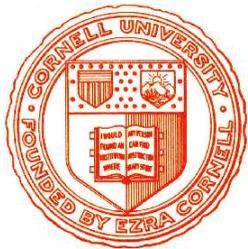


Inferenzmethoden

Teil I

Beweiskalküle

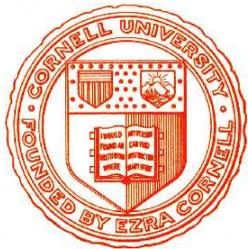
Formalisierung von Beweisen



Inferenzmethoden

Einheit 1

Formale Logik



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

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

- **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

● Erlaubte Symbole aus (abzählbaren) Alphabeten

- Variablen (\mathcal{V}): x, y, z, x_0, y_0, \dots
- Funktionssymbole (\mathcal{F}): $f, g, h, a, b, c, f_0, g_0, \dots$ (mit Stelligkeit, a, b, c oft nullstellig)
- Prädikatssymbole (\mathcal{P}): $P, Q, R, P_0, Q_0, R_0, \dots$ (mit Stelligkeit)
- Logische Symbole: $\neg, \wedge, \vee, \Rightarrow, \forall, \exists$ und Klammern

● Terme: Syntax für individuelle Objekte

- Variablen und nullstellige Funktionen (**Konstante**) sind (atomare) Terme
- Sind t_1, \dots, t_n Terme und f n -stellige Funktion, dann ist $f(t_1, \dots, t_n)$ Term

● Formeln: Syntax für Aussagen

- \neg und nullstellige Prädikate (**Aussagenvariablen**) sind (atomare) Formeln
- $P(t_1, \dots, t_n)$ ist (atomare) Formel (t_1, \dots, 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*

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\text{P} \Rightarrow \neg \text{Q}) \wedge \text{Q}) \Rightarrow \neg \text{P}$

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\text{P} \Rightarrow \neg \text{Q}) \wedge \text{Q}) \Rightarrow \neg \text{P}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \mathbf{Q}) \Rightarrow \neg \mathbf{P}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*
 - $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \neg \mathbf{P}) \Rightarrow \mathbf{Q}$ (leider nicht wahr)

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \mathbf{Q}) \Rightarrow \neg \mathbf{P}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*
 - $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \neg \mathbf{P}) \Rightarrow \mathbf{Q}$ (leider nicht wahr)
- *Wenn es nicht keinen Frost gibt, dann friert es*

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \mathbf{Q}) \Rightarrow \neg \mathbf{P}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*
 - $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \neg \mathbf{P}) \Rightarrow \mathbf{Q}$ (leider nicht wahr)
- *Wenn es nicht keinen Frost gibt, dann friert es*
 - $\neg \neg \mathbf{P} \Rightarrow \mathbf{P}$ (Achtung, regional andere Lesweise “nicht kein”= “absolut nicht”)

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \mathbf{Q}) \Rightarrow \neg \mathbf{P}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*
 - $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \neg \mathbf{P}) \Rightarrow \mathbf{Q}$ (leider nicht wahr)
- *Wenn es nicht keinen Frost gibt, dann friert es*
 - $\neg \neg \mathbf{P} \Rightarrow \mathbf{P}$ (Achtung, regional andere Lesweise “nicht kein”= “absolut nicht”)
- *Sein oder nicht sein*

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

- *Wenn es friert, fährt die S-Bahn nicht. Die S-Bahn fährt. Also friert es nicht*
 - Mit memnonischen Abkürzungen $((\text{Friert} \Rightarrow \neg \text{SBahn}) \wedge \text{SBahn}) \Rightarrow \neg \text{Friert}$
 - Ausschließlich mit erlaubten Symbolen $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \mathbf{Q}) \Rightarrow \neg \mathbf{P}$
- *Wenn es friert, fährt die S-Bahn nicht. Es friert es nicht. Also fährt die S-Bahn*
 - $((\mathbf{P} \Rightarrow \neg \mathbf{Q}) \wedge \neg \mathbf{P}) \Rightarrow \mathbf{Q}$ (leider nicht wahr)
- *Wenn es nicht keinen Frost gibt, dann friert es*
 - $\neg \neg \mathbf{P} \Rightarrow \mathbf{P}$ (Achtung, regional andere Lesweise “nicht kein”= “absolut nicht”)
- *Sein oder nicht sein*
 - $\mathbf{P} \vee \neg \mathbf{P}$ (der ganze Rest dieses inhaltsschweren Satzes geht verloren)

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

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

FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

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

- **Ermöglicht Formulierung universeller Zusammenhänge**

... und ihre Anwendung auf Individuen

“Jeder Mensch ist sterblich.

Sokrates ist ein Mensch.

Also ist Sokrates sterblich”

- **Ermöglicht Formulierung universeller Zusammenhänge**

... und ihre Anwendung auf Individuen

<i>“Jeder Mensch ist sterblich.</i>	$(\forall x (Human(x) \Rightarrow Mortal(x)))$
<i>Sokrates ist ein Mensch.</i>	$\wedge Human(socrates))$
<i>Also ist Sokrates sterblich”</i>	$\Rightarrow Mortal(socrates)$

- **Ermöglicht Formulierung universeller Zusammenhänge**

... und ihre Anwendung auf Individuen

“Jeder Mensch ist sterblich. $(\forall x (Human(x) \Rightarrow Mortal(x)))$
Sokrates ist ein Mensch. $\wedge Human(socrates))$
Also ist Sokrates sterblich” $\Rightarrow Mortal(socrates)$

- **Unterstützt unterspezifizierte Aussagen und Funktionen**

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

- **Ermöglicht Formulierung universeller Zusammenhänge**

... und ihre Anwendung auf Individuen

*“Jeder Mensch ist sterblich. $(\forall x (Human(x) \Rightarrow Mortal(x))$
Sokrates ist ein Mensch. $\wedge Human(socrates))$
Also ist Sokrates sterblich” $\Rightarrow Mortal(socrates)$*

- **Unterstützt unterspezifizierte Aussagen und Funktionen**

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

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

– Ausschließlich mit erlaubten Symbolen

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

KONVENTIONEN SPAREN KLAMMERN

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

– $\exists y (\text{Gerade}(y) \wedge \geq(y, 2)) \Rightarrow (= (y, 2) \wedge > (y, 20))$??

– $\exists y \text{ Gerade}(y) \wedge (\geq(y, 2) \Rightarrow (= (y, 2) \wedge > (y, 20)))$??

– $\exists y (\text{Gerade}(y) \wedge (\geq(y, 2) \Rightarrow = (y, 2))) \wedge > (y, 20)$??

KONVENTIONEN SPAREN KLAMMERN

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

– $\exists y (\text{Gerade}(y) \wedge \geq(y, 2)) \Rightarrow (= (y, 2) \wedge > (y, 20))$??

– $\exists y \text{ Gerade}(y) \wedge (\geq(y, 2) \Rightarrow (= (y, 2) \wedge > (y, 20)))$??

– $\exists y (\text{Gerade}(y) \wedge (\geq(y, 2) \Rightarrow = (y, 2))) \wedge > (y, 20)$??

● **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

KONVENTIONEN SPAREN KLAMMERN

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

– $\exists y (\text{Gerade}(y) \wedge \geq(y, 2)) \Rightarrow (= (y, 2) \wedge > (y, 20))$??

– $\exists y \text{ Gerade}(y) \wedge (\geq(y, 2) \Rightarrow (= (y, 2) \wedge > (y, 20)))$??

– $\exists y (\text{Gerade}(y) \wedge (\geq(y, 2) \Rightarrow = (y, 2))) \wedge > (y, 20)$??

● **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 $A \Rightarrow (B \Rightarrow C)$

KONVENTIONEN SPAREN KLAMMERN

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

– $\exists y (\text{Gerade}(y) \wedge \geq(y, 2)) \Rightarrow (= (y, 2) \wedge > (y, 20))$??

– $\exists y \text{ Gerade}(y) \wedge (\geq(y, 2) \Rightarrow (= (y, 2) \wedge > (y, 20)))$??

– $\exists y (\text{Gerade}(y) \wedge (\geq(y, 2) \Rightarrow = (y, 2))) \wedge > (y, 20)$??

● **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**

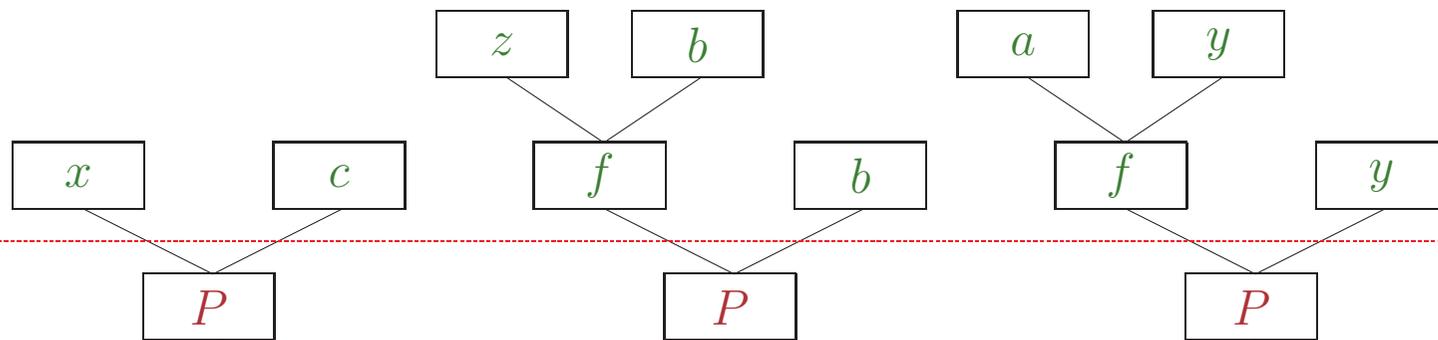
– Px entspricht $P(x)$ und fxy entspricht $f(x, y)$

– $\exists xyz A$ 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** $\forall abc \exists xyz Pxc \wedge P(fzb, b) \vee \neg P(fay, y)$

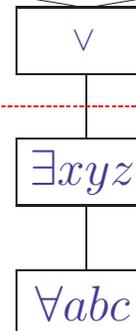
Terme
(Unifikation)



Aussagenlogik
(Ebene der Beweissuche)



Quantoren



- **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 philosophischen 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 $\varphi : \mathcal{U}^n \rightarrow \mathcal{U}$ $(f \in \mathcal{F}^n)$

- $\iota(P)$ Funktion $\Pi : \mathcal{U}^n \rightarrow \{\text{wahr, falsch}\}$ $(P \in \mathcal{P}^n)$

- **Homomorphe Fortsetzung auf Terme und Formeln**

- $\iota(f(t_1, \dots, t_n)) = \iota(f)(\iota(t_1), \dots, \iota(t_n))$

- $\iota(\text{ff}) = \text{falsch}$

- $\iota(P(t_1, \dots, t_n)) = \iota(P)(\iota(t_1), \dots, \iota(t_n))$.

- $\iota((A)) = \iota(A)$

SEMANTIK DER PRÄDIKATENLOGIK (II)

FORTSETZUNG VON ι AUF ZUSAMMENGESetzte FORMELN

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

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

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

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

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

$$\iota_x^u(x) = u, \text{ sonst } \iota_x^u = \iota$$

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

SEMANTIK DER PRÄDIKATENLOGIK (II) – KLASSISCH

FORTSETZUNG VON ι AUF ZUSAMMENGESetzte FORMELN

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

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

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

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

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

$\iota_x^u(x) = u, \text{ sonst } \iota_x^u = \iota$

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

Ist das wirklich dasselbe?

- Was genau heißt **oder, wann immer, es gibt**?
 - Gilt $A \vee B$, wenn A und B nicht beide falsch sind?
 - Gilt $A \Rightarrow B$, wenn A falsch oder B wahr ist?
 - Gilt $\exists x A$, wenn A nicht für alle x falsch ist?

- 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?

- **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”*?

- **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

- **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 Formelmengemenge \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 Formelmengemenge mit allen Formeln, die daraus logisch folgen

Syntaktische Manipulation formaler Ausdrücke unter Berücksichtigung der Semantik

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

$$\text{aus } A \text{ und } A \Rightarrow B \text{ folgt } B: \quad \frac{A, A \Rightarrow B}{B}$$

- **Regelschema** $\frac{A_1, \dots, A_n}{C}$: aus $\underbrace{A_1 \text{ und } \dots \text{ und } A_n}_{\text{Prämissen}}$ folgt $\underbrace{C}_{\text{Konklusion}}$

- **Axiom:** Regel ohne Prämissen

- $\Gamma \vdash_{r_s} C$: Konkrete Anwendung des Regelschemas r_s

- **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

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

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

● Analytisch

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

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

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

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

• Nur eine Inferenzregel

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

• 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?

$\wedge -I$	$\frac{A \quad B}{A \wedge B}$	$\wedge -E$	$\frac{A \wedge B}{A} \quad \frac{A \wedge B}{B}$
$\vee -I$	$\frac{A}{A \vee B} \quad \frac{B}{A \vee B}$	$\vee -E$	$\frac{A \vee B \quad \begin{matrix} [A] \\ C \end{matrix} \quad \begin{matrix} [B] \\ C \end{matrix}}{C}$
$\Rightarrow -I$	$\frac{\begin{matrix} [A] \\ B \end{matrix}}{A \Rightarrow B}$	$\Rightarrow -E$	$\frac{A \quad A \Rightarrow B}{B}$
$\neg -I$	$\frac{\begin{matrix} [A] \\ \text{ff} \end{matrix}}{\neg A}$	$\neg -E$	$\frac{\neg A \quad A}{\text{ff}}$
$excl-m$	$\overline{A \vee \neg A}$	$ff-E$	$\frac{\text{ff}}{\overline{A}}$

- 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. 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. 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. 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. 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. 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. 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. 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

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

$$\begin{array}{c}
 \frac{[A] \frac{[(A \Rightarrow B) \wedge (B \Rightarrow C)]}{(A \Rightarrow B)} \wedge\text{-E}}{B} \Rightarrow\text{-E} \quad \frac{[(A \Rightarrow B) \wedge (B \Rightarrow C)]}{(B \Rightarrow C)} \wedge\text{-E}}{C} \Rightarrow\text{-E} \\
 \frac{C}{(A \Rightarrow C)} \Rightarrow\text{-I} \\
 \frac{(A \Rightarrow C)}{((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)} \Rightarrow\text{-I}
 \end{array}$$

SEQUENZENKALKÜLE

- **Schließen über Aussagen mit Annahmen**

- Lokale Sicht: keine globale Verwaltung der Annahmen nötig

- **Grundkonzept Sequenz:** $\underbrace{A_1, \dots, A_n}_{\text{Antezedent } \Gamma} \vdash \underbrace{B_1, \dots, B_m}_{\text{Sukzedent } \Phi}$

- Lesart “*Eine der Formeln B_i folgt aus den Annahmen A_1, \dots, A_n ”*”

- **Zielsequenz** $\vdash C$ (“*Formel C gilt ohne weitere Annahmen*”)

- **Semantik entspricht** $A_1 \wedge \dots \wedge A_n \Rightarrow B_1 \vee \dots \vee B_m$

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

- 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})

$\neg\neg\text{-}R \quad \frac{\Gamma, A \vdash \Phi}{\Gamma \vdash \Phi, \neg A}$ $\wedge\text{-}R \quad \frac{\Gamma \vdash \Phi, A \quad \Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \wedge B}$ $\vee\text{-}R \quad \frac{\Gamma \vdash \Phi, A}{\Gamma \vdash \Phi, A \vee B} \quad \frac{\Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \vee B}$ $\Rightarrow\text{-}R \quad \frac{\Gamma, A \vdash \Phi, B}{\Gamma \vdash \Phi, A \Rightarrow B}$ $\text{axiom} \quad \frac{}{A \vdash A}$	$\neg\neg\text{-}L \quad \frac{\Gamma \vdash \Phi, A}{\Gamma, \neg A \vdash \Phi}$ $\wedge\text{-}L \quad \frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi} \quad \frac{\Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi}$ $\vee\text{-}L \quad \frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \vee B \vdash \Phi}$ $\Rightarrow\text{-}L \quad \frac{\Gamma \vdash \Phi, A \quad \Delta, B \vdash \Psi}{\Gamma, \Delta, A \Rightarrow B \vdash \Phi, \Psi}$
--	--

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

$$\frac{\frac{\frac{A \vdash A \quad B \vdash B}{A, A \Rightarrow B \vdash B} \Rightarrow\text{-}L \quad C \vdash C}{A, A \Rightarrow B, B \Rightarrow C \vdash C} \Rightarrow\text{-}L}{\frac{A, A \Rightarrow B, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}{A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C} \wedge\text{-}L} \wedge\text{-}L \text{ (+ Kontraktion!)}$$

$$\frac{A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C} \Rightarrow\text{-}R$$

$$\frac{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C}{\vdash ((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow A \Rightarrow C} \Rightarrow\text{-}R$$

- **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

$$\boxed{\begin{array}{c} H \vdash G \\ H_1 \vdash G_1 \\ \vdots \\ H_n \vdash G_n \end{array}}$$

Beweisbarkeit der Teilziele impliziert Beweisbarkeit des Hauptziels

- Regeln sind implementierbar durch Pattern Matching und Instantiierung

• Anwendung des Regelschemas für Konjunktionen

$$H \vdash A \wedge B$$
$$H \vdash A$$
$$H \vdash B$$

andR

$$\vdash (P \Rightarrow Q) \wedge (R \Rightarrow Q) \quad \text{BY andR}$$

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

• Anwendung des Regelschemas für Konjunktionen

$$H \vdash A \wedge B$$

$$H \vdash A$$

$$H \vdash B$$

andR

$$\vdash (P \Rightarrow Q) \wedge (R \Rightarrow Q) \quad \text{BY andR}$$

$$1. \vdash P \Rightarrow Q$$

$$2. \vdash R \Rightarrow Q$$

- 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

$$H, A, H' \vdash A$$

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

$$H \vdash A \Rightarrow B$$
$$H, A \vdash B$$

`impliesR`

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

$$H \vdash A \Rightarrow B$$

$$H, A \vdash B$$

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

$$H, A \Rightarrow B, H' \vdash C$$

$$H, A \Rightarrow B, H' \vdash A$$

$$H, B, H' \vdash C$$

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 <code>impliesR</code>
1. $P \vdash P$	BY <code>axiom</code>

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

• Beweis für $P \Rightarrow (Q \Rightarrow P)$

$\vdash P \Rightarrow (Q \Rightarrow P)$	BY <code>impliesR</code>
1. $P \vdash Q \Rightarrow P$	BY <code>impliesR</code>
1.1. $P, Q \vdash P$	BY <code>axiom</code>

- 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

$$H \vdash A \wedge B$$
$$H \vdash A$$
$$H \vdash B$$

andR

- **Konjunktion auf linker Seite einer Sequenz**

– Die Annahme $A \wedge B$ ist äquivalent zu den beiden Annahmen A und B

$$H, A \wedge B, H' \vdash C$$
$$H, A, B, H' \vdash C$$

andL

ANWENDUNG DER KONJUNKTIONSREGELN

• Beweis für $P \Rightarrow (Q \Rightarrow (P \wedge Q))$

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

• Beweis für $(P \wedge Q) \Rightarrow P$

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

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

$$\begin{array}{l} H \vdash A \vee B \\ H \vdash A \end{array}$$

orR1

$$\begin{array}{l} H \vdash A \vee B \\ H \vdash B \end{array}$$

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)

$$\begin{array}{l} H, A \vee B, H' \vdash C \\ H, A, H' \vdash C \\ H, B, H' \vdash C \end{array}$$

orL

ANWENDUNG DER DISJUNKTIONSREGELN

• Beweis für $P \Rightarrow (P \vee Q)$

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

• Beweis für $(P \vee Q) \Rightarrow (Q \vee P)$

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

REGELN FÜR NEGATION

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

• Negation auf rechter Seite einer Sequenz

- Um $H \vdash \neg A$ zu zeigen, muß aus Annahme A ein Widerspruch folgen

$$\boxed{\begin{array}{l} H \vdash \neg A \\ H, A \vdash \text{ff} \end{array}}$$

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 (!)

$$\boxed{\begin{array}{l} H, \neg A, H' \vdash C \\ H, \neg A, H' \vdash A \end{array}}$$

notL

ANWENDUNG DER NEGATIONSREGELN

• Beweis für $P \Rightarrow \neg\neg P$

$\vdash P \Rightarrow \neg\neg P$	BY <code>impliesR</code>
1. $P \vdash \neg\neg P$	BY <code>notR</code>
1.1. $P, (\neg P) \vdash \text{ff}$	BY <code>notL</code>
1.1.1. $P, (\neg P) \vdash P$	BY <code>axiom</code>

• Beweis für $\neg(P \vee Q) \Rightarrow \neg P$

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

EIN KOMPLEXERER BEWEIS

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

WAS PASSIERT MIT $P \vee \neg P$, $\neg\neg P \Rightarrow P$, ETC.?

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

$\vdash P \vee \neg P$	BY	orR1
1. $\vdash P$	BY	?????

$\vdash P \vee \neg P$	BY	orR2
1. $\vdash \neg P$	BY	notR
1.1. $P \vdash \text{ff}$	BY	?????

– Beide Ansätze können nicht fortgesetzt werden

WAS PASSIERT MIT $P \vee \neg P$, $\neg\neg P \Rightarrow P$, ETC.?

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

$\vdash P \vee \neg P$	BY	orR1
1. $\vdash P$	BY	?????

$\vdash P \vee \neg P$	BY	orR2
1. $\vdash \neg P$	BY	notR
1.1. $P \vdash \text{ff}$	BY	?????

– Beide Ansätze können nicht fortgesetzt werden

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

$\vdash \neg\neg P \Rightarrow P$	BY	impliesR
1. $\neg\neg P \vdash P$	BY	notL
1.1. $\neg\neg P \vdash \neg P$	BY	notR
1.1.1. $\neg\neg P, P \vdash \text{ff}$	BY	?????

– Keine sinnvolle Fortsetzung möglich

WAS PASSIERT MIT $P \vee \neg P$, $\neg\neg P \Rightarrow P$, ETC.?

• Beweisansätze für $P \vee \neg P$

$\vdash P \vee \neg P$	BY	orR1
1. $\vdash P$	BY	?????

$\vdash P \vee \neg P$	BY	orR2
1. $\vdash \neg P$	BY	notR
1.1. $P \vdash \text{ff}$	BY	?????

– Beide Ansätze können nicht fortgesetzt werden

• Beweisansatz für $\neg\neg P \Rightarrow P$

$\vdash \neg\neg P \Rightarrow P$	BY	impliesR
1. $\neg\neg P \vdash P$	BY	notL
1.1. $\neg\neg P \vdash \neg P$	BY	notR
1.1.1. $\neg\neg P, P \vdash \text{ff}$	BY	?????

– Keine sinnvolle Fortsetzung möglich

• Beweisansatz 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	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

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	$H \vdash \neg A$ $H, A \vdash \text{ff}$	notR
		$H, A, H' \vdash A$	axiom
<i>Zusatzregel für klassische Logik</i>		$H \vdash A \vee \neg A$	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

$$H \vdash C$$
$$H \vdash A$$
$$H, A \vdash C$$

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

$$H, A, H' \vdash C$$
$$H, H' \vdash C$$

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 <code>impliesR</code>
1. $\neg\neg P \vdash P$	BY <code>cut</code> $P \vee \neg P$
1.1. $\neg\neg P, P \vee \neg P \vdash P$	BY <code>orL</code>
1.1.1 $\neg\neg P, P \vdash P$	BY <code>axiom</code>
1.1.2 $\neg\neg P, \neg P \vdash P$	BY <code>notL</code>
1.1.2.1 $\neg\neg P, \neg P \vdash P$	BY <code>axiom</code>

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

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

● **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 $\iota_x^u(B)$ erklärt
· $\iota_x^u(B)$ muß für alle oder einen Wert u wahr werden
- ι_x^u modifiziert die Interpretation ι für die gebundene Variable x
- Regeln benötigen **Ersetzung von Variablen durch Terme**
um den semantischen Effekt von ι_x^u syntaktisch zu simulieren

● **Formales Konzept: Substitution $B[t/x]$** auch $B\{x \setminus t\}$ 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

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

$f(t_1, \dots, t_n)$ freie Vorkommen von x in t_i bleiben frei

$P(t_1, \dots, t_n)$ 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

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

$f(t_1, \dots, t_n)$ freie Vorkommen von x in t_i bleiben frei

$P(t_1, \dots, t_n)$ 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

$$(\forall x (P(x) \wedge Q(x))) \wedge R(x)$$

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

$f(t_1, \dots, t_n)$ freie Vorkommen von x in t_i bleiben frei

$P(t_1, \dots, t_n)$ 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

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

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

$f(t_1, \dots, t_n)$ freie Vorkommen von x in t_i bleiben frei

$P(t_1, \dots, t_n)$ 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

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

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

$f(t_1, \dots, t_n)$ freie Vorkommen von x in t_i bleiben frei

$P(t_1, \dots, t_n)$ 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

x frei und gebunden

x gebunden

$(\forall x (P(x) \wedge Q(x))) \wedge R(x)$

x frei *x frei*

SUBSTITUTION $B[t/x]$ FORMAL

Endliche Abbildung σ von Variablen in Terme

- $\sigma = [t_1, \dots, t_n / x_1, \dots, x_n] \hat{=} \sigma(x_1)=t_1, \dots, \sigma(x_n)=t_n$
- $A\sigma$: Anwendung von σ auf den Ausdruck A τ und σ

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

*: $y \neq x$, 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 $B[x'/x]$

$$H \vdash \forall x B$$

$$H \vdash B[x'/x]$$

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

$$H, \forall x B, H' \vdash C$$

$$H, \forall x B, B[t/x], H' \vdash C$$

allL t

ANWENDUNG DER ALLQUANTORREGELN

• Beweis für $\forall x (Px \Rightarrow Px)$

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

• Beweis für $(\forall x Px) \Rightarrow Pa$

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

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

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

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

$$H \vdash \exists x B$$

$$H \vdash B[t/x]$$

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 $B[x'/x]$

$$H, \exists x B, H' \vdash C$$

$$H, B[x'/x], H' \vdash C$$

exL

ANWENDUNG DER EXISTENZQUANTORREGELN

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

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

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

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

ANWENDUNG DER EXISTENZQUANTORREGELN

• Beweis für $Pa \Rightarrow (\exists x Px)$

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

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

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

– Reihenfolge der Regelanwendungen wichtig für erfolgreichen Beweis

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

EIN KOMPLEXERER BEWEIS

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

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	$H \vdash \neg A$ $H, A \vdash \text{ff}$	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
<i>t ist ein beliebiger Term, x' eine neue Variable</i>			
<i>Zusatzregel für klassische Logik</i>		$H \vdash A \vee \neg A$	magic

● 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**

- **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