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.

- Deductive proof system:

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

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

- 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:

$$\dfrac{\dfrac{\dfrac{}{+}\,\delta}{\otimes}\,\alpha \qquad \dfrac{\dfrac{}{+}\,\delta}{\times}\,\beta}{\oplus}\,\gamma$$

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:

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

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

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

- Derivation tree:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{+ \vdash +}\ \textit{axiom}}{+ \vdash \otimes}\ \alpha \qquad \dfrac{\dfrac{}{+ \vdash +}\ \textit{axiom}}{+ \vdash \times}\ \beta}{\vdash \oplus}\ \gamma}{\vdash \oplus}\ \delta$$

Natural deduction

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

  $A_1, ..., A_n \vdash A$ reads as "A follows from $A_1, ..., A_n$"
- **Derivations** are trees

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\,\textit{axiom} \qquad \dfrac{}{A, B \vdash B}\,\textit{axiom}}{A, B \vdash A \wedge B}\,\wedge\text{-}I}{A \vdash B \to A \wedge B}\,\to\text{-}I}{\vdash A \to B \to A \wedge B}\,\to\text{-}I$$

- 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 $X \in \mathcal{V}$.
  - $\bot \in \mathcal{L}_P$.
  - $A \wedge B \in \mathcal{L}_P$ 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 $B \in \mathcal{L}_P$.
  - $A \to B \in \mathcal{L}_P$ 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** $\sigma : \mathcal{V} \to \{\textbf{True}, \textbf{False}\}$ 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 $\models \subseteq \mathit{Valuations} \times \mathcal{L}_P$ such that
  - $\sigma \models X$, iff $\sigma(X) = \textbf{True}$
  - $\sigma \models A \wedge B$, iff $\sigma \models A$ and $\sigma \models B$
  - $\sigma \models A \vee B$, iff $\sigma \models A$ or $\sigma \models B$
  - $\sigma \models A \to B$, iff whenever $\sigma \models A$ then $\sigma \models B$
- Note that $\sigma \not\models \bot$, for every $\sigma \in \mathit{Valuations}$

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**: $A_1, \ldots, A_n \models A$ if

  $$\text{for all } \sigma, \text{ if } \sigma \models A_1, \ldots, \sigma \models A_n \text{ then } \sigma \models A$$

- Examples:
  - $X \wedge Y$ satisfiable, as $\sigma \models X \wedge Y$ for $\sigma(X) = \sigma(Y) = \textbf{True}$
  - $X \to X$ valid
  - $\neg X, X \vee Y \models Y$ holds, as $\sigma \models \neg X$ and $\sigma \models X \vee Y$ constrain σ to $\sigma(X) = \textbf{False}$ and $\sigma(Y) = \textbf{True}$, 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 $H \equiv A_1, \ldots, A_n$ 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

$$A_1, \ldots, A_n \vdash A$$

  where all $A, A_1, \ldots A_n$ are propositional formulae

- Intuitively: A follows from the A_is

  If logic is sound, this means A_is semantically entail A

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

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

- 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

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

- Example derivation

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

Conjunction (cont.)

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

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

- Each rule is sound in that it preserves semantic entailment.
  E.g., for $\wedge$-*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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \to\text{-}I \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B} \to\text{-}E$$

- Application of $\to$-*I* turns last derivation into a proof

$$\frac{\dfrac{\vdots}{A \wedge (B \wedge C) \vdash A \wedge C}}{\vdash A \wedge (B \wedge C) \to A \wedge C} \to\text{-}I$$

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

$\vdash X \to Y \to X$

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

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

Disjunction

- Rules

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

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

- 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

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

- Negation: define $\neg A$ as $A \to \bot$.

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \neg\text{-}E \quad \text{derived by} \quad \frac{\Gamma \vdash \overbrace{\neg A}^{A \to \bot} \qquad \Gamma \vdash A}{\dfrac{\Gamma \vdash \bot}{\Gamma \vdash B}\ \bot\text{-}E}\ \to\text{-}E$$

Intuitionistic versus classical logic

- Peirce's Law: $((A \to B) \to A) \to A$. Is this valid? Provable?
- We have only intuitionistic logic. Classical logic requires either
  - axiom of excluded middle $\dfrac{}{\Gamma \vdash A \vee \neg A}\ \mathit{TND}$ ("tertium non datur")
  - or rule $\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \mathit{RAA}$ ("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.
- 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:
$$\dfrac{\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,\wedge\text{-}EL \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,\wedge\text{-}ER}{\Gamma \vdash A \wedge B}\,\wedge\text{-}I$$
  - $\vee$-*E* + *axiom* is safe:
$$\dfrac{\dfrac{}{\Gamma \vdash A \vee B}\,\mathit{axiom} \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,\vee\text{-}E$$
  - $\wedge$-*EL* is unsafe:
$$\dfrac{\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\wedge\text{-}I}{\Gamma \vdash A}\,\wedge\text{-}EL$$
  - How about the other rules?

Summary of derivation rules for propositional logic

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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to\text{-}I \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \to\text{-}E$$

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

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

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot\text{-}E \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \neg\text{-}E$$

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. $x \in$ *Term* if $x \in \mathcal{V}$, and
2. $f^n(t_1, \ldots, t_n) \in$ *Term* if $f^n \in \mathcal{F}$ and $t_j \in$ *Term*, for all $1 \leq j \leq n$

Syntax (cont.)

- *Form*, the **formulae of first-order logic**, is the smallest set where
  1. $\bot \in$ *Form*,
  2. $p^n(t_1, \ldots, t_n) \in$ *Form* if $p^n \in \mathcal{P}$ and $t_j \in$ *Term*, for all $1 \leq j \leq n$,
  3. $A \circ B \in$ *Form* if $A \in$ *Form*, $B \in$ *Form*, and $\circ \in \{\wedge, \vee, \rightarrow\}$, and
  4. $Qx.\, A \in$ *Form* if $A \in$ *Form*, $x \in \mathcal{V}$, and $Q \in \{\forall, \exists\}$

- Each occurrence of each variable in a formula is **bound** or **free**.

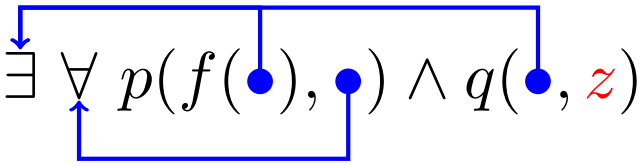
$$(q(x) \vee \exists x.\, \forall y.\, p(f(x), z) \wedge q(a)) \vee \forall x.\, r(x, z, g(x))$$

  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: $x^2 + \int_c^d x \cdot y \, dy$ or $\sum_{i=0}^{5} x \cdot i$

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.

- 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
$p(x) \to \forall x.\, p(x)$	$p(y) \to \forall y.\, p(y)$	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!

$A \vee B \wedge \neg C \rightarrow A \vee B$

$$\Big(A \vee \big(B \wedge (\neg\, C)\big)\Big) \rightarrow (A \vee B)$$

$A \rightarrow B \vee A \rightarrow C$

$$A \rightarrow \big((B \vee A) \rightarrow C\big)$$

$A \wedge \forall x.\, B(x) \vee C$

$$A \wedge \Big(\forall x.\ \big(B(x) \vee C\big)\Big)$$

$\neg\, \forall x.\, A(x) \wedge \forall x.\, (B(x) \wedge C(x)) \wedge D$

$$\neg\, \Big(\forall x.\, \Big(A(x) \wedge \Big(\forall x.\, \big(\big(B(x) \wedge C(x)\big) \wedge D\big)\Big)\Big)\Big)$$

Semantics

- A **structure** is a pair $\mathcal{S} = \langle U_\mathcal{S}, I_\mathcal{S} \rangle$ where $U_\mathcal{S}$ is an 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 $v : \mathcal{V} \to U_\mathcal{S}$ 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. $\mathcal{I}(f(t_1, \ldots, t_n)) = f^\mathcal{S}(\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n))$

Semantics (cont.)

Semantic entailment $\models \subseteq$ Interpretations $\times$ *Form* is the smallest relation satisfying

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

$$\vdots$$

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

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

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:

$$\begin{aligned} U_{\mathcal{S}} &= \mathcal{N} \\ p^{\mathcal{S}} &= \{(m, n) \mid m, n \in U_{\mathcal{S}} \textit{ and } m < n\} \\ s^{\mathcal{S}} &= \text{the successor function on } U_{\mathcal{S}} \\ &= \text{i.e., } s^{\mathcal{S}}(x) = x + 1 \end{aligned}$$

- Not a model:

$$\begin{aligned} U_{\mathcal{S}} &= \{a, b, c\} \\ p^{\mathcal{S}} &= \{(a, b), (a, c)\} \\ s^{\mathcal{S}} &= \text{the identity function} \end{aligned}$$

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 $\geq$ 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: $A(x) \equiv \exists y.\, y * x = x * z$

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

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

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

- Example derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x.\, A(x) \vdash \forall z.\, A(z)}\ \textit{axiom}}{\forall x.\, A(x) \vdash A(f(y))}\ \forall\text{-}E}{\forall x.\, A(x) \vdash \forall y.\, A(f(y))}\ \forall\text{-}I}{\vdash (\forall x.\, A(x)) \to (\forall y.\, A(f(y)))}\ \to\text{-}I$$

implicit α-conversion

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 (cont.)

- Rules $\dfrac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x.\, A(x)}\ \forall\text{-}I\ *$ $\qquad$ $\dfrac{\Gamma \vdash \forall x.\, A(x)}{\Gamma \vdash A(t)}\ \forall\text{-}E$

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

- Why this side condition? Consider the following "derivation":

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x = 0 \vdash x = 0}\ \textit{axiom}}{x = 0 \vdash \forall x.\, x = 0}\ \forall\text{-}I}{\vdash x = 0 \to \forall x.\, x = 0}\ \to\text{-}I}{\vdash \forall x.\, (x = 0 \to \forall x.\, x = 0)}\ \forall\text{-}I}{\vdash 0 = 0 \to (\forall x.\, x = 0)}\ \forall\text{-}E \qquad \dfrac{}{\vdash 0 = 0}\ \textit{ref}\ \text{(see later)}$$
$$\dfrac{\vdash 0 = 0 \to (\forall x.\, x = 0) \qquad \vdash 0 = 0}{\vdash \forall x.\, x = 0}\ \to\text{-}E$$

Universal quantification (cont.)

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

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

- Is the following a proof?

$$\dfrac{\dfrac{\dfrac{}{\forall x.\, \exists y.\, x \neq y \vdash \forall x.\, \exists y.\, x \neq y}\ \textit{axiom}}{\forall x.\, \exists y.\, x \neq y \vdash \exists y.\, y \neq y}\ \forall\text{-}E}{\vdash (\forall x.\, \exists y.\, x \neq y) \to (\exists y.\, y \neq y)}\ \to\text{-}I$$

  wrong

  correct

- 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 $(\forall x.\, p(x) \wedge q(x)) \to (\forall x.\, p(x)) \wedge (\forall x.\, q(x))$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall y.\, p(y) \wedge q(y)}\,\textit{axiom}}{\Gamma \vdash p(x) \wedge q(x)}\,\forall\textit{-E}}{\Gamma \vdash p(x)}\,\wedge\textit{-EL}}{\Gamma \vdash \forall x.\, p(x)}\,\forall\textit{-I} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall z.\;\; p(z) \wedge q(z)}\,\textit{axiom}}{\Gamma \vdash\;\; p(x) \wedge q(x)}\,\forall\textit{-E}}{\Gamma \vdash q(x)}\,\wedge\textit{-ER}}{\Gamma \vdash \forall x.\, q(x)}\,\forall\textit{-I}}{\overbrace{\forall x.\, p(x) \wedge q(x)}^{\equiv\Gamma} \vdash (\forall x.\, p(x)) \wedge (\forall x.\, q(x))}\,\wedge\textit{-I}$$

$$\dfrac{\overbrace{\forall x.\, p(x) \wedge q(x)}^{\equiv\Gamma} \vdash (\forall x.\, p(x)) \wedge (\forall x.\, q(x))}{\vdash (\forall x.\, p(x) \wedge q(x)) \to (\forall x.\, p(x)) \wedge (\forall x.\, q(x))}\,\to\textit{-I}$$

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

Existential quantification

- Rules

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

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

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

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \exists z.\, A(z)}\ \textit{axiom} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma' \vdash \forall w.\, A(w) \to B}\ \textit{axiom}}{\Gamma' \vdash\ A(z)\ \to B}\ \forall\text{-}E \qquad \dfrac{}{\Gamma' \vdash\ A(z)}\ \textit{axiom}}{\Gamma, A(z) \vdash B}\ \to\text{-}E}{\forall x.\, A(x) \to B, \exists y.\, A(y) \vdash B}\ \exists\text{-}E}{\forall x.\, A(x) \to B \vdash (\exists y.\, A(y)) \to B}\ \to\text{-}I}{\vdash (\forall x.\, A(x) \to B) \to ((\exists y.\, A(y)) \to B)}\ \to\text{-}I$$

  where $\Gamma \equiv \forall x. A(x) \to B, \exists y.\, A(y)$ 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: $t_1 = t_2 \in \mathit{Form}$ if $t_1, t_2 \in \mathit{Term}$

- 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

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

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

$$\frac{\Gamma \vdash t_1 = s_1 \quad \cdots \quad \Gamma \vdash t_n = s_n}{\Gamma \vdash f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)}\ \textit{cong}_1$$

$$\frac{\Gamma \vdash t_1 = s_1 \quad \cdots \quad \Gamma \vdash t_n = s_n \qquad \Gamma \vdash p(t_1, \ldots, t_n)}{\Gamma \vdash p(s_1, \ldots, s_n)}\ \textit{cong}_2$$

- 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 $\Gamma \vdash f(a(b)) = g(h)$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash a(b) = d(e)}\,\textit{axiom}}{\Gamma \vdash f(a(b)) = f(d(e))}\,\textit{cong}_1 \qquad \dfrac{}{\Gamma \vdash f(d(e)) = g(h)}\,\textit{axiom}}{\Gamma \vdash f(a(b)) = g(h)}\,\textit{trans}$$

- 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.