CS228 Logic for Computer Science 2020

Lecture 17: FOL - formal proofs

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2020-02-23

Topic 17.1

Formal proofs

Consequence to derivation

We also need the formal proof system for FOL.

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

Similar to propositional logic, we will now again develop a system of "derivations". We derive the following statements.

$$\Sigma \vdash F$$

Rules for propositional logic stays!

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

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

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

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

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

* Works in both directions

We are not showing the rules for $\Leftrightarrow$, $\oplus$, and punctuation.

Additionally we have seen intro for the Quantifiers

If some fact is true about some term, we can introduce the $\exists$

$$\exists-\textsc{Intro}\frac{\Sigma \vdash F(t)}{\Sigma \vdash \exists y.\ F(y)}\, y \notin \mathbf{Vars}(F(z))$$

$$\forall-\textsc{Intro}\frac{\Sigma \vdash F(x)}{\Sigma \vdash \forall y.\ F(y)}\, y \notin \mathbf{Vars}(F(z)),\ x \in \mathbf{Vars},\ \text{and } x \notin \mathbf{Vars}(\Sigma)$$

$$\forall-\textsc{Intro}\frac{\Sigma \vdash F(c)}{\Sigma \vdash \forall y.\ F(y)}\, y \notin \mathbf{Vars}(F),\ c \text{ is not referred in } \Sigma,\ \text{and } c/0 \in \mathbf{F}$$

z is some fresh variable

Example: Bad $\forall$-Intro

Example 17.1

Consider the following derivation where we used a term to $\forall$-INTRO.

1. $\Sigma \vdash H(f(c)) \land \neg H(f(a))$ *Assumption*
2. $\Sigma \vdash \forall z.\ (H(z) \land \neg H(f(a)))$ $\forall$-INTRO *applied to 1*✗

Formula in 1 is a satisfiable formula and in 2 the formula is unsatisfiable.

Relating quantifiers

If a fact is always true, then there is no evidence of its negation.

$$\forall-\textsc{Def}\frac{\Sigma \vdash \forall x.F(x)}{\Sigma \vdash \neg\exists x.\ \neg F(x)}$$

We also have the rule in the reverse direction.

$$\forall-\textsc{Def}\frac{\Sigma \vdash \neg\exists x.\ \neg F(x)}{\Sigma \vdash \forall x.F(x)}$$

Universal instantiation

Theorem 17.1

If we have $\Sigma \vdash \forall x.F(x)$, we can derive $\Sigma \vdash F(t)$ for any term t.

Proof.

1. $\Sigma \vdash \forall x.F(x)$ — Premise
2. $\Sigma \cup \{\neg F(t)\} \vdash \forall x.F(x)$ — Monotonic applied to 1
3. $\Sigma \cup \{\neg F(t)\} \vdash \neg \exists x.\neg F(x)$ — $\forall$-Def applied to 1
4. $\Sigma \cup \{\neg F(t)\} \vdash \neg F(t)$ — Assumption
5. $\Sigma \cup \{\neg F(t)\} \vdash \exists x.\neg F(x)$ — $\exists$-Intro applied to 4
6. $\Sigma \vdash \neg\neg F(t)$ — ByContra applied to 3 and 5
7. $\Sigma \vdash F(t)$ — RevDoubleNeg applied to 6

□

Therefore, we declare the following a derived proof rule.

$$\forall - \textsc{Instantiate}\frac{\Sigma \vdash \forall x.F(x)}{\Sigma \vdash F(t)}$$

Exercise: $\forall$ distributes over $\wedge$

Exercise 17.1

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

Exercise 17.2

Give an example to show that $\forall$ *does not distribute over* $\vee$*.*

$\forall$ implies $\exists$

Theorem 17.2

If we have $\Sigma \vdash \forall x.F(x)$, we can derive $\Sigma \vdash \exists x.F(x)$.

Proof.

1. $\Sigma \vdash \forall x.F(x)$ — Premise
2. $\Sigma \vdash F(x)$ — $\forall$-Instantiate applied to 1
3. $\Sigma \vdash \exists x.F(x)$ — $\exists$-Intro applied to 2

□

Exercise 17.3

Show that the proof in the reverse direction will not work.

Hint: you may need to show that proof for equivalent $\exists$-Instantiate does not work.

Provably equivalent

Definition 17.1

If statements $\{F\} \vdash G$ and $\{G\} \vdash F$ hold, then we F and G are F and G are provably equivalent.

Example 17.2

We will show that $\forall x.F(x)$ and $\forall y.F(y)$ are provably equivalent.

What is in a name?

Theorem 17.3

If $x, y \notin F(z)$, then $\forall x.F(x)$ and $\forall y.F(y)$ are provably equivalent .

Proof.

- $\{\forall x.F(x)\} \vdash \forall x.F(x)$ — Assumption
- $\{\forall x.F(x)\} \vdash F(y)$ — $\forall$-Instantiation applied to 1
- $\{\forall x.F(x)\} \vdash \forall y.F(y)$ — $\forall$-Intro applied to 2, since $y \notin \textbf{Vars}(\forall x.F(x))$

□

Exercise 17.4

Prove: if $x, y \notin F(z)$, then $\exists x.F(x)$ and $\exists y.F(y)$ are provably equivalent .

Rest of the rules for FOL

We can introduce quantifiers over implications.

$$\exists-\textsc{Distr}\frac{\Sigma \vdash F \Rightarrow G}{\Sigma \vdash \exists x.F \Rightarrow \exists x.G} \qquad \forall-\textsc{Distr}\frac{\Sigma \vdash F \Rightarrow G}{\Sigma \vdash \forall x.F \Rightarrow \forall x.G}$$

For equality

$$\textsc{Reflex}\frac{}{\Sigma \vdash t = t} \qquad \textsc{EqSub}\frac{\Sigma \vdash F(t) \quad \Sigma \vdash t = t'}{\Sigma \vdash F(t')}$$

$\exists$ defined in terms of $\forall$

Theorem 17.4

If we have $\Sigma \vdash \neg\exists x.F(x)$*, we can derive* $\Sigma \vdash \forall x.\neg F(x)$

Proof.

1. $\Sigma \cup \{\neg\neg F(x)\} \vdash \neg\neg F(x)$ — Assumption
2. $\Sigma \cup \{\neg\neg F(x)\} \vdash F(x)$ — RevDoubleNeg applied to 1
3. $\Sigma \vdash \neg\neg F(x) \Rightarrow F(x)$ — $\Rightarrow$-Intro applied to 2
4. $\Sigma \vdash \exists x.\neg\neg F(x) \Rightarrow \exists x.F(x)$ — $\exists$-Distr applied to 3
5. $\Sigma \vdash \neg\exists x.F(x) \Rightarrow \neg\exists x.\neg\neg F(x)$ — Contrapositive to 4
6. $\Sigma \vdash \neg\exists x.F(x)$ — Premise
7. $\Sigma \vdash \neg\exists x.\neg\neg F(x)$ — $\Rightarrow$-Elim applied to 5 and 6
8. $\Sigma \vdash \forall x.\neg F(x)$ — $\forall$-Def applied to 7 $\square$

Therefore, we declare the following a derived proof rule.

$$\exists - \text{NEG}\frac{\Sigma \vdash \neg\exists x.F(x)}{\Sigma \vdash \forall x.\neg F(x)}$$

$\exists$ defined in terms of $\forall$ (Reverse)

Theorem 17.5

If we have $\Sigma \vdash \forall x.\neg F(x)$, we can derive $\Sigma \vdash \neg\exists x.F(x)$.

Proof.

1. $\Sigma \cup \{F(x)\} \vdash F(x)$ — Assumption
2. $\Sigma \cup \{F(x)\} \vdash \neg\neg F(x)$ — DoubleNeg applied to 1
3. $\Sigma \vdash F(x) \Rightarrow \neg\neg F(x)$ — $\Rightarrow$-Intro applied to 2
4. $\Sigma \vdash \exists x.F(x) \Rightarrow \exists x.\neg\neg F(x)$ — $\forall$-Distr applied to 3
5. $\Sigma \vdash \neg\exists x.\neg\neg F(x) \Rightarrow \neg\exists x.F(x)$ — Contrapositive to 4
6. $\Sigma \vdash \forall x.\neg F(x)$ — Premise
7. $\Sigma \vdash \neg\exists x.\neg\neg F(x)$ — $\forall$-Def applied to 6
8. $\Sigma \vdash \neg\exists x.F(x)$ — $\Rightarrow$-Elim applied to 5 and 6 $\square$

Therefore, we declare the following a derived proof rule.

$$\exists - \text{NEG}\frac{\Sigma \vdash \forall x.\neg F(x)}{\Sigma \vdash \neg\exists x.F(x)}$$

$\exists$ distributes over $\vee$

Theorem 17.6

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

Proof.

1. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \neg\exists x.F(x) \wedge \neg\exists x.G(x)$ — Assumption
2. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \neg\exists x.F(x)$ — $\wedge$-Elim applied to 1
3. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \forall x.\neg F(x)$ — $\exists$-Neg applied to 2
4. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \neg F(y)$ — $\forall$-Instantiate applied to 3
5. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \neg\exists x.G(x)$ — $\wedge$-Symm and $\wedge$-Elim applied to 1
6. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \forall x.\neg G(x)$ — $\exists$-Neg applied to 5
7. $\{\neg\exists x.F(x) \wedge \neg\exists x.G(x)\} \vdash \neg G(y)$ — $\forall$-Instantiate applied to 6

...

$\exists$ distributes over $\lor$ (contd.)

Proof(contd.)

8. $\{\neg\exists x.F(x) \land \neg\exists x.G(x)\} \vdash \neg F(y) \land \neg G(y)$ $\land$-Intro applied to 4 and 7
9. $\{\neg\exists x.F(x) \land \neg\exists x.G(x)\} \vdash \neg(F(y) \lor G(y))$ Boolean reasoning applied on 8
10. $\{\neg\exists x.F(x) \land \neg\exists x.G(x)\} \vdash \forall y.\neg(F(y) \lor G(y))$ $\forall$-Intro applied to 9
11. $\{\neg\exists x.F(x) \land \neg\exists x.G(x)\} \vdash \neg\exists y.(F(y) \lor G(y))$ $\exists$-Neg applied to 10

... rest of the reasoning is Boolean.

□

Exercise 17.5

Give an example to show that $\exists$ does not distribute over $\land$.

Attendance quiz

Which of the following holds on FOL?

We can instantiate $\forall$ freely.
Intro $\forall$ needs no mention of the variable in Σ.
$\forall$ distributes over $\wedge$.
$\exists$ distributes over $\vee$.
FOL can express infiniteness of the domain of structure.

We can instantiate $\exists$ freely.
Intro $\exists$ needs no mention of the variable in Σ.
$\exists$ distributes over $\wedge$.
$\forall$ distributes over $\vee$.
FOL can express finiteness of the domain of structure.

Example: working with quantifiers

Exercise 17.6

Prove $\emptyset \vdash (\forall x.\ (P(x) \vee Q(x)) \Rightarrow \exists x.P(x) \vee \forall x.Q(x))$

Here is the derivation.

1. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash \forall x.\ (P(x) \vee Q(x))$ *Assumption*
2. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash P(y) \vee Q(y)$ *$\forall$-Instantiate*
3. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash \neg\exists x.P(x)$ *Assumption*
4. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash \forall x.\neg P(x)$ *NegExists applied to 3*
5. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash \neg P(y)$ *$\forall$-Instantiate applied to 4*
6. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash Q(y)$ *$\vee$-ModusPonnes applied to 2 and 5*
7. $\{\forall x.\ (P(x) \vee Q(x)), \neg\exists x.P(x)\} \vdash \forall x.Q(x)$ *$\forall$-Intro applied to 6*

..... rest is propositional reasoning

Exercise 17.7

Commentary: Usually not many steps are needed for the quantifiers.

No occurance; no issues

Theorem 17.7

Let x be a variable that does not occur as a free variable in the formula F. Then F, $\exists x.F$, and $\forall x.F$ are provably equivalent.

Proof.

We have already seen $\forall x.F$ to $\exists x.F$.

Proving from F to $\forall x.F$

1. $\Sigma \vdash F$ — Premise
2. $\Sigma \vdash (F \vee \neg(x = x)))$ — $\vee$-Intro applied to 1
3. $\Sigma \vdash (\neg(x = x) \vee F)$ — $\vee$-Symm applied to 2
4. $\Sigma \vdash x = x \Rightarrow F$ — $\Rightarrow$-Def applied to 3
5. $\Sigma \vdash \forall x.x = x \Rightarrow \forall x.F$ — $\forall$-Distr applied to 4
6. $\Sigma \vdash c = c$ — Reflex
7. $\Sigma \vdash \forall x.x = x$ — $\forall$-Intro applied to 6
8. $\Sigma \vdash \forall x.F$ — $\Rightarrow$-Elim applied to 5 and 7

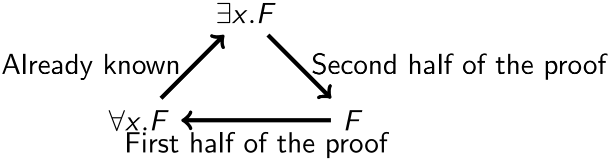
No occurance; no issues

Proof(contd.)

Proving from $\exists x.F$ to F

1. $\Sigma \vdash \exists x.F$ — Premise
2. $\Sigma \cup \{\neg F\} \vdash \exists x.F$ — Monotonic applied to 1
3. $\Sigma \cup \{\neg F\} \vdash \neg F$ — Assumption
4. $\Sigma \cup \{\neg F\} \vdash \forall x.\neg F$ — Previous proof applied to 3
5. $\Sigma \cup \{\neg F\} \vdash \neg\exists x.F$ — $\exists$-Neg applied to 4
6. $\Sigma \vdash \neg\neg F$ — ByContra applied to 5
7. $\Sigma \vdash F$ — RevDoubleNeg applied to 6

We have done full circle.



No occurance; we can distribute

Theorem 17.8

If x does not occur as a free variable of G, then $\exists x.F(x) \land \exists x.G$ and $\exists x.(F(x) \land G)$ are provably equivalent.

Proof.

1. $\Sigma \vdash \exists x.F(x) \land \exists x.G$ — Premise
2. $\Sigma \vdash \exists x.G$ — $\land$-Symm and $\land$-Elim applied to 1
3. $\Sigma \vdash G$ — Previous theorem applied to 2
4. $\Sigma \vdash F(x) \Rightarrow F(x) \land G$ — ..Boolean reasoning applied to 3
5. $\Sigma \vdash \exists x.F(x) \Rightarrow \exists x.(F(x) \land G)$ — $\exists$-Distrib applied to 4
6. $\Sigma \vdash \exists x.(F(x) \land G)$ — $\Rightarrow$-Elim applied to 5

□

Exercise 17.8

If x does not occur as a free variable of G, then $\forall x.F(x) \lor \exists x.G$ and $\forall x.(F(x) \lor G)$ are provably equivalent.

Topic 17.2

Problems

Practice formal proofs

Exercise 17.9

Prove the following statements

1. $\emptyset \vdash \forall x.\exists y.\forall z.\exists w.(R(x,y) \vee \neg R(w,z))$
2. $\emptyset \vdash \forall x.\exists y.x = y$
3. $\emptyset \vdash \forall x.\forall y.((x = y \wedge f(y) = g(y)) \Rightarrow (h(f(x)) = h(g(y))))$
4. $\emptyset \vdash \exists x_1, x_2, x_3.f(g(x_1), x_2) = f(x_3, x_1)$

Proofs on set theory**

Exercise 17.10

Consider the following axioms of set theory

$$\begin{aligned}\Sigma = \{\, & \forall x, y, z.\ (z \in x \Leftrightarrow z \in y) \Rightarrow x \approx y,\\ & \forall x, y.\ (x \subseteq y \Leftrightarrow \forall z.\ (z \in x \Rightarrow z \in y)),\\ & \forall x, y, z.\ (z \in x - y \Leftrightarrow (z \in x \land z \not\in y))\}.\end{aligned}$$

Prove the following

$$\Sigma \vdash \forall x, y.\ x \subseteq y \Rightarrow \exists z.(y - z \approx x)$$

Bad orders

Exercise 17.11

Prove that the following formulas are mutually unsat

- $\forall x. \neg E(x, x)$
- $\forall x. E(x, y) \land E(y, x) \Rightarrow x = y$
- $\forall x, y, z. E(x, y) \land E(y, z) \Rightarrow \neg E(x, z)$
- $\forall x, y, z. E(x, y) \land E(x, z) \Rightarrow (E(y, x) \lor E(z, y))$
- $\exists x, y. E(x, y)$

End of Lecture 17