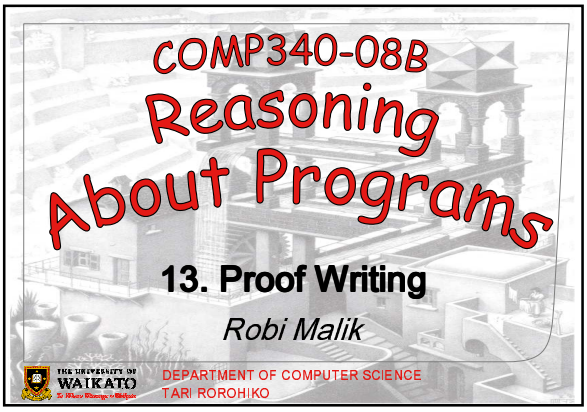


Common Phrases in Proofs (1)

→-Introduction

Assume that ⟨*precondition*⟩.

…

Therefore we have ⟨*conclusion*⟩.

It follows that ⟨*precondition*⟩ always implies ⟨*conclusion*⟩.

Common Phrases in Proofs (2)

↔-Introduction

First assume that ⟨*condition1*⟩.

…

Therefore we have ⟨*condition2*⟩.

Second assume that ⟨*condition2*⟩.

…

Therefore we have ⟨*condition1*⟩.

It follows that ⟨*condition1*⟩ and ⟨*condition2*⟩ are equivalent.

Common Phrases in Proofs (3)

∀-Introduction

Let ⟨*item*⟩ be an arbitrary ⟨*element*⟩.

…

Therefore ⟨*item*⟩ satisfies ⟨*the claim*⟩.

Since ⟨*item*⟩ was chosen arbitrarily, it follows that every ⟨*element*⟩ satisfies ⟨*the claim*⟩.

Common Phrases in Proofs (5)

∨-Elimination

(Given some disjunction, say ⟨*case1* ∨ *case2*⟩.)

Consider the following cases.

First assume that ⟨*case1*⟩ holds.

…

Then it follows that ⟨*the claim*⟩.

Second assume that ⟨*case1*⟩ holds.

…

Then it follows that ⟨*the claim*⟩.

In all cases we have ⟨*the claim*⟩.

Common Phrases in Proofs (6)

***false*-Elimination, ¬-Introduction**

Assume that ⟨*the claim*⟩ does not hold.

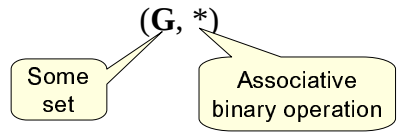
…

This is a contradiction.

Therefore, the assumption was wrong, and it follows that ⟨*the claim*⟩ holds.

Another Example: Semigroups

A **semigroup** is an algebraic structure that involves an associative operation.



Axiom

$$\forall x \forall y \forall z \;\; x * (y * z) = (x * y) * z$$

Examples of Semigroups

Examples

- $(\mathbb{N}, +)$ – Natural numbers with addition
- $(\mathbb{R}, \cdot)$ – Real numbers with multiplication
- Functions f: $\mathbb{N} \to \mathbb{N}$ with functional composition.

Identity and Inverse Elements

Let $(\mathbf{G}, *)$ be a semigroup and $e \in \mathbf{G}$.

- e is a **left identity**, if $\forall x \;\; e * x = x$.
- e is a **right identity**, if $\forall x \;\; x * e = x$.
- e is an **identity**, if e is a right and a left identity.

Let $a \in \mathrm{G}$.

- a' is a **left inverse** of a if $a' * a$ is a left identity.
- a' is a **right inverse** of a if $a * a'$ is a right identity.
- a' is an **inverse** of a if a' is a both right and left inverse of a.

Groups

A semigroup $(\mathbf{G}, *)$ is called a **group** if

- $\mathbf{G}$ contains a left identity, and
- every element of $\mathbf{G}$ has a left inverse.

Known Properties of groups:

- A group has exactly one identity element, which is both a left and a right identity.
- Every element of a group has exactly one inverse, which is both its left and right inverse.

A Proof in Group Theory

Proposition.
Let $(\mathbf{G}, *)$ be a semigroup. Then every right inverse of an element of $\mathbf{G}$ is equal to every left inverse of that element.

Proof.
Let $a \in \mathbf{G}$, let l be a left inverse of a, and let r be right inverse of a. Then $l * a$ is a left identity, and $a * r$ is a right identity. It follows that $l = l * (a * r) = (l * a) * r = r$, i.e., $l = r$. Since a, l, and r where chosen arbitrarily, it follows that every right inverse is equal to every left inverse. □

The Proof in Natural Deduction

1.	$\forall x \forall y \forall z \;\; (x * y) * z = x * (y * z)$	Premise
2.	$\forall x \; (\text{left\_id}(x) \to \forall y \;\; x * y = y)$	Premise
3.	$\forall x \; (\text{right\_id}(x) \to \forall y \;\; y * x = y)$	Premise
4.	$\forall x \forall y \;\; (\text{left\_inv}(x, y) \to \text{left\_id}(x * y))$	Premise
5.	$\forall x \forall y \;\; (\text{right\_inv}(x, y) \to \text{right\_id}(y * x))$	Premise
	…	
n.	$\forall x \forall y \forall z \; (\text{left\_inv}(y, x) \wedge \text{right\_inv}(z, x) \to y = z)$	