What is a proof?

Formal Proof System

We will consider a some set of logical formulas $\mathscr{F}$ (e.g. propositional logic)

Definition

An proof system is $(\mathscr{F}, \text{Infer})$ where $\text{Infer} \subseteq \mathscr{F}^* \times \mathscr{F}$ a decidable set of *inference steps*.

- a set is *decidable* iff there is a program to check if an element belongs to it
- given a set S, notation S^* denotes all finite sequences with elements from S

We schematically write an inference step $((P_1, \ldots, P_n), C) \in \text{Infer}$ by

$$\frac{P_1 \ldots P_n}{C}$$

and we say that from $P_1, \ldots, P_n$ (**premises**) we derive C (**conclusion**).
An inference step is called an *axiom instance* when $n = 0$ (it has no premises).
Given a proof system $(\mathscr{F}, \text{Infer})$, a proof is a finite sequence of inference steps such that, for every inference step, each premise is a conclusion of a previous step.

Proof in a Proof System

Definition

Given $(\mathscr{F}, \text{Infer})$ where $\text{Infer} \subseteq \mathscr{F}^* \times \mathscr{F}$ a **proof** in $(\mathscr{F}, \text{Infer})$ is a finite sequence of inference steps $S_0, \dots, S_m \in \text{Infer}$ such that, for each S_i where $0 \leq i \leq m$, for each premise P_j of S_i there exists $0 \leq k < i$ such that P_j is the conclusion of S_k.

$$\begin{array}{lll} S_0: & ((), & C_0) \\ & \dots & \\ S_k: & ((\dots\dots\dots), & \mathbf{P_j}) \\ & \dots & \\ S_i: & ((\dots, \mathbf{P_j}, \dots), & C_i) \end{array}$$

Given the definition of the proof, we can replace each premise P_j with the index k where P_j was the conclusion of S_k $(P_j \equiv \text{Conc}(S_k))$

A proof is then a sequence of elements from $\{0, 1, \dots\}^* \times \mathscr{F}$ where each S_i in the sequence is of the form $(k_1, \dots, k_n, C)$ for $0 \leq k_1, \dots, k_n < i$ and where $(\text{Conc}(S_{k_1}), \dots, \text{Conc}(S_{k_n}), C) \in \text{Infer}$.

Proofs as Dags

We can view proofs as directed acyclic graphs.

Given a proof as a sequence of steps, for each $(k_1, \ldots, k_n, C)$ in the sequence we introduce a node labelled by C, and directed labelled edges $(\mathrm{Conc}(S_{k_j}), j, C)$ for all premises $k_1, \ldots, k_n$.

To check such proof, for each node, follow all of its incoming edges backwards in the order of their indices to find the premises, then check that the inference step is in Infer.

An Example System for Propositional Logic

A Minimal Propositional Logic Proof System

Formulas $\mathscr{F}$ defined by $F ::= x \,|\, 0 \,|\, F \to F$

Shorthand:
$\neg F \equiv F \to 0$

Inference rules: $\mathrm{Infer} = P_2 \cup P_3 \cup \mathrm{MP}$ where: (see e.g. (W) Hilbert system)

$$\begin{array}{rcllr}
P_2 & = & \{((), & F \to (G \to F) &) \,|\, F, G \in \mathscr{F}\} \\
P_3 & = & \{((), & ((F \to (G \to H)) \to ((F \to G) \to (F \to H)) &) \,|\, F, G, H \in \mathscr{F}\} \\
\mathrm{MP} & = & \{((F \to G, F), & G &) \,|\, F, G \in \mathscr{F}\}
\end{array}$$

Elements of P_1, P_2, P_3 are all axioms. These are infinite sets, but are given a schematic way and there is an algorithm to check if a given formula satisfies each of the schemas.

Exercise: draw a DAG representing proof of $a \to a$ where a is a propositional variable.

Proof of $a \longrightarrow a$

Proof system:

$$F \longrightarrow (G \longrightarrow F) \qquad ((F \longrightarrow (G \longrightarrow H)) \longrightarrow ((F \longrightarrow G) \longrightarrow (F \longrightarrow H)) \qquad \frac{F \longrightarrow G, F}{G}$$

$$a \longrightarrow a$$

Soundness of a Proof System

Derivation is a Proof from Assumptions

Definition

Given $(\mathscr{F}, \text{Infer})$, $\text{Infer} \subseteq \mathscr{F}^* \times \mathscr{F}$ **and a set of assumptions** $A \subseteq \mathscr{F}$, a **derivation from** A in $(\mathscr{F}, \text{Infer})$ is a proof in $(\mathscr{F}, \text{Infer}')$ where:

$$\text{Infer}' = \text{Infer} \cup \{((), F) \mid F \in A\}$$

Thus, assumptions from A are treated just as axioms.

Definition

We say that $F \in \mathscr{F}$ is provable from assumptions A, denoted $A \vdash_{\text{Infer}} F$ iff there exists a derivation from A in Infer that contains an inference step whose conclusion is F.

We write $\vdash_{\text{Infer}} F$ to denote that there exists a proof in Infer containing F as a conslusion (same as $\emptyset \vdash_{\text{Infer}} F$).

Consequence and Soundness in Propositional Logic

Given a set $A \subseteq \mathscr{F}$ where $\mathscr{F}$ are in propositional logic, and $C \in \mathscr{F}$, we say that C is a **semantic consequence** of A, denoted $A \models C$ iff for every environment e that defines all variables in $FV(C) \cup \bigcup_{P \in A} FV(P)$, if $[\![P]\!]_e = 1$ for all $P \in A$, then then $[\![C]\!]_e = 1$.

Definition

Given $(\mathscr{F}, \text{Infer})$ where $\mathscr{F}$ are propositional, step $((P_1 \dots P_n), C) \in \text{Infer}$ is **sound** iff $\{P_1, \dots, P_n\} \models C$. Proof system Infer is sound if every inference step is sound.

For axioms, this definition reduces to saying that C is true for all interpretations, i.e., that C is a valid formula (tautology).

Theorem

Let $(\mathscr{F}, Infer)$ where $\mathscr{F}$ are propositional logic formulas. If every inference rule in Infer is sound, then $A \vdash_{Infer} F$ implies $A \models F$.

Proof is immediate by induction on the length of the formal proof.
Consequence: $\vdash_{\text{Infer}} F$ implies F is a tautology.