Proof Systems

Néstor Cataño

ncatano@puj.edu.co

Faculty of Engineering

Pontificia Universidad Javeriana

Proving First Order Logic Formulas

- We want to prove that a first order logic formula ϕ holds under a certain given set of assumptions Γ
- $\Gamma \models^{\mathcal{S}} \phi$ (read "ϕ follows from Γ under a structure $\mathcal{S}$")
  - When all the formulas in Γ hold, it follows that ϕ holds
  - For every assignment a, if for each $\psi \in \Gamma$, $M_a(\psi) = \text{TRUE}$, then $M_a(\phi) = \text{TRUE}$

Proving First Order Logic Formulas

- We want to prove that a first order logic formula ϕ holds under a certain given set of assumptions Γ
- $\Gamma \models^{\mathcal{S}} \phi$ (read "ϕ follows from Γ under a structure $\mathcal{S}$")
  - When all the formulas in Γ hold, it follows that ϕ holds
  - For every assignment a, if for each $\psi \in \Gamma$, $M_a(\psi) = \text{TRUE}$, then $M_a(\phi) = \text{TRUE}$
- $\Gamma \models^{\mathcal{S}} \phi$ coincides with $\models^{\mathcal{S}} \phi$ when $\Gamma = \emptyset$

Proving First Order Logic Formulas

- $\Gamma \models \phi$ (read "ϕ follows from Γ")
  - When $\Gamma \models^{\mathcal{S}} \phi$ for every structure $\mathcal{S}$

Proving First Order Logic Formulas

- $\Gamma \models \phi$ (read "ϕ follows from Γ")
  - When $\Gamma \models^{\mathcal{S}} \phi$ for every structure $\mathcal{S}$
- $\Gamma \models \phi$ coincides with $\models \phi$ when $\Gamma = \emptyset$

Proving First Order Logic Formulas

- We are interested in proving that $\Gamma \models \phi$
- The proof must consist of single steps and its correctness be clear
- The fact that ϕ is provable from the hypothesis Γ is denoted by $\Gamma \vdash \phi$
  - $\vdash \phi$ means that ϕ can be proved to hold in every structure and for every assignment

Proof System

- A proof system consists of
  1. axioms, *i.e.*, template formulas which are always true
  2. proof rules, which are used to deduce truths in underlying system

Proof System

- A proof rule includes a finite set of formulas, called antecedents and an additional formula called consequent
- For instance, in the following proof rule, $\Gamma = \{\phi, \phi \rightarrow \psi\}$ is the antecedent and ψ is the consequent

$$\frac{\phi,\ \phi \rightarrow \psi}{\psi}$$ Modus Ponens

Forward Reasoning

A proof of $\Gamma \models \phi$ consists of numbered sequence of formulas ending in ϕ. Each proof line is

- an hypothesis taken from Γ
- an instantiation of an axiom
- obtained from a previous line by using an instance of a proof rule

$$\frac{\phi,\ \phi \rightarrow \psi}{\psi}$$

Backward Reasoning

- Each proof rule prescribes the task of proving the consequent to the task of proving the premises
- One starts with the proof goal that needs to be proved, and justify it using simpler subgoals

$$\frac{\phi,\ \psi}{\phi \wedge \psi}$$

Properties of Proof Systems

- Is a proof system correct?
- Is there an algorithm that can decide if a given formula ϕ is a Tautology ?
- Is $\mathcal{S}$ a model of ϕ?

Properties of Proof Systems

- Soundness. If $\Gamma \vdash \phi$ then $\Gamma \models \phi$
- Completeness. If $\Gamma \models \phi$ then $\Gamma \vdash \phi$

Properties of Proof Systems

- Decidability. First order logic is semi-decidable.
  - There is no algorithm for checking whether $\Gamma \models \phi$ holds or not
  - However there is an algorithm that constructs a proof of $\Gamma \vdash \phi$ when $\Gamma \models \phi$ holds
  - This algorithm is not even guaranteed to terminate when $\Gamma \not\models \phi$

A Practical Proof System

- A sequent is a formula of the form
  $(\phi_1 \wedge \phi_2 \wedge ... \wedge \phi_n) \rightarrow (\psi_1 \vee \psi_2 \vee ... \vee \psi_m)$
- Each sub-formula ϕ_i is an antecedent and
- Each sub-formula ψ_i is a consequent
- A goal is a sequent that we want to prove
- The most recent lines that were changed during the proof will be marked with the symbol $*$

A Practical Proof System

- Proofs will be written

$$
\begin{array}{ll}
-1 & \phi_1 \\
-2 & \phi_2 \\
. & . \\
. & . \\
. & . \\
-n & \phi_n \\
\hline
1 & \psi_1 \\
2 & \psi_1 \\
. & . \\
. & . \\
. & . \\
m & \psi_m
\end{array}
$$

A Practical Proof System

- The proof rules presented are taken from the Pvs System
- We restrict ourselves to First Order Logic
  - Pvs itself is based on Higher Order Logic
- Instead of presenting proof rules, we present Pvs commands

Proof System Commands

- simplify. it proves the current goal given
  1. One of antecedents is false
  2. One of consequent is true
  3. One of the antecedents is the same as the consequent
  4. One of the consequents if of the form $e \equiv e$ where e is a term

Proof System Commands

- simplify. it proves the current goal given
  1. One of antecedents is false
  2. One of consequent is true
  3. One of the antecedents is the same as the consequent
  4. One of the consequents if of the form $e \equiv e$ where e is a term
- assume. It adds a formula from Γ in the antecedent.

Proof System Commands

- flatten. It creates one immediate subgoal, by simplifying the current goal, based on the special form of the sequent.

  1. It removes negation. It replaces an antecedent of the form $\neg\phi$ with a consequent of the form ϕ. It replaces a consequent of the form $\neg\psi$ with an antecedent of the form ψ.
  2. It breaks a conjunction by replacing an antecedent of the form $\phi_1 \wedge \phi_2$ with two antecedents ϕ_1 and ϕ_2
  3. It breaks a disjunction by replacing an consequent of the form $\psi_1 \vee \psi_2$ with two consequents ψ_1 and ψ_2
  4. It replaces a succedent of the form $\psi_1 \rightarrow \psi_2$ with an antecedent ψ_1 and a consequent ψ_2

Proof System Commands

- split. it splits the current goal into several subgoals
  1. If the current goal's consequent is $\psi_1 \wedge \ ... \ \wedge \psi_l$, split creates l subgoals, where in the ith new subgoal, the consequent is replaced with ψ_i
  2. If the current goal's antecedent is $\phi_1 \vee \ ... \ \vee \phi_l$, split creates l subgoals, where in the ith new subgoal, the antecedent is replaced with ϕ_i
  3. If the current goal's antecedent is $\phi \rightarrow \psi$, split creates two subgoals, the first with ϕ added as a consequent, and the second with ψ added as an antecedent

Proof System Commands

- skolemize. It eliminates the outermost external universal quantifier in a succedent, or the outermost external existential quantifier in an antecedent.

  1. If there is a succedent of the form $\forall x.\, \psi$, the skolemization creates a single subgoal by replacing the succedent with $\psi[c/x]$ for some new constant c that does not appear before in the proof
  2. If there is a antecedent of the form $\exists x.\, \phi$, the skolemization creates a single subgoal by replacing the antecedent with $\phi[c/x]$ for some new constant c that does not appear before in the proof

Proof System Commands

- instantiate. It is the complement of skolemize.

  1. If there is a succedent of the form $\exists x.\, \psi$. Then we pick up any term e, and create a single subgoal with that antecedent replaced by $\psi[e/x]$
  2. If there is a antecedent of the form $\forall x.\, \phi$. Then we pick up any term e and create a single subgoal with that antecedent replaced by $\phi[e/x]$

Proof System Commands

- replace. Given an antecedent of the form $e_1 \equiv e_2$, we can create a subgoal where e_1 is replaced by e_2 or e_2 by e_1 in either the antecedent or the consequent
- postpone. It alters the choice of the current goal.

Proof Example in Propositional Logic

$$((A \to C) \wedge (B \to C)) \to ((A \vee B) \to C)$$

Proof Example in Propositional Logic

$$\frac{}{1 \quad ((A \to C) \wedge (B \to C)) \to ((A \vee B) \to C)}$$

Proof Example in Propositional Logic

$$\frac{}{1 \quad ((A \to C) \wedge (B \to C)) \to ((A \vee B) \to C)} \text{ flatten } 1$$

Proof Example in Propositional Logic

$$\frac{* \; -1 \quad (A \to C) \wedge (B \to C)}{* \; 1 \quad (A \vee B) \to C}$$

Proof Example in Propositional Logic

$$\dfrac{\begin{array}{l} * \ -1 \quad (A \rightarrow C) \ \wedge \ (B \rightarrow C) \end{array}}{\begin{array}{l} * \ 1 \quad (A \vee B) \rightarrow C \end{array}} \ \text{flatten} \ -1$$

Proof Example in Propositional Logic

$$\begin{array}{lll} * & -1 & A \to C \\ * & -2 & B \to C \\ \hline 1 & & (A \vee B) \to C \end{array}$$

Proof Example in Propositional Logic

$$\begin{array}{lll} * & -1 & A \to C \\ * & -2 & B \to C \\ \hline 1 & & (A \vee B) \to C \end{array} \quad \text{flatten } 1$$

Proof Example in Propositional Logic

	-1	$A \rightarrow C$
	-2	$B \rightarrow C$
$*$	-3	$A \vee B$
	$*\ 1$	C

Proof Example in Propositional Logic

$$\begin{array}{lll} & -1 & A \to C \\ & -2 & B \to C \\ * & -3 & A \vee B \\ \hline & * \ 1 & C \end{array} \quad \text{split } -3$$

Proof Example in Propositional Logic

	-1	$A \to C$			-1	$A \to C$
	-2	$B \to C$			-2	$B \to C$
$*$	-3	A		$*$	-3	B
	1	C			1	C

Proof Example in Propositional Logic

	-1	$A \rightarrow C$
	-2	$B \rightarrow C$
$*$	-3	A
	1	C

Proof Example in Propositional Logic

$$\begin{array}{cll} & -1 & A \to C \\ & -2 & B \to C \\ * & -3 & A \\ \hline & 1 & C \end{array} \quad \text{split } -1$$

Proof Example in Propositional Logic

$$\begin{array}{lll} & -1 & B \to C \\ & -2 & A \\ \hline & 1 & C \\ * & 2 & A \end{array} \qquad \begin{array}{lll} * & -1 & C \\ & -2 & B \to C \\ & -3 & A \\ \hline & 1 & C \end{array}$$

Proof Example in Propositional Logic

$$
\begin{array}{lll}
-1 & B \rightarrow C & \\
-2 & A & \\
\hline
 & 1 & C \\
* & 2 & A
\end{array}
$$

Proof Example in Propositional Logic

$$\begin{array}{lll} -1 & B \rightarrow C & \\ -2 & A & \\ \hline & 1 \quad C & \text{simplify} \\ * & 2 \quad A & \end{array}$$

Proof Example in Propositional Logic

Proof Example in Propositional Logic

$*$	-1	C
	-2	$B \rightarrow C$
	-3	A
	1	C

Proof Example in Propositional Logic

$$
\begin{array}{lll}
* & -1 & C \\
 & -2 & B \rightarrow C \\
 & -3 & A \\
\hline
 & 1 & C
\end{array}
\qquad \text{simplify}
$$

Proof Example in Propositional Logic

Proof Example in Propositional Logic

	-1	$A \rightarrow C$
	-2	$B \rightarrow C$
$*$	-3	B
	1	C

Proof Example: Group Theory

	Axioms
module	There is a special element 1 such as $x \times 1 \equiv x$
associativity	$\forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z)$
right-complement	$\forall x.\exists y.\,x \times y \equiv 1$

Proof Example: Existence of a Left Complement

We want to prove that for each element x there is a left complement y such that $y \times x$ gives the unit element.

$x \times y \equiv 1 \quad (i.)$ (by right-complement)

$y \times z \equiv 1 \quad (ii.)$ (by right-complement)

$y \times x \equiv$	$(y \times x) \times 1$	(by module)
	$(y \times x) \times (y \times z)$	(by equation $(ii.)$)
	$y \times (x \times (y \times z))$	(by associativity)
	$y \times ((x \times y) \times z)$	(by associativity)
	$y \times (1 \times z)$	(by equation $(i.)$)
	$(y \times 1) \times z$	(by associativity)
	$y \times z$	(by module)
	1	(by equation $(ii.)$)

Proof Example: Existence of a Left Complement

$$\frac{}{1 \quad \forall x.\, \exists y.\, y \times x \equiv 1}$$

Proof Example: Existence of a Left Complement

$$\frac{}{1 \quad \forall x.\, \exists y.\, y \times x \equiv 1} \text{ skolemize } 1\ x'$$

Proof Example: Existence of a Left Complement

$$\frac{}{\ast \quad 1 \quad \exists y.\, y \times x' \equiv 1}\ \text{skolemize } 1\ x'$$

Proof Example: Existence of a Left Complement

$$\frac{}{\ast \quad 1 \quad \exists y.\, y \times x' \equiv 1}\ \text{assume right}-\text{complement}$$

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{lll} * & -1 & \forall x.\, \exists y.\, x \times y \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}}$$ assume right−complement

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{lll} * & -1 & \forall x.\, \exists y.\, x \times y \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \text{ instantiate } -1\ x'$$

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{cc} * & -1 \quad \exists y.\, x' \times y \equiv 1 \end{array}}{\begin{array}{cc} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \text{ instantiate } -1\ x'$$

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{cccc} * & -1 & \exists y.\, x' \times y \equiv 1 \end{array}}{\begin{array}{cccc} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \quad \text{skolemize } -1\ y'$$

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{cc} * & -1 \quad x' \times y' \equiv 1 \end{array}}{\begin{array}{cc} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \quad \text{skolemize } -1\ y'$$

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{cc} * & -1 \quad x' \times y' \equiv 1 \end{array}}{\begin{array}{cc} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \text{ assume right}-\text{complement}$$

Proof Example: Existence of a Left Complement

$$\dfrac{\begin{array}{lll} * & -1 & \forall x.\, \exists y.\, x \times y \equiv 1 \\ & -2 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} & 1 \quad \exists y.\, y \times x' \equiv 1 \end{array}}\ \text{assume right}-\text{complement}$$

Proof Example: Existence of a Left Complement

$$\dfrac{\begin{array}{lll} * & -1 & \forall x.\, \exists y.\, x \times y \equiv 1 \\ & -2 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}}\ \text{instantiate } -1\ y'$$

Proof Example: Existence of a Left Complement

$$\dfrac{\begin{array}{lll} * & -1 & \exists y.\, y' \times y \equiv 1 \\ & -2 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}}\ \text{instantiate } -1\ y'$$

Proof Example: Existence of a Left Complement

$$\frac{\begin{array}{lll} * & -1 & \exists y.\, y' \times y \equiv 1 \\ & -2 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \text{ skolemize } -1\ z'$$

Proof Example: Existence of a Left Complement

$$\dfrac{\begin{array}{lll} * & -1 & y' \times z' \equiv 1 \\ & -2 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}} \quad \text{skolemize } -1\ z'$$

Proof Example: Existence of a Left Complement

$$\dfrac{\begin{array}{lll} * & -1 & y' \times z' \equiv 1 \\ & -2 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}}\ \text{assume module}$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & \forall x.\, x \times 1 \equiv x \\
 & -2 & y' \times z' \equiv 1 \\
 & -3 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{assume module}
$$

Proof Example: Existence of a Left Complement

$$\dfrac{\begin{array}{lll} * & -1 & \forall x.\, x \times 1 \equiv x \\ & -2 & y' \times z' \equiv 1 \\ & -3 & x' \times y' \equiv 1 \end{array}}{\begin{array}{ll} 1 & \exists y.\, y \times x' \equiv 1 \end{array}}\ \text{instantiate } -1\ (y' \times x')$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \times 1 \equiv (y' \times x') \\
 & -2 & y' \times z' \equiv 1 \\
 & -3 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } -1\ (y' \times x')
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \times 1 \equiv (y' \times x') \\
 & -2 & y' \times z' \equiv 1 \\
 & -3 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -2\ -1 \text{ rl}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -2 & y' \times z' \equiv 1 \\
 & -3 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -2\ -1\ \text{rl}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -2 & y' \times z' \equiv 1 \\
 & -3 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{assume associativity}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & \forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z) \\
 & -2 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -3 & y' \times z' \equiv 1 \\
 & -4 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{assume associativity}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & \forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z) \\
 & -2 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -3 & y' \times z' \equiv 1 \\
 & -4 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } -1 \; y', x', (y' \times z')
$$

Proof Example: Existence of a Left Complement

*	-1	$(y' \times x') \times (y' \times z') \equiv y' \times (x' \times (y' \times z'))$	
	-2	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$	
	-3	$y' \times z' \equiv 1$	
	-4	$x' \times y' \equiv 1$	
	1	$\exists y.\, y \times x' \equiv 1$	instantiate -1 $y', x', (y' \times z')$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \times (y' \times z') \equiv y' \times (x' \times (y' \times z')) \\
 & -2 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -3 & y' \times z' \equiv 1 \\
 & -4 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -2\ -1 \text{ lr}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \equiv y' \times (x' \times (y' \times z')) \\
 & -2 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -3 & y' \times z' \equiv 1 \\
 & -4 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -2\ -1\ \text{lr}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times x') \equiv y' \times (x' \times (y' \times z')) \\
 & -2 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -3 & y' \times z' \equiv 1 \\
 & -4 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
$$

assume associativity

Proof Example: Existence of a Left Complement

*	-1	$\forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z)$	
	-2	$(y' \times x') \equiv y' \times (x' \times (y' \times z'))$	
	-3	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$	
	-4	$y' \times z' \equiv 1$	
	-5	$x' \times y' \equiv 1$	
	1	$\exists y.\,y \times x' \equiv 1$	assume associativity

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & \forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z) \\
 & -2 & (y' \times x') \equiv y' \times (x' \times (y' \times z')) \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } -1 \; x', y', z'
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -2 & (y' \times x') \equiv y' \times (x' \times (y' \times z')) \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } -1 \; x', y', z'
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -2 & (y' \times x') \equiv y' \times (x' \times (y' \times z')) \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -1\ -2\ \text{rl}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -2 & (y' \times x') \equiv y' \times ((x' \times y') \times z') \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -1\ -2\ \text{rl}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -2 & (y' \times x') \equiv y' \times ((x' \times y') \times z') \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -5\ -2\ \text{lr}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -2 & (y' \times x') \equiv y' \times (1 \times z') \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -5\ -2\ \text{lr}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -2 & (y' \times x') \equiv y' \times (1 \times z') \\
 & -3 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -4 & y' \times z' \equiv 1 \\
 & -5 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
$$

assume associativity

Proof Example: Existence of a Left Complement

*	-1	$\forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z)$
	-2	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
	-3	$(y' \times x') \equiv y' \times (1 \times z')$
	-4	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-5	$y' \times z' \equiv 1$
	-6	$x' \times y' \equiv 1$
	1	$\exists y.\, y \times x' \equiv 1$

assume associativity

Proof Example: Existence of a Left Complement

*	-1	$\forall x.\forall y.\forall z.\,(x \times y) \times z \equiv x \times (y \times z)$
	-2	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
	-3	$(y' \times x') \equiv y' \times (1 \times z')$
	-4	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-5	$y' \times z' \equiv 1$
	-6	$x' \times y' \equiv 1$
	1	$\exists y.\, y \times x' \equiv 1$

instantiate -1 $y', 1, z'$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times 1) \times z' \equiv y' \times (1 \times z') \\
 & -2 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -3 & (y' \times x') \equiv y' \times (1 \times z') \\
 & -4 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -5 & y' \times z' \equiv 1 \\
 & -6 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } -1 \; y', 1, z'
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & (y' \times 1) \times z' \equiv y' \times (1 \times z') \\
 & -2 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -3 & (y' \times x') \equiv y' \times (1 \times z') \\
 & -4 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -5 & y' \times z' \equiv 1 \\
 & -6 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -1\ -3\ \text{rl}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{cll}
 & -1 & (y' \times 1) \times z' \equiv y' \times (1 \times z') \\
 & -2 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
* & -3 & (y' \times x') \equiv ((y' \times 1) \times z') \\
 & -4 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -5 & y' \times z' \equiv 1 \\
 & -6 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{replace } -1\ -3\ \text{rl}
$$

Proof Example: Existence of a Left Complement

$$
\begin{array}{cll}
 & -1 & (y' \times 1) \times z' \equiv y' \times (1 \times z') \\
 & -2 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
* & -3 & (y' \times x') \equiv ((y' \times 1) \times z') \\
 & -4 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -5 & y' \times z' \equiv 1 \\
 & -6 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{assume module}
$$

Proof Example: Existence of a Left Complement

*	-1	$\forall x.\, x \times 1 \equiv x$	
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$	
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$	
	-4	$(y' \times x') \equiv ((y' \times 1) \times z')$	
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$	
	-6	$y' \times z' \equiv 1$	
	-7	$x' \times y' \equiv 1$	
	1	$\exists y.\, y \times x' \equiv 1$	assume module

Proof Example: Existence of a Left Complement

*	-1	$\forall x.\, x \times 1 \equiv x$
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
	-4	$(y' \times x') \equiv ((y' \times 1) \times z')$
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-6	$y' \times z' \equiv 1$
	-7	$x' \times y' \equiv 1$
	1	$\exists y.\, y \times x' \equiv 1$

instantiate -1 y'

Proof Example: Existence of a Left Complement

$$
\begin{array}{lll}
* & -1 & y' \times 1 \equiv y' \\
 & -2 & (y' \times 1) \times z' \equiv y' \times (1 \times z') \\
 & -3 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
 & -4 & (y' \times x') \equiv ((y' \times 1) \times z') \\
 & -5 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -6 & y' \times z' \equiv 1 \\
 & -7 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } -1\ y'
$$

Proof Example: Existence of a Left Complement

*	-1	$y' \times 1 \equiv y'$
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
	-4	$(y' \times x') \equiv ((y' \times 1) \times z')$
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-6	$y' \times z' \equiv 1$
	-7	$x' \times y' \equiv 1$
		replace -1 -4 lr
	1	$\exists y.\, y \times x' \equiv 1$

Proof Example: Existence of a Left Complement

	-1	$y' \times 1 \equiv y'$
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
*	-4	$(y' \times x') \equiv (y' \times z')$
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-6	$y' \times z' \equiv 1$
	-7	$x' \times y' \equiv 1$
	1	$\exists y.\, y \times x' \equiv 1$

replace -1 -4 lr

Proof Example: Existence of a Left Complement

	-1	$y' \times 1 \equiv y'$
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
*	-4	$(y' \times x') \equiv (y' \times z')$
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-6	$y' \times z' \equiv 1$
	-7	$x' \times y' \equiv 1$
	1	$\exists y.\, y \times x' \equiv 1$

replace -6 -4 lr

Proof Example: Existence of a Left Complement

	-1	$y' \times 1 \equiv y'$
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
$*$	-4	$y' \times x' \equiv 1$
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-6	$y' \times z' \equiv 1$
	-7	$x' \times y' \equiv 1$
	1	$\exists y.\, y \times x' \equiv 1$

replace -6 -4 lr

Proof Example: Existence of a Left Complement

$$
\begin{array}{cll}
 & -1 & y' \times 1 \equiv y' \\
 & -2 & (y' \times 1) \times z' \equiv y' \times (1 \times z') \\
 & -3 & (x' \times y') \times z' \equiv x' \times (y' \times z') \\
* & -4 & y' \times x' \equiv 1 \\
 & -5 & (y' \times x') \times (y' \times z') \equiv (y' \times x') \\
 & -6 & y' \times z' \equiv 1 \\
 & -7 & x' \times y' \equiv 1 \\
\hline
 & 1 & \exists y.\, y \times x' \equiv 1
\end{array}
\qquad \text{instantiate } 1 \ y'
$$

Proof Example: Existence of a Left Complement

	-1	$y' \times 1 \equiv y'$
	-2	$(y' \times 1) \times z' \equiv y' \times (1 \times z')$
	-3	$(x' \times y') \times z' \equiv x' \times (y' \times z')$
$*$	-4	$y' \times x' \equiv 1$
	-5	$(y' \times x') \times (y' \times z') \equiv (y' \times x')$
	-6	$y' \times z' \equiv 1$
	-7	$x' \times y' \equiv 1$
	1	$y' \times x' \equiv 1$

instantiate 1 y'