Logic and Computation – CS 2800, Fall 2023

Formal proofs (by hand)

Proof rules

Stavros Tripakis

Northeastern University
Khoury College of
Computer Sciences

October 2, 2023

SOME PROOF RULES

Closing a brach when the goal is already in the hypotheses:

Assumption

$$\frac{\texttt{DONE}}{\mathcal{H}, G \vdash G}\ \text{Assumption}$$

- This rule applies to proof states where the goal G is already in the set of hypotheses.
- Intuition: G is true by assumption (G is in my set of hypotheses).
- This rule generates only one child.

Eliminating an implication in the goal: ImpIntro

$$\frac{\mathcal{H}, A \vdash B}{\mathcal{H} \vdash A \to B}\ \text{ImpIntro}$$

- This rule applies to proof states where the goal is an implication, i.e., where the goal is of the form $A \to B$.
- Intuition: to prove $A \to B$ assuming that all things in $\mathcal{H}$ are true, it suffices to prove B assuming that all things in $\mathcal{H}$ are true and also that A is true.
- This rule generates only one child.

Eliminating a conjunction in the goal: And

$$\frac{\mathcal{H} \vdash A \qquad \mathcal{H} \vdash B}{\mathcal{H} \vdash A \wedge B}\ \text{And}$$

- This rule applies to proof states where the goal is a conjunction, i.e., where the goal is of the form $A \wedge B$.
- Intuition: to prove $A \wedge B$ assuming that all things in $\mathcal{H}$ are true, it suffices to do two separate proofs: first, prove A assuming that all things in $\mathcal{H}$ are true; and second, prove B assuming that all things in $\mathcal{H}$ are true.
- This rule generates two children.

Eliminating a disjunction in the goal by choosing to prove the left part: OrLeft

$$\frac{\mathcal{H} \vdash A}{\mathcal{H} \vdash A \vee B} \text{ OrLeft}$$

- This rule applies to proof states where the goal is an implication, i.e., where the goal is of the form $A \vee B$.
- Intuition: to prove $A \vee B$ assuming that all things in $\mathcal{H}$ are true, it suffices to prove A assuming that all things in $\mathcal{H}$ are true.
- This rule generates only one child.

Eliminating a disjunction in the goal by choosing to prove the right part: OrRight

$$\frac{\mathcal{H} \vdash B}{\mathcal{H} \vdash A \vee B}\ \text{OrRight}$$

- This rule applies to proof states where the goal is an implication, i.e., where the goal is of the form $A \vee B$.
- Intuition: to prove $A \vee B$ assuming that all things in $\mathcal{H}$ are true, it suffices to prove B assuming that all things in $\mathcal{H}$ are true.
- This rule generates only one child.

If the goal is `true` we are done: True

$$\frac{\texttt{DONE}}{\mathcal{H} \vdash \texttt{true}}\ \text{True}$$

- This rule applies to proof states where the goal is the proposition `true`.
- Intuition: `true` holds by definition.
- This rule generates only one child.

If a hypothesis is `false` we are done: False

$$\frac{\texttt{DONE}}{\mathcal{H}, \texttt{false} \vdash G}\ \text{False}$$

- This rule applies to proof states where the set of hypotheses contains the proposition `false`.
- Intuition: if I assume `false` then I can prove anything I want.
- This rule generates only one child.

Eliminating a disjunction in the hypotheses: OrHyps

$$\frac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}\ \text{OrHyps}$$

- This rule applies to proof states where one of the hypotheses is of the form $A \vee B$.
- Intuition: to prove G assuming that $A \vee B$ is true (in addition to $\mathcal{H}$), we must do two separate proofs: first, prove G assuming that A is true (in addition to $\mathcal{H}$); and second, prove G assuming that B is true (in addition to $\mathcal{H}$).
  In other words, I know that $A \vee B$ is true, so I know that at least one of A or B is true, but I don't know which one. So I must prove my goal assuming any of the two. So I must do two proofs.
- This rule generates two children.

Eliminating a disjunction in the hypotheses: OrHyps

$$\frac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}\ \text{OrHyps}$$

- Why do I need to prove two things here? What if I can complete say the left branch, but not the right branch?
- If you can only complete one branch, then your proof is incomplete!
- Example:
  - Let A be "x is a power of 2" and let B be $\neg A$ (i.e., B is "x is not a power of 2"). So $A \vee B$ is $A \vee \neg A$, which always holds.
  - Let G be "x modulo $2 = 0$".
  - Then you can prove $A \vdash G$ and $A \to G$ indeed holds.
  - But you cannot prove $B \vdash G$ and indeed, $(\neg A) \to G$ does not always hold.
  - And indeed, $(A \vee B) \to G$ does not always hold, so you shouldn't be able to prove $A \vee B \vdash G$!

Eliminating a conjunction in the hypotheses: AndHyps

$$\frac{\mathcal{H}, A, B \vdash G}{\mathcal{H}, A \wedge B \vdash G}\ \text{AndHyps}$$

- This rule applies to proof states where one of the hypotheses is of the form $A \wedge B$.
- Intuition: I know that $A \wedge B$ is true, so I know that both A and B are true.
- This rule generates one child.

Eliminating $\leftrightarrow$ in the goal: Iff

$$\frac{\mathcal{H} \vdash (A \to B) \wedge (B \to A)}{\mathcal{H} \vdash A \leftrightarrow B}\ \text{Iff}$$

- This rule applies to proof states where the goal is of the form $A \leftrightarrow B$.
- Intuition: $A \leftrightarrow B$ is the same as $(A \to B) \wedge (B \to A)$.
- This rule generates one child.

Eliminating $\leftrightarrow$ in the hypotheses: IffHyps

$$\frac{\mathcal{H}, (A \to B) \wedge (B \to A) \ \vdash \ G}{\mathcal{H}, A \leftrightarrow B \ \vdash \ G} \ \text{IffHyps}$$

- This rule applies to proof states where one of the hypotheses is of the form $A \leftrightarrow B$.
- Intuition: $A \leftrightarrow B$ is the same as $(A \to B) \wedge (B \to A)$.
- This rule generates one child.

Modus Ponens

$$\frac{\mathcal{H}, A \to B, A, B \vdash G}{\mathcal{H}, A \to B, A \vdash G}\ \text{MP}$$

- This rule applies to proof states where the set of hypotheses contains one hypothesis of the form $A \to B$ and also the hypothesis A.
- Intuition: if I know that A is true, and also that A implies B, then I can deduce that B is true.
- This rule generates one child.

Cheat sheet

$\dfrac{\texttt{DONE}}{\mathcal{H} \vdash \texttt{true}}$ True	$\dfrac{\texttt{DONE}}{\mathcal{H}, \texttt{false} \vdash G}$ False
$\dfrac{\texttt{DONE}}{\mathcal{H}, G \vdash G}$ Assumption	
$\dfrac{\mathcal{H}, A \vdash B}{\mathcal{H} \vdash A \to B}$ ImpIntro	$\dfrac{\mathcal{H}, A \to B, A, B \vdash G}{\mathcal{H}, A \to B, A \vdash G}$ MP
$\dfrac{\mathcal{H} \vdash A \qquad \mathcal{H} \vdash B}{\mathcal{H} \vdash A \wedge B}$ And	$\dfrac{\mathcal{H}, A, B \vdash G}{\mathcal{H}, A \wedge B \vdash G}$ AndHyps
$\dfrac{\mathcal{H} \vdash A}{\mathcal{H} \vdash A \vee B}$ OrLeft	$\dfrac{\mathcal{H} \vdash B}{\mathcal{H} \vdash A \vee B}$ OrRight
$\dfrac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}$ OrHyps	
$\dfrac{\mathcal{H} \vdash (A \to B) \wedge (B \to A)}{\mathcal{H} \vdash A \leftrightarrow B}$ Iff	$\dfrac{\mathcal{H}, (A \to B) \wedge (B \to A) \vdash G}{\mathcal{H}, A \leftrightarrow B \vdash G}$ IffHyps

Cheat sheet

$\dfrac{\texttt{DONE}}{\mathcal{H} \vdash \texttt{true}}$ True	$\dfrac{\texttt{DONE}}{\mathcal{H}, \texttt{false} \vdash G}$ False
$\dfrac{\texttt{DONE}}{\mathcal{H}, G \vdash G}$ Assumption	
$\dfrac{\mathcal{H}, A \vdash B}{\mathcal{H} \vdash A \to B}$ ImpIntro	$\dfrac{\mathcal{H}, A \to B, A, B \vdash G}{\mathcal{H}, A \to B, A \vdash G}$ MP
$\dfrac{\mathcal{H} \vdash A \qquad \mathcal{H} \vdash B}{\mathcal{H} \vdash A \wedge B}$ And	$\dfrac{\mathcal{H}, A, B \vdash G}{\mathcal{H}, A \wedge B \vdash G}$ AndHyps
$\dfrac{\mathcal{H} \vdash A}{\mathcal{H} \vdash A \vee B}$ OrLeft	$\dfrac{\mathcal{H} \vdash B}{\mathcal{H} \vdash A \vee B}$ OrRight
$\dfrac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}$ OrHyps	
$\dfrac{\mathcal{H} \vdash (A \to B) \wedge (B \to A)}{\mathcal{H} \vdash A \leftrightarrow B}$ Iff	$\dfrac{\mathcal{H}, (A \to B) \wedge (B \to A) \vdash G}{\mathcal{H}, A \leftrightarrow B \vdash G}$ IffHyps

What might A and B be in the rules above?

Cheat sheet

$\dfrac{\texttt{DONE}}{\mathcal{H} \vdash \texttt{true}}$ True	$\dfrac{\texttt{DONE}}{\mathcal{H}, \texttt{false} \vdash G}$ False
$\dfrac{\texttt{DONE}}{\mathcal{H}, G \vdash G}$ Assumption	
$\dfrac{\mathcal{H}, A \vdash B}{\mathcal{H} \vdash A \to B}$ ImpIntro	$\dfrac{\mathcal{H}, A \to B, A, B \vdash G}{\mathcal{H}, A \to B, A \vdash G}$ MP
$\dfrac{\mathcal{H} \vdash A \qquad \mathcal{H} \vdash B}{\mathcal{H} \vdash A \wedge B}$ And	$\dfrac{\mathcal{H}, A, B \vdash G}{\mathcal{H}, A \wedge B \vdash G}$ AndHyps
$\dfrac{\mathcal{H} \vdash A}{\mathcal{H} \vdash A \vee B}$ OrLeft	$\dfrac{\mathcal{H} \vdash B}{\mathcal{H} \vdash A \vee B}$ OrRight
$\dfrac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}$ OrHyps	
$\dfrac{\mathcal{H} \vdash (A \to B) \wedge (B \to A)}{\mathcal{H} \vdash A \leftrightarrow B}$ Iff	$\dfrac{\mathcal{H}, (A \to B) \wedge (B \to A) \vdash G}{\mathcal{H}, A \leftrightarrow B \vdash G}$ IffHyps

What might A and B be in the rules above? **Any** Prop! (any formula)

Cheat sheet

$\dfrac{\texttt{DONE}}{\mathcal{H} \vdash \texttt{true}}$ True	$\dfrac{\texttt{DONE}}{\mathcal{H}, \texttt{false} \vdash G}$ False
$\dfrac{\texttt{DONE}}{\mathcal{H}, G \vdash G}$ Assumption	
$\dfrac{\mathcal{H}, A \vdash B}{\mathcal{H} \vdash A \to B}$ ImpIntro	$\dfrac{\mathcal{H}, A \to B, A, B \vdash G}{\mathcal{H}, A \to B, A \vdash G}$ MP
$\dfrac{\mathcal{H} \vdash A \qquad \mathcal{H} \vdash B}{\mathcal{H} \vdash A \wedge B}$ And	$\dfrac{\mathcal{H}, A, B \vdash G}{\mathcal{H}, A \wedge B \vdash G}$ AndHyps
$\dfrac{\mathcal{H} \vdash A}{\mathcal{H} \vdash A \vee B}$ OrLeft	$\dfrac{\mathcal{H} \vdash B}{\mathcal{H} \vdash A \vee B}$ OrRight
$\dfrac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}$ OrHyps	
$\dfrac{\mathcal{H} \vdash (A \to B) \wedge (B \to A)}{\mathcal{H} \vdash A \leftrightarrow B}$ Iff	$\dfrac{\mathcal{H}, (A \to B) \wedge (B \to A) \vdash G}{\mathcal{H}, A \leftrightarrow B \vdash G}$ IffHyps

What might A and B be in the rules above? **Any** Prop! (any formula)
What might $\mathcal{H}$ be in the rules above?

Cheat sheet

$\dfrac{\texttt{DONE}}{\mathcal{H} \vdash \texttt{true}}$ True	$\dfrac{\texttt{DONE}}{\mathcal{H}, \texttt{false} \vdash G}$ False
$\dfrac{\texttt{DONE}}{\mathcal{H}, G \vdash G}$ Assumption	
$\dfrac{\mathcal{H}, A \vdash B}{\mathcal{H} \vdash A \to B}$ ImpIntro	$\dfrac{\mathcal{H}, A \to B, A, B \vdash G}{\mathcal{H}, A \to B, A \vdash G}$ MP
$\dfrac{\mathcal{H} \vdash A \qquad \mathcal{H} \vdash B}{\mathcal{H} \vdash A \wedge B}$ And	$\dfrac{\mathcal{H}, A, B \vdash G}{\mathcal{H}, A \wedge B \vdash G}$ AndHyps
$\dfrac{\mathcal{H} \vdash A}{\mathcal{H} \vdash A \vee B}$ OrLeft	$\dfrac{\mathcal{H} \vdash B}{\mathcal{H} \vdash A \vee B}$ OrRight
$\dfrac{\mathcal{H}, A \vdash G \qquad \mathcal{H}, B \vdash G}{\mathcal{H}, A \vee B \vdash G}$ OrHyps	
$\dfrac{\mathcal{H} \vdash (A \to B) \wedge (B \to A)}{\mathcal{H} \vdash A \leftrightarrow B}$ Iff	$\dfrac{\mathcal{H}, (A \to B) \wedge (B \to A) \vdash G}{\mathcal{H}, A \leftrightarrow B \vdash G}$ IffHyps

What might A and B be in the rules above? **Any** Prop! (any formula)
What might $\mathcal{H}$ be in the rules above? Any set of formulas.

INTERESTING STUFF ABOUT PROOF RULES

Truth vs Provability

Important distinction:

- When we say that a formula ϕ is **true** we mean that it's **semantically valid**.
  - e.g., a propositional formula is true means that it is valid; i.e., if I build its truth table, the last column contains only 1s.
- This is not the same as saying that we are **able to prove** that ϕ is valid.
- (semantic) truth $\neq$ (syntactic) provability!

Truth vs Provability

Important distinction:

- When we say that a formula ϕ is **true** we mean that it's **semantically valid**.
  - e.g., a propositional formula is true means that it is valid; i.e., if I build its truth table, the last column contains only 1s.
- This is not the same as saying that we are **able to prove** that ϕ is valid.
- (semantic) truth $\neq$ (syntactic) provability!

Examples:

- Fermat's last theorem is true (we know that now). But can you prove it? Can anyone prove it with the proof rules I have given you so far?
- $p \vee \neg p$ is true. But can you prove it with the proof rules I have given you so far?

Truth vs Provability

Important distinction:

- When we say that a formula ϕ is **true** we mean that it's **semantically valid**.
  - e.g., a propositional formula is true means that it is valid; i.e., if I build its truth table, the last column contains only 1s.
- This is not the same as saying that we are **able to prove** that ϕ is valid.
- (semantic) truth $\neq$ (syntactic) provability!

Examples:

- Fermat's last theorem is true (we know that now). But can you prove it? Can anyone prove it with the proof rules I have given you so far?
- $p \vee \neg p$ is true. But can you prove it with the proof rules I have given you so far?
  No: we have no rules that deal with negation!

Soundness and Completeness

Proof system $=$ set of proof rules.

- A proof system R is **sound** if the following holds:
  For any formula ϕ, if we can prove ϕ using the rules in R, then ϕ is true (i.e., valid).

- A proof system R is **complete** if the following holds:
  For any formula ϕ, if ϕ is true (i.e., valid), then we can prove ϕ using the rules in R.

Soundness and Completeness

Proof system $=$ set of proof rules.

- A proof system R is **sound** if the following holds:
  For any formula ϕ, if we can prove ϕ using the rules in R, then ϕ is true (i.e., valid).
- A proof system R is **complete** if the following holds:
  For any formula ϕ, if ϕ is true (i.e., valid), then we can prove ϕ using the rules in R.
- We always want soundness!
- We would love to also have completeness, but it's not always possible!

Other interesting questions about formal proof systems

- Which rules do we really need? Which rules should we have in the first place?
- How long might a formal proof get? Could it be that with a different set of rules we could have a shorter proof?
- Do we really need to write these formal proofs by hand? They seem pretty straightforward to automate! Can't we write a program that searches all possible proof trees (iterates over all possible rules) for example, until it finds the right one?

Other interesting questions about formal proof systems

- Which rules do we really need? Which rules should we have in the first place?
- How long might a formal proof get? Could it be that with a different set of rules we could have a shorter proof?
- Do we really need to write these formal proofs by hand? They seem pretty straightforward to automate! Can't we write a program that searches all possible proof trees (iterates over all possible rules) for example, until it finds the right one?

All these are great questions. We won't have time to discuss them in any depth, but we will revisit some of them soon.