CS228 Logic for Computer Science 2023

Lecture 17: FOL - formal proofs : $\exists$-Elim and Equality

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2023-02-09

Topic 17.1

Elimination rule for $\exists$

Topic 17.2

Rules for equality

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 17.1

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 17.2

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 17.1

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 (midterm 2021)

Example 17.3

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 17.3

Rules for equality

Equality rules

For equality

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

Exercise 17.2

Do we need a side condition for rule $\textsc{EqSub}$*?*

Commentary: Again applying $\textsc{EqSub}$ gets tricky. You need to identify $F(z)$ for some fresh z like other rules.

Example : example for equality

Example 17.4

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

1. $\{x = y\} \vdash x = y$ *Assumption*
2. $\{x = y\} \vdash f(x) = f(x)$ *Reflex*
3. $\{x = y\} \vdash f(x) = f(y)$ *EqSub applied to 1 and 2*
4. $\{\} \vdash \neg(x = y) \lor f(x) = f(y)$ *propositional rules applied to 3*
5. $\{\} \vdash \forall x, y.\ (\neg(x = y) \lor f(x) = f(y))$ *$\forall$-Intro applied twice to 4*

Exercise 17.3

Write $F(z)$s in the application of $\forall$-Intro.

Deriving symmetry for equality

Theorem 17.1

If we have $\Sigma \vdash s = t$*, we can derive* $\Sigma \vdash t = s$

Proof.

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

$\square$

Therefore, we declare the following as a derived proof rule.

$$\textsc{EqSymm}\frac{\Sigma \vdash s = t}{\Sigma \vdash t = s}$$

Example : finding evidence of $\exists$ is hard

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

Example 17.5

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. $\emptyset \vdash f(g(h(j(c), a)), j(c), h(j(c), a)) = f(g(h(j(c), a)), j(c), h(j(c), a))$ *Reflex*
2. $\emptyset \vdash \exists x_1.f(x_1, j(c), h(j(c), a)) = f(g(h(j(c), a)), j(c), h(j(c), a))$ *$\exists$-Intro applied to 1*
3. $\emptyset \vdash \exists x_2.\exists x_1.f(x_1, j(c), x_2) = f(g(x_2), j(c), h(j(c), a))$ *$\exists$-Intro applied to 2*
4. $\emptyset \vdash \exists x_3.\exists x_2.\exists x_1.f(x_1, x_3, x_2) = f(g(x_2), j(c), h(x_3, a))$ *$\exists$-Intro applied to 3*
5. $\emptyset \vdash \exists x_4.\exists x_3.\exists x_2.\exists x_1.f(x_1, x_3, x_2) = f(g(x_2), j(x_4), h(x_3, a))$ *$\exists$-Intro applied to 4*

Topic 17.4

Problems

Practice formal proofs

Exercise 17.4

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. $\emptyset \vdash \exists x_1, x_2, x_3.f(g(x_1), x_2) = f(x_3, x_1)$

Exercise: modeling equality using a predicate and axioms

Exercise 17.5

1. *Give a formal proof that shows that following formulas are mutually unsatisfiable.*
   - $\forall x, y.\ x = y$
   - $\forall x.\ \neg R(x, x)$
   - $\exists x, y.\ R(x, y)$

2. *Give a model that satisfies the following set of formulas.*
   - $\forall x.\ E(x, x)$
   - $\forall x, y.\ (E(x, y) \Rightarrow E(y, x))$
   - $\forall x, y, z.\ (E(x, y) \land E(y, z) \Rightarrow E(x, z))$
   - $\forall x, y.\ E(x, y)$
   - $\forall x.\ \neg R(x, x)$
   - $\exists x, y.\ R(x, y)$

3. *Give a formal proof that shows that the following formulas are mutually unsatisfiable.*
   - $\forall x.\ E(x, x)$
   - $\forall x, y.\ (E(x, y) \Rightarrow E(y, x))$
   - $\forall x, y, z.\ (E(x, y) \land E(y, z) \Rightarrow E(x, z))$
   - $\forall x_1, x_2, y_1, y_2.\ (E(x_1, x_2) \land E(y_1, y_2) \land R(x_1, y_1) \Rightarrow R(x_2, y_2))$
   - $\forall x, y.\ E(x, y)$
   - $\forall x.\ \neg R(x, x)$
   - $\exists x, y.\ R(x, y)$

Exercise : derived rules for equality

Exercise 17.6

Prove the following derived rules

$$\textsc{EqTrans}\frac{\Sigma \vdash s = t \qquad \Sigma \vdash t = r}{\Sigma \vdash s = r} \qquad \textsc{Paramodulation}\frac{\Sigma \vdash s = t}{\Sigma \vdash r(s) = r(t)}$$

Exercise: bad orders

Exercise 17.7

Prove that the following formulas are mutually unsatisfiable.

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

Proofs on arrays(midterm 2022)

Exercise 17.8

Let Σ contain the following FOL sentences (all free symbols are functions or constants)

1. $\forall z, i, x.\ read(store(z, i, x), i) = x$
2. $\forall z, i, j, v.\ (\ i = j \lor read(store(z, i, v), j) = read(z, j)\ )$
3. $store(a, n, read(b, n)) = store(b, n, read(a, n))$
4. $read(b, m) \neq read(a, m)$

Using the formal proof system, show that Σ can derive contradiction.

Commentary: **Solution:** The following proof is repetitive. Key observation is what to substitute for v and x and aim to derive $m = n$.

1. $\Sigma \vdash store(a, n, read(b, n)) = store(b, n, read(a, n))$ — Assumption
2. $\Sigma \vdash \forall z, i, j, v.\ (\ i = j \lor read(store(z, i, v), j) = read(z, j)\ )$ — Assumption
3. $\Sigma \vdash (\ n = m \lor read(store(a, n, read(b, n)), m) = read(a, m)\ )$ — $\forall$-Elim applied to 1 with substitutions $\{z \mapsto a, i \mapsto n, j \mapsto m, v \mapsto read(b, n)\}$
4. $\Sigma \vdash (\ n = m \lor read(store(b, n, read(a, n)), m) = read(b, m)\ )$ — $\forall$-Elim applied to 1 with substitutions $\{z \mapsto b, i \mapsto n, j \mapsto m, v \mapsto read(a, n)\}$
5. $\Sigma \vdash (\ n = m \lor read(store(b, n, read(a, n)), m) = read(a, m)\ )$ — EqSub applied to 3 and 1
6. $\Sigma \vdash (\ n = m \lor read(b, m) = read(a, m)\ )$ — EqSub applied to 3 and 5, and some propositional reasoning
7. $\Sigma \vdash read(b, m) \neq read(a, m)$ — Assumption
8. $\Sigma \vdash n = m$ — Resolution applied to 6 and 7
9. $\Sigma \vdash \forall z, i, x.\ read(store(z, i, x), i) = x$ — Assumption
10. $\Sigma \vdash read(store(a, n, read(b, n)), n) = read(b, n)$ — $\forall$-Elim applied to 9 with substitutions $\{z \mapsto a, i \mapsto n, x \mapsto read(b, n)\}$
11. $\Sigma \vdash read(store(b, n, read(a, n)), n) = read(a, n)$ — $\forall$-Elim applied to 9 with substitutions $\{z \mapsto b, i \mapsto n, x \mapsto read(a, n)\}$
12. $\Sigma \vdash read(store(b, n, read(a, n)), n) = read(b, n)$ — Eqsub applied to 10 and 1
13. $\Sigma \vdash read(b, n) = read(a, n)$ — Eqsub applied to 11 and 12
14. $\Sigma \vdash read(b, m) = read(a, m)$ — Eqsub applied to 13 and 8

Proofs on set theory**

Exercise 17.9

Consider the following axioms of set theory

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

Prove the following

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

End of Lecture 17