CS228 Logic for Computer Science 2021

Lecture 16: FOL - formal proofs

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2021-02-25



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!

$$\operatorname{Assumption}_{\overline{\Sigma \vdash F}} F \in \Sigma \quad \operatorname{Monotonic}_{\overline{\Sigma' \vdash F}}^{\overline{\Sigma \vdash F}} \Sigma \subseteq \Sigma' \quad \operatorname{DoubleNeg}_{\overline{\Sigma \vdash \neg \neg F}}^{\overline{\Sigma \vdash F}}$$

$$\wedge -\operatorname{INTRO} \frac{\Sigma \vdash F \quad \Sigma \vdash G}{\Sigma \vdash F \land G} \quad \wedge -\operatorname{ELIM} \frac{\Sigma \vdash F \land G}{\Sigma \vdash F} \quad \wedge -\operatorname{Symm} \frac{\Sigma \vdash F \land G}{\Sigma \vdash G \land F}$$

$$\vee - \operatorname{INTRO} \frac{\Sigma \vdash F}{\Sigma \vdash F \lor G} \quad \vee - \operatorname{Symm} \frac{\Sigma \vdash F \lor G}{\Sigma \vdash G \lor F} \quad \vee - \operatorname{DEF} \frac{\Sigma \vdash F \lor G}{\Sigma \vdash \neg (\neg F \land \neg G)} *$$

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

$$\Rightarrow -\text{INTRO}\frac{\Sigma \cup \{F\} \vdash G}{\Sigma \vdash F \Rightarrow G} \quad \Rightarrow -\text{ELIM}\frac{\Sigma \vdash F \Rightarrow G \quad \Sigma \vdash F}{\Sigma \vdash G} \quad \Rightarrow -\text{DEF}\frac{\Sigma \vdash F \Rightarrow G}{\Sigma \vdash \neg F \lor G} *$$

* Works in both directions

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



Rules for quantifiers and equality

We will introduce the following four rules.









 \blacktriangleright \forall -ELIM

► ∃-ELIM

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 \forall and \exists



∃-Intro quantifiers

If a fact is true about a term, we can introduce \exists

Recall some substitutions are not defined. The condition is often not explicitly written. By writing F(y) and F(t), we can imply that the substitutions are defined.

$$\exists -\text{INTRO} \underbrace{\sum \vdash F(t)}_{\sum \vdash \exists y. \ F(y)} y \notin FV(F(z)), F(z)\{z \mapsto t\} \text{ and } F(z)\{z \mapsto y\} \text{ are defined}$$

for some variable z.

Example 16.1

- 1. $\{H(x)\} \vdash H(x)$
- 2. $\{H(x)\} \vdash \exists y. H(y)$

Assumption

 \exists -Intro applied to 1



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

Example 16.2

1.
$$\{x = 1, y = 2\} \vdash x \neq y$$

2. $\{x = 1, y = 2\} \vdash \exists y. y \neq y$
because $y \in FV(z \neq y)$.

Premise ∃-Intro applied to 1**X**

Exercise 16.1

1.
$$\Sigma \vdash F(f(x), y)$$

2.
$$\Sigma \vdash \exists y.F(y,y)$$

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

Premise ∃-Intro applied to 1**X**



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

Example 16.3

1. $\{\exists y. c \neq y\} \vdash \exists y. c \neq y$ 2. $\{\exists y. c \neq y\} \vdash \exists y. \exists y. y \neq y$ because $(\exists y. z \neq y)\{z \mapsto y\}$ is not defined. Assumption ∃-Intro applied to 1**X**

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

Exercise 16.2

1.
$$\Sigma \vdash \exists w. (c \neq w \land \forall y. P(y))$$

2.
$$\Sigma \vdash \exists y. \exists w. (y \neq w \land \forall y. P(y))$$

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.

000

Assumption ∃-Intro applied to 1√ Bad derivations that violate the side condition F(z) $\{z \mapsto t\}$ is defined'

Example 16.4
1.
$$\Sigma \vdash \forall x. f(x) = x$$

2. $\Sigma \vdash \exists y \forall x. y = x$
2. $\Sigma \vdash \exists y \forall x. y = x$

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

Premise \exists -Intro applied to 1X

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 *t*'s need to be replaced.

Example 16.5

1.
$$\emptyset \vdash \exists x_2$$
. $f(g(c), x_2) = f(g(c), c)$

2.
$$\emptyset \vdash \exists x_1, x_2. f(x_1, x_2) = f(g(c), c)$$

Premise ∃-Intro applied to 1√

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



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

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.

$$\forall -\text{INTRO} \underbrace{\sum \vdash F(x)}{\sum \vdash \forall y. F(y)} y \notin FV(F(z)), \ x, z \in \text{Vars, and } x \notin FV(\Sigma \cup \{F(z)\}).$$

No reference condition

Example 16.6

1.
$$\{H(x)\} \vdash H(x)$$
Assumption2. $\{H(x)\} \vdash \forall y. H(y)$ \forall -Intro applied to 1X

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.

	@() (8)()	CS228 Logic for Computer Science 2021	Instructor: Ashutosh Gupta	IITB, India	16
--	------------------------------------	---------------------------------------	----------------------------	-------------	----

∀-Intro (for constants)

Constants may play the similar role

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

for some variable z.

Example 16.7

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

Commentary:	The rule has implicit side condition that $F(z)\{z \mapsto x\}$ and $F(z)\{z \mapsto x\}$	$\{z \mapsto y\}$ are defined.		
000	CS228 Logic for Computer Science 2021	Instructor: Ashutosh Gupta	IITB, India	17

Example: Bad ∀-Intro

Example 16.8

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

- 1. $\emptyset \vdash \exists y. f(y) \neq y \lor f(c) = c$ Premise2. $\emptyset \vdash \forall x. (\exists y. f(y) \neq y \lor x = c)$ \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 \forall and \exists



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

$$\forall - \operatorname{ELIM} \frac{\Sigma \vdash \forall x.F(x)}{\Sigma \vdash F(t)}$$

Commentary:	The above rule has an implicit side condition that $F\{x\mapsto t\}$ is a	defined.		
@ () \$0	CS228 Logic for Computer Science 2021	Instructor: Ashutosh Gupta	IITB, India	20

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



Exercise 16.4

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



One more example: working with quantifiers

Example 16.9

Prove $\emptyset \vdash (\forall x. (P(x) \lor Q(x)) \Rightarrow \exists x.P(x) \lor \forall x.Q(x))$. *Here is the derivation.*

1.
$$\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x)\} \vdash \forall x. (P(x) \lor Q(x))$$
Assumption2. $\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x)\} \vdash P(y) \lor Q(y)$ \forall -Elim applied to 13. $\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x)\} \vdash \neg \exists x.P(x)$ Assumption4. $\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x), P(y)\} \vdash P(y)$ Assumption5. $\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x), P(y)\} \vdash \exists x.P(x)$ \exists -Intro applied to 46. $\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x)\} \vdash Q(y)$ propositional rules applied to 2, 3, and 57. $\{\forall x. (P(x) \lor Q(x)), \neg \exists x.P(x)\} \vdash \forall x.Q(x)$ \forall -Intro applied to 6

Exercise 16.5

@**()**\\$0

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.

CS228 Logic for Comp	uter Science 2021	Instructor: Ashutosh Gupta

How to understand substitutions in the proof rules?

In proof rules, there is a leaving term t and an arriving term s, and there is F(z).

Antecedent has F(t) and consequence has F(s). For example,

$$F(z) = \underbrace{P(z) \land \forall z. Q(z) \land (\forall w. R(w, u) \lor \exists y. R(z, y))}_{\text{No worry occurrences}} \bigvee \underbrace{Q(z) \land (\forall w. R(w, u) \lor \exists y. R(z, y))}_{\text{a quantified variable is not important to outside worlds}}$$

We have the following four possibilities.

- 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

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

Commentary: A good way to think is that the name of a quantified variable is not important to 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. This 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 and c++ allows you to declare namespaces.

(troubling case)

ତାତି

Instructor: Ashutosh Gupta

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

©⊕⊛⊚ CS228 Logic for Computer Science 2021 Instructor: Ashutosh Gupta IITB, India

Where is \exists instantiation?

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. :
- 3. details of robbery
- **4**. :
- 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 : 3. symbolic details of robbery 4 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?

24

The following rule plays the role of \exists instantiation.

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

Commentary: Note that y and x can be same variables. 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. $\{A(x) \land B(x)\} \vdash A(x)$	$\wedge ext{-Elim}$ 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. $\emptyset \vdash \exists x.(A(x) \land B(x)) \Rightarrow \exists x. A(x)$	∃-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.

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

Topic 16.4

Rules for equality



Equality rules

For equality

000

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

Exercise 16.7 Do we need side condition for rule EqSub?

Commentary: Again applying EQSUB gets trick. You need to identify F(z) for some fresh z like other rules.

Example : example for equality

Example 16.13

Let us prove $\emptyset \vdash \forall x, y$. $(x \neq y \lor f(x) = f(y))$

1.
$$\{x = y\} \vdash x = y$$

2. $\{x = y\} \vdash f(x) = f(x)$
3. $\{x = y\} \vdash f(x) = f(y)$
4. $\{\} \vdash \neg x = y \lor f(x) = f(y)$
5. $\{\} \vdash \forall x, y. (\neg x = y \lor f(x) = f(y))$

Exercise 16.8 Write F(z)s in the application of \forall -Intro. Assumption Reflex EqSub applied to 1 and 2 propositional rules applied to 3 ∀-Intro applied twice to 4 Deriving symmetry for equality

Theorem 16.2 If we have $\Sigma \vdash s = t$, we can derive $\Sigma \vdash t = s$ Proof. 1. $\Sigma \vdash s = t$ 2. $\Sigma \vdash s = s$

3. $\Sigma \vdash t = s$ EqSub applied to 2 and 1 where F(z) = (z = s)

Therefore, we declare the following a derived proof rule.

$$EQSYMM \frac{\Sigma \vdash s = t}{\Sigma \vdash t = s}$$

Premise

Reflex

Example : finding evidence of \exists is hard

There are magic terms that can provide evidence of \exists . Here is an extreme example.

Example 16.14

Consider $\emptyset \vdash \exists x_4, x_3, x_2, x_1$. $f(x_1, x_3, x_2) = f(g(x_2), j(x_4), h(x_3, a))$ Let us construct a proof for the above as follows

- 1. $\emptyset \vdash f(g(h(j(c), a)), j(c), h(j(c), a)) = f(g(h(j(c), a)), j(c), h(j(c), a))$
- 2. $\emptyset \vdash \exists x_1.f(x_1, j(c), h(j(c), a)) = f(g(h(j(c), a)), j(c), h(j(c), a))$
- 3. $\emptyset \vdash \exists x_2. \exists x_1. f(x_1, j(c), x_2) = f(g(x_2), j(c), h(j(c), a))$
- 4. $\emptyset \vdash \exists x_3 . \exists x_2 . \exists x_1 . f(x_1, x_3, x_2) = f(g(x_2), j(c), h(x_3, a))$

5.
$$\emptyset \vdash \exists x_4 . \exists x_3 . \exists x_2 . \exists x_1 . f(x_1, x_3, x_2) = f(g(x_2), j(x_4), h(x_3, a))$$

Reflex ∃-Intro applied to 1 ∃-Intro applied to 2 ∃-Intro applied to 3

 \exists -Intro applied to 4



Topic 16.5

Problems



Exercise: extended \forall -elim rule

Exercise 16.9

Show that the following derived rule is sound

$$\forall - \text{ELIM} - \frac{\Sigma \vdash \forall x_1 \dots x_n . F}{\Sigma \vdash F\sigma} F$$
 is quantifier-free

Exercise 16.10

Show that the following derived rule is sound

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



Exercise : derived rules for equality

Exercise 16.11 Prove the following derived rules

$$\operatorname{EQTRANS} \frac{\Sigma \vdash s = t \quad \Sigma \vdash t = r}{\Sigma \vdash s = r} \quad \operatorname{PARAMODULATION} \frac{\Sigma \vdash s = t}{\Sigma \vdash r(s) = r(t)}$$



Practice formal proofs

Exercise 16.12 Prove the following statements

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

2.
$$\emptyset \vdash \forall x. \exists y. x = y$$

3.
$$\emptyset \vdash \forall x. \forall y. ((x = y \land f(y) = g(y)) \Rightarrow (h(f(x)) = h(g(y))))$$

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 16.13

Consider the following axioms of set theory

$$\Sigma = \{ \forall x, y, z. (z \in x \Leftrightarrow z \in y) \Rightarrow x = y, \\ \forall x, y. (x \subseteq y \Leftrightarrow \forall z. (z \in x \Rightarrow z \in y)), \\ \forall x, y, z. (z \in x - y \Leftrightarrow (z \in x \land z \notin y)) \}.$$

Prove the following

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



Bad orders

Exercise 16.14

Prove that the following formulas are mutually unsatisfiable.

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

Exercise: different proof systems

Exercise 16.15

Let us suppose we remove $\forall - ELIM$ from our FOL proof system and we add the following proof rule in our proof system.

$$\exists - \mathrm{Def} rac{\Sigma \vdash orall x. F(x)}{\Sigma \vdash \neg \exists x. \neg F(x)}$$

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

Comm	entary: Solution:	
1.	$\Sigma \vdash \forall x.F(x)$	Premise
2.	$\Sigma \cup \{\neg F(t)\} \vdash \forall x.F(x)$	Monotonic applied to 1
3.	$\Sigma \cup \{\neg F(t)\} \vdash \neg \exists x. \neg F(x)$	∃-Def applied to 1
4.	$\Sigma \cup \{ \neg F(t) \} \vdash \neg F(t)$	Assumption
5.	$\Sigma \cup \{\neg F(t)\} \vdash \exists x. \neg F(x)$	∃-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



39

Topic 16.6

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 16.3

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

 $m, \nu \models F(z)$ iff $m, \nu \models F(t)$

Proof.

Not so trivial proof by structural induction.

Exercise 16.16

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



Soundness: $\exists - INTRO$ is sound

Theorem 16.4

The following rule is sound.

$$\exists -\text{INTRO} \frac{\Sigma \vdash F(t)}{\Sigma \vdash \exists y. F(y)} y \notin FV(F(z)), F(z)\{z \mapsto t\} \text{ and } F(z)\{z \mapsto y\} \text{ are defined}$$

for some variable z.

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 $z \notin FV(F(t))$, $m, \nu[z \mapsto v] \models F(t)$.
- 4. Since $F(z)\{z \mapsto t\}$ is defined, $m, \nu[z \mapsto v] \models F(z)._{(why?)}$
- 5. Since $y \notin FV(F(z))$, $m, \nu[z \mapsto v, y \mapsto v] \models F(z)$.
- 6. Since $F(z)\{z \mapsto y\}$ is defined, $m, \nu[z \mapsto v, y \mapsto v] \models F(y)$.
- 7. Therefore, $m, \nu[z \mapsto v] \models \exists y. F(y)$.
- 8. Since $z \notin FV(F(t))$, $m, \nu \models \exists y. F(y)$

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.

Soundness: $\forall - INTRO$ is sound

Theorem 16.5

The following rule is sound.

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

Proof.

- Let us assume $m, \nu \models \Sigma$. Let ν 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 $m, v \models \forall y. F(y)$.

IITB, India

44

Soundness: $\forall - ELIM \text{ is sound}$

Theorem 16.6

The following rule is sound.

$$\forall - \text{ELIM} \frac{\Sigma \vdash \forall x.F(x)}{\Sigma \vdash F(t)}$$

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: $\exists - ELIM \text{ is sound}$

Theorem 16.7

The following rule is sound.

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

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 $x \notin FV(G)$, $m, \nu \models G$.

46

End of Lecture 16

