Programming Research Laboratory

FLOLAC '16

Elementary logic

Classical semantics of propositional logic

8 July 2016

柯向上

(日本) 国立情報学研究所

hsiang-shang@nii.ac.jp

Purpose of deduction systems (like NJ and NK)

Constructing derivations in a deduction system is like playing a game of symbols, with the rules being strictly followed. But is there any meaning in playing the game?

Yes! We informally introduced the intuitionistic meaning of propositions and explained how each inference rule in NJ is valid in terms of this meaning. Thus every (correct) derivation gives a valid entailment.

We can make the connection mathematically precise, starting from defining a *semantics* for propositional logic, i.e., translating propositional formulas to mathematical entities.

Preliminary: structured proof

Lamport proposes an informal yet principled way of writing proofs, *inspired by natural deduction*.

- Analyse a proof goal into assumptions and conclusion.
- Separate a proof into intermediate steps, with the last one being "QED", i.e., the conclusion we set out to establish.
  - The granularity of steps should be fine enough such that proof of each step is straightforward.
- Organise intermediate steps as nested, numbered lists, explicitly showing the tree structure of the proof, and making it easy to refer to previous steps.

A sample structured proof

Theorem. If a function is bijective, it has a two-sided inverse.

ASSUME $f : A \to B$
(injectivity) $\forall a, a' : A.\ f\,a = f\,a' \Rightarrow a = a'$
(surjectivity) $\forall b : B.\ \exists a : A.\ f\,a = b$

GOAL There exists $g : B \to A$ such that
$\forall a : A.\ g\,(f\,a) = a$ and $\forall b : B.\ f\,(g\,b) = b$.

PROOF Construct the inverse and verify the inverse properties.

0 There exists $g : B \to A$.

1 $\forall b : B.\ f\,(g\,b) = b$

2 $\forall a : A.\ g\,(f\,a) = a$

3 QED.

PROOF The inverse is constructed by $\boxed{0}$, and the inverse properties are verified by $\boxed{1}$ and $\boxed{2}$.

A sample structured proof (continued)

0 There exists $g : B \to A$.

PROOF Given any $b : B$, let $g\,b$ be the element of A that is asserted to exist by surjectivity.

1 $\forall b : B.\ f\,(g\,b) = b$

ASSUME $b : B$

GOAL $f\,(g\,b) = b$

PROOF $g\,b$ is, by definition in $\boxed{0}$ (in terms of surjectivity), an element $a : A$ satisfying $f\,a = b$.

A sample structured proof (continued)

$\boxed{2}$ $\forall a : A.\ g\,(f\,a) = a$

$\boxed{\text{ASSUME}}$ $a : A$

$\boxed{\text{GOAL}}$ $g\,(f\,a) = a$

$\boxed{\text{PROOF}}$ Use injectivity.

$\boxed{2.0}$ $f\,(g\,(f\,a)) = f\,a$ $\boxed{\text{PROOF}}$ $\boxed{1}$, substituting $f\,a$ for b.

$\boxed{2.1}$ QED. $\boxed{\text{PROOF}}$ Injectivity and $\boxed{2.0}$.

Exercise. If a function has a two-sided inverse, it is bijective.

$\boxed{\text{ASSUME}}$ $f : A \to B;\quad g : B \to A$

$\forall a : A.\ g\,(f\,a) = a;\quad \forall b : B.\ f\,(g\,b) = b$

$\boxed{\text{GOAL}}$ $\forall a, a' : A.\ f\,a = f\,a' \Rightarrow a = a'$

$\forall b : B.\ \exists a : A.\ f\,a = b$

Exercise. Read Lamport's papers on structured proofs. What do you think about such proofs (compared with unstructured ones)?

Classical semantics of propositional logic

Classical semantics adopts the *principle of bivalence*: every proposition denotes exactly one of the two truth-values, 0 (false) or 1 (true).

Definition. The set of *valuations* is defined to be $\mathcal{PV} \to \mathbf{2}$, where $\mathbf{2} := \{0, 1\}$.

Definition. The *truth-value interpretation* $[\![\_]\!] : \textsc{Prop} \to (\mathcal{PV} \to \mathbf{2}) \to \mathbf{2}$ of propositional formulas maps each propositional formula to a function from valuations to truth values, and is defined by

$$
\begin{array}{lcl}
[\![\bot]\!]\ \sigma & = & 0 \\
[\![v : \mathcal{PV}]\!]\ \sigma & = & \sigma\, v \\
[\![\varphi \wedge \psi]\!]\ \sigma & = & \mathit{min}\ ([\![\varphi]\!]\ \sigma)\ ([\![\psi]\!]\ \sigma) \\
[\![\varphi \vee \psi]\!]\ \sigma & = & \mathit{max}\ ([\![\varphi]\!]\ \sigma)\ ([\![\psi]\!]\ \sigma) \\
[\![\varphi \to \psi]\!]\ \sigma & = & \mathbf{if}\ [\![\varphi]\!]\ \sigma \leqslant [\![\psi]\!]\ \sigma\ \mathbf{then}\ 1\ \mathbf{else}\ 0
\end{array}
$$

Meta-connectives

Lemma. $[\![\top]\!]\ \sigma = 1$ for any valuation σ.

ASSUME $\sigma : \mathcal{PV} \to \mathbf{2}$

GOAL $[\![\top]\!]\ \sigma = 1$

PROOF Expand the definitions:

$$
\begin{aligned}
& [\![\top]\!]\ \sigma \\
= \quad & \{\ \text{definition of } \top\ \} \\
& [\![\bot \to \bot]\!]\ \sigma \\
= \quad & \{\ \text{definition of } [\![\_]\!] \text{ for `}\!\to\!\text{'}\ \} \\
& \mathbf{if}\ [\![\bot]\!]\ \sigma \leqslant [\![\bot]\!]\ \sigma\ \mathbf{then}\ 1\ \mathbf{else}\ 0 \\
= \quad & \{\ \text{definition of } [\![\_]\!] \text{ for } \bot\ \} \\
& \mathbf{if}\ 0 \leqslant 0\ \mathbf{then}\ 1\ \mathbf{else}\ 0 \\
= \quad & \{\ 0 \leqslant 0\ \} \\
& 1
\end{aligned}
$$

Exercise. $[\![\neg\varphi]\!]\ \sigma = 1 - [\![\varphi]\!]\ \sigma$ for any valuation σ.

Semantic consequence

Definition. A valuation σ *satisfies* a formula φ exactly when $[\![\varphi]\!]\,\sigma = 1$; it satisfies a list Γ of formulas exactly when it satisfies every formula in Γ.

Definition. φ is a *semantic consequence* of Γ exactly when, for any valuation σ, φ is satisfied by σ whenever Γ is satisfied by σ. In this case we write $\Gamma \models \varphi$.

Definition. φ is *valid* exactly when $\models \varphi$. In this case φ is called a *tautology*.

Example: $\models \varphi \vee \neg\varphi$

$\boxed{\text{ASSUME}}$ $\sigma : \mathcal{PV} \to \mathbf{2}$

$\boxed{\text{GOAL}}$ $[\![\varphi \vee \neg\varphi]\!]\ \sigma = 1$

$\boxed{\text{PROOF}}$ Case analysis on $[\![\varphi]\!]\ \sigma$.

$\boxed{0}$ $\boxed{\text{CASE}}$ $[\![\varphi]\!]\ \sigma = 1$

$\boxed{\text{PROOF}}$ $[\![\varphi \vee \neg\varphi]\!]\ \sigma = \mathit{max}\ ([\![\varphi]\!]\ \sigma)\ (1 - [\![\varphi]\!]\ \sigma) = \mathit{max}\ 1\ 0 = 1.$

$\boxed{1}$ $\boxed{\text{CASE}}$ $[\![\varphi]\!]\ \sigma = 0$

$\boxed{\text{PROOF}}$ $[\![\varphi \vee \neg\varphi]\!]\ \sigma = \mathit{max}\ ([\![\varphi]\!]\ \sigma)\ (1 - [\![\varphi]\!]\ \sigma) = \mathit{max}\ 0\ 1 = 1.$

$\boxed{2}$ QED.

$\boxed{\text{PROOF}}$ Either $[\![\varphi]\!]\ \sigma = 1$ or $[\![\varphi]\!]\ \sigma = 0$; $\boxed{1}$ and $\boxed{2}$.

Notation. "$\boxed{\text{CASE}}$ C" abbreviates "$\boxed{\text{ASSUME}}$ C $\boxed{\text{GOAL}}$ QED".

Exercise. $\varphi \vee \psi, \neg\psi \models \varphi$

$\models \varphi \vee \neg\varphi$ — truth table method

We may just summarise the case analysis on $[\![\varphi]\!]\ \sigma$ and evaluation of the value of the entire propositional formula in a *truth table*.

φ	φ	$\vee$	$\neg$	φ
0	0	1	1	0
1	1	1	0	1

Theorem. Validity in classical propositional logic is *decidable*, i.e., there is a mechanical procedure that, given a propositional formula, decides whether it is valid or not in a finite amount of time.

Exercise. How do you use a truth table to show $\varphi \vee \psi, \neg\psi \models \varphi$?

Relationship between deduction system and semantics

Theorem. NK is *sound* with respect to the classical semantics: $\Gamma \vdash_{\mathrm{NK}} \varphi$ implies $\Gamma \models \varphi$ for any Γ and φ.

Corollary. NJ is sound with respect to the classical semantics.

PROOF Every NJ derivation is an NK derivation.

Theorem. NK is *complete* with respect to the classical semantics: $\Gamma \models \varphi$ implies $\Gamma \vdash_{\mathrm{NK}} \varphi$ for any Γ and φ.

NJ is, however, not complete with respect to the classical semantics, since, for instance, $\mathtt{A} \vee \neg\mathtt{A}$ is classically valid but not derivable in NJ.

Detour: proving underivability semantically

Theorem (consistency)**.** There is no NJ/NK derivation of $\vdash \bot$.

$\boxed{\text{ASSUME}}$ $\vdash \bot$ derivable

$\boxed{\text{GOAL}}$ contradiction

$\boxed{\text{PROOF}}$ By soundness we get $\models \bot$, which is false however.

It is possible to prove this theorem purely syntactically, but it takes more than a straightforward induction.

Detour: proving underivability semantically

Theorem. There is no derivation of $\vdash_{\mathrm{NJ}} \mathtt{A} \vee \neg\mathtt{A}$.

ASSUME $\vdash_{\mathrm{NJ}} \mathtt{A} \vee \neg\mathtt{A}$ derivable

GOAL contradiction

PROOF

0 NJ is sound with respect to the *Heyting algebra* semantics.

1 Open subsets of $\mathbb{R}$ give rise to a Heyting algebra.

2 $\mathtt{A} \vee \neg\mathtt{A}$ is not valid with respect to the Heyting algebra in $\boxed{1}$.

3 QED.

PROOF By $\boxed{0}$, $\mathtt{A} \vee \neg\mathtt{A}$ should have been valid with respect to any Heyting algebra, but $\boxed{2}$ gives a counterexample.

Soundness proof

Theorem. NK is *sound* with respect to the classical semantics: $\Gamma \vdash_{\mathrm{NK}} \varphi$ implies $\Gamma \models \varphi$ for any Γ and φ.

Intuitively, proving this theorem is just formalising how we justified the inference rules yesterday: For each rule,

- assume that the premises are semantic consequences, and
- prove that the conclusion is also a semantic consequence.

Example: soundness of implication introduction

Lemma. $\Gamma, \varphi \models \psi$ implies $\Gamma \models \varphi \to \psi$.

ASSUME $\Gamma : \textsc{List Prop}$; $\varphi, \psi : \textsc{Prop}$; $\Gamma, \varphi \models \psi$
$\sigma : \mathcal{PV} \to \mathbf{2}$; σ satisfies Γ

GOAL $[\![\varphi \to \psi]\!]\ \sigma = 1$

PROOF Case analysis on the truth value of φ.

0 CASE $[\![\varphi]\!]\ \sigma = 0$

1 CASE $[\![\varphi]\!]\ \sigma = 1$

2 QED.

PROOF $\boxed{0}$ and $\boxed{1}$ cover all possible values of $[\![\varphi]\!]\ \sigma$.

Example: soundness of implication introduction

0 CASE $[\![\varphi]\!]\ \sigma = 0$

PROOF

$$
\begin{array}{ll}
 & [\![\varphi \to \psi]\!]\ \sigma = 1 \\
\Leftrightarrow & \quad \{\text{ definition of } [\![\_]\!] \text{ for '}\!\to\!\text{' }\} \\
 & [\![\varphi]\!]\ \sigma \leqslant [\![\psi]\!]\ \sigma \\
\Leftrightarrow & \quad \{\text{ assumption }\} \\
 & 0 \leqslant [\![\psi]\!]\ \sigma \\
\Leftrightarrow & \quad \{\text{ truth value is either } 0 \text{ or } 1 \} \\
 & \textit{true}
\end{array}
$$

Example: soundness of implication introduction

1 $\boxed{\text{CASE}}$ $[\![\varphi]\!]\ \sigma = 1$

$\boxed{\text{PROOF}}$ ψ must be true, and therefore so must $\varphi \to \psi$.

1.0 σ satisfies Γ, φ. $\boxed{\text{PROOF}}$ σ satisfies Γ and φ.

1.1 $[\![\psi]\!]\ \sigma = 1$. $\boxed{\text{PROOF}}$ $\Gamma, \varphi \models \psi$ and $\boxed{1.0}$.

1.2 QED.

$\boxed{\text{PROOF}}$

$$
\begin{array}{ll}
 & [\![\varphi \to \psi]\!]\ \sigma = 1 \\
\Leftrightarrow & \quad \{\ \text{definition of } [\![\_]\!] \text{ for '}\to\text{'}\ \} \\
 & [\![\varphi]\!]_\sigma \leqslant [\![\psi]\!]_\sigma \\
\Leftrightarrow & \quad \{\ 2.2\ \} \\
 & [\![\varphi]\!]_\sigma \leqslant 1 \\
\Leftrightarrow & \quad \{\ \text{truth value is either } 0 \text{ or } 1\ \} \\
 & \textit{true}.
\end{array}
$$

Exercise. What about soundness of other rules?

Induction

Every inductively defined set, e.g., the set $\mathbb{N}$ of natural numbers and $\textsc{Prop}$, is equipped with an *induction principle*.

Let $P\,\varphi$ be a property on $\varphi : \textsc{Prop}$. If we can show that P is "propagated" by every construction rule of $\textsc{Prop}$, then for any $\varphi : \textsc{Prop}$, a proof of $P\,\varphi$ can be derived in the same way as how φ is constructed.

Slightly more formally, $P\,\varphi$ holds for every $\varphi : \textsc{Prop}$ if

- $P\,v$ holds for every $v : \mathcal{PV}$,
- $P\,\bot$ holds,
- for any φ, $\psi \in \textsc{Prop}$, $P\,(\varphi \wedge \psi)$ holds if $P\,\varphi$ and $P\,\psi$ hold,
- for any φ, $\psi \in \textsc{Prop}$, $P\,(\varphi \vee \psi)$ holds if $P\,\varphi$ and $P\,\psi$ hold, and
- for any φ, $\psi \in \textsc{Prop}$, $P\,(\varphi \to \psi)$ holds if $P\,\varphi$ and $P\,\psi$ hold.

Inductive definition of derivations

For brevity, let us focus on the "implicational fragment" of $\textsc{Prop}$, calling the subset $\textsc{Prop}^-$.

Definition. The sets $\mathrm{NJ}^-[\Gamma;\varphi]$ of derivations, where Γ ranges over $\textsc{List}\ \textsc{Prop}^-$ and φ over $\textsc{Prop}^-$, are inductively defined by the following rules:

- $\dfrac{}{\Gamma \vdash \varphi}\,(\text{assum}) : \mathrm{NJ}^-[\Gamma;\varphi]$ if $\varphi \in \Gamma$;
- $\dfrac{d}{\Gamma \vdash \varphi}\,(\bot\mathsf{E}) : \mathrm{NJ}^-[\Gamma;\varphi]$ if $d : \mathrm{NJ}^-[\Gamma;\bot]$;
- $\dfrac{d}{\Gamma \vdash \varphi \to \psi}\,(\to\mathsf{I}) : \mathrm{NJ}^-[\Gamma;\varphi \to \psi]$ if $d : \mathrm{NJ}^-[\Gamma,\varphi;\psi]$;
- $\dfrac{d \qquad e}{\Gamma \vdash \psi}\,(\to\mathsf{E}) : \mathrm{NJ}^-[\Gamma;\psi]$ if $d : \mathrm{NJ}^-[\Gamma;\varphi \to \psi]$ and $e : \mathrm{NJ}^-[\Gamma;\varphi]$.

Induction principle on NJ^-

The rule

- $\dfrac{d}{\Gamma \vdash \varphi \to \psi}$ $(\to\mathsf{I}) : \mathrm{NJ}^-[\Gamma; \varphi \to \psi]$ if $d : \mathrm{NJ}^-[\Gamma, \varphi; \psi]$

is interpreted as "if d is a derivation with conclusion $\Gamma, \varphi \vdash \psi$, then $\dfrac{d}{\Gamma \vdash \varphi \to \psi}$ $(\to\mathsf{I})$ is a derivation with conclusion $\Gamma \vdash \varphi \to \psi$".

Let $P\ \Gamma\ \varphi\ d$ be a property on $\Gamma : \textsc{List Prop}^-$, $\varphi : \textsc{Prop}^-$, and $d : \mathrm{NJ}^-[\Gamma; \varphi]$, i.e., P talks about a derivation d and the context Γ and formula φ in the conclusion of d. The corresponding case of the above rule in the induction principle on NJ^- is

- For any $\Gamma : \textsc{List Prop}^-$, φ, $\psi \in \textsc{Prop}^-$, and $d : \mathrm{NJ}^-[\Gamma, \varphi; \psi]$,
  $P\ \Gamma\ (\varphi \to \psi)\ \left(\dfrac{d}{\Gamma \vdash \varphi \to \psi}\ (\to\mathsf{I})\right)$ holds if $P\ (\Gamma, \varphi)\ \psi\ d$ holds.

Exercise. Do you accept this induction principle? Can you prove soundness formally with this induction principle? And Glivenko's theorem from yesterday?