CS228 Logic for Computer Science 2023

Lecture 16: FOL - formal proofs

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2023-02-07

Topic 16.1

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.

$$\Sigma \vdash F$$

Formal rules for FOL

- The old rules will continue to work
- We need new rules for.....

quantifiers and equality

- Let us see how do we develop those!

Rules for propositional logic stays!

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

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

$$\vee - \text{INTRO}\,\frac{\Sigma \vdash F}{\Sigma \vdash F \vee G} \qquad \vee - \textsc{Symm}\,\frac{\Sigma \vdash F \vee G}{\Sigma \vdash G \vee F} \qquad \vee - \text{DEF}\,\frac{\Sigma \vdash F \vee G}{\Sigma \vdash \neg(\neg F \wedge \neg G)}\,*$$

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

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

* Works in both directions

We are not showing the rules for ⇔, ⊕, and punctuation.

Rules for quantifiers and equality

We will introduce the following four rules.

- $\forall$-Intro
- $\forall$-Elim
- $\exists$-Intro
- $\exists$-Elim

We will also introduce rules for equality

- Reflex
- Eqsub

Note

We will not show all steps due to propositional rules.

We will write ‘propositional rules applied to ...’

Provably equivalent

Definition 16.1

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

Topic 16.2

Introduction rules for ∀ and ∃

∃-Intro quantifiers

The condition is often not explicitly written. By writing $F(y)$ and $F(t)$, people may imply that the substitutions are defined.

If a fact is true about a term, we can introduce ∃

$$\exists - \textsc{Intro}\ \frac{\Sigma \vdash F(t)}{\Sigma \vdash \exists y.\ F(y)}\ y \not\in FV(F(z)), F(z)\{z \mapsto t\} \text{ and } F(z)\{z \mapsto y\} \text{ are defined}$$

for some variable z.

Example 16.1

1. $\{H(x)\} \vdash H(x)$ *Assumption*
2. $\{H(x)\} \vdash \exists y.\ H(y)$ *∃-Intro applied to 1*

Bad derivations that violate the side condition $y \notin FV(F(z))$

Example 16.2

1. $\{1 \neq 2, x = 1, y = 2\} \vdash x \neq y$ *Premise*
2. $\{1 \neq 2, x = 1, y = 2\} \vdash \exists y.\ y \neq y$ *$\exists$-Intro applied to 1*✗

because $y \in FV(z \neq y)$.

Exercise 16.1

1. $\Sigma \vdash F(f(x), y)$ *Premise*
2. $\Sigma \vdash \exists y. F(y, y)$ *$\exists$-Intro applied to 1*✗

Give $F(z)$ that shows $y \in FV(F(z))$.

Bad derivation that violate the side condition '$F(z)\{z \mapsto y\}$ is defined'

Example 16.3

1. $\{\exists y.\ c \neq y\} \vdash \exists y.\ c \neq y$ *Assumption*
2. $\{\exists y.\ c \neq y\} \vdash \exists y.\ \exists y.\ y \neq y$ *$\exists$-Intro applied to 1*✗

because $(\exists y.\ z \neq y)\{z \mapsto y\}$ is not defined.

The following derivation is correct even if y is quantified somewhere in the formula.

Exercise 16.2

1. $\Sigma \vdash \exists w.\ (c \neq w \land \forall y.P(y))$ *Assumption*
2. $\Sigma \vdash \exists y.\ \exists w.\ (y \neq w \land \forall y.P(y))$ *$\exists$-Intro applied to 1*✓

Give $F(z)$ that shows all conditions are satisfied.

Commentary: In the first example, y being quantified is not solely responsible. The problem is that z is occurring in a scope where where y is quantified.

Bad derivations that violate the side condition '$F(z)\{z \mapsto t\}$ is defined'

Example 16.4

1. $\Sigma \vdash \forall x.\ f(x) = x$ *Premise*
2. $\Sigma \vdash \exists y \forall x.\ y = x$ *∃-Intro applied to 1*✗

Statement 2 says that the domain is singleton, which is not implied by 1

because $(\forall x.\ z = x)\{z \mapsto f(x)\}$ *is not defined.*

We get $F(t)$, we need to identify $F(z)$.

Commentary: z is a placeholder. $F(z)$ neither occurs in antecedents nor in consequent of the proof rule. Therefore, it is our choice (the person who is writing the proof) to choose z and $F(z)$. If we choose a z that is already around, then we may potentially run into a situation where some actions are not allowed. Therefore, it is cleaner to assume z is not being used for any other purpose in the context. Therefore, we should always choose such that z is not quantified in $F(z)$. If we choose $F(z)$ poorly, we may not be able to apply the rule.

Good derivations that may look bad

Not all occurrences of t are replaced.

One may complain that not all copies of $g(c)$ were replaced.

Example 16.5

1. $\emptyset \vdash \exists x_2.\ f(g(c), x_2) = f(g(c), c)$ *Premise*
2. $\emptyset \vdash \exists x_1, x_2.\ f(x_1, x_2) = f(g(c), c)$ *$\exists$-Intro applied to 1*✓

$F(z) = \exists x_2.\ f(z, x_2) = f(g(c), c)$ *satisfies all the side conditions.*

How to intro $\forall$?

We have seen the following proof in our life.

- Consider a fresh name x to represent a number.
- We prove $Fact(x)$
- We conclude $\forall x.Fact(x)$.

$\forall$-Intro for variables

If something is true about a variable that is not referred elsewhere.

Then it must be true for any value in the universe.

No reference condition

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

Example 16.6

1. $\{H(x)\} \vdash H(x)$ *Assumption*
2. $\{H(x)\} \vdash \forall y.\ H(y)$ *$\forall$-Intro applied to 1*✗

Since x is referred in left hand side, the above derivation is wrong.

Exercise 16.3

Why $FV(F(z))$ must not contain x?

Commentary: The rule has implicit side condition that $F(z)\{z \mapsto x\}$ and $F(z)\{z \mapsto y\}$ are defined.

∀-Intro (for constants)

Constants may play the similar role

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

for some variable z.

Example 16.7

1. $\Sigma \vdash H(c)$ *Premise and c is not referred in Σ*
2. $\Sigma \vdash \forall y.\ H(y)$ *∀-Intro applied to 1*

Commentary: The rule has implicit side condition that $F(z)\{z \mapsto x\}$ and $F(z)\{z \mapsto y\}$ are defined.

Example: Bad $\forall$-Intro

Example 16.8

Consider the following derivation where we used a term for $\forall$-Intro.

1. $\emptyset \vdash \exists y.\ f(y) \neq y \lor f(c) = c$ *Premise*
2. $\emptyset \vdash \forall x.\ (\exists y.\ f(y) \neq y \lor x = c)$ $\forall$-Intro *applied to 1*✗

Our $F(z) = \exists y.\ f(y) \neq y \lor z = c$.

$f(c)$ *does not occur in* $F(z)$.

The formula in 1 is a valid formula and the formula in 2 is not a valid formula.

Topic 16.3

Elimination rules for ∀ and ∃

Universal instantiation

If some thing is always true, we should be able to make it true on any value.

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

Commentary: The above rule has an implicit side condition that $F\{x \mapsto t\}$ is defined.

Our first FOL proof : $\forall$ implies $\exists$

Theorem 16.1

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

the proof does not work in the reverse direction

Proof.

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

□

Exercise 16.4

Show $\Sigma \vdash \forall x.(F(x) \wedge G(x))$ and $\Sigma \vdash \forall x.F(x) \wedge \forall x.G(x)$ are provably equivalent.

One more example: working with quantifiers

Example 16.9

A derivation for $\emptyset \vdash (\forall x.\ (P(x) \lor Q(x)) \Rightarrow \exists x.P(x) \lor \forall x.Q(x))$.

1. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x)\} \vdash \forall x.\ (P(x) \lor Q(x))$ *Assumption*
2. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x)\} \vdash P(y) \lor Q(y)$ *∀-Elim applied to 1*
3. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x)\} \vdash \neg\exists x.P(x)$ *Assumption*
4. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x), P(y)\} \vdash P(y)$ *Assumption*
5. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x), P(y)\} \vdash \exists x.P(x)$ *∃-Intro applied to 4*
6. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x)\} \vdash Q(y)$ *propositional rules applied to 2, 3, and 5*
7. $\{\forall x.\ (P(x) \lor Q(x)), \neg\exists x.P(x)\} \vdash \forall x.Q(x)$ *∀-Intro applied to 6*

..... *rest is propositional reasoning*

Exercise 16.5

Fill the gaps in the step 6 and the tail of the proof.

Commentary: To understand the interplay of propositional reasoning and quantifiers, please solve the above exercise.

How to understand substitutions in the proof rules?

In the proof rules, there is a leaving term t and an arriving term s, and there is $F(z)$. Antecedents have $F(t)$ and consequences have $F(s)$.

For example,

$$F(z) = \underbrace{P(z) \land \forall z.Q(z) \land (\forall w.R(w,u)}_{\text{No worry occurrences of z}} \lor \exists y.R(z,y))$$

Commentary: A good way to think is that the name of a quantified variable is not important to the outside world, except when we try to substitute a free variable in its scope by a term, which may have a variable with the same name.

The name conflict issue is a mute point. As long as we follow some naming discipline, which ensures that free variables in a system and quantified variables do not 'clash'. We need not worry. This is often done in programming languages. For example, import in python prefixes every imported name.

There are four cases of occurrences of z.

- z may occur free under no scope
- z is quantified in a scope
- free z does not occur in scope of a quantifier w
- free z occurs in scope of a quantifier y (troubling case)

Only the last case causes a restriction that t and s cannot have y.

Where is $\exists$ instantiation?

$\exists$ can not behave like $\forall$.

If there is something, should we not be able to choose it? Not an arbitrary choice.

Example 16.10

Let us suppose we want to prove, "If there is a door in the building, I can steal diamonds."

Intuitively, we do...

1. *Assume door x is there*
2. $\vdots$
3. *details of robbery*
4. $\vdots$
5. *I steal diamonds.*
6. *We say, therefore the theorem holds.*

Formally, we need to do the following.

1. $\Sigma \cup \{D(x)\} \vdash D(x)$ *Assumption*
2. $\vdots$
3. *symbolic details of robbery*
4. $\vdots$
5. $\Sigma \cup \{D(x)\} \vdash Stolen$ ...
6. $\Sigma \vdash D(x) \Rightarrow Stolen$ *$\Rightarrow$-Intro applied to 5*
7. $\Sigma \vdash \exists x.D(x) \Rightarrow Stolen$ *What rule?*

Commentary: We expect the *Stolen* formula does not have x free. Therefore, the above reasoning may work as $\exists$ instantiation.

Instantiation rule for exists

The following rule plays the role of $\exists$ instantiation.

$$\exists-\textsc{Elim}\frac{\Sigma \vdash F(x) \Rightarrow G}{\Sigma \vdash \exists y.F(y) \Rightarrow G}\, x \notin FV(\Sigma \cup \{G, F(z)\}), y \notin FV(F(z))$$

Commentary: Note that y and x can be same variables. Whenever we apply the rule, we need to make a distinction between incoming variable x and outgoing variable y.

Example: using $\exists$-Elim

Example 16.11

The following derivation proves $\emptyset \vdash \exists x.(A(x) \land B(x)) \Rightarrow \exists x.A(x)$

1.	$\{A(x) \land B(x)\} \vdash A(x) \land B(x)$	Assumption
2.	$\{A(x) \land B(x)\} \vdash A(x)$	$\land$-Elim applied to 1
3.	$\{A(x) \land B(x)\} \vdash \exists x.\ A(x)$	$\exists$-Intro applied to 2
4.	$\emptyset \vdash A(x) \land B(x) \Rightarrow \exists x.\ A(x)$	$\Rightarrow$-Intro applied to 3
5.	$\emptyset \vdash \exists x.(A(x) \land B(x)) \Rightarrow \exists x.\ A(x)$	$\exists$-Elim applied to 4

We cannot instantiate $\exists$ out of the blue. We assume instantiated formula (step 1), prove the goal (step 3), and produce an implication (step 4), which is followed by $\exists$-Elim.

Exercise 16.6

Show $\Sigma \vdash \exists x.(F(x) \lor G(x))$*, and* $\Sigma \vdash \exists x.F(x) \lor \exists x.G(x)$ *are provably equivalent.*

Example: Disastrous derivations

Example 16.12

Here are two derivations that apply proof rules incorrectly and derive a bad statement.

1. $\{A(x)\} \vdash A(x)$ *Assumption*
2. $\{A(x)\} \vdash \forall x.\ A(x)$ *$\forall$-Intro applied to 1*✗
3. $\emptyset \vdash A(x) \Rightarrow \forall x.\ A(x)$ *$\Rightarrow$-Intro applied to 2*
4. $\emptyset \vdash \exists x.A(x) \Rightarrow \forall x.\ A(x)$ *$\exists$-Elim applied to 3*

1. $\{\exists x.A(x)\} \vdash \exists x.A(x)$ *Assumption*
2. $\{\exists x.A(x)\} \vdash A(x)$ *$\exists$-Elim applied to 1*✗
3. $\{\exists x.A(x)\} \vdash \forall x.\ A(x)$ *$\forall$-Intro applied to 2*
4. $\emptyset \vdash \exists x.A(x) \Rightarrow \forall x.\ A(x)$ *$\Rightarrow$-Intro applied to 3*

Topic 16.4

Problems

Exercise: extended ∀-elim rule

Exercise 16.7

Show that the following derived rule is sound

$$\forall-\textsc{Elim}\frac{\Sigma \vdash \forall x_1 ... x_n . F}{\Sigma \vdash F\sigma}\ F \textit{ is quantifier-free}$$

Exercise 16.8

Show that the following derived rule is sound

$$\forall-\textsc{Subst}\frac{\Sigma \vdash \forall x_1 ... x_n . F}{\Sigma \vdash \forall Vars(F\sigma).\ F\sigma}\ F \textit{ is quantifier-free and } FV(\Sigma) = \emptyset$$

Practice formal proofs

Exercise 16.9

Prove the following statements

1. $\emptyset \vdash \forall x.\exists y.\forall z.\exists w.(R(x,y) \lor \neg R(w,z))$

Exercise: bad orders

Exercise 16.10

Prove that the following formulas are mutually unsatisfiable.

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

Exercise: different proof systems (midterm 2021)

Exercise 16.11

Let us suppose we remove $\forall - \textsc{Elim}$ *from our FOL proof system and we add the following proof rule in our proof system.*

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

Show that we can drive $\forall - \textsc{Elim}$ *from the modified proof system. Give detailed derivation without skipping any step. Only formal derivations will be accepted.*

Topic 16.5

Extra slides: Soundness

Soundness of the proof system

We need to show that the proof rules derive only valid statements.

We only need to prove the soundness of the new proof rules in addition to the propositional rule.

Substitution

Theorem 16.2

For a variable z, a term t, and a formula $F(z)$, if $m^{\nu}(z) = m^{\nu}(t)$ and $F(t)$ is defined, then

$$m, \nu \models F(z) \qquad \textit{iff} \qquad m, \nu \models F(t).$$

Proof.

Not so trivial proof by structural induction. □

Exercise 16.12

Write down the above proof. *Hint: You need to case split when we quantify over z or some other variable.*

Soundness: $\exists - \textsc{Intro}$ is sound

Theorem 16.3

The following rule is sound.

$$\exists - \textsc{Intro}\frac{\Sigma \vdash F(t)}{\Sigma \vdash \exists y.\ F(y)}\ y \not\in FV(F(z)), F(z)\{z \mapsto t\} \textit{ and } F(z)\{z \mapsto y\} \textit{ are defined}$$

for some variable z.

Commentary: All soundness proofs are repeated applications of similar arguments. However, in each rule the side conditions play their role differently. To understand the side conditions, please look into all the soundness arguments in the extra slides of this lecture.

Proof.

1. Let us assume $m, \nu \models \Sigma$.
2. Due to the antecedent, $m, \nu \models F(t)$. Let $m^\nu(t) = v$.
3. Since $z \not\in FV(F(t))$, $m, \nu[z \mapsto v] \models F(t)$.
4. Since $F(z)\{z \mapsto t\}$ is defined, $m, \nu[z \mapsto v] \models F(z)$. (why?) (Theorem 16.2)
5. Since $y \not\in FV(F(z))$, $m, \nu[z \mapsto v, y \mapsto v] \models F(z)$.
6. Since $F(z)\{z \mapsto y\}$ is defined, $m, \nu[z \mapsto v, y \mapsto v] \models F(y)$. (Theorem 16.2)
7. Therefore, $m, \nu[z \mapsto v] \models \exists y.\ F(y)$.
8. Since $z \not\in FV(F(y))$, $m, \nu \models \exists y.\ F(y)$ □

Soundness: $\forall - \textsc{Intro}$ is sound

Theorem 16.4

The following rule is sound.

$$\forall - \textsc{Intro}\,\frac{\Sigma \vdash F(x)}{\Sigma \vdash \forall y.\ F(y)}\, y \notin FV(F(z)),\ x, z \in \textbf{Vars},\ \textit{and } x \notin FV(\Sigma \cup \{F(z)\}).$$

Proof.

- Let us assume $m, \nu \models \Sigma$. Let v be some value in the domain of model m.
- Since $x \notin FV(\Sigma)$, $m, \nu[x \mapsto v] \models \Sigma$. Due to the antecedent, $m, \nu[x \mapsto v] \models F(x)$.
- Since $z \notin FV(F(x))$, $m, \nu[x \mapsto v, z \mapsto v] \models F(x)$.
- Since $F(z)\{z \mapsto x\}$ is defined, $m, \nu[x \mapsto v, z \mapsto v] \models F(z)$(why?).
- Since $x \notin FV(F(z))$, $m, \nu[z \mapsto v] \models F(z)$.
- Since $y \notin FV(F(z))$, $m, \nu[z \mapsto v, y \mapsto v] \models F(z)$.
- Since $F(z)\{z \mapsto y\}$ is defined, $m, \nu[x \mapsto v, z \mapsto v] \models F(y)$(why?).
- Since $z \notin FV(F(y))$(why?), $m, \nu[y \mapsto v] \models F(y)$.
- Since v is an arbitrary value, we have $m, \nu \models \forall y.\ F(y)$. □

Soundness: $\forall - \textsc{Elim}$ is sound

Theorem 16.5

The following rule is sound.

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

Proof.

1. Let $t' = t\{x \mapsto z\}$, where z is a fresh variable.
2. Since $F\{x \mapsto t\}$ is defined, $F\{x \mapsto t'\}$ is defined and $F(t')\{z \mapsto x\}$ is defined.
3. Let us assume $m, \nu \models \Sigma$. Let $\nu' \triangleq \nu[z \mapsto \nu(x)]$. Since $z \notin FV(\Sigma)$, $m, \nu' \models \Sigma$.
4. Due to the antecedent, $m, \nu' \models \forall x.\ F(x)$.
5. Let $v \triangleq m^{\nu'}(t')$. Since $x \notin Vars(t')$, $v = m^{\nu'[x \mapsto v]}(t')$.
6. Due to $\forall$ semantics, $m, \nu'[x \mapsto v] \models F(x)$.
7. Since $F\{x \mapsto t'\}$ is defined , $m, \nu'[x \mapsto v] \models F(t')$.
8. Since $x \notin FV(F(t'))$, $m, \nu' \models F(t')$.
9. Therefore, $m, \nu \models F(t)$.(why?)

□

Commentary: If x does not occur in t, the proof is simpler. However, it occurs very often in practice.

Soundness: $\exists - \textsc{Elim}$ is sound

Theorem 16.6

The following rule is sound.

$$\exists - \textsc{Elim}\frac{\Sigma \vdash F(x) \Rightarrow G}{\Sigma \vdash \exists y.F(y) \Rightarrow G} x \notin FV(\Sigma \cup \{G, F(z)\}), y \notin FV(F(z))$$

Proof.

- Let us assume $m, \nu \models \Sigma$ and $m, \nu \models \exists y.F(y)$.
- There is v in domain of m such that $m, \nu[y \mapsto v] \models F(y)$.
- Since $x, y \notin FV(F(z))$, and $F(x)$ and $F(y)$ substitutions are defined, $m, \nu[x \mapsto v] \models F(x)$.
- Since $x \notin FV(\Sigma)$, $m, \nu[x \mapsto v] \models \Sigma$.
- Due to the antecedent, $m, \nu[x \mapsto v] \models F(x) \Rightarrow G$.
- Therefore, $m, \nu[x \mapsto v] \models G$.
- Since $x \notin FV(G)$, $m, \nu \models G$.

□

End of Lecture 16