CS228 Logic for Computer Science 2021

Lecture 5: Formal proofs - derived rules

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2021-01-15

Derived rules

In logical thinking, we have many deductions that are not listed in our rules.

The deductions are consequence of our rules. We call them derived rules.

Let us look at a few.

Commentary: A derived rule may be viewed as a macro or function in programs, which can do some routine task for us in one step that needs several steps.

Topic 5.1

Derived rules: modus ponens, tautology, contradiction, contrapositive

Derived rules : modus ponens

Theorem 5.1

If we he have $\Sigma \vdash \neg F \vee G$ and $\Sigma \vdash F$, we can derive $\Sigma \vdash G$.

Proof.

1. $\Sigma \vdash \neg F \vee G$ — Premise
2. $\Sigma \vdash F$ — Premise
3. $\Sigma \vdash F \Rightarrow G$ — $\Rightarrow$-Def applied to 1
4. $\Sigma \vdash G$ — $\Rightarrow$-Elim applied to 2 and 3

$\square$

We can use the above derivation as a sub-procedure and introduce the following proof rule.

$$\vee\text{-}\textsc{ModusPonens}\frac{\Sigma \vdash \neg F \vee G \qquad \Sigma \vdash F}{\Sigma \vdash G}$$

Example: implication

Example 5.1

Let us prove $\{(\neg p \lor r), (p \lor \neg q)\} \vdash (q \Rightarrow p \land r)$.

1. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash q$ — *Assumption*
2. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash (p \lor \neg q)$ — *Assumption*
3. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash (\neg q \lor p)$ — $\lor$*-Symm applied to 2*
4. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash p$ — $\lor$*-ModusPonens applied to 1 and 3*
5. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash (\neg p \lor r)$ — *Assumption*
6. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash r$ — $\lor$*-ModusPonens applied to 4 and 5*
7. $\{(\neg p \lor r), (p \lor \neg q)\} \cup \{q\} \vdash p \land r$ — $\land$*-Intro applied to 4 and 6*
8. $\{(\neg p \lor r), (p \lor \neg q)\} \vdash (q \Rightarrow p \land r)$ — $\Rightarrow$*-Intro applied to 7*

Tautology

I run when it rains or when it does not.

A convoluted way of saying something is always true.

Derived rules: tautology rule

Theorem 5.2

For any F and a set Σ of formulas, we can always derive $\Sigma \vdash \neg F \lor F$.

Proof.

1. $\Sigma \cup \{F\} \vdash F$ — Assumption
2. $\Sigma \vdash F \Rightarrow F$ — $\Rightarrow$-Intro applied to 1
3. $\Sigma \vdash \neg F \lor F$ — $\Rightarrow$-Def applied to 2

□

Again, we can introduce the following proof rule.

$$\textsc{Tautology}\ \frac{}{\Sigma \vdash \neg F \lor F}$$

Contradiction

If I eat a cake and not eat it, then sun is cold.

Once we introduce an absurdity (formally contradiction), there are no limits in absurdity.

Commentary: To explain the importance of logic. Once Bertrand Russell made the following argument,
1. 2+2 = 5 2. 4=5 3. 4-3 = 5-3 4. 1=2 5. I and Pope are two. 6. I and Pope are one. 6. I am Pope.

Derived rules: contradiction rule

Theorem 5.3

If we have $\Sigma \vdash F \wedge \neg F$, *we can always derive* $\Sigma \vdash G$.

Proof.

1. $\Sigma \vdash F \wedge \neg F$ Premise
2. $\Sigma \vdash \neg F \wedge F$ $\wedge$-Symm applied to 1
3. $\Sigma \vdash \neg F$ $\wedge$-Elim applied to 2
4. $\Sigma \vdash \neg F \vee G$ $\vee$-Intro applied to 3
5. $\Sigma \vdash F$ $\wedge$-Elim applied to 1
6. $\Sigma \vdash G$ $\wedge$-Modus Ponens applied to 4 and 5

$\square$

Therefore, we may declare the following derived proof rule

$$\textsc{Contra}\frac{\Sigma \vdash \neg F \wedge F}{\Sigma \vdash G}$$

Contrapositive

I think, therefore I am. -Descartes

$$\Leftrightarrow$$

I am not, therefore I do not think.

In an argument, negation of the conclusion implies negation of premise.

Derived rules: contrapositive rule

Theorem 5.4

If we have $\Sigma \cup \{F\} \vdash G$, we can always derive $\Sigma \cup \{\neg G\} \vdash \neg F$.

Proof.

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

$\square$

Therefore, we may declare the following derived proof rule

$$\textsc{Contrapositive}\frac{\Sigma \cup \{F\} \vdash G}{\Sigma \cup \{\neg G\} \vdash \neg F}$$

Topic 5.2

More derived rule: proof by cases and contradiction, reverse double negation, and resolution

Proof by cases and contradiction

We must have seen the following proof structure

- Proof by cases

  If I have money, I run.
  If I do not have money, I run.
  Therefore, I run.

- Proof by contradiction

  Assume, I ate a dinosaur.
  My tummy is far smaller than a dianour. Contradiction.
  Therefore, I did not eat dinosaur.

Derived rules: proof by cases

Theorem 5.5

If we have $\Sigma \cup \{F\} \vdash G$ and $\Sigma \cup \{\neg F\} \vdash G$, we can always derive $\Sigma \vdash G$.

Proof.

1. $\Sigma \cup \{F\} \vdash G$ — Premise
2. $\Sigma \cup \{\neg F\} \vdash G$ — Premise
3. $\Sigma \vdash F \vee \neg F$ — Tautology
4. $\Sigma \vdash G$ — $\vee$-Elim applied to 1,2, and 3

$\square$

Therefore, we may declare the following derived proof rule

$$\textsc{ByCases}\frac{\Sigma \cup \{F\} \vdash G \qquad \Sigma \cup \{\neg F\} \vdash G}{\Sigma \vdash G}$$

Derived rules: proof by contradiction

Theorem 5.6

If we have $\Sigma \cup \{F\} \vdash G$ and $\Sigma \cup \{F\} \vdash \neg G$, we can always derive $\Sigma \vdash \neg F$.

Proof.

1. $\Sigma \cup \{F\} \vdash G$ — Premise
2. $\Sigma \cup \{F\} \vdash \neg G$ — Premise
3. $\Sigma \cup \{\neg G\} \vdash \neg F$ — Contrapositive applied to 1
4. $\Sigma \cup \{\neg\neg G\} \vdash \neg F$ — Contrapositive applied to 2
5. $\Sigma \vdash \neg F$ — ByCases 3 and 4

$\square$

Therefore, we may declare the following derived proof rule

$$\textsc{ByContra}\frac{\Sigma \cup \{F\} \vdash G \qquad \Sigma \cup \{F\} \vdash \neg G}{\Sigma \vdash \neg F}$$

Reverse double negation

I do not dislike apples.

Therefore, I like apples.

Derived rule: reverse Double Negation

Theorem 5.7

If we have $\Sigma \vdash \neg\neg F$, we can always derive $\Sigma \vdash F$.

Proof.

1. $\Sigma \vdash \neg\neg F$ — Premise
2. $\Sigma \cup \{\neg F\} \vdash \neg\neg F$ — Monotonic applied to 1
3. $\Sigma \cup \{\neg F\} \vdash \neg F$ — Assumption
4. $\Sigma \cup \{\neg F\} \vdash \neg F \land \neg\neg F$ — $\land$-Intro applied to 2 and 3
5. $\Sigma \cup \{\neg F\} \vdash F$ — Contradiction applied to 4
6. $\Sigma \cup \{F\} \vdash F$ — Assumption
7. $\Sigma \vdash F$ — Proof by cases applied to 5 and 6 $\square$

Therefore, we may declare the following derived proof rule

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

Resolution

I ate or ran. I did not eat or sleep.

Therefore, I ran or sleep.

Derived rules : resolution

Theorem 5.8

If we he have $\Sigma \vdash \neg F \vee G$ and $\Sigma \vdash F \vee H$, we can derive $\Sigma \vdash G \vee H$.

Proof.

1. $\Sigma \vdash \neg F \vee G$ — Premise
2. $\Sigma \cup \{F\} \vdash \neg F \vee G$ — Monotonic applied to 1
3. $\Sigma \cup \{F\} \vdash F$ — Assumption
4. $\Sigma \cup \{F\} \vdash G$ — Modes Ponens applied to 2 and 3
5. $\Sigma \cup \{F\} \vdash G \vee H$ — $\vee$-Intro applied to 4

Case 1

...

Commentary: Resolution is generalization of Modus ponens. We also refer Modus ponens as unit resolution.

Derived rules : resolution (contd.)

Proof(contd.)

7. $\Sigma \vdash F \lor H$ — Premise
8. $\Sigma \cup \{F\} \vdash \neg\neg F$ — DoubleNeg applied to 3
9. $\Sigma \cup \{F\} \vdash \neg\neg F \lor H$ — $\lor$-Intro applied to 7
10. $\Sigma \cup \{H\} \vdash H$ — Assumption
11. $\Sigma \cup \{H\} \vdash H \lor \neg\neg F$ — $\lor$-Intro applied to 9
12. $\Sigma \cup \{H\} \vdash \neg\neg F \lor H$ — $\lor$-Symm applied to 10
13. $\Sigma \vdash \neg\neg F \lor H$ — $\lor$-Elim applied to 6, 8, and 11

Substitution from F to $\neg\neg F$

...

Derived rules : resolution (contd.)

Proof(contd.)

13. $\Sigma \cup \{\neg F\} \vdash \neg\neg F \vee H$ — Monotonic applied to 12
14. $\Sigma \cup \{\neg F\} \vdash \neg F$ — Assumption
15. $\Sigma \cup \{\neg F\} \vdash H$ — Modes Ponens applied to 13 and 14
16. $\Sigma \cup \{\neg F\} \vdash H \vee G$ — $\vee$-Intro applied to 15
17. $\Sigma \cup \{\neg F\} \vdash G \vee H$ — $\vee$-Symm applied to 16

Case 2 (steps 13–17)

18. $\Sigma \vdash G \vee H$ — Proof by cases applied to 5 and 17

$\square$

Therefore, we may declare the following derived proof rule

$$\textsc{Resoluton}\frac{\Sigma \vdash F \vee G \qquad \Sigma \vdash \neg F \vee H}{\Sigma \vdash G \vee H}$$

Topic 5.3

Substitution and formal proofs

Derivations for substitutions

Theorem 5.9

Let $F_1(p)$ and $F_2(p)$ be formulas. If we he have $\Sigma \vdash F_1(G) \Leftrightarrow F_1(H)$, $\Sigma \vdash F_2(G) \Leftrightarrow F_2(H)$, and $\Sigma \vdash F_1(G) \land F_2(G)$, we can derive $\Sigma \vdash F_1(H) \land F_2(H)$.

Proof.

1. $\Sigma \vdash F_1(G) \Leftrightarrow F_1(H)$ Premise
2. $\Sigma \vdash F_2(G) \Leftrightarrow F_2(H)$ Premise
3. $\Sigma \vdash F_1(G) \land F_2(G)$ ✓ Premise
4. $\Sigma \vdash F_1(G)$ $\land$-Elim applied to 3
5. $\Sigma \vdash F_1(G) \Rightarrow F_1(H)$ $\Leftrightarrow$-Def applied to 1
6. $\Sigma \vdash F_1(H)$ $\Rightarrow$-Elim applied to 4 and 5
7. $\Sigma \vdash F_2(G) \land F_1(G)$ $\land$-Symm applied to 3
8. $\Sigma \vdash F_2(G)$ $\land$-Elim applied to 7
9. $\Sigma \vdash F_2(G) \Rightarrow F_2(H)$ $\Leftrightarrow$-Def applied to 2
10. $\Sigma \vdash F_2(H)$ $\Rightarrow$-Elim applied to 8 and 9
11. $\Sigma \vdash F_1(H) \land F_2(H)$ $\land$-Intro applied to 6 and 10

$\square$

Exercise 5.1

Write similar proofs for $\lor$, $\neg$, $\Rightarrow$, $\oplus$, and $\Leftrightarrow$.

Substitution rule

Theorem 5.10

Let $F(p)$ be a formula. If we he have $\Sigma \vdash G \Leftrightarrow H$ and $\Sigma \vdash F(G)$, we can derive $\Sigma \vdash F(H)$.

Proof.

Using theorems like theorem 5.9 for each connective, we can build an induction argument for the above. □

We shall not introduce substitution as a rule.

Exercise 5.2

Write the inductive proof for the above theorem.

Commentary: The above theorem is not like other theorems in this lecture. Replacing $F(G)$ by $F(H)$ causes long range changes in the formula. Considering such transformation as a unit step in a proof is not ideal. Ideally, we should be able to check a proof step in constant time. We need linear time in terms of formula size to check a proof step due to substitution. Some theorem provers allow substitution as a single step. In this course, we will not.

Example: disallowed substitution operation

Example 5.2

The following proof step is not allowed in our proof system.

1. $\Sigma \vdash \neg(\neg\neg F \vee G)$ ....
2. $\Sigma \vdash \neg(F \vee G)$ *RevDoubleNeg applied to $\neg\neg F$ in 1*

We can apply transformations only on the top formulas.

Exercise 5.3

Write an acceptable version of the above derivation.

Commentary: In the proof resolution rule, we needed a similar shortcut when we needed to derive statement $\Sigma \vdash \neg\neg F \vee H$ from $\Sigma \vdash F \vee H$. We spent 5-6 step to derive the statement.

Topic 5.4

Motivate next lecture

Mathematics vs. computer science

So far we see rules of reasoning.

We have seen that the rules are correct and will see in a few lectures that they are also sufficient, i.e., all true statements are derivable.

Our inner mathematician is happy!!

However, our inner computer scientist is unhappy

- Too many rules - dozens of rules
- no instructions (or algorithm) for applying them on a given problem

We will embark upon simplifying and automating the reasoning process.

Topic 5.5

Problems

Formal proofs

Exercise 5.4

Derive the following statements

1. $\{(p \Rightarrow q), (p \lor q)\} \vdash q$
2. $\{(p \Rightarrow q), (q \Rightarrow r)\} \vdash \neg(\neg r \land p)$
3. $\{(q \lor (r \land s)), (q \Rightarrow t), (t \Rightarrow s)\} \vdash s$
4. $\{(p \lor q), (r \lor s)\} \vdash ((p \land r) \lor q \lor s)$
5. $\{(((p \Rightarrow q) \Rightarrow q) \Rightarrow q)\} \vdash (p \Rightarrow q)$
6. $\emptyset \vdash (p \Rightarrow (q \lor r)) \lor (r \Rightarrow \neg p)$
7. $\{p\} \vdash (q \Rightarrow p)$
8. $\{(p \Rightarrow (q \Rightarrow r))\} \vdash ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
9. $\{(\neg p \Rightarrow \neg q)\} \vdash (q \Rightarrow p)$
10. $\{r \lor (s \land \neg t), (r \lor s) \Rightarrow (u \lor \neg t)\} \vdash t \Rightarrow u$

End of Lecture 5