt, und in der F **wahr** ist (meiner Meinung nach ...).
 - Die Individuen der Welt sind alle lebenden Schauspielerinnen.
 - a ist Emma Stone.
 - $P(y, x)$ bedeutet „ y ist mindestens so attraktiv wie x “.



- Semantik der Prädikatenlogik – Intuition:
 - Eine Welt, die zu $F = \forall x P(a, x)$ passt, und in der F falsch ist (diesmal mit Sicherheit).
 - Die Individuen der Welt sind die natürlichen Zahlen.
 - a ist die 7.
 - $P(y, x)$ bedeutet „ y ist ein Vielfaches von x “.



- Semantik der Prädikatenlogik – Intuition:
 - Eine Welt, die zu $F = \forall x P(a, x)$ nicht passt.
 - Die Individuen der Welt sind alle lebenden Schauspielerinnen.
 - $P(y, x)$ bedeutet „ y ist mindestens so attraktiv wie x “.
 - ...und noch eine.
 - Die Individuen der Welt sind die natürlichen Zahlen.
 - a ist die 0.
 - Die Frage nach dem Wahrheitswert einer Formel in einer Welt, die zur Formel nicht passt, ist sinnlos.
 - Eine „passende Welt“ für $\forall x P(y, x)$ muss der freien Variable y ein Individuum zuordnen (das Individuum, auf das y „zeigt“).



- Formale Semantik der Prädikatenlogik:
 - Das Fachwort für „Welt“ ist **Struktur**.
 - Eine **Struktur** S besteht aus zwei Teilen:
 - Eine nichtleere Menge U_S , genannt **Universum** (Wertebereich, Individuenbereich, Grundmenge, Domäne, ...)
„Die Menge aller Individuen der Welt“.
 - Eine **Interpretation** I_S .



- Formale Semantik der Prädikatenlogik:
 - Die **Interpretation** I_S ist eine partielle Funktion, die
 - einer Variablen x ein Element x_S von U ,
 - einer Konstante a ein Element a_S von U ,
 - einem k -stelligen Prädikatsymbol P eine Menge $P_S \subseteq U^k$, und
 - einem k -stelligen Funktionssymbol f eine Funktion $f_S: U^k \rightarrow U$ zuordnet.



- Formale Semantik der Prädikatenlogik:
 - Intuition:
 - x_S ist das Individuum, auf das die Variable x „zeigt“.
 - a_S ist das Individuum mit dem Namen „ a “.
 - P_S ist die Menge der Tupel von Individuen mit der Eigenschaft P .
 - f_S ist die Funktion mit dem Namen f .
 - Beachte: P_S kann **extensional** beschrieben werden, wir zählen die Tupel von P_S auf. Ähnlich für f_S .
 - Das Universum kann jedoch **unendlich** sein!



- Formale Semantik der Prädikatenlogik:
 - Eine Struktur $S = (U_S, I_S)$ **passt** zu einer Formel F , falls die Interpretation I_S für alle in F vorkommenden Prädikatsymbole, Konstanten und **freien** Variablen definiert ist.
 - Beispiel: S passt zu $\forall x P(x, a, y)$, wenn a_S, y_S und P_S definiert sind.
 - Die Semantik einer Formel F ist eine Funktion $[F]$, die jeder Struktur S , die zu F passt, („jeder Welt“) einen Wahrheitswert $[F](S)$ zuordnet.



- Formale Semantik der Prädikatenlogik:
 - Beispiel: Einige passende Strukturen für die Formel

$$\forall x (P(x) \rightarrow \exists y Q(x, y)):$$

- Struktur $S_1 = (U_1, I_1)$:
 - $U_1 = \mathbb{N}_0$,
 - $P_1 = \{n \in \mathbb{N}_0 \mid n \text{ ist gerade}\}$,
 - $Q_1 = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n + m = 5\}$.
- Struktur $S_2 = (U_2, I_2)$:
 - $U_2 = \{0, 1, 2\}$,
 - $P_2 = \{0\}$,
 - $Q_2 = \{(n, m) \in \{0, 1, 2\} \times \{0, 1, 2\} \mid n \leq m\}$.



- Formale Semantik der Prädikatenlogik:
 - Beispiel: Einige passende Strukturen für die Formel

$$\forall x (P(x) \rightarrow \exists y Q(x, y)):$$

- Struktur $S_3 = (U_3, I_3)$:
 - $U_3 =$ die Menge M der Personen in diesem Hörsaal,
 - $P_3 =$ die Menge der Männer in diesem Hörsaal,
 - $Q_3 = \{ (n, m) \in M \times M \mid n \text{ ist mindestens so schlau wie } m \}$.
- Struktur $S_4 = (U_4, I_4)$:
 - $U_4 = \{ a, b \}$,
 - $P_4 = \{ a \}$,
 - $Q_4 = \{ (a, b), (b, a), (b, b) \}$.



- Formale Semantik der Prädikatenlogik:
 - Beispiel: Einige passende Strukturen für die Formel
$$\forall x (P(x) \rightarrow \exists y Q(x, y)):$$
 - Struktur $S_5 = (U_5, I_5)$:
 - $U_5 = \mathbb{N}_0$,
 - $P_5 = \emptyset$,
 - $Q_5 = \emptyset$.
 - Struktur $S_6 = (U_6, I_6)$:
 - $U_6 =$ die Menge der Fußballer, die am nächsten Samstag mindestens ein Tor in der 1. Bundesliga schießen werden,
 - $P_6 = \{f \in U_6 \mid f \text{ spielt für Borussia Dortmund}\}$,
 - $Q_6 = \{(f_1, f_2) \in U_6 \times U_6 \mid f_1 \text{ und } f_2 \text{ schießen am nächsten Sonntag gleich viele Tore}\}$.



- Formale Semantik der Prädikatenlogik:
 - Die Funktion $[F]$ ist folgendermaßen definiert in Abhängigkeit von F :

(1) Semantik der Formeln $P(u_1, \dots, u_n)$:

Sei $F = P(u_1, \dots, u_n)$.

$$[F](S) = \begin{cases} 1, & \text{falls } (u_{1S}, \dots, u_{nS}) \in P_S; \\ 0, & \text{falls } (u_{1S}, \dots, u_{nS}) \notin P_S. \end{cases}$$

(2) Semantik der Formeln $t = u$:

$$[t = u](S) = \begin{cases} 1, & \text{falls } t_S = u_S; \\ 0, & \text{falls } t_S \neq u_S. \end{cases}$$



- Formale Semantik der Prädikatenlogik:
 - Die Funktion $[F]$ ist folgendermaßen definiert in Abhängigkeit von F :

(3) Semantik der Booleschen Operatoren:

Wie für die Aussagenlogik. Beispiel:

Sei $F = (G \rightarrow H)$ für Formeln F und G .

$$[F](S) = \begin{cases} 1, & \text{falls } [G](S) = 0 \text{ oder } [H](S) = 1; \\ 0, & \text{falls } [G](S) = 1 \text{ und } [H](S) = 0. \end{cases}$$



- Formale Semantik der Prädikatenlogik:
 - Die Funktion $[F]$ ist folgendermaßen definiert in Abhängigkeit von F :

(4) Semantik der Quantoren:

Sei $S_{x:=d}$ die Struktur, die identisch mit S ist, bis auf die Tatsache, dass in $S_{x:=d}$ die Variable x auf das Individuum d „zeigt“, d.h., $x_{S_{x:=d}} = d$ (x_S kann nicht definiert sein oder auf ein anderes Individuum „zeigen“).



- Formale Semantik der Prädikatenlogik
 - Die Funktion $[F]$ ist folgendermaßen definiert in Abhängigkeit von F :

(4.1) Semantik des Existenzquantors:

$F = \exists x G$ für eine Formel G .

$$[F](S) = \begin{cases} 1, & \text{falls es ein } d \in U_S \text{ gibt mit } [G](S_{x:=d}) = 1; \\ 0, & \text{falls für alle } d \in U_S \text{ gilt: } [G](S_{x:=d}) = 0. \end{cases}$$

Sei $F = \exists x P(x)$, $U_S = \{a, b\}$, $P_S = \{a\}$.

Wir haben $[F](S) = 1$, denn $[P(x)](S_{x:=a}) = 1$.



- Formale Semantik der Prädikatenlogik:
 - Die Funktion $[F]$ ist folgendermaßen definiert in Abhängigkeit von F :

(4.2) Semantik des Allquantors:

$F = \forall x G$ für eine Formel G .

$$[F](S) = \begin{cases} 1, & \text{falls für alle } d \in U_S \text{ gilt: } [G](S_{x:=d}) = 1; \\ 0, & \text{falls es ein } d \in U_S \text{ gibt mit } [G](S_{x:=d}) = 0. \end{cases}$$

Sei $F = \forall x P(x)$, $U_S = \{a, b\}$, $P_S = \{a\}$.

Wir haben $[F](S) = 0$, denn $[P(x)](S_{x:=b}) = 0$.



- Geschachtelte Quantoren:
 - Formel: $F: \forall x \exists y P(x, y)$.
 - Struktur $S: U_S = \mathbb{N}_0$,
 $P_S = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n < m\}$,
(„ $P(x, y)$ bedeutet $x < y$ “).
 - **Frage:** Ist F wahr in S ?



- Geschachtelte Quantoren:
 - Formel $F: \forall x \exists y P(x, y)$.
 - Struktur $S: U_S = \mathbb{N}_0$,
 $P_S = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n < m\}$,
(„ $P(x, y)$ bedeutet $x < y$ “).
 - **Frage:** Ist F wahr in S ?
 - Ja. Intuitiv bedeutet F in S : „Für jede Zahl x gibt es eine größere Zahl y .“



- Geschachtelte Quantoren:

- Formel $F: \forall x \exists y P(x, y)$.

- Struktur $S: U_S = \mathbb{N}_0$,

- $P_S = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n < m\}$,

- („ $P(x, y)$ bedeutet $x < y$ “).

- **Frage:** ist F wahr in S ?

- Wir zeigen $[\forall x \exists y P(x, y)](S) = 1$ nach der Definition:

- Es reicht zu zeigen: $[\exists y P(x, y)](S_{x:=d}) = 1$ für $d = 0, 1, \dots$
 - Wir müssen also ein e finden mit $[P(x, y)](S_{x:=d, y:=e}) = 1$.
 - D.h.: Wir müssen ein e finden mit $d < e$.
 - Wir nehmen z.B. $e = d + 1$. Fertig.



- Geschachtelte Quantoren:
 - Formel $G: \exists y \forall x P(x, y)$.
 - Struktur $S: U_S = \mathbb{N}_0$,
 $P_S = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n < m\}$,
(„ $P(x, y)$ bedeutet $x < y$ “).
 - **Frage:** Ist G wahr in S ?



- Geschachtelte Quantoren:
 - Formel $G: \exists y \forall x P(x, y)$.
 - Struktur $S: U_S = \mathbb{N}_0$,
 $P_S = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n < m\}$,
(„ $P(x, y)$ bedeutet $x < y$ “).
 - **Frage:** ist G wahr in S ?
 - Nein. Intuitiv sagt G in S : „Es gibt eine Zahl, die größer ist als alle andere (sogar größer als sie selbst!).“



- Aufgabe:

Sei die Interpretation von $R(x, y)$:

„ x verlässt sich auf y .“

Welche Formel gehört zu welchem Satz?

1. $\forall x \exists y R(x, y)$ a) „Es gibt einen, der sich auf alle verlässt.“
2. $\exists y \forall x R(x, y)$ b) „Jeder kann sich auf jemanden verlassen.“
3. $\exists x \forall y R(x, y)$ c) „Auf jeden verlässt sich irgend jemand.“
4. $\forall y \exists x R(x, y)$ d) „Es gibt einen, auf den sich alle verlassen.“
5. $\forall x \forall y R(x, y)$ e) „Jeder verlässt sich auf alle.“



- Tautologie, Widerspruch, Erfüllbarkeit,...:
 - Eine Formel F ist **allgemeingültig** wenn für jede Struktur S , die zu F passt, gilt: $[F](S) = 1$.
 - Eine Formel F ist ein **Widerspruch** wenn für jede Struktur S , die zu F passt, gilt: $[F](S) = 0$.
 - Eine Formel F ist **erfüllbar** wenn es eine Struktur S gibt, die zu F passt, und $[F](S) = 1$ erfüllt.
 - Zwei Formeln F und G sind **logisch äquivalent** (symbolisch: $F \equiv G$) genau dann, wenn für jede Struktur S , die zu F und zu G passt, gilt: $[F](S) = [G](S)$.
 - G **folgt aus** F (symbolisch: $F \models G$) genau dann, wenn $F \rightarrow G$ gültig ist.



- S -Tautologien, S -Widersprüche,....:
 - Sei S eine Menge von Strukturen. Eine Formel ist S -gültig, wenn für alle Strukturen $S \in S$ gilt: $[F](S) = 1$.
 - Sei *null* eine Konstante und sei *nach* ein einstelliges Funktionssymbol.
 - Sei N die Menge aller Strukturen $S = (U_S, I_S)$ mit
 - $U_S = \mathbb{N}_0$,
 - $null_S = 0$,
 - $nach(n) = n + 1$,
 - (I_S kann für andere Konstanten und Prädikatensymbolen beliebig definiert sein).



- Tautologie, Widerspruch, Erfüllbarkeit,...:
 - Das **Induktionsprinzip** ist die Formel:
$$(P(\text{null}) \wedge \forall y (P(y) \rightarrow P(\text{nach}(y))) \rightarrow \forall x P(x).$$
 - In allen Strukturen aus \mathbb{N} „sagt“ diese Formel:
Wenn 0 die Eigenschaft P hat, und
für alle Zahlen n gilt: wenn n die Eigenschaft P hat,
dann hat auch $n + 1$ die Eigenschaft P ,
dann haben alle Zahlen die Eigenschaft P .
 - Das Induktionsprinzip ist nicht gültig, aber \mathbb{N} -gültig.



- Äquivalenz- und Folgerungsregeln für Quantoren:

De Morgan's:

$$\neg \forall x F \equiv \exists x \neg F,$$
$$\neg \exists x F \equiv \forall x \neg F.$$

Kommutativität:

$$\forall x \forall y F \equiv \forall y \forall x F,$$
$$\exists x \exists y F \equiv \exists y \exists x F,$$
$$\exists x \forall y F \not\equiv \forall y \exists x F.$$

Distributivität:

$$\forall x (F \wedge G) \equiv \forall x F \wedge \forall x G,$$
$$\exists x (F \vee G) \equiv \exists x F \vee \exists x G,$$
$$\forall x F \vee \forall x G \not\equiv \forall x (F \vee G),$$
$$\exists x (F \wedge G) \not\equiv \exists x F \wedge \exists x G.$$



- Äquivalenz- und Folgerungsregeln für Quantoren:

– Falls x in G nicht

frei vorkommt:

$$\exists x (F \wedge G) \equiv \exists x F \wedge G,$$

$$\exists x (F \vee G) \equiv \exists x F \vee G,$$

$$\forall x (F \wedge G) \equiv \forall x F \wedge G,$$

$$\forall x (F \vee G) \equiv \forall x F \vee G.$$



- Prädikatenlogik in der Mathematik:

Mathematiker mischen oft Notationen aus der Logik, der Arithmetik und der Mengenlehre. Z.B. schreiben sie

$$\forall x \in \mathbb{R}: \exists y \in \mathbb{R}: x \cdot y = 1.$$

- $x \in \mathbb{R}$ ist ein einstelliges Prädikat. Wir schreiben z.B. *Reell(x)*.
- $x \cdot y$ ist ein zweistelliges Funktionssymbol. Wir schreiben z.B. *prod(x, y)*.
- $\exists x \in \mathbb{R}: F$ ist eine Abkürzung für $\exists x(\text{Reell}(x) \wedge F)$.
- $\forall x \in \mathbb{R}: F$ ist eine Abkürzung für $\forall x(\text{Reell}(x) \rightarrow F)$.



- Formalisierung von Aussagen:
 - Aussagen werden durch eine Formel und eine Basisstruktur formalisiert.
 - Die Struktur legt die Bedeutung der Prädikate fest, die man für allgemein bekannt hält.
 - Die Namen der Prädikate werden so gewählt, dass sie ihre Bedeutung in der Basisstruktur suggerieren. Oft wird dann die Basisstruktur nicht explizit angegeben.
 - Wir betrachten folgendes Beispiel:

„Für jede Zahl gibt es eine größere Primzahl“
(es gibt unendlich viele Primzahlen).



- Formalisierung von Aussagen:
 - Wenn die Prädikate „Primzahl“ und „größer“ bekannt sind, dann wird die Aussage formalisiert durch:

Formel: $\forall x \exists y (Prim(y) \wedge Gr(y, x))$.

Basisstruktur: $U_S = \mathbb{N}$,

$Prim_S = \{ n \in \mathbb{N} \mid n \text{ ist Primzahl} \}$,

$Gr_S = \{ (n, m) \in \mathbb{N} \times \mathbb{N} \mid n > m \}$.



- Formalisierung von Aussagen:
 - Wenn die Prädikate „Primzahl“ und „größer“ bekannt sind, dann wird die Aussage formalisiert durch:
Formel: $\forall x \exists y (Prim(y) \wedge Gr(y, x))$.
Basisstruktur: $U_S = \mathbb{N}$,
 $Prim_S = \{ n \in \mathbb{N} \mid n \text{ ist Primzahl} \}$,
 $Gr_S = \{ (n, m) \in \mathbb{N} \times \mathbb{N} \mid n > m \}$.
 - Und wenn die Bedeutung von „Primzahl“ nicht allgemein bekannt ist?



- Formalisierung von Aussagen

- Wenn die Bedeutung von „teilt“ bekannt ist, dann kann das Prädikat Primzahl **durch eine Formel** definiert werden:

$$\forall x (Prim(x) \leftrightarrow \forall y (Teilt(y, x) \rightarrow (y = x \oplus y = eins))).$$

- Die Basisstruktur fixiert nun die Bedeutung des Prädikats *Teilt* und der Konstante *eins*.

$$Teilt_S = \{ (n, m) \in \mathbb{N} \mid n \text{ teilt } m \},$$

$$eins_S = 1.$$



- Formalisierung von Aussagen:
 - Wenn die Bedeutung von „teilt“ bekannt ist, dann kann das Prädikat Primzahl **durch eine Formel** definiert werden:

$$\forall x (Prim(x) \leftrightarrow \forall y (Teilt(y, x) \rightarrow (y = x \oplus y = eins)))$$

- Die Basisstruktur fixiert nun die Bedeutung des Prädikaten *Teilt*, und der Konstante *eins*.

$$Teilt_S = \{ (n, m) \in \mathbb{N} \mid n \text{ teilt } m \}$$

$$eins_S = 1$$

- **Und wenn die Bedeutung von „Teilt“ nicht allgemein bekannt ist?**



- Formalisierung von Aussagen:
 - Wenn die Bedeutung von „Produkt“ bekannt ist, dann wird „teilt“ durch folgende Formel definiert:

$$\forall x \forall y (Teilt(x, y) \rightarrow \exists z y = prod(x, z)).$$

- Die Basisstruktur fixiert die Bedeutung von *prod* und *eins*.

$$prod_S(n, m) = n \cdot m,$$

$$eins_S = 1.$$



- Formalisierung von Aussagen:
 - Wenn die Bedeutung von „Produkt“ bekannt ist, dann wird „teilt“ durch folgende Formel definiert:

$$\forall x \forall y (Teilt(x, y) \rightarrow \exists z y = prod(x, z)).$$

- Die Basisstruktur fixiert die Bedeutung von *prod* und *eins*.

$$prod_S(n, m) = n \cdot m,$$

$$eins_S = 1.$$

- Und wenn die Bedeutung von „Produkt“ nicht allgemein bekannt ist?



- Formalisierung von Aussagen:
 - Wenn die Bedeutung von „Summe“ und „Nachfolger“ bekannt ist, dann kann das Produkt so definiert werden:

$$x \cdot 1 = x,$$

$$x \cdot \text{nach}(u) = x \cdot u + x.$$

- Diese Definition kann mit der folgenden Formeln formalisiert werden:

$$\forall x \forall y \forall z \exists u (z = \text{prod}(x, y) \leftrightarrow ((y = \text{eins} \wedge z = x) \vee (y = \text{nach}(u) \wedge z = \text{sum}(\text{prod}(x, u), x)))))$$



- Formalisierung von Aussagen:
 - Die Basisstruktur fixiert nun die Bedeutung von *sum*, *nach* und *eins*.

$$\text{sum}_S(n, m) = n + m,$$

$$\text{nach}_S(n) = n + 1,$$

$$\text{eins}_S = 1.$$



- Formalisierung von Aussagen:
 - Die Basisstruktur fixiert nun die Bedeutung von *sum*, *nach* und *eins*.

$$\text{sum}_S(n, m) = n + m,$$

$$\text{nach}_S(n) = n + 1,$$

$$\text{eins}_S = 1.$$

- Und wenn die Definition von „Summe“ nicht allgemein bekannt ist?



- Formalisierung von Aussagen:
 - Die „Summe“ kann mit Hilfe von „Nachfolger“ so definiert werden:

$$\begin{aligned}x + 1 &= \text{nach}(x), \\x + \text{nach}(u) &= \text{nach}(x) + u.\end{aligned}$$

Diese Definition wird durch die folgende Formeln formalisiert:

$$\forall x \forall y \forall z \exists u (z = \text{sum}(x, y) \leftrightarrow ((y = \text{eins} \wedge z = \text{nach}(x)) \vee (y = \text{nach}(u) \wedge z = \text{sum}(\text{nach}(x), u))))$$



- Ein Kalkül für logische Inferenzen:
 - Das Kalkül enthält alle Regeln des Kalküls für die Aussagenlogik plus vier Regeln für die Einführung und Beseitigung von Quantoren.
 - Sei F eine Formel und a eine Konstante. Mit $F[x/a]$ bezeichnen wir die Formel, die man erhält, in dem alle **FREIEN** Vorkommnisse von x in F durch a ersetzt werden.
 - Beispiele:

$$F_1 = \forall y Q(x, y)$$

$$F_1[x/a] = \forall y Q(a, y),$$

$$F_2 = P(x) \wedge \forall x Q(x)$$

$$F_2[x/a] = P(a) \wedge \forall x Q(x),$$

$$F_3 = \forall x P(x)$$

$$F_3[x/a] = \forall x P(x).$$



- Ein Kalkül für logische Inferenzen:

- Allquantoreinführung:

Für jede Sequenz A , Variable x , Formel F und für jede Konstante a , die weder in A noch in F vorkommt:

$$\frac{A \vdash F[x/a]}{A \vdash \forall x F} .$$

- Intuition: Um $\forall x F$ zu zeigen, zeige, dass $F[x/a]$ für ein beliebiges aber festes a gilt.



- Ein Kalkül für logische Inferenzen:
 - Allquantorbeseitigung:
Für jede Sequenz A , Variable x , Formel F und für jede Konstante a :

$$\frac{A \vdash \forall x F}{A \vdash F[x/a]}$$

- Intuition: Wenn $\forall x F$ gilt, dann gilt auch $F[x/a]$ für ein beliebiges a .



- Ein Kalkül für logische Inferenzen:

- Existenzquantorbeseitigung:

Für jede Sequenz A , Variable x , Formel F und für jede Konstante a , die weder in A noch in F noch in G vorkommt :

$$\frac{A \vdash \exists x F \quad A, F[x/a] \vdash G}{A \vdash G} .$$

- Intuition: Wir wählen einen **frischen** Namen a für „das x , für das F gilt“, und zeigen, dass G aus $F[x/a]$ folgt.



- Ein Kalkül für logische Inferenzen:
 - Existenzquantoreinführung:
Für jede Sequenz A , Variable x , Formel F und für jede Konstante a :

$$\frac{A \vdash F[x/a]}{A \vdash \exists x F} .$$

- Intuition: Um $\exists x F$ zu beweisen, finde ein a , für das $F[x/a]$ gilt.



- Ein Kalkül für logische Inferenzen:
 - Beispiel:
Zeige, dass aus den zwei Annahmen
 - „Jemand in dieser Vorlesung weiß nicht, wer Harry Potter ist“
 - „Alle in dieser Vorlesung haben die Prüfung bestanden“
- Folgendes folgt:
- „Es gibt jemanden, der die Prüfung bestanden hat und nicht weiß, wer Harry Potter ist“.



- Inferenzregeln für Quantoren:
 - Sei $S = (U_S, I_S)$ die Struktur mit
 - U_S = alle Menschen,
 - V_S = Studenten dieser Vorlesung,
 - H_S = Menschen, die Harry Potter kennen,
 - P_S = Menschen, die die Prüfung bestanden haben.
 - In dieser Struktur sind die Annahmen A :
 - (a) $\exists x (V(x) \wedge \neg H(x))$ und (b) $\forall x (V(x) \rightarrow P(x))$.
 - Die Konklusion ist $\exists x (P(x) \wedge \neg H(x))$.
 - Wir zeigen: $A \vdash \exists x (P(x) \wedge \neg H(x))$.



- Inferenzregeln für Quantoren:

Schritt

1. $A, V(a) \wedge \neg H(a) \vdash V(a) \wedge \neg H(a)$
2. $A, V(a) \wedge \neg H(a) \vdash V(a)$
3. $A, V(a) \wedge \neg H(a) \vdash \forall x (V(x) \rightarrow P(x))$
4. $A, V(a) \wedge \neg H(a) \vdash V(a) \rightarrow P(a)$
5. $A, V(a) \wedge \neg H(a) \vdash P(a)$
6. $A, V(a) \wedge \neg H(a) \vdash \neg H(a)$
7. $A, V(a) \wedge \neg H(a) \vdash P(a) \wedge \neg H(a)$
8. $A, V(a) \wedge \neg H(a) \vdash \exists x (P(x) \wedge \neg H(x))$
9. $A \vdash \exists x (V(x) \wedge \neg H(x))$
10. $A \vdash \exists x (P(x) \wedge \neg H(x))$

Bewiesen durch

- An.
Kon.Bes. 1
An. (b)
All.Bes. 3
Imp.Bes 2,4
Kon.Bes. 1
Kon.Ein. 5,6
Exi.Ein.
An. (a)
Exi.Ein. 8,9



- Zusammenfassung Prädikatenlogik:
 - Erweiterung der Aussagenlogik
 - Individuenvariablen und Konstanten,
 - Prädikate (mehrstellig),
 - Quantoren.
 - Semantik mit Hilfe von Strukturen.
 - Tautologie, Widerspruch, Erfüllbarkeit, Äquivalenz.
 - Äquivalenzregeln.
 - Formalisierung von Aussagen.



Praktische Anwendungen in der Informatik:

- Syntax von Programmiersprachen
- Semantik eines Programms
- Unterscheidung von freien und gebundenen Variablen in der Programmierung

sum=0;

***for**(int i=1; i<=n; i++)*

sum=sum+i;

