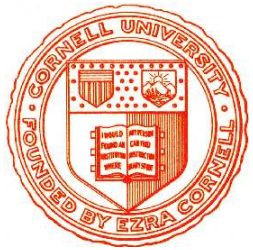
Inferenzmethoden

Teil I

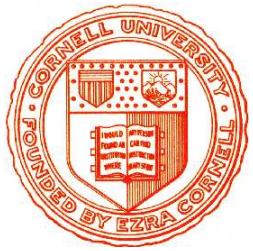


Beweiskalküle

Formalisierung von Beweisen

Inferenzmethoden

Einheit 1



Formale Logik

1. Syntax & Semantik der Prädikatenlogik
2. Inferenzkalküle für die Prädikatenlogik

Formale Kalküle

Simulation semantischer Schlußfolgerungen durch Regeln für symbolische Manipulation

- **Regelanwendung ohne Nachdenken**
  - Umgeht Mehrdeutigkeiten der natürlichen Sprache
  - Erlaubt schematische Lösung mathematischer Probleme

  Beispiele: Differentialkalkül, Fourier-Transformationen, Computer Algebra, Formale Logik
- **Kernbestandteile:**
  - Formale Sprache (Syntax + Semantik)
  - Ableitungssystem (Axiome + Inferenzregeln)
- **Wichtige Eigenschaften logischer Kalküle**
  - Korrekt, vollständig, automatisierbar
  - Leicht verständlich, ausdrucksstark

Beschreibung formaler Sprachen

- **Syntax: Präzisierung des Vokabulars**
  - Definiert formale Struktur der Sprache wie bei Programmiersprachen
    - Frei wählbare Symbole als Platzhalter für Aussagen
    - Reservierte Schlüsselwörter/Symbole für logische Bezüge
  - Komplexe Formeln werden induktiv aus einfacheren zusammengesetzt
  - Eindeutige Syntaxdefinition unterstützt spätere Implementierung
  - Beschreibbar durch formale Definitionsgleichungen oder Grammatiken
- **Semantik: Präzisierung der Bedeutung von Text**
  - Interpretation syntaktisch korrekter Ausdrücke in informaler Zielsprache
    Beschreibbar durch Interpretationsfunktion: Quellsymbole $\mapsto$ Zielobjekte
  - Direkte Semantik für Grundlagentheorien (Mengentheorie, Typentheorie)
    Mathematische Präzisierung der intuitiven Bedeutung

Syntax der Prädikatenlogik

- **Erlaubte Symbole aus (abzählbaren) Alphabeten**
  - Variablen ($\mathcal{V}$): $x, y, z, x_0, y_0,, \ldots$
  - Funktionssymbole ($\mathcal{F}$): $f, g, h, a, b, c, f_0, g_0,, ..$ (mit Stelligkeit, a, b, c oft nullstellig)
  - Prädikatssymbole ($\mathcal{P}$): $P, Q, R, P_o, Q_0, R_0,, \ldots$ (mit Stelligkeit)
  - Logische Symbole: ff, $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\forall$, $\exists$ und Klammern
- **Terme: Syntax für individuelle Objekte**
  - Variablen und nullstellige Funktionen (Konstante) sind (atomare) Terme
  - Sind $t_1, .., t_n$ Terme und f n-stellige Funktion, dann ist $f(t_1, \ldots, t_n)$ Term
- **Formeln: Syntax für Aussagen**
  - ff und nullstellige Prädikate (Aussagenvariablen) sind (atomare) Formeln
  - $P(t_1, \ldots, t_n)$ ist (atomare) Formel ($t_1, .., t_n$ Terme, P n-stelliges Prädikat)
  - Sind A und B Formeln, dann auch $\neg A$, $(A \Rightarrow B)$, $(A \wedge B)$, $(A \vee B)$
  - Ist B Formel und x eine Variable, dann sind $\forall x\, B$ und $\exists x\, B$ Formeln

    Alternative Notationen: $\forall x.\, B$ / $\exists x.\, B$ oder $(\forall x)\, B$ / $(\exists x)\, B$ u.v.a.

Formalisierung umgangssprachlicher Aussagen

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
  - Mit memnonischen Abkürzungen $(((Friert \Rightarrow \neg SBahn) \wedge SBahn) \Rightarrow \neg Friert)$
  - Aussschließlich mit erlaubten Symbolen $\boldsymbol{(((P \Rightarrow \neg Q) \wedge Q) \Rightarrow \neg P)}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*
  - $\boldsymbol{(((P \Rightarrow \neg Q) \wedge \neg P) \Rightarrow Q)}$ (leider nicht wahr)
- *Wenn es nicht keinen Frost gibt, dann friert es*
  - $\boldsymbol{\neg\neg P \Rightarrow P}$ (Achtung, regional andere Lesweise "nicht kein"= "absolut nicht")
- *Sein oder nicht sein*
  - $\boldsymbol{P \vee \neg P}$ (der ganze Rest dieses inhaltsschweren Satzes geht verloren)
- *Dieser Satz ist wahr*
  - Nicht formulierbar in Aussagen- oder Prädikatenlogik

Formalisierung quantifizierter Aussagen

- **Ermöglicht Formulierung universeller Zusammenhänge**

  ... und ihre Anwendung auf Individuen

  "*Jeder Mensch ist sterblich.*
  Sokrates ist ein Mensch.
  Also ist Sokrates sterblich"

  $$(\forall x\ (Human(x) \Rightarrow Mortal(x)) \wedge Human(socrates)) \Rightarrow Mortal(socrates)$$

- **Unterstützt unterspezifizierte Aussagen und Funktionen**

  "*Studierende, die mindestens 120 Leistungspunkte erworben haben, können ein Thema für die Bachelorarbeit bekommen*"

  $$\forall s\ (lp(s) \geq 120 \Rightarrow \exists t\ (BA(t) \wedge Bekommt(s,t)))$$

  – Aussschließlich mit erlaubten Symbolen

  $$\forall x\ (P(f(x),a) \Rightarrow \exists y\ (Q(y) \wedge R(x,y)))$$

Konventionen sparen Klammern

$\exists y\ Gerade(y) \wedge \geq(y, 2) \Rightarrow\ = (y, 2) \wedge > (y, 20)$ **heißt?**

- $\exists y\ (Gerade(y) \wedge \geq(y, 2)) \Rightarrow (= (y, 2)\ \wedge > (y, 20))$??
- $\exists y\ Gerade(y) \wedge (\geq(y, 2)\ \Rightarrow (= (y, 2)\ \wedge > (y, 20)))$??
- $\exists y\ (Gerade(y) \wedge (\geq(y, 2)\ \Rightarrow\ = (y, 2))) \wedge > (y, 20)$??

- **Prioritäten zwischen verschiedenen Konnektiven**

  $\neg$ bindet stärker als $\wedge$, dann folgt $\vee$, dann $\Rightarrow$, dann $\exists$, dann $\forall$.

  $\neg A \wedge B$ entspricht $(\neg A) \wedge B$

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

  $\exists x\ A \wedge B$ entspricht $\exists x\ (A \wedge B)$

  Bindungsbereich von Quantoren (Scope) ist die längste Formel, die darauf folgt

  Achtung: Unterschiedliche Konventionen in verschiedenen Lehrbüchern

- **Rechtsassoziativität bei Iteration von $\wedge$, $\vee$, $\Rightarrow$**

  – $A \Rightarrow B \Rightarrow C$ entspricht $A \Rightarrow (B \Rightarrow C)$

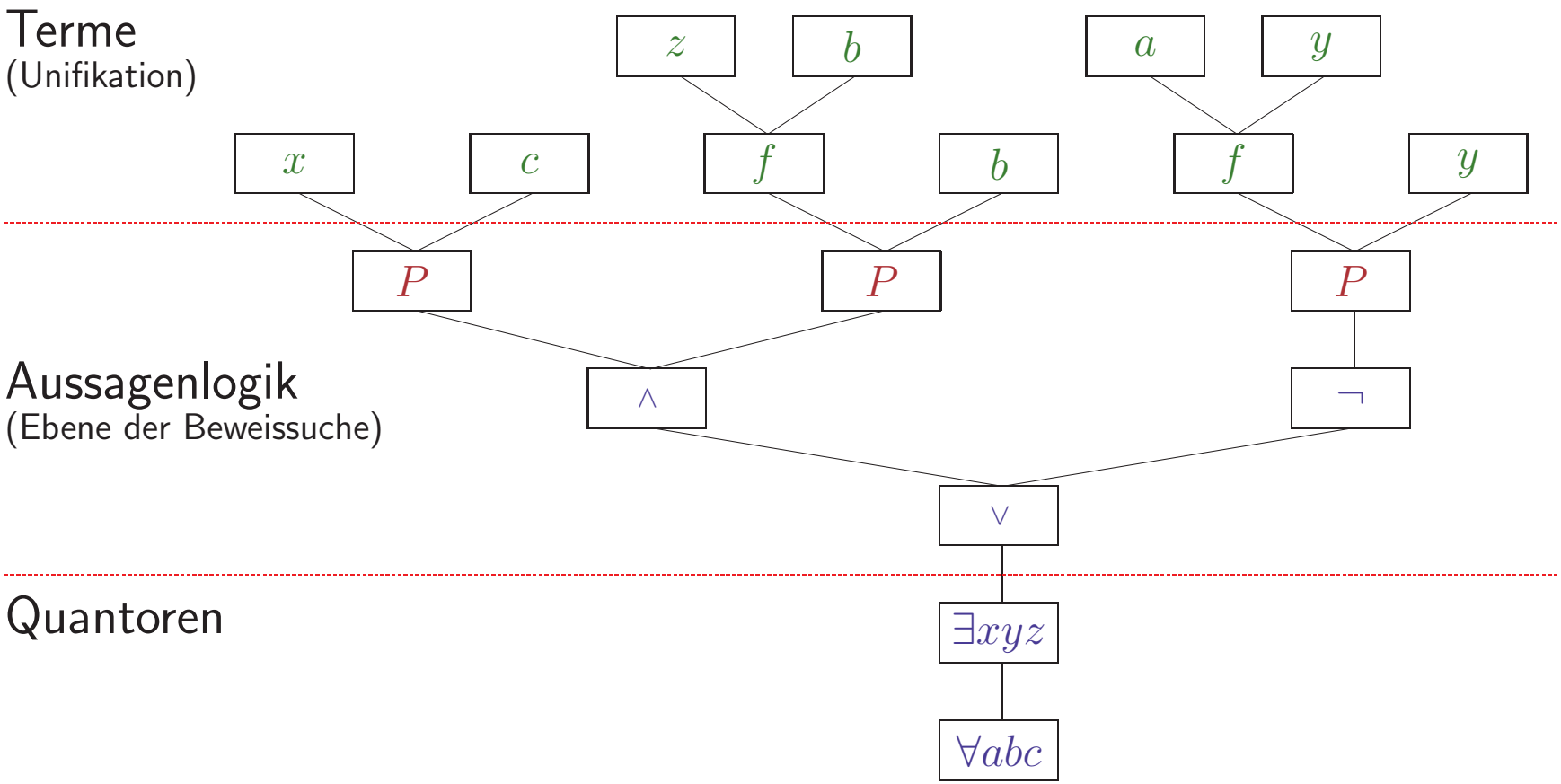
- **Keine Klammern bei Funktions-/Prädikatssymbolen**

  – Px entspricht $P(x)$ und fxy entspricht $f(x, y)$

  – $\exists xyz\ A$ entspricht $\exists x \exists y \exists z\ A$ und $\forall xyz\ A$ entspricht $\forall x \forall y \forall z\ A$

Formelbäume: Interne Darstellung von Formeln

- **Abstrakter Syntaxbaum, erzeugt durch Parsen der Formel**
- **Baumstruktur, annotiert mit Konnektiven und Symbolen**
- **Formelbaum für** $\forall abc\ \exists xyz\ Pxc \wedge P(fzb, b) \vee \neg P(fay, y)$



Semantik der Prädikatenlogik

- **Logik ist mehr als nur eine formale Kurzschreibweise**
  - Formeln haben eine intendierte Bedeutung (Semantik)
  - Man kann feststellen, ob eine Aussage/Schlußfolgerung gültig ist
  - Hierzu muß man die Bedeutung von Formeln präzise festlegen
- **Wahrheitstabellen sind kein sinnvoller Weg**
  - Mischen Mathematik mit metaphysischem Konzept der Wahrheit
  - Nehmen an, daß philosphischen Frage '*Was ist Wahrheit?*' geklärt ist
- **Standard ist Interpretation in Zielsprache**
  - Erklärt Logik durch Begriffe einer Zielsprache (z.B. Mengentheorie)

  . . . *aber was ist die Bedeutung der Zielsprache?*
- **Alternative wäre eine evidenzbasierte Semantik**
  - Beschreibt die Bedeutung logischer Formeln durch Angabe von Belegen (d.h. Rechtfertigungen) für ihre Gültigkeit

(Automatisierte Logik & Programmierung)

Standard-Semantik der Prädikatenlogik (I)
Interpretation in der Mengentheorie

- **Interpretation $\mathcal{I}$:**
  - **Universum $\mathcal{U}$ + Interpretationsfunktion ι**
- **Freie Wahl von ι auf elementaren Symbolen**
  - $\iota(x)$ Objekt aus $\mathcal{U}$ $(x \in \mathcal{V})$
  - $\iota(f)$ n-stellige Funktion $\varphi : \mathcal{U}^n \to \mathcal{U}$ $(f \in \mathcal{F}^n)$
  - $\iota(P)$ Funktion $\Pi : \mathcal{U}^n \to \{\mathsf{wahr}, \mathsf{falsch}\}$ $(P \in \mathcal{P}^n)$
- **Homomorphe Fortsetzung auf Terme und Formeln**
  - $\iota(f(t_1, \ldots, t_n)) = \iota(f)(\iota(t_1), \ldots, \iota(t_n))$
  - $\iota(\mathsf{ff}) = \mathsf{falsch}$
  - $\iota(P(t_1, \ldots, t_n)) = \iota(P)(\iota(t_1), \ldots, \iota(t_n))$.
  - $\iota((A)) = \iota(A)$

Semantik der Prädikatenlogik (II)

Fortsetzung von ι auf zusammengesetzte Formeln

$$\iota(\neg A) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{falsch} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \wedge B) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{wahr und } \iota(B) = \text{wahr} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \vee B) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{wahr oder } \iota(B) = \text{wahr} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \Rightarrow B) = \begin{cases} \text{wahr} & \text{falls aus } \iota(A) = \text{wahr immer } \iota(B) = \text{wahr folgt} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(\forall x\, A) = \begin{cases} \text{wahr} & \text{falls } \iota^u_x(A) = \text{wahr für alle } u \in \mathcal{U} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(\exists x\, A) = \begin{cases} \text{wahr} & \text{falls } \iota^u_x(A) = \text{wahr für ein } u \in \mathcal{U} \\ \text{falsch} & \text{sonst} \end{cases}$$

$\iota^u_x(x) = u$, sonst $\iota^u_x = \iota$

Semantik der Prädikatenlogik (II) – klassisch

Fortsetzung von ι auf zusammengesetzte Formeln

$$\iota(\neg A) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{falsch} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \wedge B) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{wahr und } \iota(B) = \text{wahr} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \vee B) = \begin{cases} \text{falsch} & \text{falls } \iota(A) = \text{falsch und } \iota(B) = \text{falsch} \\ \text{wahr} & \text{sonst} \end{cases}$$

$$\iota(A \Rightarrow B) = \begin{cases} \text{falsch} & \text{falls } \iota(A) = \text{wahr und } \iota(B) = \text{falsch} \\ \text{wahr} & \text{sonst} \end{cases}$$

$$\iota(\forall x\, A) = \begin{cases} \text{wahr} & \text{falls } \iota^u_x(A) = \text{wahr für alle } u \in \mathcal{U} \\ \text{falsch} & \text{sonst} \end{cases}$$

$\iota^u_x(x) = u$, sonst $\iota^u_x = \iota$

$$\iota(\exists x\, A) = \begin{cases} \text{falsch} & \text{falls } \iota^u_x(A) = \text{falsch für alle } u \in \mathcal{U} \\ \text{wahr} & \text{sonst} \end{cases}$$

Ist das wirklich dasselbe?

Intuitionistische vs. klassische Mathematik

- **Was genau heißt oder, wann immer, es gibt?**
  - Gilt $A \vee B$, *wenn man angeben kann, welches von beiden wahr ist?*
  - Gilt $A \Rightarrow B$, *wenn man zeigen kann, wie B aus A folgt?*
  - Gilt $\exists x\ A$, *wenn man ein x angeben kann, für das A wahr ist?*
- **Gesetz vom ausgeschlossenen Dritten: $A \vee \neg A$**
  - Heißt "*Jede beliebige Aussage ist ~~wahr oder nicht~~*"? Das steht da nicht!
    Genauer "*Jede beliebige Aussage ist gültig oder ihre Negation ist gültig*"
  - Unbeweisbare Grundannahme der "klassischen" Mathematik, die aus Sicht der Informatik bedeutet, daß man jede(!) Aussage entscheiden kann
- **Intuitionistische (konstruktive) Mathematik**
  - Versteht alle mathematischen Aussagen konstruktiv
  - Ist für Schließen über Algorithmen naheliegender
  - Gesetz vom ausgeschlossenen Dritten wird Entscheidbarkeitsaussage
  - Formaler Unterschied gering aber Beweise werden z.T. komplizierter

Nichtkonstruktive mathematische Gesetze sind aus Sicht der Informatik nicht ganz unproblematisch

- $\neg\neg A \Rightarrow A$
  - Wenn das Gegenteil falsch ist, dann muß eine Aussage nicht wahr sein
  - Der Widerspruchsbeweis sagt nicht, warum die Aussage wahr sein soll
  - $\neg\neg A \Rightarrow A$ ist äquivalent zu $A \vee \neg A$
- $A \Rightarrow B \Rightarrow \neg A \vee B$
  - Wenn wir wissen warum eine Aussage aus einer anderen folgt, dann wissen wir noch nicht ob die erste falsch oder die zweite wahr ist
- $\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$
  - Wenn zwei Aussagen nicht gleichzeitig falsch sind, dann ist noch nicht klar, welche von beiden wahr ist.
- $\neg(\forall x\, \neg P(x)) \Rightarrow \exists x\, P(x)$
  - Wenn eine Aussage nicht für alle Elemente falsch ist, dann wissen wir noch nicht, für welches sie wahr ist

Modelle und Gültigkeit

- **Modell $\mathcal{M}$ von A** ($\mathcal{M} \models A$)
  - Interpretation $\mathcal{M} = (\iota, \mathcal{U})$ mit $\iota(A) = \text{wahr}$
- **A gültig** jede Interpretation ist ein Modell für A

  A erfüllbar es gibt ein Modell für A

  A widerlegbar es gibt ein Modell für $\neg A$

  A widersprüchlich es gibt kein Modell für A
- **A folgt logisch aus Formelmenge $\mathcal{E}$** ($\mathcal{E} \models A$)
  - Aus $\mathcal{I} \models E$ für alle $E \in \mathcal{E}$ folgt $\mathcal{I} \models A$ (semantisch gültiger Schluß)

Deduktionstheorem: $\mathcal{E} \cup \{E\} \models F$ genau dann, wenn $\mathcal{E} \models E \Rightarrow F$

- **Theorie $\mathcal{T}$**
  - Erfüllbare Formelmenge mit allen Formeln, die daraus logisch folgen

Syntaktische Manipulation formaler Ausdrücke unter Berücksichtigung der Semantik

- **Inferenz:** Erzeugung von logischen Konsequenzen einer Formelmenge

  aus A *und* $A \Rightarrow B$ *folgt* B: $\dfrac{A,\ A \Rightarrow B}{B}$

- **Regelschema** $\dfrac{A_1, \ldots, A_n}{C}$: *aus* $\underbrace{A_1 \text{ und } \ldots A_n}_{\text{Prämissen}}$ *folgt* $\underbrace{C}_{\text{Konklusion}}$
  - **Axiom**: Regel ohne Prämissen
  - $\Gamma \vdash_{rs} C$: Konkrete Anwendung des Regelschemas rs
- **Theorem**
  - Formel, die sich durch Anwendung endlich vieler Regeln ableiten läßt
- **Wahrheit ist nicht dasselbe wie Beweisbarkeit**
  - **Korrektheit** eines Kalküls: alle Theoreme sind gültig

    ... einer Regel: Gültigkeit der Konklusion folgt aus Gültigkeit der Prämissen
  - **Vollständigkeit**: alle gültigen Aussagen sind Theoreme

Kalkülarten: synthetisch vs. analytisch

Kalküle sind Hilfsmittel, keine Beweismethode

- **Synthetisch**

$$\dfrac{\dfrac{\dfrac{[A \wedge B]}{B}\,\wedge\text{-}E \qquad \dfrac{[A \wedge B]}{A}\,\wedge\text{-}E}{B \wedge A}\,\wedge\text{-}I}{(A \wedge B) \Rightarrow (B \wedge A)}\,\Rightarrow\text{-}I$$

  - Bottom-up Vorgehensweise
  - Schlüsse von Axiomen zur Aussage
  - Übliche Art, fertige Beweise zu präsentieren
  - Ungünstig für Suche nach Beweisen

- **Analytisch**

$\vdash A \wedge B \Rightarrow B \wedge A$	BY impliesR
1. $A \wedge B \vdash B \wedge A$	BY andL
1.1. $A,\ B \vdash B \wedge A$	BY andR
1.1.1. $A,\ B \vdash B$	BY axiom
1.1.2. $A,\ B \vdash A$	BY axiom

  - Schlüsse von Zielaussage zu hinreichenden Voraussetzungen
  - Top-down Vorgehensweise, hilfreicher für Entwicklung von Beweisen

Kalkülarten: Redundanz vs. Verdichtung

- **Formale Logik und Semantik** ✓
  - Repräsentation mathematischer Aussagen in präziser Sprache
  - Beweise sind mathematische Argumente auf Basis der Semantik
- **Kalkül des natürlichen Schließens** ($\mathcal{NK}$) ↦ nächste Folien
  - Schematische Inferenzfiguren für logische Konnektive
- **Sequenzenkalküle** ($\mathcal{LK}$, Refinement Logik) ↦ nächste Folien
  - Lokale Verwaltung von Annahmen vereinfacht Anwendung von Regeln
  - Analytische Formulierung unterstützt Beweissuche
- **Tableaux-Kalküle** ↦ §2
  - Zusammenfassung strukturell gleichartiger Inferenzregeln in Klassen
- **Matrix-Kalküle** ↦ §3
  - Kompakte Beweisrepräsentation durch Beweisführung im Formelbaum
  - Gezielte Auswahl beweisrelevanter Teilformeln durch Konnektionen
  - Gezielte Instantiierung von Quantoren durch Unifikation

Resolutionskalküle entstanden durch eine andersartige Entwicklung

Historisch interessant: Frege–Hilbert–Kalküle

- **Sehr viele Axiomenschemata**

(A1) $A \Rightarrow A$
(A2) $A \Rightarrow (B \Rightarrow A)$
(A3) $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$
(A4) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
(A5) $A \Rightarrow A \vee B$
(A6) $A \Rightarrow B \vee A$
(A7) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$
(A8) $A \wedge B \Rightarrow A$
(A9) $A \wedge B \Rightarrow B$
(A10) $(C \Rightarrow A) \Rightarrow ((C \Rightarrow B) \Rightarrow (C \Rightarrow A \wedge B))$
(A11) $(A \wedge B \vee C) \Rightarrow (A \vee C) \wedge (B \vee C)$
(A12) $(A \vee C) \wedge (B \vee C) \Rightarrow (A \wedge B \vee C)$
(A13) $(A \vee B) \wedge C \Rightarrow (A \wedge C \vee B \wedge C)$
(A14) $(A \wedge C \vee B \wedge C) \Rightarrow (A \vee B) \wedge C$
(A15) $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$
(A16) $A \wedge \neg A \Rightarrow B$
(A17) $(A \wedge (A \Rightarrow B)) \Rightarrow B$
(A18) $(A \wedge C \Rightarrow B) \Rightarrow (C \Rightarrow (A \Rightarrow B))$
(A19) $(A \Rightarrow (A \wedge \neg A)) \Rightarrow \neg A$
$\vdots$ $\vdots$

- **Nur eine Inferenzregel**

$$\text{(mp)} \qquad \frac{A \quad , \quad A \Rightarrow B}{B}$$

- **Beweise mathematisch elegant aber unnatürlich**

(1) $A \wedge B \Rightarrow A$ (A8)
(2) $A \wedge B \Rightarrow B$ (A9)
(3) $(A \wedge B \Rightarrow B) \Rightarrow ((A \wedge B \Rightarrow A) \Rightarrow (A \wedge B \Rightarrow B \wedge A))$ (A10)
(4) $(A \wedge B \Rightarrow A) \Rightarrow (A \wedge B \Rightarrow B \wedge A)$ (mp mit (2), (3))
(5) $(A \wedge B \Rightarrow B \wedge A)$ (mp mit (1), (4))

Natürliche Deduktion ($\mathcal{NK}$)

- **Lesbare, kompaktifizierte Beweisdarstellung**
  - Beweisbaum mit Formeln und schematischen Inferenzregeln als Übergänge
  - Synthetischer Aufbau mit globaler Verwaltung temporärer Annahmen
- **Inferenzfiguren gruppiert nach logischen Symbolen**
  - Einführungsregel: Welche Voraussetzungen machen eine Formel gültig?
  - Eliminationsregel: Was folgt aus einer gegebenen Formel?

$\wedge$-*I*	$\dfrac{A \quad B}{A \wedge B}$		$\wedge$-*E*	$\dfrac{A \wedge B}{A}$ $\quad$ $\dfrac{A \wedge B}{B}$
$\vee$-*I*	$\dfrac{A}{A \vee B}$	$\dfrac{B}{A \vee B}$	$\vee$-*E*	$\dfrac{A \vee B \quad \begin{matrix}[A]\\ C\end{matrix} \quad \begin{matrix}[B]\\ C\end{matrix}}{C}$
$\Rightarrow$-*I*	$\dfrac{\begin{matrix}[A]\\ B\end{matrix}}{A \Rightarrow B}$		$\Rightarrow$-*E*	$\dfrac{A \quad A \Rightarrow B}{B}$
$\neg$-*I*	$\dfrac{\begin{matrix}[A]\\ \mathsf{ff}\end{matrix}}{\neg A}$		$\neg$-*E*	$\dfrac{\neg A \quad A}{\mathsf{ff}}$
excl-m	$\dfrac{}{A \vee \neg A}$		ff-*E*	$\dfrac{\mathsf{ff}}{A}$

  - Einziges Axiom $A \vee \neg A$ ist nur für klassische Logik erforderlich

Beispiel: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ mathematischer Beweis

1. Wir nehmen an $(A \Rightarrow B) \wedge (B \Rightarrow C)$ sei erfüllt
2. Wir nehmen weiter an, daß A gilt.
3. Aus der ersten Annahme folgt $(A \Rightarrow B)$
4. und mit der zweiten dann auch B.
5. Aus der ersten Annahme folgt auch, daß $(B \Rightarrow C)$ gilt
6. und mit der vierten dann auch C.
7. Es ergibt sich, daß C unter der Annahme A gilt. Also folgt $A \Rightarrow C$
8. Insgesamt folgt $A \Rightarrow C$ unter der Annahme $(A \Rightarrow B) \wedge (B \Rightarrow C)$.
   Damit gilt die Behauptung: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

Beispiel: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ Beweis in $\mathcal{NK}$

1. $(A \Rightarrow B) \wedge (B \Rightarrow C)$ — Annahme
2. A — Annahme
3. $(A \Rightarrow B)$ — $\wedge$-E mit (1)
4. B — $\Rightarrow$-E mit (2) und (3)
5. $(B \Rightarrow C)$ — $\wedge$-E mit (1)
6. C — $\Rightarrow$-E mit (4) und (5)
7. $(A \Rightarrow C)$ — $\Rightarrow$-I mit (2) und (6), Annahme (2) entfällt
8. $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$ — $\Rightarrow$-I mit (1) und (7), (1) entfällt

Schematischer Beweis in Baumstruktur

$$\dfrac{\dfrac{\dfrac{[A] \quad \dfrac{[(A \Rightarrow B) \wedge (B \Rightarrow C)]}{(A \Rightarrow B)}\,\wedge\text{-}E}{B} \quad \Rightarrow\text{-}E \quad \dfrac{[(A \Rightarrow B) \wedge (B \Rightarrow C)]}{(B \Rightarrow C)}\,\wedge\text{-}E}{C}\,\Rightarrow\text{-}E}{(A \Rightarrow C)}\,\Rightarrow\text{-}I}{((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)}\,\Rightarrow\text{-}I$$

Sequenzenkalküle

- **Schließen über Aussagen mit Annahmen**
  - Lokale Sicht: keine globale Verwaltung der Annahmen nötig
- **Grundkonzept Sequenz:** $\underbrace{A_1, \ldots, A_n}_{\text{Antezedent } \Gamma} \vdash \underbrace{B_1, \ldots, B_m}_{\text{Sukzedent } \Phi}$
  - Lesart "*Eine der Formeln B_i folgt aus den Annahmen $A_1, \ldots, A_n$*"
  - Zielsequenz $\vdash C$ ("*Formel C gilt ohne weitere Annahmen*")
- **Semantik entspricht** $A_1 \wedge \ldots \wedge A_n \Rightarrow B_1 \vee \ldots \vee B_m$

$$\iota(A_1, \ldots, A_n \vdash B_1, \ldots, B_m) = \begin{cases} \text{wahr} & \text{falls aus } \iota(A_1) = \text{wahr} \\ & \text{und } \ldots \iota(A_n) = \text{wahr} \\ & \text{immer } \iota(B_1) = \text{wahr} \\ & \text{oder } \ldots \iota(B_m) = \text{wahr folgt} \\ \text{falsch} & \text{sonst} \end{cases}$$

  - Begriffe Modell, Gültigkeit, Erfüllbarkeit analog
- **Synthetische und analytische Form möglich**
  - Synthetische Form $\mathcal{LK}$ für Beweispräsentation
  - Analytische Form Refinement Logic für interaktive Beweissuche

Synthetische Sequenzenkalküle ($\mathcal{LK}$)

$$\neg\text{–}R\ \frac{\Gamma, A \vdash \Phi}{\Gamma \vdash \Phi, \neg A} \qquad \neg\text{–}L\ \frac{\Gamma \vdash \Phi, A}{\Gamma, \neg A \vdash \Phi}$$

$$\wedge\text{–}R\ \frac{\Gamma \vdash \Phi, A \quad \Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \wedge B} \qquad \wedge\text{–}L\ \frac{\Gamma, A \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi} \quad \frac{\Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi}$$

$$\vee\text{–}R\ \frac{\Gamma \vdash \Phi, A}{\Gamma \vdash \Phi, A \vee B} \quad \frac{\Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \vee B} \qquad \vee\text{–}L\ \frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \vee B \vdash \Phi}$$

$$\Rightarrow\text{–}R\ \frac{\Gamma, A \vdash \Phi, B}{\Gamma \vdash \Phi, A \Rightarrow B} \qquad \Rightarrow\text{–}L\ \frac{\Gamma \vdash \Phi, A \quad \Delta, B \vdash \Psi}{\Gamma, \Delta, A \Rightarrow B \vdash \Phi, \Psi}$$

$$\textit{axiom}\ \frac{}{A \vdash A}$$

- **Beweiszeilen verwalten alle Annahmen und Zielformeln**
  - Mehrere Sukzedentenformeln nur für klassische Logik erforderlich
- **Sequenzenbeweis für $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$**

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, A \Rightarrow B \vdash B}\Rightarrow\text{–}L \qquad C \vdash C}{A, A \Rightarrow B, B \Rightarrow C \vdash C}\Rightarrow\text{–}L}{A, A \Rightarrow B, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}\wedge\text{–}L}{A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}\wedge\text{–}L\ (+\ \text{Kontraktion!})}{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C}\Rightarrow\text{–}R}{\vdash ((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow A \Rightarrow C}\Rightarrow\text{–}R$$

Refinement Logik: Analytische Sequenzenbeweise

- **Informaler Beweis für $P \Rightarrow (Q \Rightarrow (P \wedge Q))$**
  - Wir nehmen an, daß P gilt und müssen $Q \Rightarrow (P \wedge Q)$ zeigen
  - Dafür nehmen wir an, daß zusätzlich Q gilt und müssen $P \wedge Q$ zeigen
  - Da P und Q gilt, gilt auch $P \wedge Q$

  Methodik läßt sich durch formale (Verfeinerungs-)Regeln beschreiben

- **Notationen und Begriffe**
  - Kalkül verwaltet zu beweisende Formel und Annahmen
  - Regeln operieren auf Beweiszielen (Sequenzen) der Form $H \vdash C$

    Lesart: *Konklusion C folgt aus Liste der Annahmen (Hypothesen) H*
  - Initialziel ist $\vdash A$, d.h. Beweis der Formel A ohne weitere Annahmen
  - Regeln transformieren Beweisziele in Listen von Teilzielen

    Regeln werden als Regelschemata dargestellt mit Platzhaltern für Formeln

    $$\frac{H_1 \vdash G_1 \quad \vdots \quad H_n \vdash G_n}{H \vdash G}$$

    Beweisbarkeit der Teilziele impliziert Beweisbarkeit des Hauptziels
  - Regeln sind implementierbar durch Pattern Matching und Instantiierung

Anwendung von Regeln der Refinement Logik

- **Anwendung des Regelschemas für Konjunktionen**

$$\frac{H \vdash A \wedge B}{H \vdash A \qquad H \vdash B}\ \texttt{andR}$$

$$\vdash\ (P \Rightarrow Q) \wedge (R \Rightarrow Q) \quad \texttt{BY}\ \texttt{andR}$$
$$1.\ \vdash\ P \Rightarrow Q$$
$$2.\ \vdash\ R \Rightarrow Q$$

  - Beweisbarkeit von $A \wedge B$ folgt aus Beweisbarkeit von A und von B
  - Anwendung der Regel `andR` auf konkrete Formel $(P \Rightarrow Q) \wedge (R \Rightarrow Q)$ instantiiert A mit $P \Rightarrow Q$ und B mit $R \Rightarrow Q$
  - Entstehende Teilziele werden numeriert

- **Das Regelschema für Aussagenvariablen**
  - Aussagenvariablen können nicht in kleinere Teile zerlegt werden
  - Es gibt keinen festen Beweis für A, solange nichts über A bekannt ist
  - Aber A kann bewiesen werden, wenn A eine der Hypothesen ist

$$\frac{}{H, A, H' \vdash A}\ \texttt{axiom}$$

  - H und H' sind (möglicherweise leere) Listen von Formeln
  - Es werden keine Teilziele generiert, da Sequenz selbsterklärend ist
  - Position der Hypothese A kann als Parameter angegeben werden

Regeln für Implikationen

- **Implikation auf rechter Seite einer Sequenz**
  - Um $H \vdash A \Rightarrow B$ zu zeigen, nimmt man A an und zeigt B
  - A wird zusätzliche Hypothese im Teilziel

$$\frac{H, A \vdash B}{H \vdash A \Rightarrow B}\ \texttt{impliesR}$$

- **Implikation auf linker Seite einer Sequenz**
  - Um C unter der Annahme $A \Rightarrow B$ zu zeigen, braucht man einen Beweis für A und kann dann die Annahme B verwenden, um C zu zeigen

$$\frac{H, A \Rightarrow B, H' \vdash A \qquad H, B, H' \vdash C}{H, A \Rightarrow B, H' \vdash C}\ \texttt{impliesL}$$

  - B wird zusätzliche Hypothese im Teilziel 2
  - Annahme $A \Rightarrow B$ wird im Teilziel 1 möglicherweise noch benötigt

Anwendung der Implikationsregeln

- **Beweis für $P \Rightarrow P$**

$\vdash\ P \Rightarrow P$	BY `impliesR`
`1.` $P \vdash P$	BY `axiom`

  - `impliesR` erzeugt Teilziel mit neuer Hypothese P
  - `axiom` beweist Teilziel

- **Beweis für $P \Rightarrow (Q \Rightarrow P)$**

$\vdash\ P \Rightarrow (Q \Rightarrow P)$	BY `impliesR`
`1.` $P \vdash Q \Rightarrow P$	BY `impliesR`
`1.1.` $P, Q \vdash P$	BY `axiom`

  - Zwei Anwendungen von `impliesR` erzeugen Beweisbaum der Tiefe 2
  - Numerierung `1.1.` beschreibt erstes Teilziel des Teilziels 1

Regeln für Konjunktion

- **Konjunktion auf rechter Seite einer Sequenz**
  - Um $H \vdash A \wedge B$ zu zeigen, muß A und B gezeigt werden

$$\frac{H \vdash A \qquad H \vdash B}{H \vdash A \wedge B}\ \texttt{andR}$$

- **Konjunktion auf linker Seite einer Sequenz**
  - Die Annahme $A \wedge B$ ist äquivalent zu den beiden Annahmen A und B

$$\frac{H, A, B, H' \vdash C}{H, A \wedge B, H' \vdash C}\ \texttt{andL}$$

Anwendung der Konjunktionsregeln

- **Beweis für $P \Rightarrow (Q \Rightarrow (P \wedge Q))$**

$\vdash\ P \Rightarrow (Q \Rightarrow (P \wedge Q))$	BY impliesR
1. $P \vdash\ Q \Rightarrow (P \wedge Q)$	BY impliesR
1.1. $P, Q \vdash\ P \wedge Q$	BY andR
1.1.1. $P, Q \vdash\ P$	BY axiom
1.1.2. $P, Q \vdash\ Q$	BY axiom

- **Beweis für $(P \wedge Q) \Rightarrow P$**

$\vdash\ (P \wedge Q) \Rightarrow P$	BY impliesR
1. $(P \wedge Q) \vdash\ P$	BY andL
1.1. $P, Q \vdash\ P$	BY axiom

Regeln für Disjunktionen

- **Disjunktion auf rechter Seite einer Sequenz**
  - Um $H \vdash A \vee B$ zu zeigen, muß A oder B gezeigt werden
  - Zwei Regeln ermöglichen es, eine Wahl zu treffen

$$\frac{H \vdash A}{H \vdash A \vee B}\ \texttt{orR1} \qquad \frac{H \vdash B}{H \vdash A \vee B}\ \texttt{orR2}$$

- **Disjunktion auf linker Seite einer Sequenz**
  - Um C unter der Annahme $A \vee B$ zu zeigen, muß C unter der Annahme A und unter der Annahme B gezeigt werden können (Fallanalyse)

$$\frac{H, A, H' \vdash C \qquad H, B, H' \vdash C}{H, A \vee B, H' \vdash C}\ \texttt{orL}$$

Anwendung der Disjunktionsregeln

- **Beweis für $P \Rightarrow (P \vee Q)$**

$\vdash\ P \Rightarrow (P \vee Q)$	BY impliesR
1. $P \vdash P \vee Q$	BY orR1
1.1. $P \vdash P$	BY axiom

- **Beweis für $(P \vee Q) \Rightarrow (Q \vee P)$**

$(P \vee Q) \Rightarrow (Q \vee P)$	BY impliesR
1. $(P \vee Q) \vdash Q \vee P$	BY orL
1.1. $P \vdash Q \vee P$	BY orR2
1.1.1. $P \vdash P$	BY axiom
1.2. $Q \vdash Q \vee P$	BY orR1
1.2.1. $Q \vdash Q$	BY axiom

Regeln für Negation

Spezialisierte Implikationsregeln, da $\neg A \;\hat{=}\; A \Rightarrow \mathsf{ff}$

- **Negation auf rechter Seite einer Sequenz**
  - Um $H \vdash \neg A$ zu zeigen, muß aus Annahme A ein Widerspruch folgen

$$\frac{H \vdash \neg A}{H, A \vdash \mathsf{ff}}\ \texttt{notR}$$

  - Teilziel ist nur beweisbar, wenn Annahmen widersprüchlich sind

- **Negation auf linker Seite einer Sequenz**
  - Um C unter Annahme $\neg A$ zu zeigen, benötigt man einen Beweis für A
  - Aus dem resultierenden Widerspruch folgt C ohne weiteren Beweis (!)

$$\frac{H, \neg A, H' \vdash C}{H, \neg A, H' \vdash A}\ \texttt{notL}$$

Anwendung der Negationsregeln

- **Beweis für $P \Rightarrow \neg\neg P$**

$\vdash\ P \Rightarrow \neg\neg P$	BY impliesR
1. $P \vdash \neg\neg P$	BY notR
1.1. $P, (\neg P) \vdash \mathsf{ff}$	BY notL
1.1.1. $P, (\neg P) \vdash P$	BY axiom

- **Beweis für $\neg(P \vee Q) \Rightarrow \neg P$**

$\vdash\ \neg(P \vee Q) \Rightarrow \neg P$	BY impliesR
1. $\neg(P \vee Q) \vdash \neg P$	BY notR
1.1. $\neg(P \vee Q), P \vdash \mathsf{ff}$	BY notL
1.1.1. $\neg(P \vee Q), P \vdash P \vee Q$	BY orR1
1.1.1.1. $\neg(P \vee Q), P \vdash P$	BY axiom

Ein komplexerer Beweis

$\vdash\ ((P \vee Q) \wedge ((P \Rightarrow R) \wedge (Q \Rightarrow R))) \Rightarrow R$	BY impliesR
1. $(P \vee Q) \wedge ((P \Rightarrow R) \wedge (Q \Rightarrow R)) \vdash R$	BY andL
1.1. $P \vee Q, (P \Rightarrow R) \wedge (Q \Rightarrow R) \vdash R$	BY andL
1.1.1. $P \vee Q, P \Rightarrow R, Q \Rightarrow R \vdash R$	BY orL
1.1.1.1. $P, P \Rightarrow R, Q \Rightarrow R \vdash R$	BY impliesL
1.1.1.1.1. $P, P \Rightarrow R, Q \Rightarrow R \vdash P$	BY axiom
1.1.1.1.2. $P, R, Q \Rightarrow R \vdash R$	BY axiom
1.1.1.2. $Q, P \Rightarrow R, Q \Rightarrow R \vdash R$	BY impliesL
1.1.1.2.1. $Q, P \Rightarrow R, Q \Rightarrow R \vdash Q$	BY axiom
1.1.1.2.2. $Q, P \Rightarrow R, R \vdash R$	BY axiom

Was passiert mit $P \vee \neg P$, $\neg\neg P \Rightarrow P$, etc.?

- **Beweisansätze für $P \vee \neg P$**

```
⊢ P ∨ ¬P          BY orR1
1. ⊢ P            BY ?????
```

```
⊢ P ∨ ¬P          BY orR2
1. ⊢ ¬P           BY notR
1.1. P ⊢ ff       BY ?????
```

  – Beide Ansätze können nicht fortgesetzt werden

- **Beweisansatz für $\neg\neg P \Rightarrow P$**

```
⊢ ¬¬P ⇒ P                BY impliesR
1. ¬¬P ⊢ P               BY notL
1.1. ¬¬P ⊢ ¬P            BY notR
1.1.1. ¬¬P, P ⊢ ff       BY ?????
```

  – Keine sinnvolle Fortsetzung möglich

- **Beweisansatz für $(P \Rightarrow Q) \Rightarrow (\neg P \vee Q)$**

```
⊢ (P ⇒ Q) ⇒ (¬P ∨ Q)      BY impliesR
1. P ⇒ Q ⊢ ¬P ∨ Q         BY impliesL?, orR1?, orR2?
```

  – Keine der drei möglichen Fortsetzungen führt zum Erfolg

Was ist das denn für ein Kalkül?

- **Bekannte logische Gesetze gelten nicht?**
  - Gesetz vom ausgeschlossenen Dritten $P \vee \neg P$
  - Gesetz der Doppelten Negation $\neg\neg P \Rightarrow P$
  - Zusammenhang Implikation und Disjunktion $(P \Rightarrow Q) \Rightarrow (\neg P \vee Q)$

    ... und viele andere mehr

- **Refinement Logik ist konstruktive Logik**
  - Regeln zur Dekomposition/Verfeinerung von Konnektiven in Formeln sind von Natur aus konstruktiv
  - Klassische Logik kann nicht durch diese Regeln alleine erfaßt werden
  - Ein vollständiger Kalkül für klassische Logik benötigt das Gesetz vom ausgeschlossenen Dritten als explizite (Axiom-)regel

    $H \vdash A \vee \neg A$ `magic`

  - Regelname `magic` drückt aus, daß es keine "natürliche" Begründung für dieses Axiom gibt

Refinement Logik – Aussagenlogischer Teil

Links		Rechts	
$H, A \Rightarrow B, H' \vdash C$ $H, A \Rightarrow B, H' \vdash A$ $H, B, H' \vdash C$	impliesL	$H \vdash A \Rightarrow B$ $H, A \vdash B$	impliesR
$H, A \wedge B, H' \vdash C$ $H, A, B, H' \vdash C$	andL	$H \vdash A \wedge B$ $H \vdash A$ $H \vdash B$	andR
$H, A \vee B, H' \vdash C$ $H, A, H' \vdash C$ $H, B, H' \vdash C$	orL	$H \vdash A \vee B$ $H \vdash A$ $H \vdash A \vee B$ $H \vdash B$	orR1 orR2
$H, \neg A, H' \vdash C$ $H, \neg A, H' \vdash A$	notL	$H \vdash \neg A$ $H, A \vdash \mathsf{ff}$	notR
		$H, A, H' \vdash A$	axiom
Zusatzregel für klassische Logik		$H \vdash A \vee \neg A$	magic

Namen der Regeln können in implementierte Systemen anders sein.

Sinnvolle Zusatzregeln

- **Einfügen von Zwischenbehauptungen**
  - C ist gültig, wenn C aus der Annahme A folgt und A gültig ist
  - Um C zu zeigen, kann man eine Zwischenbehauptung A beweisen und dann C unter der Annahme A beweisen

$$\begin{array}{l} H \vdash C \\ \quad H \vdash A \\ \quad H, A \vdash C \end{array} \quad \texttt{cut}\ A$$

  - A kann eine beliebige "Schnitt"-Formel sein
  - Beweise werden signifikant kürzer, wenn A mehrfach benutzt wird
- **Ausdünnen von Annahmen**
  - Hypothesen, die nicht gebraucht werden, können entfernt werden

$$\begin{array}{l} H, A, H' \vdash C \\ \quad H, H' \vdash C \end{array} \quad \texttt{thin}\ A$$

  - Sinnvoll, um Hypothesenliste übersichtlich zu halten

Beide Regeln können (mühsam) simuliert werden

Beweise in "klassischer" Refinement Logik

- **Beweis für $P \vee \neg P$ wird Instanz der `magic` Regel**
- **Beweis für $\neg\neg P \Rightarrow P$**

$\vdash\ \neg\neg P \Rightarrow P$	BY impliesR
1. $\neg\neg P \vdash P$	BY cut $P \vee \neg P$
1.1. $\neg\neg P,\ P \vee \neg P \vdash P$	BY orL
1.1.1 $\neg\neg P,\ P \vdash P$	BY axiom
1.1.2 $\neg\neg P,\ \neg P \vdash P$	BY notL
1.1.2.1 $\neg\neg P,\ \neg P \vdash P$	BY axiom

- **Beweis für $(P \Rightarrow Q) \Rightarrow (\neg P \vee Q)$**

$\vdash\ (P \Rightarrow Q) \Rightarrow (\neg P \vee Q)$	BY impliesR
1. $P \Rightarrow Q \vdash \neg P \vee Q$	BY cut $P \vee \neg P$
1.1. $P \Rightarrow Q,\ P \vee \neg P \vdash \neg P \vee Q$	BY orL
1.1.1. $P \Rightarrow Q,\ P \vdash \neg P \vee Q$	BY orR2
1.1.1.1 $P \Rightarrow Q,\ P \vdash Q$	BY impliesL
1.1.1.1.1. $P \Rightarrow Q,\ P \vdash P$	BY axiom
1.1.1.1.2. $P \Rightarrow Q,\ P,\ Q \vdash Q$	BY axiom
1.1.2. $P \Rightarrow Q,\ \neg P \vdash \neg P \vee Q$	BY orR1
1.1.2.1. $P \Rightarrow Q,\ \neg P \vdash \neg P$	BY axiom

Prädikatenlogische Refinement Logik

- **Behandlung von Quantoren, mathematisch**
  - Um $(\forall x)B$ zu zeigen, muß man B für jede Instanz von x zeigen
    Hierzu wählt man x' beliebig aber fest und zeigt B für x' statt x
  - Um $(\exists x)B$ zu zeigen, muß man eine B für eine Instanz von x zeigen
    Hierzu gibt man ein Objekt a an und zeigt B für a statt x
  - In formaler Semantik wird $\iota(\forall x\ B)$ / $\iota(\exists x\ B)$ wird durch $\iota^u_x(B)$ erklärt
    · $\iota^u_x(B)$ muß für alle oder einen Wert u wahr werden
  - ι^u_x modifiziert die Interpretation ι für die gebundene Variable x
  - Regeln benötigen Ersetzung von Variablen durch Terme
    um den semantischen Effekt von ι^u_x syntaktisch zu simulieren
- **Formales Konzept: Substitution $B[t/x]$** auch $B\{x\backslash t\}$ o.ä.
  - Ersetzen der Variablen x in Formel B durch Term t
    Unvollständiger Ersatz für Instantiierung, wenn Universum überabzählbar
  - Substitution muß Verständnis von "für alle" und "es gibt" erhalten
    wichtig: $\forall x\ P\,x$ und $\forall y\ P\,y$ bedeuten dasselbe
  - Nur ungebundene Variablen dürfen ersetzt werden

Vorkommen von Variablen in Formeln

- **Vorkommen der Variablen x in Formel B, informal**
  - – Gebunden: x erscheint im Scope eines Quantors $\forall x$ oder $\exists x$
  - – Frei: x kommt in B vor, ohne gebunden zu sein
  - – B heißt geschlossen falls B keine freien Variablen enthält
- **Präzise, induktive Definition**

x	die Variable x kommt frei vor; $y \neq x$ kommt nicht vor
ff	die Variable x kommt nicht vor
$f(t_1, ..., t_n)$	freie Vorkommen von x in t_i bleiben frei
$P(t_1, ..., t_n)$	gebundene Vorkommen von x bleiben gebunden.
$\neg A$, $A \Rightarrow B$	freie Vorkommen von x in A, B bleiben frei
$A \wedge B$, $A \vee B$	gebundene Vorkommen von x bleiben gebunden.
$\forall x\ B$	beliebige Vorkommen von x in B werden gebunden
$\exists x\ B$	Vorkommen von $y \neq x$ in B bleiben unverändert

$$\overbrace{\overbrace{(\forall x\ \underbrace{(P(x) \wedge Q(x))}_{x \text{ frei}})}^{x \text{ gebunden}} \wedge \underbrace{R(x)}_{x \text{ frei}}}^{x \text{ frei und gebunden}}$$

Substitution $B[t/x]$ formal

Endliche Abbildung σ von Variablen in Terme

– $\boldsymbol{\sigma = [t_1, .., t_n/x_1, .., x_n]} \mathrel{\hat{=}} \sigma(x_1){=}t_1, \ldots, \sigma(x_n){=}t_n$

– $\boldsymbol{A\sigma}$: Anwendung von σ auf den Ausdruck A τ und σ

$\lfloor x \rfloor[t/x]$	$= t$	$\lfloor x \rfloor[t/y]$	$= x$	$(y{\neq}x)$
$\lfloor f(t_1, .., t_n) \rfloor\sigma$	$= f(t_1\sigma, .., t_n\sigma)$	$\lfloor \mathsf{ff} \rfloor\sigma$	$= \mathsf{ff}$	
$\lfloor P(t_1, .., t_n) \rfloor\sigma$	$= P(t_1\sigma, .., t_n\sigma)$			
$\lfloor \neg A \rfloor\sigma$	$= \neg A\sigma$	$\lfloor A \wedge B \rfloor\sigma$	$= A\sigma \wedge B\sigma$	
$\lfloor A \vee B \rfloor\sigma$	$= A\sigma \vee B\sigma$	$\lfloor A \Rightarrow B \rfloor\sigma$	$= A\sigma \Rightarrow B\sigma$	
$\lfloor \forall x\ B \rfloor[t/x]$	$= \forall x\ B$	$\lfloor \exists x\ B \rfloor[t/x]$	$= \exists x\ B$	
$\lfloor \forall x\ B \rfloor[t/y]$	$= \lfloor \forall z\ B[z/x] \rfloor[t/y]$	$\lfloor \exists x\ B \rfloor[t/y]$	$= \lfloor \exists z\ B[z/x] \rfloor[t/y]$	*
$\lfloor \forall x\ B \rfloor[t/y]$	$= \forall x \lfloor B[t/y] \rfloor$	$\lfloor \exists x\ B \rfloor[t/y]$	$= \exists x \lfloor B[t/y] \rfloor$	**

*: *$y{\neq}x$, y frei in B, x frei in t, z neue Variable*

**: *$y{\neq}x$, y nicht frei in B oder x nicht frei in t*

Regeln für den Allquantor

- **Allquantor auf rechter Seite einer Sequenz**
  - Um $H \vdash \forall x\ B$ zu zeigen, muß man B für jede Instanz von x zeigen
    Einziger Weg ist generischer Beweis, der nicht von Instanz abhängt
  - Wähle neue Variable x' und beweise $B[x'/x]$

$$\frac{H \vdash B[x'/x]}{H \vdash \forall x\ B}\ \texttt{allR}$$

- **Allquantor auf linker Seite einer Sequenz**
  - Um C unter Annahme $\forall x\ B$ zu zeigen, darf man jede Instanz von x verwenden, also die Annahme $B[t/x]$ für beliebige Terme t ergänzen

$$\frac{H, B[t/x], H' \vdash C}{H, \forall x\ B, H' \vdash C}\ \texttt{allL}\ t$$

Anwendung der Allquantorregeln

- **Beweis für $\forall x\ (Px \Rightarrow Px)$**

$\vdash\ \forall x\ (Px \Rightarrow Px)$	BY allR
$1\ \ \vdash\ Px \Rightarrow Px$	BY impliesR
$1.1\ , Px\ \vdash\ Px$	BY axiom

- **Beweis für $(\forall x\ Px) \Rightarrow Pa$**

$\vdash (\forall x\ Px) \Rightarrow Pa$	BY impliesR
$1\ \forall x\ Px \vdash Pa$	BY allL a
$1.1\ \forall x\ Px, Pa \vdash Pa$	BY axiom

- **Beweis für $(\forall x\ Px) \Rightarrow (Pa \wedge Pb)$**

$\vdash (\forall x\ Px) \Rightarrow (Pa \wedge Pb)$	BY impliesR
$1\ \forall x\ Px \vdash Pa \wedge Pb$	BY allL a
$1.1\ \forall x\ Px, Pa \vdash Pa \wedge Pb$	BY allL b
$1.1.1\ \forall x\ Px, Pa, Pb \vdash Pa \wedge Pb$	BY andR
$1.1.1.1\ \forall x\ Px, Pa, Pb \vdash Pa$	BY axiom
$1.1.1.2\ \forall x\ Px, Pa, Pb \vdash Pb$	BY axiom

Regeln für Existenzquantor

- **Existenzquantor auf rechter Seite einer Sequenz**
  - Um $H \vdash \exists x\ B$ zu zeigen, muß $B[t/x]$ für einen Term t gezeigt werden

$$\frac{H \vdash B[t/x]}{H \vdash \exists x\ B}\ \texttt{exR}\ t$$

- **Existenzquantor auf linker Seite einer Sequenz**
  - Um C unter Annahme $\exists x\ B$ zu beweisen, muß man C unter der Annahme B für eine beliebige Instanz von x (generisch) zeigen können
  - Wähle neue Variable x' und verwende Annahme $B[x'/x]$

$$\frac{H, B[x'/x], H' \vdash C}{H, \exists x\ B, H' \vdash C}\ \texttt{exL}$$

Anwendung der Existenzquantorregeln

- **Beweis für $Pa \Rightarrow (\exists x\ Px)$**

$\vdash\ Pa \Rightarrow (\exists x\ Px)$	BY impliesR
1 $Pa\ \vdash\ \exists x\ Px$	BY exR a
1.1 $Pa\ \vdash\ Pa$	BY axiom

- **Beweis für $(\exists x\ Px) \Rightarrow ((\exists y) Py)$**

$\vdash\ (\exists x\ Px) \Rightarrow ((\exists y) Py)$	BY impliesR
1 $\exists x\ Px\ \vdash\ (\exists y) Py$	BY exL
1.1 $, Px\ \vdash\ (\exists y) Py$	BY exR x
1.1.1 $, Px\ \vdash\ Px$	BY axiom

  – Reihenfolge der Regelanwendungen wichtig für erfolgreichen Beweis

$\vdash\ (\exists x\ Px) \Rightarrow ((\exists y) Py)$	BY impliesR
1 $\exists x\ Px\ \vdash\ (\exists y) Py$	BY exR x
1.1 $\exists x\ Px\ \vdash\ Px$	BY exL
1.1.1 $, Px' \vdash\ Px$	BY ???

Ein komplexerer Beweis

$\vdash (\forall x\ (Px \wedge Qx)) \Rightarrow (\forall x\ Px \wedge \forall x\ Qx)$	BY impliesR
$1.\ \forall x\ (Px \wedge Qx) \vdash (\forall x\ Px \wedge \forall x\ Qx)$	BY andR
$1.1.\ \forall x\ (Px \wedge Qx) \vdash \forall x\ Px$	BY allR
$1.1.1.\ , \forall x\ (Px \wedge Qx) \vdash Px$	BY allL x
$1.1.1.1.\ , \forall x\ (Px \wedge Qx), (Px \wedge Qx) \vdash Px$	BY andL
$1.1.1.1.1.\ , \forall x\ (Px \wedge Qx), Px, Qx \vdash Px$	BY axiom
$1.2.\ \forall x\ (Px \wedge Qx) \vdash \forall x\ Qx$	BY allR
$1.2.1.\ , \forall x\ (Px \wedge Qx) \vdash Qx$	BY allL x
$1.2.1.1.\ , \forall x\ (Px \wedge Qx), (Px \wedge Qx) \vdash Qx$	BY andL
$1.2.1.1.1.\ , \forall x\ (Px \wedge Qx), Px, Qx \vdash Qx$	BY axiom

Refinement Logik – Zusammenfassung

Links		Rechts	
$H, A \Rightarrow B, H' \vdash C$ $H, A \Rightarrow B, H' \vdash A$ $H, B, H' \vdash C$	impliesL	$H \vdash A \Rightarrow B$ $H, A \vdash B$	impliesR
$H, A \wedge B, H' \vdash C$ $H, A, B, H' \vdash C$	andL	$H \vdash A \wedge B$ $H \vdash A$ $H \vdash B$	andR
$H, A \vee B, H' \vdash C$ $H, A, H' \vdash C$ $H, B, H' \vdash C$	orL	$H \vdash A \vee B$ $H \vdash A$ $H \vdash A \vee B$ $H \vdash B$	orR1 orR2
$H, \neg A, H' \vdash C$ $H, \neg A, H' \vdash A$	notL	$H \vdash \neg A$ $H, A \vdash \mathsf{ff}$	notR
		$H, A, H' \vdash A$	axiom
$H, \forall x\ B, H' \vdash C$ $H, \forall x\ B, B[t/x], H' \vdash C$	allL t	$H \vdash \forall x\ B$ $H \vdash B[x'/x]$	allR
$H, \exists x\ B, H' \vdash C$ $H, B[x'/x], H' \vdash C$	exL	$H \vdash \exists x\ B$ $H \vdash B[t/x]$	exR t
t ist ein beliebiger Term, x' eine neue Variable			
Zusatzregel für klassische Logik		$H \vdash A \vee \neg A$	magic

Korrektheit und Vollständigkeit des Kalküls

- **Refinement Logik ist korrekt**
  - Alle Regeln der Refinement Logik sind korrekt ↦ Übung
  - Alle vollständigen Beweise haben gültige Formeln als Wurzeln

    Beweis durch strukturelle Induktion über Beweisbaum
    - · Blätter sind Regelanwendungen ohne Teilziele (`axiom`, `magic`)
    - · Knoten im Beweisbaum sind Regelanwendungen

  ↦ **Alle beweisbaren Formeln sind gültig**

- **Refinement Logik ist vollständig**
  - Für jede gültige Formel C gibt es einen Beweis mit Wurzel $\vdash C$

    Beschreibe systematische Beweisprozedur
    - · Erzeuge alle möglichen Substitutionen aller Quantoren (ineffizient!)
    - · Zeige: wenn Prozedur nicht terminiert, ist die Formel widerlegbar

    Details aufwendig – mehr später bei Tableauxverfahren

  ↦ **Alle gültigen Formeln sind beweisbar**

Sequenzenkalkül: Beweismethodik

- **Kalkül garantiert Korrektheit formaler Beweise**
  - Kalkül ist selbst keine Methode um Beweise zu finden
- **Es gibt Leitlinien für erfolgreiche Beweissuche**
  - Versuche vorrangig Zweige abzuschließen (`axiom`)
  - Verwende Dekompositionsregeln, die Formeln äquivalent aufbrechen
  - Verwende `orL` vor `orR1` / `orR2`
  - Verwende `exL` und `allR` vor `exR` und `allL`
  - Wähle anwendbare Regel, welche die wenigsten Teilziele erzeugt

  Methodik ist als "Taktik" programmierbar
- **Beweismethodik läßt Fragen offen**
  - Auswahl der Substitution für Quantoren erfordert "Vorausschau"
  - Maschinennahe Methoden finden Substitution durch Unifikation

Mehr dazu in §5ff