CS228 Logic for Computer Science 2022

Lecture 4: Formal proofs

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2022-02-27

Topic 4.1

Formal proofs

Consequence to derivation

Let us suppose for a (in)finite set of formulas Σ and a formula F, we have $\Sigma \models F$.

Can we syntactically infer $\Sigma \models F$ without writing the truth tables, which may be impossible if the size of Σ is infinite?

We call the syntactic inference "derivation". We derive the following statements.

$$\Sigma \vdash F$$

Example: derivation

Example 4.1

Let us consider the following simple example.

$$\underbrace{\Sigma \cup \{F\}}_{\text{Left hand side(lhs)}} \vdash F$$

If F occurs in lhs, then F is clearly a consequence of the lhs.

Therefore, we should be able to derive the above statement.

Proof rules

A proof rule provides us a means to derive new statements from the old statements.

premises

$$\textsc{RuleName}\;\frac{\text{Stuff-already-there}}{\text{Stuff-to-be-added}}\;\text{Conditions to be met}$$

conclusion

A derivation proceeds by applying the proof rules.

What rules do we need for the propositional logic?

Proof rules - Basic

$$\textsc{Assumption}\frac{}{\Sigma \vdash F} F \in \Sigma$$

$$\textsc{Monotonic}\frac{\Sigma \vdash F}{\Sigma' \vdash F} \Sigma \subseteq \Sigma'$$

Derivation

Definition 4.1

A derivation is a list of statements that are derived from the earlier statements.

Example 4.2

A derivation due to the previous rules

1. $\{p \lor q, \neg\neg q\} \vdash \neg\neg q$ — Assumption
2. $\{p \lor q, \neg\neg q, r\} \vdash \neg\neg q$ — Monotonic applied to 1

Since assumption does not depend on any other statement, no need to refer.

We need to point at an earlier statement.

Proof rules for Negation

$$\textsc{DoubleNeg}\frac{\Sigma \vdash F}{\Sigma \vdash \neg\neg F}$$

Example 4.3

The following is a derivation

1. $\{p \lor q, r\} \vdash r$ *Assumption*
2. $\{p \lor q, \neg\neg q, r\} \vdash r$ *Monotonic applied to 1*
3. $\{p \lor q, \neg\neg q, r\} \vdash \neg\neg r$ *DoubleNeg applied to 2*

Proof rules for $\wedge$

$$\wedge-\text{INTRO}\frac{\Sigma \vdash F \quad \Sigma \vdash G}{\Sigma \vdash F \wedge G} \quad \wedge-\textsc{Elim}\frac{\Sigma \vdash F \wedge G}{\Sigma \vdash F} \quad \wedge-\textsc{Symm}\frac{\Sigma \vdash F \wedge G}{\Sigma \vdash G \wedge F}$$

Example 4.4

The following is a derivation

1. $\{p \wedge q, \neg\neg q, r\} \vdash p \wedge q$ *Assumption*
2. $\{p \wedge q, \neg\neg q, r\} \vdash p$ *$\wedge$-Elim applied to 1*
3. $\{p \wedge q, \neg\neg q, r\} \vdash q \wedge p$ *$\wedge$-Symm applied to 1*

Proof rules for $\vee$

$$\vee-\text{INTRO}\frac{\Sigma \vdash F}{\Sigma \vdash F \vee G} \qquad \vee-\text{SYMM}\frac{\Sigma \vdash F \vee G}{\Sigma \vdash G \vee F}$$

$$\vee-\text{DEF}\frac{\Sigma \vdash F \vee G}{\Sigma \vdash \neg(\neg F \wedge \neg G)} \qquad \vee-\text{DEF}\frac{\Sigma \vdash \neg(\neg F \wedge \neg G)}{\Sigma \vdash F \vee G}$$

$$\vee-\text{ELIM}\frac{\Sigma \vdash F \vee G \qquad \Sigma \cup \{F\} \vdash H \qquad \Sigma \cup \{G\} \vdash H}{\Sigma \vdash H}$$

Commentary: We will use the same rule name if a rule can be applied in both the directions. For example, $\vee-\text{DEF}$.

Example : distributivity

Example 4.5

Let us show if we have $\Sigma \vdash (F \land G) \lor (F \land H)$*, we can derive* $\Sigma \vdash F \land (G \lor H)$*.*

1. $\Sigma \vdash (F \land G) \lor (F \land H)$ — Premise
2. $\Sigma \cup \{F \land G\} \vdash F \land G$ — Assumption
3. $\Sigma \cup \{F \land G\} \vdash F$ — $\land$-Elim applied to 2
4. $\Sigma \cup \{F \land G\} \vdash G \land F$ — $\land$-Symm applied to 2
5. $\Sigma \cup \{F \land G\} \vdash G$ — $\land$-Elim applied to 4
6. $\Sigma \cup \{F \land G\} \vdash G \lor H$ — $\lor$-Intro applied to 5
7. $\Sigma \cup \{F \land G\} \vdash F \land (G \lor H)$ — $\land$-Intro applied to 3 and 6

Example : distributivity (contd.)

8. $\Sigma \cup \{F \wedge H\} \vdash F \wedge H$ — Assumption
9. $\Sigma \cup \{F \wedge H\} \vdash F$ — $\wedge$-Elim applied to 8
10. $\Sigma \cup \{F \wedge H\} \vdash H \wedge F$ — $\wedge$-Symm applied to 8
11. $\Sigma \cup \{F \wedge H\} \vdash H$ — $\wedge$-Elim applied to 10
12. $\Sigma \cup \{F \wedge H\} \vdash H \vee G$ — $\vee$-Intro applied to 11
13. $\Sigma \cup \{F \wedge H\} \vdash G \vee H$ — $\vee$-Symm applied to 12
14. $\Sigma \cup \{F \wedge H\} \vdash F \wedge (G \vee H)$ — $\wedge$-Intro applied to 9 and 13

15. $\Sigma \vdash F \wedge (G \vee H)$ — $\vee$-elim applied to 1, 7, and 14

Topic 4.2

Rules for implication and others

Proof rules for $\Rightarrow$

$$\Rightarrow-\textsc{Intro}\frac{\Sigma \cup \{F\} \vdash G}{\Sigma \vdash F \Rightarrow G} \qquad \Rightarrow-\textsc{Elim}\frac{\Sigma \vdash F \Rightarrow G \quad \Sigma \vdash F}{\Sigma \vdash G}$$

$$\Rightarrow-\text{DEF}\frac{\Sigma \vdash F \Rightarrow G}{\Sigma \vdash \neg F \vee G} \qquad \Rightarrow-\text{DEF}\frac{\Sigma \vdash \neg F \vee G}{\Sigma \vdash F \Rightarrow G}$$

Example: central role of implication

Example 4.6

Let us prove $\{\neg p \lor q, p\} \vdash q$.

1. $\{\neg p \lor q, p\} \vdash p$ *Assumption*
2. $\{\neg p \lor q, p\} \vdash \neg p \lor q$ *Assumption*
3. $\{\neg p \lor q, p\} \vdash p \Rightarrow q$ $\Rightarrow$*-Def applied to 2*
4. $\{\neg p \lor q, p\} \vdash q$ $\Rightarrow$*-Elim applied to 1 and 3*

Commentary: Around binary operator formulas, we are not writing parentheses. They are there but not written for ease as we discussed in shorthands section.

All the rules so far

$$\textsc{Assumption}\frac{}{\Sigma \vdash F} F \in \Sigma \qquad \textsc{Monotonic}\frac{\Sigma \vdash F}{\Sigma' \vdash F} \Sigma \subseteq \Sigma' \qquad \textsc{DoubleNeg}\frac{\Sigma \vdash F}{\Sigma \vdash \neg\neg F}$$

$$\wedge - \textsc{intro}\frac{\Sigma \vdash F \quad \Sigma \vdash G}{\Sigma \vdash F \wedge G} \qquad \wedge - \textsc{Elim}\frac{\Sigma \vdash F \wedge G}{\Sigma \vdash F} \qquad \wedge - \textsc{Symm}\frac{\Sigma \vdash F \wedge G}{\Sigma \vdash G \wedge F}$$

$$\vee - \textsc{intro}\frac{\Sigma \vdash F}{\Sigma \vdash F \vee G} \qquad \vee - \textsc{Symm}\frac{\Sigma \vdash F \vee G}{\Sigma \vdash G \vee F} \qquad \vee - \textsc{def}\frac{\Sigma \vdash F \vee G}{\Sigma \vdash \neg(\neg F \wedge \neg G)}*$$

$$\vee - \textsc{Elim}\frac{\Sigma \vdash F \vee G \qquad \Sigma \cup \{F\} \vdash H \qquad \Sigma \cup \{G\} \vdash H}{\Sigma \vdash H}$$

$$\Rightarrow - \textsc{Intro}\frac{\Sigma \cup \{F\} \vdash G}{\Sigma \vdash F \Rightarrow G} \qquad \Rightarrow - \textsc{Elim}\frac{\Sigma \vdash F \Rightarrow G \quad \Sigma \vdash F}{\Sigma \vdash G} \qquad \Rightarrow - \textsc{def}\frac{\Sigma \vdash F \Rightarrow G}{\Sigma \vdash \neg F \vee G}*$$

* Works in the both directions

Example: another proof

Example 4.7

Let us prove $\emptyset \vdash (p \Rightarrow q) \lor p$.

1. $\{\neg p\} \vdash \neg p$	*Assumption*	Case 1
2. $\{\neg p\} \vdash \neg p \lor q$	$\lor$-*Intro applied to 1*	
3. $\{\neg p\} \vdash p \Rightarrow q$	$\Rightarrow$-*Def applied to 2*	
4. $\{\neg p\} \vdash (p \Rightarrow q) \lor p$	$\lor$-*Intro applied to 3*	
5. $\{p\} \vdash p$	*Assumption*	Case 2
6. $\{p\} \vdash p \lor (p \Rightarrow q)$	$\lor$-*Intro applied to 5*	
7. $\{p\} \vdash (p \Rightarrow q) \lor p$	$\lor$-*Symm applied to 6*	
8. $\{\} \vdash p \Rightarrow p$	$\Rightarrow$-*Intro applied to 5*	Only two cases
9. $\{\} \vdash \neg p \lor p$	$\Rightarrow$-*Def applied to 8*	
10. $\{\} \vdash (p \Rightarrow q) \lor p$	$\lor$-*Elim applied to 4, 7, and 9*	

Proof rules for $\Leftrightarrow$

$$\Leftrightarrow -\mathrm{DEF}\frac{\Sigma \vdash F \Leftrightarrow G}{\Sigma \vdash G \Rightarrow F} \qquad \Leftrightarrow -\mathrm{DEF}\frac{\Sigma \vdash F \Leftrightarrow G}{\Sigma \vdash F \Rightarrow G}$$

$$\Leftrightarrow -\mathrm{DEF}\frac{\Sigma \vdash G \Rightarrow F \qquad \Sigma \vdash F \Rightarrow G}{\Sigma \vdash G \Leftrightarrow F}$$

Exercise 4.1

Define similar rules for $\oplus$

Commentary: $\top$ and $\bot$ symbols are not covered in the proof system. They are also macros. $\top$ represents $\neg p \vee p$ and $\bot$ represents $p \wedge \neg p$ for some variable p. We can introduce Def rules to handle the symbols. However, in practice, they are not very useful.

Topic 4.3

Soundness

Commentary: In a later lecture, we will prove the reverse direction of the following theorem, which is called completeness.

Please also note that we are not writing the proof of the following theorem about the proof system using the proof system. Which may appear to be odd? However, there is no way of avoiding it. You need to know some English before start learning English grammar.

Soundness

We need to show that

Theorem 4.1

if

proof rules derive a statement $\Sigma \vdash F$

then

$$\Sigma \models F.$$

Proof.

We will make an inductive argument. We will assume that the theorem holds for the premises of the rules and show that it is also true for the conclusions. …

Proving soundness

Proof(contd.)

Consider the following rule

$$\wedge - \textsc{Elim}\frac{\Sigma \vdash F \wedge G}{\Sigma \vdash F}$$

Consider model $m \models \Sigma$. By the induction hypothesis, $m \models F \wedge G$.

Using the the truth table, we can show that if $m \models F \wedge G$ then $m \models F$.

$m(F)$	$m(G)$	$m(F \wedge G)$
0	0	0
0	1	0
1	0	0
1	1	1

Therefore, $\Sigma \models F$.

...

Proof

Proof.
Consider one more rule

$$\Rightarrow-\textsc{Intro}\frac{\Sigma \cup \{F\} \vdash G}{\Sigma \vdash F \Rightarrow G}$$

Consider model $m \models \Sigma$. There are two possibilities.

- **case** $m \models F$:
  Therefore, $m \models \Sigma \cup \{F\}$. By the induction hypothesis, $m \models G$. Therefore, $m \models (F \Rightarrow G)$.
- **case** $m \not\models F$: Therefore, $m \models (F \Rightarrow G)$.

Therefore, $\Sigma \vdash F \Rightarrow G$.

Similarly, we draw truth table or case analysis for each of the rules to check the soundness. □

Topic 4.4

Problems

Exercise: the other direction of distributivity

Exercise 4.2

Show if we have $\Sigma \vdash F \wedge (G \vee H)$*, we can derive* $\Sigma \vdash (F \wedge G) \vee (F \wedge H)$*.*

Hint: Case split on G and $\neg G$.

Exercise: proving a puzzle

Exercise 4.3

a. Convert the following argument into a propositional statement, i.e., $\Sigma \vdash F$.

If the laws are good and their enforcement is strict, then crime will diminish. If strict enforcement of laws will make crime diminish, then our problem is a practical one. The laws are good. Therefore our problem is a practical one. (Hint: needed propositional variables G, S, D, P)
(Source : Copi, Introduction of logic)

b. Write a formal proof proving the statement in the previous problem.

Redundant rules

Exercise 4.4

Show that the following rule(s) can be derived from the other rules.

1. $\vee$-*Symm*
2. $\Rightarrow$-*Elim*

Commentary: **Solution:** Part 1:

Let us prove Contrapositive from the next lecture without using $\vee$-Symm

1. $\Sigma \cup \{F\} \vdash G$ — Premise
2. $\Sigma \vdash F \Rightarrow G$ — $\Rightarrow$-Intro applied to 1
3. $\Sigma \vdash \neg F \vee G$ — $\Rightarrow$-Def applied to 2
4. $\Sigma \cup \{\neg G\} \vdash \neg F \vee G$ — Monotonic applied to 3
5. $\Sigma \cup \{\neg G, \neg F\} \vdash \neg F$ — Assumption
6. $\Sigma \cup \{\neg G, G\} \vdash G$ — Assumption
7. $\Sigma \cup \{\neg G, G\} \vdash \neg G$ — Assumption
8. $\Sigma \cup \{\neg G, G\} \vdash \neg G \vee \neg F$ — $\vee$-Intro applied to 7
9. $\Sigma \cup \{\neg G, G\} \vdash G \Rightarrow \neg F$ — $\Rightarrow$-Def applied to 8
10. $\Sigma \cup \{\neg G, G\} \vdash \neg F$ — $\Rightarrow$-Elim applied to 6,9
11. $\Sigma \cup \{\neg G\} \vdash \neg F$ — $\vee$-Elim applied to 3, 5, and 10

Proving $\vee$-Symm using Contrapositive

1. $\Sigma \cup \{(\neg F \wedge \neg G)\} \vdash (\neg F \wedge \neg G)$ — Assumption
2. $\Sigma \cup \{(\neg F \wedge \neg G)\} \vdash (\neg G \wedge \neg F)$ — $\wedge$-Symm applied to 1
3. $\Sigma \cup \{\neg(\neg G \wedge \neg F)\} \vdash \neg(\neg F \wedge \neg G)$ — Contrapositive applied to 2
4. $\Sigma \vdash \neg(\neg G \wedge \neg F) \Rightarrow \neg(\neg F \wedge \neg G)$ — $\Rightarrow$-Intro applied to 3
5. $\Sigma \vdash (G \vee F)$ — Premise
6. $\Sigma \vdash \neg(\neg G \wedge \neg F)$ — $\vee$-Def applied to 5
7. $\Sigma \vdash \neg(\neg F \wedge \neg G)$ — $\Rightarrow$-Elim applied to 4 and 6
8. $\Sigma \vdash (F \vee G)$ — $\vee$-Def applied to 7

Redundancy***

Exercise 4.5

Find a minimal subset of the proof rules which has no redundancy, i.e., none of the rules can be derived from others. Prove that the subset has no redundancy.

Commentary: This is a very difficult problem. I have picked our proof system from the book A First Course in Logic by Shawn Hedman. I am not sure that the book proves that the proof system has no redundancy. I can point at another book that has proof of redundancy for another proof system for propositional logic. In section 7.4 of Symbolic Logic by Copi, you will find proof. You may need to work to adopt his proof to our proof system. The technique is to find a "characteristic property for the consequent of each rule", which other proof rules cannot produce. It is difficult to find the properties.

Irredundant rules (midterm 2022)

Exercise 4.6

Let us give three valued interpretation to the variables of propositional logic. The three values are 0, 1, *and* 2. *We give meaning to* $\neg$, $\wedge$, *and* $\Rightarrow$ *as follows. Let* m *be a model in the three valued logic.*

$$m(\neg F) = 2 - m(F) \qquad m(F \wedge G) = min(m(F) + m(G), 2) \qquad m(F \Rightarrow G) = m(\neg(F \wedge \neg G))$$

Show that any formula of form $F \wedge G \Rightarrow F$ *will have value zero.*

Exercise 4.7

Consider the following proof system with four rules.

$$Axiom1\,\frac{}{F \Rightarrow F \wedge F} \quad Axiom2\,\frac{}{F \wedge G \Rightarrow F} \quad Axiom3\,\frac{}{(F \Rightarrow G) \Rightarrow (\neg(G \wedge H) \Rightarrow \neg(H \wedge F))} \quad Elim\,\frac{F \Rightarrow G \quad F}{G}$$

Show that rules *Axiom*2, *Axiom*3, and *Elim* cannot derive any instance of *Axiom*1.

Commentary: Solution: Hint: Show that $m((F \Rightarrow G) \Rightarrow (\neg(G \wedge H) \Rightarrow \neg(H \wedge F)))$ is always zero (a lot of calculation; there are clever shortcuts; but bruteforce is doable). Show if $m(F \Rightarrow G)$ is zero and $m(F)$ is zero, then $m(G)$ must be zero. Therefore, *Axiom*2, *Axiom*3, and *Elim* can only produce formulas that are always zero. $m(F \Rightarrow F \wedge F)$ is not zero if $m(F) = 1$. Can we also prove that the other two axioms also not redundant?

End of Lecture 4