

Natural Deduction*

Andreas Lochbihler

Department of Computer Science
ETH Zurich

*Thanks to David Basin for slide material

Formal reasoning about systems

- Requirements
 1. Language
 2. Semantics
 3. Deductive system for carrying out proofs
- Metatheorems relate these, e.g., soundness and completeness
 - ▶ We focus on (1) and (3) and only comment briefly on (2)
 - ▶ Most of this should be a review (logic/discrete math)
- Proofs are essential for both parts of the course

Some formality now allows (slightly) less formality later

Road map

Natural deduction

- Propositional logic
- First-order logic
- Equality

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

- Prove \oplus !

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

- Prove \oplus !

1. $+$ holds by δ .

2. \otimes holds by α with **1**.

3. \times holds by β with **1**.

4. \oplus holds by γ with **2** and **3**.

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

1. $+$ holds by δ .
2. \otimes holds by α with **1**.
3. \times holds by β with **1**.
4. \oplus holds by γ with **2** and **3**.

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

1. $+$ holds by δ .
2. \otimes holds by α with **1**.
3. \times holds by β with **1**.
4. \oplus holds by γ with **2** and **3**.

- Derivation tree:

$$\oplus$$

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

- $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Derivation tree:

$$\frac{\otimes \qquad \times}{\oplus} \gamma$$

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

- $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Derivation tree:

$$\frac{\frac{+}{\otimes} \alpha \qquad \times}{\oplus} \gamma$$

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

- $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Derivation tree:

$$\frac{\frac{\frac{}{+} \delta}{\otimes} \alpha \quad \times}{\oplus} \gamma$$

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

- $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Derivation tree:

$$\frac{\frac{\frac{}{+} \delta}{\otimes} \alpha \quad \frac{+}{\times} \beta}{\oplus} \gamma$$

An abstract example of a formal proof

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.
- Deductive proof system:

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : $+$ holds.

$$\frac{+}{\otimes} \alpha \qquad \frac{+}{\times} \beta$$

$$\frac{\otimes \quad \times}{\oplus} \gamma \qquad \frac{}{+} \delta$$

- Prove \oplus !

- $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Derivation tree:

$$\frac{\frac{\frac{}{+} \delta}{\otimes} \alpha \quad \frac{\frac{}{+} \delta}{\times} \beta}{\oplus} \gamma$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

1. Assume $+$ holds by δ .
2. \otimes holds by α with 1.
3. \times holds by β with 1.
4. \oplus holds by γ with 2 and 3.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

1. Assume $+$ holds by δ .
2. \otimes holds by α with 1.
3. \times holds by β with 1.
4. \oplus holds by γ with 2 and 3.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\vdash \oplus$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

- Assume $+$ holds by δ .
- \otimes holds by α with 1.
- \times holds by β with 1.
- \oplus holds by γ with 2 and 3.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\frac{+ \vdash \oplus}{\vdash \oplus} \delta$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

- Assume $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Deductive proof system:

$$\frac{}{\dots, A, \dots \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\frac{\frac{\frac{+ \vdash \otimes \quad + \vdash \times}{\quad} \gamma}{+ \vdash \oplus} \delta}{\vdash \oplus}$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

- Assume $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\frac{\frac{\frac{+ \vdash +}{+ \vdash \otimes} \alpha \quad + \vdash \times}{+ \vdash \oplus} \gamma}{\vdash \oplus} \delta$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

- Assume $+$ holds by δ .
- \otimes holds by α with 1.
- \times holds by β with 1.
- \oplus holds by γ with 2 and 3.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\frac{\frac{\frac{}{+ \vdash +} \text{ axiom}}{+ \vdash \otimes} \alpha \quad + \vdash \times}{+ \vdash \oplus} \gamma \quad \frac{}{\vdash \oplus} \delta$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

- Assume $+$ holds by δ .
- \otimes holds by α with **1**.
- \times holds by β with **1**.
- \oplus holds by γ with **2** and **3**.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\frac{\frac{\frac{}{+ \vdash +} \text{ axiom}}{+ \vdash \otimes} \alpha \quad \frac{+ \vdash +}{+ \vdash \times} \beta}{+ \vdash \oplus} \gamma \quad \frac{}{\vdash \oplus} \delta$$

Natural deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$.

- Rules:

α : If $+$, then \otimes .

β : If $+$, then \times .

γ : If \otimes and \times , then \oplus .

δ : We may assume $+$
only when proving \oplus .

- Prove \oplus !

1. Assume $+$ holds by δ .
2. \otimes holds by α with 1.
3. \times holds by β with 1.
4. \oplus holds by γ with 2 and 3.

- Deductive proof system:

$$\frac{}{..., A, ... \vdash A} \text{ axiom}$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \otimes} \alpha$$

$$\frac{\Gamma \vdash +}{\Gamma \vdash \times} \beta$$

$$\frac{\Gamma \vdash \otimes \quad \Gamma \vdash \times}{\Gamma \vdash \oplus} \gamma$$

$$\frac{\Gamma, + \vdash \oplus}{\Gamma \vdash \oplus} \delta$$

- Derivation tree:

$$\frac{\frac{\frac{}{+ \vdash +} \text{ axiom}}{+ \vdash \otimes} \alpha \quad \frac{\frac{}{+ \vdash +} \text{ axiom}}{+ \vdash \times} \beta}{+ \vdash \oplus} \gamma}{\vdash \oplus} \delta$$

Natural deduction

- Developed by Gentzen (1930s) and Prawitz (1960s)
- **Rules** are used to construct derivations under assumptions.

$A_1, \dots, A_n \vdash A$ reads as “ A follows from A_1, \dots, A_n ”

- **Derivations** are trees

$$\begin{array}{c}
 \frac{}{A, B \vdash A} \textit{axiom} \qquad \frac{}{A, B \vdash B} \textit{axiom} \\
 \hline
 \frac{}{A, B \vdash A \wedge B} \wedge\text{-I} \\
 \frac{}{A \vdash B \rightarrow A \wedge B} \rightarrow\text{-I} \\
 \hline
 \vdash A \rightarrow B \rightarrow A \wedge B \quad \rightarrow\text{-I}
 \end{array}$$

- A **proof** is a derivation whose root has no assumptions

Road map

- Natural deduction

Propositional logic

- First-order logic
- Equality

Propositional logic: syntax

- Propositions are built from a collection of variables and closed under disjunction, conjunction, implication, . . .
- More formally: Let a set \mathcal{V} of variables be given. \mathcal{L}_P , the **language of propositional logic**, is the smallest set where:
 - ▶ $X \in \mathcal{L}_P$ if $X \in \mathcal{V}$.
 - ▶ $\perp \in \mathcal{L}_P$.
 - ▶ $A \wedge B \in \mathcal{L}_P$ if $A \in \mathcal{L}_P$ and $B \in \mathcal{L}_P$.
 - ▶ $A \vee B \in \mathcal{L}_P$ if $A \in \mathcal{L}_P$ and $B \in \mathcal{L}_P$.
 - ▶ $A \rightarrow B \in \mathcal{L}_P$ if $A \in \mathcal{L}_P$ and $B \in \mathcal{L}_P$.
- In the following: X ranges over variables, A and B over formulae

Propositional logic: semantics

- A **valuation** $\sigma : \mathcal{V} \rightarrow \{\mathbf{True}, \mathbf{False}\}$ is a function mapping variables to truth values (truth assignment).
Let *Valuations* be the set of valuations.
 - ▶ Valuations are simple kinds of models (interpretations).
- **Satisfiability**: smallest relation $\models \subseteq \text{Valuations} \times \mathcal{L}_P$ such that
 - ▶ $\sigma \models X$, iff $\sigma(X) = \mathbf{True}$
 - ▶ $\sigma \models A \wedge B$, iff $\sigma \models A$ and $\sigma \models B$
 - ▶ $\sigma \models A \vee B$, iff $\sigma \models A$ or $\sigma \models B$
 - ▶ $\sigma \models A \rightarrow B$, iff whenever $\sigma \models A$ then $\sigma \models B$
- Note that $\sigma \not\models \perp$, for every $\sigma \in \text{Valuations}$

Propositional logic: semantics (cont.)

- A formula $A \in \mathcal{L}_P$ is **satisfiable** if
$$\sigma \models A, \text{ for some valuation } \sigma$$
- A formula $A \in \mathcal{L}_P$ is **valid** (a **tautology**) if
$$\sigma \models A, \text{ for all valuations } \sigma$$
- **Semantic entailment**: $A_1, \dots, A_n \models A$ if
$$\text{for all } \sigma, \text{ if } \sigma \models A_1, \dots, \sigma \models A_n \text{ then } \sigma \models A$$
- Examples:
 - ▶ $X \wedge Y$

Propositional logic: semantics (cont.)

- A formula $A \in \mathcal{L}_P$ is **satisfiable** if
$$\sigma \models A, \text{ for some valuation } \sigma$$
- A formula $A \in \mathcal{L}_P$ is **valid** (a **tautology**) if
$$\sigma \models A, \text{ for all valuations } \sigma$$
- **Semantic entailment**: $A_1, \dots, A_n \models A$ if
$$\text{for all } \sigma, \text{ if } \sigma \models A_1, \dots, \sigma \models A_n \text{ then } \sigma \models A$$
- Examples:
 - ▶ $X \wedge Y$ satisfiable, as $\sigma \models X \wedge Y$ for $\sigma(X) = \sigma(Y) = \mathbf{True}$
 - ▶ $X \rightarrow X$

Propositional logic: semantics (cont.)

- A formula $A \in \mathcal{L}_P$ is **satisfiable** if
$$\sigma \models A, \text{ for some valuation } \sigma$$
- A formula $A \in \mathcal{L}_P$ is **valid** (a **tautology**) if
$$\sigma \models A, \text{ for all valuations } \sigma$$
- **Semantic entailment**: $A_1, \dots, A_n \models A$ if
$$\text{for all } \sigma, \text{ if } \sigma \models A_1, \dots, \sigma \models A_n \text{ then } \sigma \models A$$
- Examples:
 - ▶ $X \wedge Y$ satisfiable, as $\sigma \models X \wedge Y$ for $\sigma(X) = \sigma(Y) = \mathbf{True}$
 - ▶ $X \rightarrow X$ valid
 - ▶ $\neg X, X \vee Y \models Y$

Propositional logic: semantics (cont.)

- A formula $A \in \mathcal{L}_P$ is **satisfiable** if
$$\sigma \models A, \text{ for some valuation } \sigma$$
- A formula $A \in \mathcal{L}_P$ is **valid** (a **tautology**) if
$$\sigma \models A, \text{ for all valuations } \sigma$$
- **Semantic entailment**: $A_1, \dots, A_n \models A$ if
$$\text{for all } \sigma, \text{ if } \sigma \models A_1, \dots, \sigma \models A_n \text{ then } \sigma \models A$$
- Examples:
 - ▶ $X \wedge Y$ satisfiable, as $\sigma \models X \wedge Y$ for $\sigma(X) = \sigma(Y) = \mathbf{True}$
 - ▶ $X \rightarrow X$ valid
 - ▶ $\neg X, X \vee Y \models Y$ holds, as $\sigma \models \neg X$ and $\sigma \models X \vee Y$ constrain σ to $\sigma(X) = \mathbf{False}$ and $\sigma(Y) = \mathbf{True}$, so $\sigma \models Y$.

Requirements for a deductive system

- Syntactic entailment \vdash (derivation rules) and semantic entailment \models (truth tables) should agree

- This requirement has two parts:

Soundness: If $H \vdash A$ can be derived, then $H \models A$

Completeness: If $H \models A$, then $H \vdash A$ can be derived

For $H \equiv A_1, \dots, A_n$ some collection of formulae.

- These are key requirements for any logic
- **Decidability** is another important property

What is the complexity of determining if a proposition is satisfiable? A tautology?

Natural deduction for propositional formulae

- A **sequent** is an assertion (judgement) of the form

$$A_1, \dots, A_n \vdash A$$

where all A, A_1, \dots, A_n are propositional formulae

- Intuitively: A follows from the A_i s

If logic is sound, this means A_i s semantically entail A

- **Axiom**: starting point for building derivation trees

$$\frac{}{\dots, A, \dots \vdash A} \text{ axiom}$$

- A **proof** of A is a derivation tree with root $\vdash A$.

If logic is sound, then A is a tautology

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$X \wedge (Y \wedge Z) \vdash X \wedge Z$$

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$\frac{\Gamma \vdash X \quad \Gamma \vdash Z}{\underbrace{X \wedge (Y \wedge Z)}_{\equiv \Gamma} \vdash X \wedge Z} \wedge\text{-}I$$

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$\frac{\frac{\Gamma \vdash X \wedge \quad ???}{\Gamma \vdash X} \wedge\text{-}EL \quad \Gamma \vdash Z}{\underbrace{X \wedge (Y \wedge Z)}_{\equiv \Gamma} \vdash X \wedge Z} \wedge\text{-}I$$

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$\frac{\frac{\frac{}{\Gamma \vdash X \wedge (Y \wedge Z)} \text{axiom}}{\Gamma \vdash X} \wedge\text{-}EL \quad \Gamma \vdash Z}{\underbrace{X \wedge (Y \wedge Z)}_{\equiv \Gamma} \vdash X \wedge Z} \wedge\text{-}I$$

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$\frac{\frac{\frac{}{\Gamma \vdash X \wedge (Y \wedge Z)} \text{axiom}}{\Gamma \vdash X} \wedge\text{-}EL \quad \frac{\Gamma \vdash ? \wedge Z}{\Gamma \vdash Z} \wedge\text{-}ER}{\underbrace{X \wedge (Y \wedge Z)}_{\equiv \Gamma} \vdash X \wedge Z} \wedge\text{-}I$$

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$\frac{\frac{\frac{}{\Gamma \vdash X \wedge (Y \wedge Z)} \text{axiom}}{\Gamma \vdash X} \wedge\text{-}EL \quad \frac{\frac{\frac{\Gamma \vdash ?? \wedge (? \wedge Z)}{\Gamma \vdash ? \wedge Z} \wedge\text{-}ER}{\Gamma \vdash Z} \wedge\text{-}ER}{\underbrace{X \wedge (Y \wedge Z)}_{\equiv \Gamma} \vdash X \wedge Z} \wedge\text{-}I$$

Conjunction

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Example derivation

$$\frac{\frac{\frac{\Gamma \vdash X \wedge (Y \wedge Z)}{\Gamma \vdash X} \wedge\text{-}EL \quad \frac{\frac{\frac{\Gamma \vdash X \wedge (Y \wedge Z)}{\Gamma \vdash Y \wedge Z} \wedge\text{-}ER \quad \frac{\Gamma \vdash Y \wedge Z}{\Gamma \vdash Z} \wedge\text{-}ER}{\Gamma \vdash Z} \wedge\text{-}I}{\underbrace{X \wedge (Y \wedge Z)}_{\equiv \Gamma} \vdash X \wedge Z} \wedge\text{-}I \quad \text{axiom} \quad \text{axiom}$$

Conjunction (cont.)

- Rules of two kinds: **introduce** and **eliminate** connectives

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

- Each rule is sound in that it preserves semantic entailment.
E.g., for $\wedge\text{-}I$

$$\text{if } \Gamma \models A \text{ and } \Gamma \models B \text{ then } \Gamma \models A \wedge B$$

- If all rules preserve semantic entailment, logic is sound. (proof?)
- Can we **prove** anything with just these three rules?

Equivalently: which (purely conjunctive) formulae are tautologies?

Implication

- Rules

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow{-I} \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow{-E}$$

- Application of $\rightarrow{-I}$ turns last derivation into a proof

$$\frac{\vdots \quad \overline{A \wedge (B \wedge C) \vdash A \wedge C}}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C} \rightarrow{-I}$$

- Examples: (\rightarrow right associative and \wedge binds stronger than \rightarrow)

$$\vdash X \rightarrow Y \rightarrow X$$

$$\vdash (X \rightarrow Y \rightarrow Z) \rightarrow (X \rightarrow Y) \rightarrow X \rightarrow Z$$

$$\vdash (X \wedge Y) \rightarrow (Y \wedge X)$$

Disjunction

- Rules

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee\text{-}IL \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee\text{-}IR$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-}E$$

- Elimination rule formalizes proof by cases
- Example: formalize and prove

When it rains then I wear my jacket.

When it snows then I wear my jacket.

It is raining or snowing.

Therefore I wear my jacket.

Falsity and negation

- Falsity

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \perp\text{-}E$$

- Negation: define $\neg A$ as $A \rightarrow \perp$.

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash B} \neg\text{-}E \quad \text{derived by} \quad \frac{\Gamma \vdash \overbrace{\neg A}^{A \rightarrow \perp} \quad \Gamma \vdash A}{\frac{\Gamma \vdash \perp}{\Gamma \vdash B} \perp\text{-}E} \rightarrow\text{-}E$$

Intuitionistic versus classical logic

- Peirce's Law: $((A \rightarrow B) \rightarrow A) \rightarrow A$. Is this valid? Provable?
 - We have only intuitionistic logic. Classical logic requires either
 - ▶ axiom of excluded middle $\frac{}{\Gamma \vdash A \vee \neg A} TND$ ("tertium non datur")
 - ▶ or rule $\frac{\Gamma, \neg A \vdash \perp}{\Gamma \vdash A} RAA$ ("reductio ad absurdum")
 - Example: There exist irrationals a and b such that a^b is rational
- Proof:** Let b be $\sqrt{2}$ and consider whether or not b^b is rational
- Case 1: If rational, let $a = b = \sqrt{2}$
- Case 2: If irrational, let $a = \sqrt{2}^{\sqrt{2}}$ then

$$a^b = \left(\sqrt{2}^{\sqrt{2}} \right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$$

Finding ND proofs

- Prove statement on paper first, then translate to formal proof.

Finding ND proofs

- Prove statement on paper first, then translate to formal proof.
- Heuristic for backwards proofs: Apply safe rules first.
 - ▶ Rule is **safe** if we only enlarge Γ or can get the conclusion back.

▶ \wedge -I is safe:

$$\frac{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER}{\Gamma \vdash A \wedge B} \wedge\text{-}I$$

Finding ND proofs

- Prove statement on paper first, then translate to formal proof.
- Heuristic for backwards proofs: Apply safe rules first.
 - Rule is **safe** if we only enlarge Γ or can get the conclusion back.

► \wedge -I is safe:

$$\frac{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-EL} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-ER}}{\Gamma \vdash A \wedge B} \wedge\text{-I}$$

► \vee -E + *axiom* is safe:

$$\frac{\frac{\text{axiom}}{\Gamma \vdash A \vee B} \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-E}$$

Finding ND proofs

- Prove statement on paper first, then translate to formal proof.
- Heuristic for backwards proofs: Apply safe rules first.
 - Rule is **safe** if we only enlarge Γ or can get the conclusion back.

► \wedge -I is safe:

$$\frac{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-EL} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-ER}}{\Gamma \vdash A \wedge B} \wedge\text{-I}$$

► \vee -E + *axiom* is safe:

$$\frac{\frac{}{\Gamma \vdash A \vee B} \text{axiom} \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-E}$$

► \wedge -EL is unsafe:

$$\frac{\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-I}}{\Gamma \vdash A} \wedge\text{-EL}$$

Finding ND proofs

- Prove statement on paper first, then translate to formal proof.
- Heuristic for backwards proofs: Apply safe rules first.
 - Rule is **safe** if we only enlarge Γ or can get the conclusion back.

► \wedge -I is safe:

$$\frac{\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-EL} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-ER}}{\Gamma \vdash A \wedge B} \wedge\text{-I}$$

► \vee -E + *axiom* is safe:

$$\frac{\frac{\text{axiom}}{\Gamma \vdash A \vee B} \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-E}$$

► \wedge -EL is unsafe:

$$\frac{\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-I}}{\Gamma \vdash A} \wedge\text{-EL}$$

► How about the other rules?

Summary of derivation rules for propositional logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-}I \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-}EL \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-}ER$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow\text{-}I \quad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow\text{-}E$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee\text{-}IL \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee\text{-}IR$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee\text{-}E$$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \perp\text{-}E \quad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash B} \neg\text{-}E$$

Road map

- Natural deduction
- Propositional logic

First-order logic

- ▶ Syntax: variables over domain + functions, relations, quantifiers
- ▶ Semantics: interpreting domain, functions, and relations
- Equality

First-Order Logic: Syntax

- Two syntactic categories: **terms** and **formulae**
- A **signature** consists of a set of function symbols \mathcal{F} and a set of predicate symbols \mathcal{P} (and their arities)

Write f^i [or p^i] to indicate function symbol f [predicate symbol p] has arity $i \in \mathcal{N}$

N.B. constants are 0-ary function symbols

- Let \mathcal{V} be a set of variables
- *Term*, the **terms of first-order logic**, is the smallest set where
 1. $x \in \text{Term}$ if $x \in \mathcal{V}$, and
 2. $f^n(t_1, \dots, t_n) \in \text{Term}$ if $f^n \in \mathcal{F}$ and $t_j \in \text{Term}$, for all $1 \leq j \leq n$

Syntax (cont.)

- *Form*, the **formulae of first-order logic**, is the smallest set where
 1. $\perp \in \text{Form}$,
 2. $p^n(t_1, \dots, t_n) \in \text{Form}$ if $p^n \in \mathcal{P}$ and $t_j \in \text{Term}$, for all $1 \leq j \leq n$,
 3. $A \circ B \in \text{Form}$ if $A \in \text{Form}$, $B \in \text{Form}$, and $\circ \in \{\wedge, \vee, \rightarrow\}$, and
 4. $Qx.A \in \text{Form}$ if $A \in \text{Form}$, $x \in \mathcal{V}$, and $Q \in \{\forall, \exists\}$
- Each occurrence of each variable in a formula is **bound** or **free**.

$$(q(\textcolor{red}{x}) \vee \exists \textcolor{blue}{x}. \forall \textcolor{blue}{y}. p(f(\textcolor{blue}{x}), \textcolor{red}{z}) \wedge q(a)) \vee \forall \textcolor{blue}{x}. r(\textcolor{blue}{x}, \textcolor{red}{z}, g(\textcolor{blue}{x}))$$

A variable occurrence x in a formula A is **bound** if x occurs within a subformula of A of the form $\exists x.B$ or $\forall x.B$

- Analog from mathematics: $\textcolor{red}{x}^2 + \int_c^d \textcolor{red}{x} \cdot \textcolor{blue}{y} d\textcolor{blue}{y}$ or $\sum_{\textcolor{blue}{i}=0}^5 \textcolor{red}{x} \cdot \textcolor{blue}{i}$

Binding and α -conversion

- Names of bound variables are irrelevant, they just encode the binding structure.

$\exists x. \forall y. p(f(x), y) \wedge q(x, z)$ stands for 

- We can rename **bound** variables at any time (α -conversion).
 - Must preserve binding structure.

Binding and α -conversion

- Names of bound variables are irrelevant, they just encode the binding structure.

$\exists x. \forall y. p(f(x), y) \wedge q(x, z)$ stands for 

- We can rename **bound** variables at any time (α -conversion).
 - Must preserve binding structure.

- Examples:

α -convertible?

$$\forall x. \exists y. p(x, y)$$

$$\forall y. \exists x. p(y, x)$$

$$\exists z. \forall y. p(z, f(y))$$

$$\exists y. \forall y. p(y, f(y))$$

$$(\forall x. p(x)) \vee (\exists x. q(x)) \quad (\forall z. p(z)) \vee (\exists y. q(y))$$

$$p(x) \rightarrow \forall x. p(x)$$

$$p(y) \rightarrow \forall y. p(y)$$

Binding and α -conversion

- Names of bound variables are irrelevant, they just encode the binding structure.

$\exists x. \forall y. p(f(x), y) \wedge q(x, z)$ stands for 

- We can rename **bound** variables at any time (α -conversion).
 - Must preserve binding structure.

- Examples:

$$\forall x. \exists y. p(x, y)$$

$$\forall y. \exists x. p(y, x)$$

α -convertible?

yes

$$\exists z. \forall y. p(z, f(y))$$

$$\exists y. \forall y. p(y, f(y))$$

$$(\forall x. p(x)) \vee (\exists x. q(x))$$

$$(\forall z. p(z)) \vee (\exists y. q(y))$$

$$p(x) \rightarrow \forall x. p(x)$$

$$p(y) \rightarrow \forall y. p(y)$$

Binding and α -conversion

- Names of bound variables are irrelevant, they just encode the binding structure.

$\exists x. \forall y. p(f(x), y) \wedge q(x, z)$ stands for

- We can rename **bound** variables at any time (**α -conversion**).
 - ▶ Must preserve binding structure.

- Examples:

		α -convertible?
$\forall x. \exists y. p(x, y)$	$\forall y. \exists x. p(y, x)$	yes
$\exists z. \forall y. p(z, f(y))$	$\exists y. \forall y. p(y, f(y))$	no
$(\forall x. p(x)) \vee (\exists x. q(x))$	$(\forall z. p(z)) \vee (\exists y. q(y))$	
$p(x) \rightarrow \forall x. p(x)$	$p(y) \rightarrow \forall y. p(y)$	

Binding and α -conversion

- Names of bound variables are irrelevant, they just encode the binding structure.

$\exists x. \forall y. p(f(x), y) \wedge q(x, z)$ stands for 

- We can rename **bound** variables at any time (α -conversion).
 - Must preserve binding structure.

Examples:		α -convertible?
$\forall x. \exists y. p(x, y)$	$\forall y. \exists x. p(y, x)$	yes
$\exists z. \forall y. p(z, f(y))$	$\exists y. \forall y. p(y, f(y))$	no
$(\forall x. p(x)) \vee (\exists x. q(x))$	$(\forall z. p(z)) \vee (\exists y. q(y))$	yes
$p(x) \rightarrow \forall x. p(x)$	$p(y) \rightarrow \forall y. p(y)$	

Binding and α -conversion

- Names of bound variables are irrelevant, they just encode the binding structure.

$\exists x. \forall y. p(f(x), y) \wedge q(x, z)$ stands for

- We can rename **bound** variables at any time (α -conversion).
 - Must preserve binding structure.

Examples:		α -convertible?
$\forall x. \exists y. p(x, y)$	$\forall y. \exists x. p(y, x)$	yes
$\exists z. \forall y. p(z, f(y))$	$\exists y. \forall y. p(y, f(y))$	no
$(\forall x. p(x)) \vee (\exists x. q(x))$	$(\forall z. p(z)) \vee (\exists y. q(y))$	yes
$p(x) \rightarrow \forall x. p(x)$	$p(y) \rightarrow \forall y. p(y)$	no

Omitting parentheses

- Binary operators:
 - ▶ \wedge binds stronger than \vee stronger than \rightarrow .
 - ▶ \wedge , \vee , and \rightarrow associate to the right.
- Negation binds stronger than binary operators.
- Quantifiers extend to the right as far as possible: end of line or $)$.
They override the binding of binary operators!

$$A \vee B \wedge \neg C \rightarrow A \vee B \quad \left(\underline{A \vee \left(\underline{B \wedge (\neg C)} \right)} \right) \rightarrow (\underline{A \vee B})$$

$$A \rightarrow B \vee A \rightarrow C \quad A \rightarrow \left(\underline{(B \vee A) \rightarrow C} \right)$$

$$A \wedge \forall x. B(x) \vee C \quad A \wedge \left(\underline{\forall x. \left(\underline{B(x) \vee C} \right)} \right)$$

$$\neg \forall x. A(x) \wedge \forall x. (B(x) \wedge C(x)) \wedge D \quad \neg \left(\underline{\forall x. \left(\underline{A(x) \wedge \left(\underline{\forall x. \left(\underline{(B(x) \wedge C(x)) \wedge D} \right)} \right)} \right)} \right)$$

Semantics

- A **structure** is a pair $\mathcal{S} = \langle U_{\mathcal{S}}, I_{\mathcal{S}} \rangle$ where $U_{\mathcal{S}}$ is a nonempty set, the **universe**, and $I_{\mathcal{S}}$ is a mapping where
 1. $I_{\mathcal{S}}(p^n)$ is an n -ary relation on $U_{\mathcal{S}}$, for $p^n \in \mathcal{P}$, and
 2. $I_{\mathcal{S}}(f^n)$ is an n -ary (total) function on $U_{\mathcal{S}}$, for $f^n \in \mathcal{F}$

As shorthand, write $p^{\mathcal{S}}$ for $I_{\mathcal{S}}(p)$ and $f^{\mathcal{S}}$ for $I_{\mathcal{S}}(f)$

- An **interpretation** is a pair $\mathcal{I} = \langle \mathcal{S}, v \rangle$, where $\mathcal{S} = \langle U_{\mathcal{S}}, I_{\mathcal{S}} \rangle$ is a structure and $v : \mathcal{V} \rightarrow U_{\mathcal{S}}$ a valuation.
- The **value** of a term t under the interpretation $\mathcal{I} = \langle \mathcal{S}, v \rangle$ is written as $\mathcal{I}(t)$ and defined by
 1. $\mathcal{I}(x) = v(x)$, for $x \in \mathcal{V}$, and
 2. $\mathcal{I}(f(t_1, \dots, t_n)) = f^{\mathcal{S}}(\mathcal{I}(t_1), \dots, \mathcal{I}(t_n))$

Semantics (cont.)

Semantic entailment $\models \subseteq \text{Interpretations} \times \text{Form}$ is the smallest relation satisfying

$$\langle \mathcal{S}, v \rangle \models p(t_1, \dots, t_n) \quad \text{if} \quad (\mathcal{I}(t_1), \dots, \mathcal{I}(t_n)) \in p^{\mathcal{S}}, \text{ where } \mathcal{I} = \langle \mathcal{S}, v \rangle$$

$$\vdots$$

$$\langle \mathcal{S}, v \rangle \models \forall x. A \quad \text{if} \quad \langle \mathcal{S}, v[x \mapsto a] \rangle \models A, \text{ for all } a \in U_{\mathcal{S}}$$

$$\langle \mathcal{S}, v \rangle \models \exists x. A \quad \text{if} \quad \langle \mathcal{S}, v[x \mapsto a] \rangle \models A, \text{ for some } a \in U_{\mathcal{S}}$$

Here $v[x \mapsto a]$ is the valuation v' identical to v , except that $v'(x) = a$

Semantics (cont.)

- When $\langle \mathcal{S}, v \rangle \models A$ we say **A is satisfied with respect to $\langle \mathcal{S}, v \rangle$** or **$\langle \mathcal{S}, v \rangle$ is a model of A .**
- Note that if A does not have free variables, satisfaction does not depend on the valuation v . We write $\mathcal{S} \models A$.
- When every suitable interpretation is a model, we write $\models A$ and say **A is valid.**
- **A is satisfiable** if there is at least one model for A (and **contradictory** otherwise)
- Complexity of these problems?

An example

$$\forall x. p(x, s(x))$$

- A model:

An example

$$\forall x. p(x, s(x))$$

- A model:

$$U_{\mathcal{S}} = \mathcal{N}$$

$$p^{\mathcal{S}} = \{(m, n) \mid m, n \in U_{\mathcal{S}} \text{ and } m < n\}$$

$$s^{\mathcal{S}} = \text{the successor function on } U_{\mathcal{S}}$$

$$= \text{i.e., } s^{\mathcal{S}}(x) = x + 1$$

- Not a model:

An example

$$\forall x. p(x, s(x))$$

- A model:

$$U_{\mathcal{S}} = \mathcal{N}$$

$$p^{\mathcal{S}} = \{(m, n) \mid m, n \in U_{\mathcal{S}} \text{ and } m < n\}$$

$$s^{\mathcal{S}} = \text{the successor function on } U_{\mathcal{S}}$$

$$= \text{i.e., } s^{\mathcal{S}}(x) = x + 1$$

- Not a model:

$$U_{\mathcal{S}} = \{a, b, c\}$$

$$p^{\mathcal{S}} = \{(a, b), (a, c)\}$$

$$s^{\mathcal{S}} = \text{the identity function}$$

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

- $\forall x. \forall y. x < y \rightarrow \exists z. x < z \wedge z < y$

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

- $\forall x. \forall y. x < y \rightarrow \exists z. x < z \wedge z < y$

satisfied WRT any dense order

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

- $\forall x. \forall y. x < y \rightarrow \exists z. x < z \wedge z < y$

satisfied WRT any dense order

- $\exists x. x \neq 0$

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

- $\forall x. \forall y. x < y \rightarrow \exists z. x < z \wedge z < y$

satisfied WRT any dense order

- $\exists x. x \neq 0$

satisfied WRT structures \mathcal{S} with ≥ 2 elements in $U_{\mathcal{S}}$

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

- $\forall x. \forall y. x < y \rightarrow \exists z. x < z \wedge z < y$

satisfied WRT any dense order

- $\exists x. x \neq 0$

satisfied WRT structures \mathcal{S} with ≥ 2 elements in $U_{\mathcal{S}}$

- $(\forall x. p(x, x)) \rightarrow p(a, a)$

More examples

Which of following are satisfiable? Valid?

- $\forall x. \exists y. y * 2 = x$

satisfied WRT rationals

- $\forall x. \forall y. x < y \rightarrow \exists z. x < z \wedge z < y$

satisfied WRT any dense order

- $\exists x. x \neq 0$

satisfied WRT structures \mathcal{S} with ≥ 2 elements in $U_{\mathcal{S}}$

- $(\forall x. p(x, x)) \rightarrow p(a, a)$

valid

Substitution

- Replace in A all occurrences of a free variable x with some term t .
- We write $A(x)$ to indicate that we want to substitute for x , and $A(t)$ for substituting t for x .
- Example: $A(x) \equiv \exists y. y * x = x * z$

$$A(2 - 1) \equiv \exists y. y * (2 - 1) = (2 - 1) * z$$

$$A(z) \equiv \exists y. y * z = z * z$$

Substitution

- Replace in A all occurrences of a free variable x with some term t .
- We write $A(x)$ to indicate that we want to substitute for x , and $A(t)$ for substituting t for x .
- Example: $A(x) \equiv \exists y. y * x = x * z$

$$A(2 - 1) \equiv \exists y. y * (2 - 1) = (2 - 1) * z$$

$$A(z) \equiv \exists y. y * z = z * z$$

- All free variables of t must still be free in $A(t)$. **Avoid capture!**
If necessary, α -convert A before substitution.

$$A(3 + y) \not\equiv \exists y. y * (3 + y) = (3 + y) * z$$

Substitution

- Replace in A all occurrences of a free variable x with some term t .
- We write $A(x)$ to indicate that we want to substitute for x , and $A(t)$ for substituting t for x .
- Example: $A(x) \equiv \exists y. y * x = x * z$

$$A(2 - 1) \equiv \exists y. y * (2 - 1) = (2 - 1) * z$$

$$A(z) \equiv \exists y. y * z = z * z$$

- All free variables of t must still be free in $A(t)$. **Avoid capture!**
If necessary, α -convert A before substitution.

$$A(3 + y) \not\equiv \exists y. y * (3 + y) = (3 + y) * z$$

$$A(3 + y) \equiv \exists w. w * (3 + y) = (3 + y) * z$$

Universal quantification

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition $*$: x not free in any assumption in Γ .

- Example derivation:

$$\vdash (\forall x. A(x)) \rightarrow (\forall y. A(f(y)))$$

Universal quantification

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition $*$: x not free in any assumption in Γ .

- Example derivation:

$$\frac{\forall x. A(x) \vdash \forall y. A(f(y))}{\vdash (\forall x. A(x)) \rightarrow (\forall y. A(f(y)))} \rightarrow\text{-}I$$

- N.B. we continue to use rules from propositional logic, but now for first-order formulae.

Universal quantification

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition $*$: x not free in any assumption in Γ .

- Example derivation:

$$\frac{\frac{\forall x. A(x) \vdash A(f(y))}{\forall x. A(x) \vdash \forall y. A(f(y))} \forall\text{-}I \quad y \text{ not free in } \forall x. A(x)}{\vdash (\forall x. A(x)) \rightarrow (\forall y. A(f(y)))} \rightarrow\text{-}I$$

- N.B. we continue to use rules from propositional logic, but now for first-order formulae.

Universal quantification

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall-I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall-E$$

Side condition *: x not free in any assumption in Γ .

- Example derivation:

$$\frac{\frac{\frac{\forall x. A(x) \vdash \forall z. A(z)}{\forall x. A(x) \vdash A(f(y))} \forall-E}{\forall x. A(x) \vdash \forall y. A(f(y))} \forall-I}{\vdash (\forall x. A(x)) \rightarrow (\forall y. A(f(y)))} \rightarrow-I$$

with $t \equiv f(y)$
 y not free in $\forall x. A(x)$

- N.B. we continue to use rules from propositional logic, but now for first-order formulae.

Universal quantification

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition $*$: x not free in any assumption in Γ .

- Example derivation:

$$\frac{\frac{\frac{\overline{\forall x. A(x) \vdash \forall z. A(z)} \text{ axiom} \quad \text{implicit } \alpha\text{-conversion}}{\forall x. A(x) \vdash A(f(y))} \forall\text{-}E \quad \text{with } t \equiv f(y)}{\forall x. A(x) \vdash \forall y. A(f(y))} \forall\text{-}I \quad y \text{ not free in } \forall x. A(x)}{\vdash (\forall x. A(x)) \rightarrow (\forall y. A(f(y)))} \rightarrow\text{-}I$$

- N.B. we continue to use rules from propositional logic, but now for first-order formulae.

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition?

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition $*$: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition $*$: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\vdash x = 0 \rightarrow \forall x. x = 0}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-I}$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\frac{x = 0 \vdash \forall x. x = 0}{\vdash x = 0 \rightarrow \forall x. x = 0} \rightarrow\text{-I}}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-I}$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\frac{\frac{x = 0 \vdash x = 0}{x = 0 \vdash \forall x. x = 0} \forall\text{-I} \quad \vdash x = 0 \rightarrow \forall x. x = 0}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \rightarrow\text{-I} \quad \forall\text{-I}$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\frac{\frac{\overline{x = 0 \vdash x = 0} \text{ axiom}}{x = 0 \vdash \forall x. x = 0} \forall\text{-I}}{\vdash x = 0 \rightarrow \forall x. x = 0} \rightarrow\text{-I}}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-I}$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\frac{\frac{\frac{}{\textcolor{red}{x} = 0 \vdash x = 0} \textit{axiom}}{\textcolor{red}{x} = 0 \vdash \forall x. x = 0} \textcolor{red}{\forall\text{-I}}}{\vdash x = 0 \rightarrow \forall x. x = 0} \rightarrow\text{-I}}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-I} \quad \frac{}{\vdash 0 = 0 \rightarrow (\forall x. x = 0)} \forall\text{-E}$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\frac{\frac{\frac{\frac{}{\text{axiom}}{x = 0 \vdash x = 0}}{x = 0 \vdash \forall x. x = 0} \forall\text{-}I}{\vdash x = 0 \rightarrow \forall x. x = 0} \rightarrow\text{-}I}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-}I}{\vdash 0 = 0 \rightarrow (\forall x. x = 0)} \forall\text{-}E \qquad \vdash 0 = 0 \rightarrow\text{-}E$$

$$\vdash \forall x. x = 0$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-}I^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-}E$$

Side condition *: x not free in any assumption in Γ .

- Why this side condition? Consider the following “derivation”:

$$\frac{\frac{\frac{\frac{\frac{\frac{}{\text{axiom}}{x = 0 \vdash x = 0}}{x = 0 \vdash \forall x. x = 0} \forall\text{-}I}{\vdash x = 0 \rightarrow \forall x. x = 0} \rightarrow\text{-}I}{\vdash \forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-}I}{\vdash 0 = 0 \rightarrow (\forall x. x = 0)} \forall\text{-}E \quad \frac{}{\vdash 0 = 0} \text{ref (see later)}}{\vdash \forall x. x = 0} \rightarrow\text{-}E$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\frac{\frac{}{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y} \text{axiom}}{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y} \forall\text{-E}}{\vdash (\forall x. \exists y. x \neq y) \rightarrow (\exists y. y \neq y)} \rightarrow\text{-I}$$

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\frac{\frac{}{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y} \text{axiom}}{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y} \forall\text{-E}}{\vdash (\forall x. \exists y. x \neq y) \rightarrow (\exists y. y \neq y)} \rightarrow\text{-I}$$

- Conclusion is not valid. Reason:

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\frac{\frac{}{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y} \text{axiom}}{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y} \forall\text{-E}}{\vdash (\forall x. \exists y. x \neq y) \rightarrow (\exists y. y \neq y)} \rightarrow\text{-I}$$

- Conclusion is not valid. Reason: false if $U_{\mathcal{S}}$ has ≥ 2 elements.
- Proof incorrect. Reason:

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\forall x. \exists y. x \neq y \vdash \exists y. y \neq y}{\vdash (\forall x. \exists y. x \neq y) \rightarrow (\exists y. y \neq y)} \rightarrow\text{-I}$$

- Conclusion is not valid. Reason: false if $U_{\mathcal{S}}$ has ≥ 2 elements.
- Proof incorrect. Reason:

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\forall x. \exists y. x \neq y \vdash \exists y. y \neq y}{\vdash (\forall x. \exists y. x \neq y) \rightarrow (\exists y. y \neq y)} \rightarrow\text{-I} \quad \text{correct}$$

- Conclusion is not valid. Reason: false if $U_{\mathcal{S}}$ has ≥ 2 elements.
- Proof incorrect. Reason:

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y}{\forall x. \exists y. x \neq y \vdash \exists y. y \neq y} \forall\text{-E}$$

- Conclusion is not valid. Reason: false if $U_{\mathcal{S}}$ has ≥ 2 elements.
- Proof incorrect. Reason:

Universal quantification (cont.)

- Rules

$$\frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x. A(x)} \forall\text{-I}^* \qquad \frac{\Gamma \vdash \forall x. A(x)}{\Gamma \vdash A(t)} \forall\text{-E}$$

Side condition *: x not free in any assumption in Γ .

- Is the following a proof?

$$\frac{\forall x. \exists y. x \neq y \vdash \forall x. \exists y. x \neq y}{\forall x. \exists y. x \neq y \vdash \exists y. y \neq y} \forall\text{-E} \quad \text{wrong}$$

- Conclusion is not valid. Reason: false if $U_{\mathcal{S}}$ has ≥ 2 elements.
- Proof incorrect. Reason: Substitution must avoid capture.
 Here: $A(x) \equiv \exists y. x \neq y$
 When substituting $t = y$ for x , we must rename bound y in A !

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\frac{\forall x. p(x) \wedge q(x) \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-I}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\frac{\overbrace{\forall x. p(x) \wedge q(x) \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}^{\equiv \Gamma}}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-I}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{\Gamma \vdash \forall x. p(x) \qquad \Gamma \vdash \forall x. q(x)}{\wedge\text{-I}} \\
 \frac{\overbrace{\forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-I}
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \dfrac{\Gamma \vdash p(x)}{\Gamma \vdash \forall x. p(x)} \forall\text{-I} \qquad \Gamma \vdash \forall x. q(x) \\
 \hline
 \Gamma \vdash \forall x. p(x) \wedge q(x) \quad \wedge\text{-I} \\
 \hline
 \overbrace{\Gamma \vdash \forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x)) \\
 \hline
 \vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x)) \rightarrow\text{-I}
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{\Gamma \vdash p(x) \wedge \quad ?}{\Gamma \vdash p(x)} \wedge\text{-}EL \\
 \frac{\Gamma \vdash p(x)}{\Gamma \vdash \forall x. p(x)} \forall\text{-}I \\
 \frac{\Gamma \vdash \forall x. p(x) \quad \Gamma \vdash \forall x. q(x)}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \wedge\text{-}I \\
 \frac{\overbrace{\Gamma \vdash \forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-}I
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{\Gamma \vdash \forall y. p(y) \wedge ?(y)}{\Gamma \vdash p(x) \wedge ?(x)} \forall\text{-}E \\
 \frac{\Gamma \vdash p(x) \wedge ?(x)}{\Gamma \vdash p(x)} \wedge\text{-}EL \\
 \frac{\Gamma \vdash p(x)}{\Gamma \vdash \forall x. p(x)} \forall\text{-}I \\
 \frac{\Gamma \vdash \forall x. p(x) \quad \Gamma \vdash \forall x. q(x)}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \wedge\text{-}I \\
 \frac{\overbrace{\Gamma \vdash \forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-}I
 \end{array}$$

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

Spring Semester, 2014

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{}{\Gamma \vdash \forall y. p(y) \wedge q(y)} \text{axiom} \\
 \frac{}{\Gamma \vdash \forall y. p(y) \wedge q(y)} \forall\text{-}E \\
 \frac{}{\Gamma \vdash p(x) \wedge q(x)} \wedge\text{-}EL \\
 \frac{}{\Gamma \vdash p(x)} \forall\text{-}I \\
 \frac{}{\Gamma \vdash \forall x. p(x)} \forall\text{-}I \\
 \frac{}{\Gamma \vdash q(x)} \forall\text{-}I \\
 \frac{}{\Gamma \vdash \forall x. q(x)} \forall\text{-}I \\
 \frac{}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \wedge\text{-}I \\
 \frac{}{\overbrace{\forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-}I \\
 \vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{}{\Gamma \vdash \forall y. p(y) \wedge q(y)} \text{axiom} \\
 \frac{}{\Gamma \vdash p(x) \wedge q(x)} \forall\text{-}E \\
 \frac{}{\Gamma \vdash p(x)} \wedge\text{-}EL \\
 \frac{}{\Gamma \vdash \forall x. p(x)} \forall\text{-}I \\
 \frac{}{\Gamma \vdash q(x)} \wedge\text{-}ER \\
 \frac{}{\Gamma \vdash \forall x. q(x)} \forall\text{-}I \\
 \frac{}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \wedge\text{-}I \\
 \frac{}{\overbrace{\forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-}I \\
 \vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{\frac{\frac{\Gamma \vdash \forall y. p(y) \wedge q(y)}{\Gamma \vdash p(x) \wedge q(x)} \text{axiom}}{\Gamma \vdash p(x)} \text{ } \wedge\text{-}EL \quad \frac{\frac{\Gamma \vdash \forall z. ??(z) \wedge q(z)}{\Gamma \vdash ??(x) \wedge q(x)} \text{ } \wedge\text{-}ER}{\Gamma \vdash q(x)} \text{ } \wedge\text{-}ER \\
 \frac{\Gamma \vdash p(x)}{\Gamma \vdash \forall x. p(x)} \text{ } \forall\text{-}I \quad \frac{\Gamma \vdash q(x)}{\Gamma \vdash \forall x. q(x)} \text{ } \forall\text{-}I \\
 \frac{\Gamma \vdash \forall x. p(x) \quad \Gamma \vdash \forall x. q(x)}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \text{ } \wedge\text{-}I \\
 \frac{\overbrace{\forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \text{ } \rightarrow\text{-}I
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{\frac{\frac{\Gamma \vdash \forall y. p(y) \wedge q(y)}{\Gamma \vdash p(x) \wedge q(x)} \text{axiom}}{\Gamma \vdash p(x)} \forall\text{-}E \quad \frac{\frac{\frac{\Gamma \vdash \forall z. p(z) \wedge q(z)}{\Gamma \vdash p(x) \wedge q(x)} \text{axiom}}{\Gamma \vdash q(x)} \forall\text{-}E \\
 \frac{\Gamma \vdash p(x)}{\Gamma \vdash \forall x. p(x)} \wedge\text{-}EL \quad \frac{\Gamma \vdash q(x)}{\Gamma \vdash \forall x. q(x)} \wedge\text{-}ER \\
 \frac{\Gamma \vdash \forall x. p(x)}{\Gamma \vdash \forall x. p(x)} \forall\text{-}I \quad \frac{\Gamma \vdash \forall x. q(x)}{\Gamma \vdash \forall x. q(x)} \forall\text{-}I \\
 \frac{\Gamma \vdash \forall x. p(x)}{\Gamma \vdash \forall x. p(x)} \wedge\text{-}I \quad \frac{\Gamma \vdash \forall x. q(x)}{\Gamma \vdash \forall x. q(x)} \wedge\text{-}I \\
 \frac{\overbrace{\forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-}I
 \end{array}$$

Universal quantification (cont.)

- Prove $(\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))$

$$\begin{array}{c}
 \frac{\frac{\frac{\Gamma \vdash \forall y. p(y) \wedge q(y)}{\Gamma \vdash p(x) \wedge q(x)} \text{axiom}}{\Gamma \vdash p(x)} \forall\text{-}E \quad \frac{\frac{\frac{\Gamma \vdash \forall z. p(z) \wedge q(z)}{\Gamma \vdash p(x) \wedge q(x)} \text{axiom}}{\Gamma \vdash q(x)} \forall\text{-}E \\
 \frac{\Gamma \vdash p(x)}{\Gamma \vdash \forall x. p(x)} \wedge\text{-}EL \quad \frac{\Gamma \vdash q(x)}{\Gamma \vdash \forall x. q(x)} \wedge\text{-}ER \\
 \frac{\Gamma \vdash \forall x. p(x)}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \wedge\text{-}I \quad \frac{\Gamma \vdash \forall x. q(x)}{\Gamma \vdash \forall x. p(x) \wedge q(x)} \wedge\text{-}I \\
 \frac{\overbrace{\Gamma \vdash \forall x. p(x) \wedge q(x)}^{\equiv \Gamma} \vdash (\forall x. p(x)) \wedge (\forall x. q(x))}{\vdash (\forall x. p(x) \wedge q(x)) \rightarrow (\forall x. p(x)) \wedge (\forall x. q(x))} \rightarrow\text{-}I
 \end{array}$$

- Generalise proof:
 - Can use any formulae A and B instead of relations p and q .
 - Side conditions of $\forall\text{-}I$ are trivial: x not free in Γ .

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \qquad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation:

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \qquad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation:

$$\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)$$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation:

$$\frac{\forall x. A(x) \rightarrow B \vdash (\exists y. A(y)) \rightarrow B}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}$$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation:

$$\frac{\frac{\frac{\forall x. A(x) \rightarrow B, \exists y. A(y) \vdash B}{\forall x. A(x) \rightarrow B \vdash (\exists y. A(y)) \rightarrow B} \rightarrow\text{-I}}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}$$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation, assuming z does not occur free in B :

$$\frac{\Gamma \vdash \exists z. ?(z) \quad \Gamma, ?(z) \vdash B}{\frac{\frac{\frac{\Gamma \vdash \exists z. ?(z) \quad \Gamma, ?(z) \vdash B}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}} \exists\text{-E}$$

where $\Gamma \equiv \forall x. A(x) \rightarrow B, \exists y. A(y)$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation, assuming z does not occur free in B :

$$\frac{\frac{\frac{\frac{\frac{\frac{\Gamma \vdash \exists z. A(z)}{\Gamma \vdash \exists z. A(z)} \text{ axiom}}{\Gamma, A(z) \vdash B} \exists\text{-E}}{\forall x. A(x) \rightarrow B, \exists y. A(y) \vdash B} \rightarrow\text{-I}}{\forall x. A(x) \rightarrow B \vdash (\exists y. A(y)) \rightarrow B} \rightarrow\text{-I}}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}$$

where $\Gamma \equiv \forall x. A(x) \rightarrow B, \exists y. A(y)$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation, assuming z does not occur free in B :

$$\frac{\frac{\frac{}{\Gamma \vdash \exists z. A(z)} \text{axiom} \quad \frac{\Gamma' \vdash \text{??} \rightarrow B \quad \Gamma' \vdash \text{??}}{\Gamma, A(z) \vdash B} \rightarrow\text{-E}}{\Gamma \vdash \exists z. A(z) \rightarrow B} \exists\text{-E} \quad \frac{\frac{\frac{\frac{\frac{\Gamma \vdash \exists z. A(z) \rightarrow B}{\Gamma \vdash \exists y. A(y)} \rightarrow\text{-I}}{\Gamma \vdash \forall x. A(x) \rightarrow B} \rightarrow\text{-I}}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}$$

where $\Gamma \equiv \forall x. A(x) \rightarrow B, \exists y. A(y)$ and $\Gamma' \equiv \Gamma, A(z)$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation, assuming z does not occur free in B :

$$\frac{\frac{\frac{}{\Gamma \vdash \exists z. A(z)} \text{axiom} \quad \frac{\frac{\Gamma' \vdash \forall w. \text{??}(w) \rightarrow B}{\Gamma' \vdash \text{??}(\text{???}) \rightarrow B} \forall\text{-E} \quad \Gamma' \vdash \text{??}(\text{???})}{\Gamma, A(z) \vdash B} \rightarrow\text{-E}}{\Gamma \vdash \exists z. A(z) \quad \Gamma, A(z) \vdash B} \exists\text{-E} \quad \frac{\forall x. A(x) \rightarrow B, \exists y. A(y) \vdash B}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I}$$

where $\Gamma \equiv \forall x. A(x) \rightarrow B, \exists y. A(y)$ and $\Gamma' \equiv \Gamma, A(z)$

- Rules

Side condition *: x is neither free in B nor free in Γ .

- where $\Gamma \equiv \forall x. A(x) \rightarrow B, \exists y. A(y)$ and $\Gamma' \equiv \Gamma, A(z)$

Existential quantification

- Rules

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists\text{-I} \quad \frac{\Gamma \vdash \exists x. A(x) \quad \Gamma, A(x) \vdash B}{\Gamma \vdash B} \exists\text{-E}^*$$

Side condition *: x is neither free in B nor free in Γ .

- Sample derivation, assuming z does not occur free in B :

$$\frac{\frac{\frac{\frac{\frac{\frac{\Gamma \vdash \exists z. A(z)}{\Gamma \vdash \exists z. A(z)} \text{ axiom}}{\Gamma \vdash \exists z. A(z)} \text{ axiom}}{\Gamma \vdash \exists z. A(z)} \text{ axiom}}{\Gamma \vdash \exists z. A(z)} \text{ axiom}}{\Gamma, A(z) \vdash B} \rightarrow\text{-E} \quad \frac{\frac{\frac{\frac{\frac{\Gamma' \vdash \forall w. A(w) \rightarrow B}{\Gamma' \vdash \forall w. A(w) \rightarrow B} \text{ axiom}}{\Gamma' \vdash \forall w. A(w) \rightarrow B} \text{ axiom}}{\Gamma' \vdash A(z) \rightarrow B} \forall\text{-E}}{\Gamma, A(z) \vdash B} \rightarrow\text{-E}}{\frac{\forall x. A(x) \rightarrow B, \exists y. A(y) \vdash B}{\forall x. A(x) \rightarrow B \vdash (\exists y. A(y)) \rightarrow B} \rightarrow\text{-I}}{\vdash (\forall x. A(x) \rightarrow B) \rightarrow ((\exists y. A(y)) \rightarrow B)} \rightarrow\text{-I} \quad \exists\text{-E}$$

where $\Gamma \equiv \forall x. A(x) \rightarrow B, \exists y. A(y)$ and $\Gamma' \equiv \Gamma, A(z)$

Road map

- Natural deduction
- Propositional logic
- First-order logic

 **Equality**

FOL with equality

- Equality is a **logical** symbol with associated proof rules

One speaks of **first-order logic with equality** rather than equality being “just another predicate”

- Extended language: $t_1 = t_2 \in \text{Form}$ if $t_1, t_2 \in \text{Term}$
- Extend definition of semantic entailment \models :

$$\mathcal{I} \models t_1 = t_2 \quad \text{if} \quad \mathcal{I}(t_1) = \mathcal{I}(t_2)$$

- ▶ Recall $\mathcal{I}(t)$ is the value of t under the interpretation $\mathcal{I} = \langle \mathcal{S}, v \rangle$
- ▶ Note the two completely different uses of “=” here!

Equality

- Equality is an equivalence relation

$$\frac{}{\Gamma \vdash t = t} \text{ref} \qquad \frac{\Gamma \vdash t = s}{\Gamma \vdash s = t} \text{sym} \qquad \frac{\Gamma \vdash t = s \quad \Gamma \vdash s = r}{\Gamma \vdash t = r} \text{trans}$$

- Equality is also a congruence on terms and all (definable) relations

$$\frac{\Gamma \vdash t_1 = s_1 \quad \dots \quad \Gamma \vdash t_n = s_n}{\Gamma \vdash f(t_1, \dots, t_n) = f(s_1, \dots, s_n)} \text{cong}_1$$

$$\frac{\Gamma \vdash t_1 = s_1 \quad \dots \quad \Gamma \vdash t_n = s_n \quad \Gamma \vdash p(t_1, \dots, t_n)}{\Gamma \vdash p(s_1, \dots, s_n)} \text{cong}_2$$

- Soundness:

Equality

- Equality is an equivalence relation

$$\frac{}{\Gamma \vdash t = t} \text{ref} \qquad \frac{\Gamma \vdash t = s}{\Gamma \vdash s = t} \text{sym} \qquad \frac{\Gamma \vdash t = s \quad \Gamma \vdash s = r}{\Gamma \vdash t = r} \text{trans}$$

- Equality is also a congruence on terms and all (definable) relations

$$\frac{\Gamma \vdash t_1 = s_1 \quad \dots \quad \Gamma \vdash t_n = s_n}{\Gamma \vdash f(t_1, \dots, t_n) = f(s_1, \dots, s_n)} \text{cong}_1$$

$$\frac{\Gamma \vdash t_1 = s_1 \quad \dots \quad \Gamma \vdash t_n = s_n \quad \Gamma \vdash p(t_1, \dots, t_n)}{\Gamma \vdash p(s_1, \dots, s_n)} \text{cong}_2$$

- Soundness: equality on $U_{\mathcal{S}}$ is a congruence

On the shape of proofs

- Let $\Gamma \equiv a(b) = d(e), f(d(e)) = g(h)$. Prove $\Gamma \vdash f(a(b)) = g(h)$

$$\frac{\frac{\overline{\Gamma \vdash a(b) = d(e)} \text{ axiom}}{\Gamma \vdash f(a(b)) = f(d(e))} \text{ cong}_1 \quad \frac{\overline{\Gamma \vdash f(d(e)) = g(h)} \text{ axiom}}{\Gamma \vdash f(a(b)) = g(h)} \text{ trans}$$

- Compare with following linear equational derivation

$$f(a(b)) = f(d(e)) = g(h)$$

- In general, any equality proof can be converted into such a linear style. We will usually carry out equality reasoning this linear way.
- We will see many examples shortly, e.g., in proofs by induction.

What next?

- We consider the correctness question for functional programs.
- I will usually not write formal proofs using these rules.
- However, all proofs given can be translated to formal ones.
- You should check this, also for your own proofs.
- Topic is also of central importance in course's second half.