Natural Deduction

David Basin

Department of Computer Science
ETH Zurich

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

Natural Deduction

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

  $A_1, ..., A_n \vdash A$ denotes that A follows from $A_1, ..., A_n$.
- **Derivations** are trees

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

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

Natural Deduction: an abstract example

- Language $\mathcal{L} = \{\oplus, \otimes, \times, +\}$
- Deductive system given by **rules of proof**:

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

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

  Last rule says that assumption $+$ **may** be discharged

- Proof of $\oplus$

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

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 V of variables be given. L_P, the **language of propositional logic**, is the smallest set where:
  - $X \in L_P$ if $X \in V$.
  - $\bot \in L_p$.
  - $A \wedge B \in L_P$ if $A \in L_P$ and $B \in L_P$.
  - $A \vee B \in L_P$ if $A \in L_P$ and $B \in L_P$.
  - $A \to B \in L_P$ if $A \in L_P$ and $B \in L_P$.

- In following, X ranges over variables and A and B over formulae

Propositional Logic: semantics

- A **valuation** $\sigma : V \to \{\textbf{True}, \textbf{False}\}$ is a function mapping variables to truth values. Let *Valuations* be the set of valuations.

  Valuations are simple kinds of models (interpretations).

- **Satisfiability**: smallest relation $\models \subseteq \mathit{Valuations} \times L_P$ such that
  - $\sigma \models X$, if $\sigma(X) = \textbf{True}$
  - $\sigma \models A \wedge B$, if $\sigma \models A$ and $\sigma \models B$
  - $\sigma \models A \vee B$, if $\sigma \models A$ or $\sigma \models B$
  - $\sigma \models A \to B$, if whenever $\sigma \models A$ then $\sigma \models B$
- A formula $A \in L_P$ is **valid** (a **tautology**) if

  $$\sigma \models A, \text{ for all valuations } \sigma$$

- **Semantic entailment**: $A_1, \ldots A_n \models A$ if

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

Requirements for a deductive system

- Syntactic entailment $\vdash$ and semantic entailment $\models$ 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: basics

- 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_i

  If logic is sound, this means A_i semantically entail A

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

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

- 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

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

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

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

- If all rules preserve semantic entailment, logic is sound. (proof?)

Conjunction (cont.)

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

- Example derivation where $\Gamma \equiv A \wedge (B \wedge C)$

$$\dfrac{\dfrac{\Gamma \vdash A \wedge (B \wedge C)}{\Gamma \vdash A}\ \wedge\text{-}EL \qquad \dfrac{\dfrac{\Gamma \vdash A \wedge (B \wedge C)}{\Gamma \vdash B \wedge C}\ \wedge\text{-}ER}{\Gamma \vdash C}\ \wedge\text{-}ER}{\Gamma \vdash A \wedge C}\ \wedge\text{-}I$$

Note implicit use of axiom at derivation's leaves

- Can we **prove** anything with just these three rules?

  Equivalently: which (purely conjunctive) formulae are tautologies?

Implication

- Rules

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

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

$$\dfrac{\dfrac{\vdots}{A \wedge (B \wedge C) \vdash A \wedge C}}{\vdash A \wedge (B \wedge C) \to A \wedge C}$$

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

  $\vdash A \to B \to A$
  $\vdash (A \to B \to C) \to (A \to B) \to A \to C$
  $\vdash (A \wedge B) \to (B \wedge A)$

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

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

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

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

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: $A \vee \neg A$
  - or rule "Reductio ad absurdum"

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \mathit{RAA}$$

- 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

$$a^b = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{(\sqrt{2} * \sqrt{2})} = \sqrt{2}^2 = 2$$

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**
- Let a finite collection of function symbols $\mathcal{F}$ and predicates $\mathcal{P}$ be given (a **signature**) as well as a set $\mathcal{V}$ of variables

  Write f^i [or p^i] to indicate function symbol f [predicate p] has arity $i \in \mathcal{N}$
- *Term*, the **terms in first-order logic**, is the smallest set where

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

  N.B. constants are 0-ary function symbols

Syntax (cont.)

- *Form*, the **formulae in 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. $\neg\phi \in$ *Form* if $\phi \in$ *Form*,
  4. $\phi \circ \psi \in$ *Form* if $\phi \in$ *Form*, $\psi \in$ *Form* and $\circ \in \{\wedge, \vee, \rightarrow\}$,
  5. $\forall x.\, \phi \in$ *Form* and $\exists x.\, \phi \in$ *Form* if $\phi \in$ *Form* and $x \in \mathcal{V}$

- All occurrences of a variable in a formula are **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 ϕ is **bound** if x occurs within a subformula of ϕ of the form $\exists x.\psi$ or $\forall x.\, \psi$

Semantics

- A **structure** is a pair $\mathcal{A} = \langle U_\mathcal{A}, I_\mathcal{A} \rangle$ where $U_\mathcal{A}$ is an nonempty set, the **universe**, and $I_\mathcal{A}$ is a mapping where

  1. $I_\mathcal{A}(p^n)$ is an n-ary relation on $U_\mathcal{A}$, for $p^n \in \mathcal{P}$,
  2. $I_\mathcal{A}(f^n)$ is an n-ary (total) function on $U_\mathcal{A}$, for $f^n \in \mathcal{F}$, and
  3. $I_\mathcal{A}(x)$ is an element of $U_\mathcal{A}$, for each $x \in \mathcal{V}$

  As shorthand, write $p^\mathcal{A}$ for $I_\mathcal{A}(p)$, etc.

- For $\mathcal{A}$ a structure, define the **value of a term t under $\mathcal{A}$**, written $\mathcal{A}(t)$ by

  1. $\mathcal{A}(x) = x^\mathcal{A}$, for $x \in \mathcal{V}$, and
  2. $\mathcal{A}(f(t_1, \ldots, t_n)) = f^\mathcal{A}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$

Semantics (cont.)

Define the **(truth-)value** of formula ϕ, written $\mathcal{A}(\phi)$ under $\mathcal{A}$ as:

$$\mathcal{A}(\bot) = \textbf{False}$$

$$\mathcal{A}(p(t_1,\ldots,t_n)) = \begin{cases} \textbf{True} & \text{if } (\mathcal{A}(t_1),\ldots,\mathcal{A}(t_n)) \in p^{\mathcal{A}} \\ \textbf{False} & \text{otherwise} \end{cases}$$

$$\mathcal{A}(\neg\phi) = \begin{cases} \textbf{True} & \text{if } \mathcal{A}(\phi) = \textbf{False} \\ \textbf{False} & \text{if } \mathcal{A}(\phi) = \textbf{True} \end{cases}$$

$$\vdots$$

$$\mathcal{A}(\forall x.\,\phi) = \begin{cases} \textbf{True} & \text{if for all } u \in U_{\mathcal{A}}, \mathcal{A}_{[u/x]}(\phi) = \textbf{True} \\ \textbf{False} & \text{otherwise} \end{cases}$$

$$\mathcal{A}(\exists x.\,\phi) = \begin{cases} \textbf{True} & \text{if for some } u \in U_{\mathcal{A}}, \mathcal{A}_{[u/x]}(\phi) = \textbf{True} \\ \textbf{False} & \text{otherwise} \end{cases}$$

Here $\mathcal{A}_{[u/x]}$ is the structure $\mathcal{A}'$ identical to $\mathcal{A}$, except $x^{\mathcal{A}'} = u$.

Semantics (cont.)

- When $\mathcal{A}(\phi) = \textbf{True}$, we write $\mathcal{A} \models \phi$ and say ϕ **is satisfied with respect to** $\mathcal{A}$ or $\mathcal{A}$ **is a model** of ϕ. When every suitable structure is a model, we write $\models \phi$ and say ϕ **is valid**.

- If there is at least one model for ϕ, ϕ **is satisfiable** (and **contradictory** otherwise).

- Complexity of these problems?

An example

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

- A model:

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

- Not a model:

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

More examples

Which of following are satisfiable? Valid?

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

  satisfied WRT rationals

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

  satisfied WRT any dense order

- $\exists x.x \neq 0$

  satisfied WRT domains with $\geq$ 2 elements

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

  valid

Universal quantification

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

  Side condition (*): x not free in any assumptions in Γ.

- Why the side condition? Consider the following "derivation".

$$\dfrac{\dfrac{\dfrac{x = 0 \vdash x = 0}{x = 0 \vdash \forall x.\, x = 0}\ \forall\text{-}I}{\vdash x = 0 \to \forall x.\, x = 0}\ \to\text{-}I}{\vdash \forall x.\, (x = 0 \to \forall x.\, x = 0)}\ \forall\text{-}I$$

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

Universal quantification (cont.)

- Is the following a proof?

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

- Conclusion is not valid. Reason: false if $U_{\mathcal{A}}$ has ≥ 2 elements.
- Proof incorrect. Reason: substitution must be capture-avoiding.

  i.e., y must not occur free in substituted term t, where here $t = y$.
- This detail concerns substitution (and renaming of bound variables), not $\forall$-E.

Universal quantification (cont.)

- Prove: $\forall x.\, A(x) \wedge B(x) \rightarrow \forall x.\, A(x) \wedge \forall x.\, B(x)$

- Proof: Let $\Gamma \equiv \forall x.\, A(x) \wedge B(x)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash \forall x.\, A(x) \wedge B(x)}{\Gamma \vdash A(x) \wedge B(x)}\,\forall\text{-}E}{\Gamma \vdash A(x)}\,\wedge\text{-}EL}{\Gamma \vdash \forall x.\, A(x)}\,\forall\text{-}I \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash \forall x.\, A(x) \wedge B(x)}{\Gamma \vdash A(x) \wedge B(x)}\,\forall\text{-}E}{\Gamma \vdash B(x)}\,\wedge\text{-}ER}{\Gamma \vdash \forall x.\, B(x)}\,\forall\text{-}I}{\Gamma \vdash \forall x.\, A(x) \wedge \forall x.\, B(x)}\,\wedge\text{-}I}{\vdash (\forall x.\, A(x) \wedge B(x)) \rightarrow (\forall x.\, A(x) \wedge \forall x.\, B(x))}\,\rightarrow\text{-}I$$

- Is it correct? Yes, check side conditions of $\forall$-*I*

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 not free in B or Γ.

- Sample derivation, assuming x does not occur free in B
  Let $\Gamma \equiv \forall x.A(x) \to B, \exists x.\, A(x), A(x)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash \forall x.A(x) \to B}{\Gamma \vdash A(x) \to B}\ \forall\text{-}E \qquad \Gamma \vdash A(x)}{\Gamma \vdash B}\ \to\text{-}E \qquad \forall x.A(x) \to B, \exists x.\, A(x) \vdash \exists x.\, A(x)}{\forall x.A(x) \to B, \exists x.\, A(x) \vdash B}\ \exists\text{-}E}{\forall x.A(x) \to B \vdash (\exists x.\, A(x)) \to B}\ \to\text{-}I}{\vdash (\forall x.\, A(x) \to B) \to ((\exists x.\, A(x)) \to B)}\ \to\text{-}I$$

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 $t_1, t_2 \in \mathit{Term}$

- Semantics: recall a structure is a pair $\mathcal{A} = \langle U_\mathcal{A}, I_\mathcal{A} \rangle$ and $I_\mathcal{A}(t)$ is the interpretation of t.

- $$I_\mathcal{A}(s = t) = \begin{cases} \textbf{True} & I_\mathcal{A}(s) = I_\mathcal{A}(t) \\ \textbf{False} & \text{otherwise} \end{cases}$$

  Note the three completely different uses of "=" here!

Equality

- Equality is an equivalence relation

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

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

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

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

- Soundness: equality in $I_{\mathcal{A}}$ is a congruence

On the shape of proofs

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

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

- 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.