Frege proof system(s)

Narusevych M.

14.10.22

(propositional) formulas

Syntax

In general, just some <u>well-formed</u> string:

- element of a ring $T[\bar{x}]$;
- real/rational inequality;
- term in a given type theory;

...

We stick to the most convenient reprent.:

- (countable) set of variables $V = \{p_1, p_2, \dots\}$
- finite set of Boolean connectives: $\neg, \wedge, \vee, \supset, \leftrightarrow, \oplus$,

<u>Remark</u>: $\supset$ stands for the usual $\to$.
$\oplus$ stands for the exclusive or.

In fact, any <u>complete</u> set of connectives may be used: $\{\neg, \wedge\}$, $\{\neg, \vee\}$, $\{NAND\}$, ...

formulas (cont.)

Semantics

May depend on representation, but, in general, must provide means to define <u>truth/satisfiability</u>

In our case:

$$\varphi : A \to \{T, F\},$$

where A - the set of <u>truth assignments</u>, i.e. maps from $V \to \{T, F\}$.

For $T : V \to \{T, F\}$ denote $\varphi(T)$ as $\overline{T}(\varphi)$.

$\overline{T}(\varphi)$ is computed using the usual method of <u>truth-tables</u>

We then have our usual definitions:

$$\models \varphi \qquad \Gamma \models \varphi \qquad \varphi \in SAT$$

$\models \varphi$: <u>tautology</u>

$\Gamma \models \varphi$: <u>tautological implication</u>

of particular importance for proof theory

Proof systems

Problem $\models \varphi$? is decidable (is co-NP-complete)

Bud the most obvious (brute-force) method does nod provide any reason why given formula is a dautology.

We need feasible/understandable witnesses, a.k.a. proofs.

Proof

In general just some data witnessing $\models \varphi$ (or $\Gamma \models \varphi$).

The only major restriction is that an alleged proof is easily checkable (Cook-Reckhow)

Differend implementations of the above give rise to differend proof systems.

$\mathcal{F}$-system

Each proof system defines $\vdash$.
There are criteria any proof system <u>must</u> obey:

- $\vdash \varphi \Rightarrow \models \varphi$ $(\Gamma \vdash \varphi \Rightarrow \Gamma \models \varphi)$ ... <u>soundness</u>
- $\models \varphi \Rightarrow \vdash \varphi$ $(\Gamma \models \varphi \Rightarrow \Gamma \vdash \varphi)$ ... <u>(implicational) completeness</u>

Frege system(s)

The most well-known.

Finite set of axiom schemas	Finite set of derivation rules
A	R

We will focus on a particular implementation (from a proof-complexity perspective they are all the same ... Reckhow)

<u>$\mathcal{F}$-system</u>: $R = \{$<u>modus ponens</u>$\}$

$$\frac{A \quad A \supset B}{B}$$

$\mathcal{F}$-system (cond.)

Axiom schemas:

- $p_1 \supset (p_2 \supset p_1)$
- $(p_1 \supset p_2) \supset (p_1 \supset (p_2 \supset p_3)) \supset (p_1 \supset p_3)$
- $p_1 \supset p_1 \vee p_2$, $p_2 \supset p_1 \vee p_2$
- $(p_1 \supset p_3) \supset (p_2 \supset p_3) \supset (p_1 \vee p_2 \supset p_3)$

  <u>proof by cases</u>

- $p_1 \wedge p_2 \supset p_1$, $p_1 \wedge p_2 \supset p_2$
- $p_1 \supset p_2 \supset p_1 \wedge p_2$
- $(p_1 \supset p_2) \supset (p_1 \supset \neg p_2) \supset \neg p_1$

  <u>proof by contradiction</u>

- $(\neg\neg p_1) \supset p_1$

Definitions of proof ($\vdash$) or derivation ($\Gamma \vdash$) are clear. (Implicational) soundness of $\mathcal{F}$ is clear.

Compactness

Before we show completeness of $\vdash$ we need to prove compactness of $\models$.

Usually, compactness is derived as a direct consequence of completeness.

FO compactness can be shown by ultrapowers.

We are presenting a topological argument.

Thm: ① Γ is sat. iff every $\Gamma_0 \subseteq_{fin.} \Gamma$ is sat.

② $\Gamma \models \varphi$ iff $\exists \Gamma_0 \subseteq_{fin.} \Gamma : \Gamma_0 \models \varphi$.

Pr.: Enough to prove ① since $\Gamma \models \varphi$ iff $\Gamma \cup \{\neg\varphi\}$ is unsat.

Let V be the set of variables used in Γ (or just the set of all variables)

$\{T,F\}^V$ is the set of all truth assignments of V. Note that $\{T,F\}^V \simeq \underbrace{\{T,F\} \times \{T,F\} \times \ldots}_{|V|\text{-times}}$.

$\{T,F\}$ can be viewed as a topological space endowed with the discrete topology.

Compactness (cont.)

$\{T,F\}^V$ is then endowed with the <u>product topology</u>, i.e. the smallest topology making natural projections continuous.

This means $\forall v \in V$ and $\forall i \in \{T,F\}$ the set $B_{v,i} = \{\tau \in \{T,F\}^V \mid \tau(v) = i\}$ is <u>clopen</u>.

(note that any subset of $\{T,F\}$ is clopen in the discrete topology).

Since $\{T,F\}$ is <u>compact</u>, the product $\{T,F\}^V$ is compact as well (Tychonoff).

For $\varphi \in \Gamma$ denote $D_\varphi = \{\tau \in \{T,F\}^F \mid \overline{\tau}(\varphi) = T\}$

φ involves only finitely many variables and so D_φ is clopen, e.g.:

$$D_{a \wedge \neg b} = B_{a,T} \cap B_{b,F} \; , \; D_{d \vee e} = B_{d,T} \cup B_{e,T}$$

Compactness (end.)

Γ is satisfiable iff $\bigcap_{\varphi \in \Gamma} D_\varphi \neq \emptyset$,

which is equivalent to

$$\bigcup_{\varphi \in \Gamma} D_\varphi^c \neq \{T, F\}^V.$$

Note that each D_φ^c is also clopen and due to compactness of $\{T, F\}^V$ it follows:

$$\bigcup_{\varphi \in \Gamma} D_\varphi^c = \bigcup_{\varphi \in \Gamma_0} D_\varphi^c \text{ for } \Gamma_0 \underset{\text{fin.}}{\subseteq} \Gamma.$$

So, $\forall \Gamma_0 \underset{\text{fin.}}{\subseteq} \Gamma : \Gamma_0$ is sat. $\Rightarrow$ ...

... $\Rightarrow \forall \Gamma_0 \underset{\text{fin.}}{\subseteq} \Gamma : \bigcup_{\varphi \in \Gamma_0} D_\varphi^c \neq \{T, F\}^V \Rightarrow$ ...

... $\Rightarrow \bigcup_{\varphi \in \Gamma} D_\varphi^c \neq \{T, F\}^V \Rightarrow \bigcap_{\varphi \in \Gamma} D_\varphi \neq \emptyset \Rightarrow$ ...

... $\Rightarrow \Gamma$ is sat.

$\blacksquare$

Completness

Thm: The system $\mathcal{F}$ is complete and implicationally complete, i.e.:

1. If φ is tautology, then $\vdash \varphi$,
2. if $\Gamma \models \varphi$, then $\Gamma \vdash \varphi$.

Pr: We first reduce 2 to 1.

By compactness $\exists \Gamma_0 \underset{fin.}{\subseteq} \Gamma$ s.t. $\Gamma_0 \models \varphi$.

Let $\Gamma_0 = \{\varphi_0, \dots, \varphi_k\}$.

But then $\varphi_0 \supset \varphi_1 \supset \dots \supset \varphi_k \supset \varphi$ is a tautology and so, by 1, is provable.

We can then use modus ponens $k+1$-times to derive $\varphi_0, \dots, \varphi_k \vdash \varphi$ $\blacksquare$

We now show 1. This is done by simulating truth-tables method in $\mathcal{F}$.

Completness (cond.)

The method of truth-tables can be presented (rather ridiculously) in a following manner:

I. we are given a tautology φ consisting of different variables $x_0, \dots, x_n$. This means that for any $\sigma_0, \dots, \sigma_n$, where σ_i is either x_i or $\neg x_i$ it holds that:

$$\sigma_0, \dots, \sigma_n \models \varphi.$$

II. By induction we show that $\forall i < n$ and for any $\sigma_0, \dots, \sigma_i$ it holds that

$$\left.\begin{array}{l} \sigma_0, \dots, \sigma_i, x_{i+1} \models \varphi \\ \sigma_0, \dots, \sigma_i, \neg x_{i+1} \models \varphi \end{array}\right\} \Rightarrow \sigma_0, \dots, \sigma_i \models \varphi$$

This implies (letting $i = -1$) $\models \varphi$, thus deriving φ is a tautology.

We want to proceed in a similar manner but changing every appearence of $\models$ to $\vdash$ and the last appearence of "tautology" to "provable".

Completness (cont.)

Lemma: Let φ be a formula (not necessarily a tautology) consisting of different variables $x_0, \dots, x_n$.
Then, for any $\sigma_0, \dots, \sigma_n$ ($\sigma_i = x_i$ or $\neg x_i$):

$$\sigma_0, \dots, \sigma_n \vdash \varphi \quad \text{or} \quad \sigma_0, \dots, \sigma_n \vdash \neg\varphi$$

Pr: by induction on φ's complexity.

- in case φ is a variable, the statement is clear;
- Let $\varphi = \varphi_0 \vee \varphi_1$. Assume $\sigma_0, \dots, \sigma_n \vdash \varphi_0$, then $\varphi_0 \vdash \varphi_0 \vee \varphi_1$ since $\varphi_0 \supset \varphi_0 \vee \varphi_1$ is an axiom.

  In case $\sigma_0, \dots, \sigma_n \vdash \neg\varphi_0$ and $\sigma_0, \dots, \sigma_n \vdash \neg\varphi_1$, it follows that:

  $$\neg\varphi_0, \neg\varphi_1 \vdash \neg(\varphi_0 \vee \varphi_1) \text{. since } \dots\dots$$

- other outer connectives are done analogously

$\blacksquare$

Note that the above lemma shows the step I in our truth-table simulation.

Completness (cont.)

<u>Lemma</u>: Let φ and σ_i's be as before. Assume $\sigma_0, \dots, \sigma_i, x_{i+1} \vdash \varphi$ and $\sigma_0, \dots, \sigma_i, \neg x_{i+1} \vdash \varphi$. Then, $\sigma_0, \dots, \sigma_i \vdash \varphi$.

<u>Pr</u>: This follows from a more general principle:

$$\underbrace{\Gamma, \psi \vdash \varphi \qquad \Gamma, \neg\psi \vdash \varphi}$$
$$\Downarrow$$
$$\Gamma \vdash \varphi$$

We prove this using two fundamental principle, which are not so hard to prove:

(D) $\Gamma, \psi \vdash \varphi \implies \Gamma \vdash \psi \supset \varphi$ ... <u>deduction lemma</u>

(C) $\varphi \supset \psi \vdash \neg\psi \supset \neg\varphi$ ... <u>contra-positive</u>

$$\Gamma, \psi \vdash \varphi \qquad\qquad \Gamma, \neg\psi \vdash \varphi$$
$$\Downarrow \text{(D)} + \text{(C)} \qquad\qquad \Downarrow \text{(D)} + \text{(C)}$$
$$\Gamma \vdash \neg\varphi \supset \neg\psi \qquad\qquad \Gamma \vdash \neg\varphi \supset \neg\neg\psi$$

[modus ponens + axiom:

$$(\neg\varphi \supset \neg\psi) \supset (\neg\varphi \supset \neg\neg\psi) \supset \neg\neg\varphi$$
$$\Downarrow$$
$$\Gamma \vdash \neg\neg\varphi$$

$\Downarrow$ axiom $\neg\neg\varphi \supset \varphi$ + modus ponens

$\Gamma \vdash \varphi$ ■ This finishes step <u>II</u>.