

Computer Supported Modeling and Reasoning

First-Order Logic: Equality, Theories, Sets

David Basin

30.10.02

Overview

Last lecture: [first-order logic](#)

This lecture:

- [first-order logic with equality](#) and [first-order theories](#)

Extend language and deductive system to formalize and reason about the (mathematical) world

- [Set theoretic reasoning](#)

Equality

FOL with equality

Equality is a logical symbol rather than a mathematical one. Speak of **first-order logic with equality** rather than adding equality as “just another predicate”.

Syntax and Semantics

Syntax: = is a binary infix predicate.

$t_1 = t_2 \in \textit{Form}$ if $t_1, t_2 \in \textit{Term}$.

Syntax and Semantics

Syntax: $=$ is a binary infix predicate.

$$t_1 = t_2 \in \textit{Form} \text{ if } t_1, t_2 \in \textit{Term}.$$

Semantics: recall a **structure** is a pair $\mathcal{A} = \langle U_{\mathcal{A}}, I_{\mathcal{A}} \rangle$ and $I_{\mathcal{A}}(t)$ is the interpretation of t .

$$I_{\mathcal{A}}(s = t) = \begin{cases} 1 & I_{\mathcal{A}}(s) = I_{\mathcal{A}}(t) \\ 0 & \text{otherwise} \end{cases}$$

Note the three completely **different** uses of “ $=$ ” here!

Rules

- Equality is an **equivalence relation**

$$\frac{}{x = x} \textit{ refl} \quad \frac{x = y}{y = x} \textit{ sym} \quad \frac{x = y \quad y = z}{x = z} \textit{ trans}$$

- Equality is also a **congruence** on terms and all relations

$$\frac{x_1 = y_1 \cdots x_n = y_n}{t(x_1, \dots, x_n) = t(y_1, \dots, y_n)} \textit{ cong}_1$$

$$\frac{x_1 = y_1 \cdots x_n = y_n \quad A(x_1, \dots, x_n)}{A(y_1, \dots, y_n)} \textit{ cong}_2$$

Soundness of Rules

Equality in $I_{\mathcal{A}}$ is an **equivalence relation** and functions/predicates/logical-operators are “**truth functional**” . Adding further rules gives us an **equational theory**, e.g. **groups**.

Congruence: Alternatives

One can specialize congruence rules to replace only **some** term occurrences.

$$\frac{x_1 = y_1 \cdots x_n = y_n}{t([x_1, \dots, x_n/z_1, \dots, z_n]) = t([y_1, \dots, y_n/z_1, \dots, z_n])} \text{cong}_1$$

$$\frac{x_1 = y_1 \cdots x_n = y_n \quad A([x_1, \dots, x_n/z_1, \dots, z_n])}{A([y_1, \dots, y_n/z_1, \dots, z_n])} \text{cong}_2$$

One time the z 's are replaced with x 's and one time with y 's.

Examples

How many ways are there to choose some occurrences of x in $x^2 + y^2 > 12x$?

Examples

How many ways are there to choose some occurrences of x in $x^2 + y^2 > 12x$? 4, namely:

$$A = x^2 + y^2 > 12x, \quad A = z^2 + y^2 > 12x,$$

$$A = x^2 + y^2 > 12z, \quad A = z^2 + y^2 > 12z.$$

Examples

How many ways are there to choose some occurrences of x in $x^2 + y^2 > 12x$? 4, namely:

$$A = x^2 + y^2 > 12x, \quad A = z^2 + y^2 > 12x,$$

$$A = x^2 + y^2 > 12z, \quad A = z^2 + y^2 > 12z.$$

We show two ways:

$$\frac{x = 3 \quad x^2 + y^2 > 12x}{3^2 + y^2 > 12x} \text{ with } A = z^2 + y^2 > 12x$$

$$\frac{x = 3 \quad x^2 + y^2 > 12x}{x^2 + y^2 > 12 \cdot 3} \text{ with } A = x^2 + y^2 > 12z$$

Isabelle Rule

The Isabelle FOL rule is *simply*:

$$\frac{x = y \quad P(x)}{P(y)} \textit{subst}$$

Proving $\exists x. t = x$

$$\frac{\frac{}{t = t} \text{ refl}}{\exists x. t = x} \exists\text{-I}$$

Proving $\exists x. t = x$

$$\frac{\frac{}{t = t} \text{ refl}}{\exists x. t = x} \exists\text{-I}$$

In the rule $\frac{A(t)}{\exists x. A(x)} \exists\text{-I}$, “ $A(x)$ ” is **metanotation**. In the example, $A(x) = (t = x)$.

Proving $\exists x. t = x$

$$\frac{\frac{}{t = t} \text{ refl}}{\exists x. t = x} \exists\text{-I}$$

In the rule $\frac{A(t)}{\exists x. A(x)} \exists\text{-I}$, “ $A(x)$ ” is **metanotation**. In the example, $A(x) = (t = x)$.

Notational confusion avoided by a **precise metalanguage**.

Proving $\exists x. t = x$

$$\frac{\frac{}{t = t} \text{ refl}}{\exists x. t = x} \exists\text{-I}$$

In the rule $\frac{A(t)}{\exists x. A(x)} \exists\text{-I}$, “ $A(x)$ ” is **metanotation**. In the example, $A(x) = (t = x)$.

Notational confusion avoided by a **precise metalanguage**.

Why do we insist that all functions in a structure are total?

Theories

Example: Theory of Partial Orders

- Language: \leq

Example: Theory of Partial Orders

- Language: \leq
- Axioms

$$\forall x, y, z. x \leq y \wedge y \leq z \rightarrow x \leq z$$

$$\forall x, y. x \leq y \wedge y \leq x \leftrightarrow x = y$$

Example: Theory of Partial Orders

- Language: \leq

- Axioms

$$\forall x, y, z. x \leq y \wedge y \leq z \rightarrow x \leq z$$

$$\forall x, y. x \leq y \wedge y \leq x \leftrightarrow x = y$$

- Alternative to axioms is to convert to rules

$$\frac{x \leq y \quad y \leq z}{x \leq z} \textit{trans} \quad \frac{x \leq y \quad y \leq x}{x = y} \textit{antisym} \quad \frac{x = y}{x \leq y} \textit{eq_refl}$$

Such conversion possible since implication is main connective.

A Redundant Rule

One may also consider adding the rule

$$\frac{x = y}{y \leq x} \text{eq_refl2}$$

to the system. This rule can be **derived** as follows:

$$\frac{x = y}{y = x} \text{sym}$$
$$\frac{y = x}{y \leq x} \text{eq_refl}$$

Example (cont.)

- A partial order is a linear or total order when

$$\forall x, y. x \leq y \vee y \leq x$$

Note: no “pure” rule formulation of this disjunction.

Example (cont.)

- A partial order is a linear or total order when

$$\forall x, y. x \leq y \vee y \leq x$$

Note: no “pure” rule formulation of this disjunction.

- A total order is dense when, in addition

$$\forall x, y. x < y \rightarrow \exists z. (x < z \wedge z < y)$$

Give Structures . . .

Give **structures** for orders that are:

1. Partial but not total:

Give Structures . . .

Give **structures** for orders that are:

1. Partial but not total: \subseteq -relation
2. Total but not dense:

Give Structures . . .

Give **structures** for orders that are:

1. Partial but not total: \subseteq -relation
2. Total but not dense: Integers with \leq
3. Dense:

Give Structures . . .

Give **structures** for orders that are:

1. Partial but not total: \subseteq -relation
2. Total but not dense: Integers with \leq
3. Dense: Reals with \leq

Example 2: Groups

- Language: Function symbols \cdot , $^{-1}$, e

Example 2: Groups

- Language: Function symbols $_ \cdot _$, $_^{-1}$, e
- A **group** is a model of

$$\forall x, y, z. (x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (\text{assoc})$$

$$\forall x. x \cdot e = x \quad (\text{r-neutr})$$

$$\forall x. x \cdot x^{-1} = e \quad (\text{r-inv})$$

Example 2: Groups

- Language: Function symbols $_ \cdot _$, $_^{-1}$, e
- A **group** is a model of

$$\forall x, y, z. (x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (\text{assoc})$$

$$\forall x. x \cdot e = x \quad (\text{r-neutr})$$

$$\forall x. x \cdot x^{-1} = e \quad (\text{r-inv})$$

It is an example of an **equational theory**.

Theorems: (1) $x^{-1} \cdot x = e$ and (2) $e \cdot x = x \dots$

Theorem 1

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$x^{-1} \cdot x =$$

Theorem 1

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$x^{-1} \cdot x = x^{-1} \cdot (x \cdot e)$$

Theorem 1

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$x^{-1} \cdot x = x^{-1} \cdot (x \cdot e)$$

Theorem 1

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$x^{-1} \cdot x = x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}}))$$

Theorem 1

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$x^{-1} \cdot x = x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}}))$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ &= x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ &= x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ &= x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) = x^{-1} \cdot (e \cdot x^{-1^{-1}}) \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ &= x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) = x^{-1} \cdot (e \cdot x^{-1^{-1}}) \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) &= x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \\ (x^{-1} \cdot e) \cdot x^{-1^{-1}} & \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) &= x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \\ (x^{-1} \cdot e) \cdot x^{-1^{-1}} & \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) &= x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \\ (x^{-1} \cdot e) \cdot x^{-1^{-1}} &= x^{-1} \cdot x^{-1^{-1}} \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) &= x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \\ (x^{-1} \cdot e) \cdot x^{-1^{-1}} &= x^{-1} \cdot x^{-1^{-1}} \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) &= x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \\ (x^{-1} \cdot e) \cdot x^{-1^{-1}} &= x^{-1} \cdot x^{-1^{-1}} = e \end{aligned}$$

Theorem 1

$$\begin{aligned} \forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)} \end{aligned}$$

$$x^{-1} \cdot x = e \tag{1}$$

$$\begin{aligned} x^{-1} \cdot x &= x^{-1} \cdot (x \cdot e) = x^{-1} \cdot (x \cdot (x^{-1} \cdot x^{-1^{-1}})) = \\ x^{-1} \cdot ((x \cdot x^{-1}) \cdot x^{-1^{-1}}) &= x^{-1} \cdot (e \cdot x^{-1^{-1}}) = \\ (x^{-1} \cdot e) \cdot x^{-1^{-1}} &= x^{-1} \cdot x^{-1^{-1}} = e. \end{aligned}$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x)$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x)$$

Theorem 2

$$\forall x, y, z. (x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (\text{assoc})$$

$$\forall x. x \cdot e = x \quad (\text{r-neutr})$$

$$\forall x. x \cdot x^{-1} = e \quad (\text{r-inv})$$

$$e \cdot x = x \quad (2)$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) = x \cdot e \quad (\text{Theorem 1})$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) = x \cdot e$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) = x \cdot e = x$$

Theorem 2

$$\begin{aligned}\forall x, y, z. (x \cdot y) \cdot z &= x \cdot (y \cdot z) && \text{(assoc)} \\ \forall x. x \cdot e &= x && \text{(r-neutr)} \\ \forall x. x \cdot x^{-1} &= e && \text{(r-inv)}\end{aligned}$$

$$e \cdot x = x \tag{2}$$

$$e \cdot x = (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) = x \cdot e = x$$

Lessons Learned from These Examples

Equational proofs are often tricky!

- Equalities used in different directions, “eureka” terms, etc.
- In some cases (the **word problem** is) decidable

Equational versus ND Proofs

- Above proofs were of a particular, equational form.

Equational versus ND Proofs

- Above proofs were of a particular, **equational form**.
- In Isabelle this is accomplished by term rewriting.
Term rewriting is a process for replacing equals by equals (see next lecture).

Equational versus ND Proofs

- Above proofs were of a particular, **equational form**.
- In Isabelle this is accomplished by term rewriting.
Term rewriting is a process for replacing equals by equals (see next lecture).
- Alternative is **natural deduction**:
 - requires explicit proofs using equality rules;
 - tedious in practice. **Try it on above examples!**

Sets

Naive Set Theory: Basics

- A **set** is a collection of objects where order and repetition are unimportant.

Sets are central in mathematical reasoning [Vel94]. E.g., set of prime numbers.

Naive Set Theory: Basics

- A **set** is a collection of objects where order and repetition are unimportant.

Sets are central in mathematical reasoning [Vel94]. E.g., set of prime numbers.

- In what follows we consider a simple, intuitive formalization: “naive set theory”

Naive Set Theory: Basics

- A **set** is a collection of objects where order and repetition are unimportant.

Sets are central in mathematical reasoning [Vel94]. E.g., set of prime numbers.

- In what follows we consider a simple, intuitive formalization: “naive set theory”

We will be somewhat less formal than usual. Our goal is to understand standard mathematical practice.

Naive Set Theory: Basics

- A **set** is a collection of objects where order and repetition are unimportant.

Sets are central in mathematical reasoning [Vel94]. E.g., set of prime numbers.

- In what follows we consider a simple, intuitive formalization: “naive set theory”

We will be somewhat less formal than usual. Our goal is to understand standard mathematical practice.

Later, in HOL, we will be completely formal.

Sets: Language

Assuming any first-order language with equality, we add:

- **set-comprehension** $\{x|P(x)\}$ and a binary **membership predicate** \in .

Sets: Language

Assuming any first-order language with equality, we add:

- **set-comprehension** $\{x|P(x)\}$ and a binary **membership predicate** \in .
- **Term/formula distinction inadequate**: need a syntactic category for sets.

Sets: Language

Assuming any first-order language with equality, we add:

- **set-comprehension** $\{x|P(x)\}$ and a binary **membership predicate** \in .
- **Term/formula distinction inadequate**: need a syntactic category for sets.
- We will be more formal about syntax later (HOL).

Sets: Language

Assuming any first-order language with equality, we add:

- **set-comprehension** $\{x|P(x)\}$ and a binary **membership predicate** \in .
- **Term/formula distinction inadequate**: need a syntactic category for sets.
- We will be more formal about syntax later (HOL).
- Comprehension is a binding operator: x **bound in** $\{x|P(x)\}$.

Examples

- $\forall x. x \in \{y \mid y \bmod 6 = 0\} \rightarrow (x \bmod 2 = 0 \wedge x \bmod 3 = 0)$.

Examples

- $\forall x. x \in \{y \mid y \bmod 6 = 0\} \rightarrow (x \bmod 2 = 0 \wedge x \bmod 3 = 0)$.
- What does the following say?

$$2 \in \{w \mid 6 \notin \{x \mid x \text{ is divisible by } w\}\}$$

Examples

- $\forall x. x \in \{y \mid y \bmod 6 = 0\} \rightarrow (x \bmod 2 = 0 \wedge x \bmod 3 = 0)$.
- What does the following say?

$$2 \in \{w \mid 6 \notin \{x \mid x \text{ is divisible by } w\}\}$$

Answer: $6 \notin \{x \mid x \text{ divisible by } 2\}$ i.e., 6 not divisible by 2.

Proof Rules for Sets

Introduction, elimination, extensional equality

$$\frac{P(t)}{t \in \{x | P(x)\}} \text{ compr_I} \qquad \frac{t \in \{x | P(x)\}}{P(t)} \text{ compr_E}$$

$$\frac{\forall x. x \in A \leftrightarrow x \in B}{A = B} \qquad \frac{A = B}{\forall x. x \in A \leftrightarrow x \in B}$$

Following equivalence is derivable:

$$\forall x. P(x) \leftrightarrow x \in \{y | P(y)\}$$

Digression: Sorted Reasoning

- In mathematical arguments we often (implicitly) assume that variables are restricted to some **universe of discourse**.
E.g., $x^2 < 9$ (universe either \mathcal{R} , \mathcal{N} , . . .)
- To **avoid ambiguity** we can include sort information in formulae:

members x of U where $P(x) \equiv \{x \in U \mid P(x)\}$

Formally

$$\{x \in U \mid P(x)\} \equiv \{x \mid U(x) \wedge P(x)\}.$$

Sorted Reasoning in an Unsorted Logic

We may introduce the additional set comprehension syntax $\{x \in U \mid P(x)\}$, but our logic is still **unsorted**. We have

$$y \in \{x \in U \mid P(x)\} \leftrightarrow y \in \{x \mid U(x) \wedge P(x)\} \leftrightarrow U(y) \wedge P(y)$$

Sorted Quantification

$$\forall x \in U. P(x) \equiv \forall x. U(x) \rightarrow P(x)$$

$$\exists x \in U. P(x) \equiv \exists x. U(x) \wedge P(x)$$

Axiomatizing Operations on Sets

- Functions on sets

$$A \cap B \equiv \{x \mid x \in A \wedge x \in B\}$$

$$A \cup B \equiv \{x \mid x \in A \vee x \in B\}$$

$$A \setminus B \equiv \{x \mid x \in A \wedge x \notin B\}$$

- Predicates on sets

$$A \subseteq B \equiv \forall x. x \in A \rightarrow x \in B$$

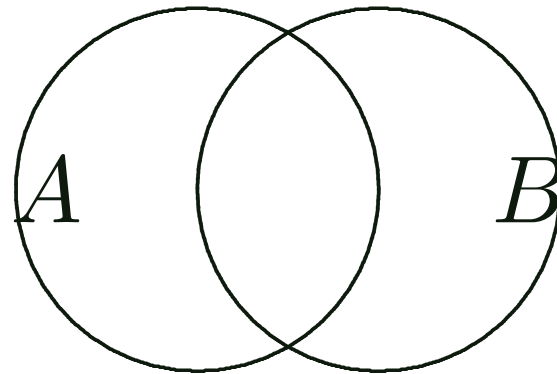
Example of Operations on Sets

Example: $A \equiv \{x \mid x \text{ is a man}\}$, $B \equiv \{x \mid x \text{ has brown hair}\}$.

Example of Operations on Sets

Example: $A \equiv \{x \mid x \text{ is a man}\}$, $B \equiv \{x \mid x \text{ has brown hair}\}$.

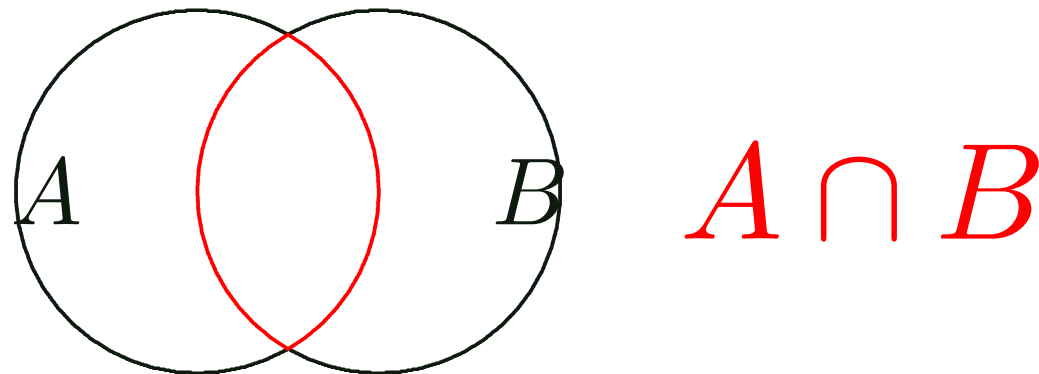
What are $A \cap B$, $A \cup B$, $A \setminus B$?



Example of Operations on Sets

Example: $A \equiv \{x \mid x \text{ is a man}\}$, $B \equiv \{x \mid x \text{ has brown hair}\}$.

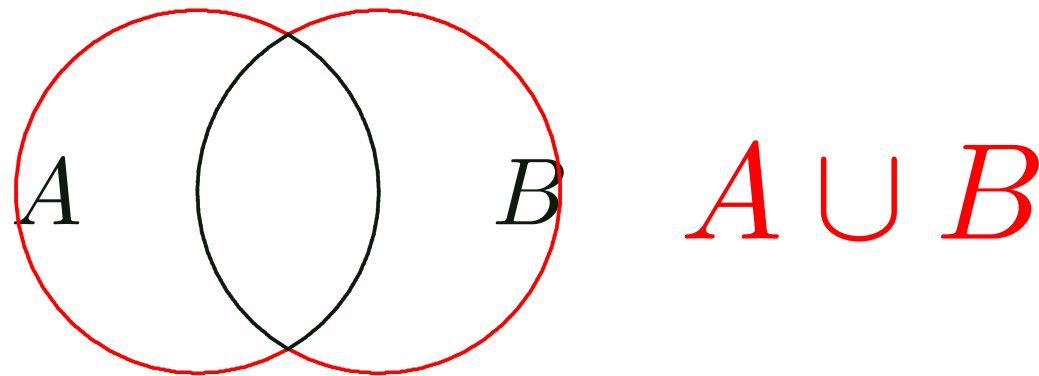
What are $A \cap B$, $A \cup B$, $A \setminus B$?



Example of Operations on Sets

Example: $A \equiv \{x \mid x \text{ is a man}\}$, $B \equiv \{x \mid x \text{ has brown hair}\}$.

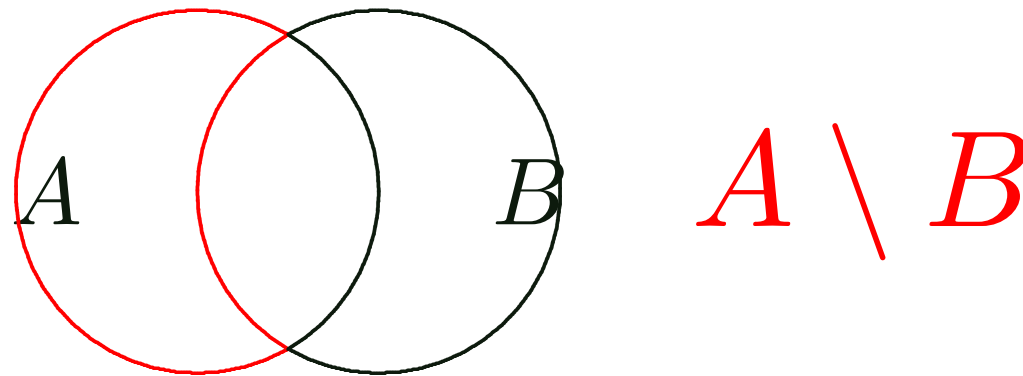
What are $A \cap B$, $A \cup B$, $A \setminus B$?



Example of Operations on Sets

Example: $A \equiv \{x \mid x \text{ is a man}\}$, $B \equiv \{x \mid x \text{ has brown hair}\}$.

What are $A \cap B$, $A \cup B$, $A \setminus B$?



Correspondence between set theoretic and logical operators

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$$

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B$$

$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B$$

These correspondences follow from the definitions of the set-theoretic operators and $\forall x. P(x) \leftrightarrow x \in \{y | P(y)\}$.

Correspondence between set theoretic and logical operators

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$$

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B$$

$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B$$

These correspondences follow from the definitions of the set-theoretic operators and $\forall x. P(x) \leftrightarrow x \in \{y | P(y)\}$.

Example: what is logical structure of $x \in ((A \cap B) \cup (A \cap C))$?

Correspondence between set theoretic and logical operators

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$$

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B$$

$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B$$

These correspondences follow from the definitions of the set-theoretic operators and $\forall x. P(x) \leftrightarrow x \in \{y | P(y)\}$.

Example: what is logical structure of $x \in ((A \cap B) \cup (A \cap C))$?

$$(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$$

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (1)

Venn diagram (Is this a proof?)

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (2)

Natural deduction (refinement style, natural language)

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (2)

Natural deduction ([refinement style](#), natural language)

By [extensionality](#), suffices to show

$$\forall x. x \in A \cap (B \cup C) \leftrightarrow x \in (A \cap B) \cup (A \cap C).$$

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (2)

Natural deduction ([refinement style](#), natural language)

By [extensionality](#), suffices to show

$$\forall x. x \in A \cap (B \cup C) \leftrightarrow x \in (A \cap B) \cup (A \cap C).$$

For an arbitrary x , this is equivalent to establishing

$$\begin{aligned} (x \in A \wedge (x \in B \vee x \in C)) &\leftrightarrow \\ (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \end{aligned}$$

Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (2)

Natural deduction ([refinement style](#), natural language)

By [extensionality](#), suffices to show

$$\forall x. x \in A \cap (B \cup C) \leftrightarrow x \in (A \cap B) \cup (A \cap C).$$

For an arbitrary x , this is equivalent to establishing

$$\begin{aligned} (x \in A \wedge (x \in B \vee x \in C)) &\leftrightarrow \\ (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) & \end{aligned}$$

But that is a propositional tautology.

Same in Isabelle

Last proof carries over to Isabelle: **extensionality**, rewriting, **tautology** checking.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Let x be element of $(A \cup B) \setminus B$.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Let x be element of $(A \cup B) \setminus B$.

So $(x \in A \vee x \in B) \wedge \neg x \in B$.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Let x be element of $(A \cup B) \setminus B$.

So $(x \in A \vee x \in B) \wedge \neg x \in B$.

Therefore $x \in A$.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Let x be element of $(A \cup B) \setminus B$.

So $(x \in A \vee x \in B) \wedge \neg x \in B$.

Therefore $x \in A$.

Therefore $x \in (A \cup B) \setminus B \rightarrow x \in A$.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Let x be element of $(A \cup B) \setminus B$.

So $(x \in A \vee x \in B) \wedge \neg x \in B$.

Therefore $x \in A$.

Therefore $x \in (A \cup B) \setminus B \rightarrow x \in A$.

Therefore $((A \cup B) \setminus B) \subseteq A$.

Prove: for all sets A and B , $((A \cup B) \setminus B) \subseteq A$

Not obvious? Just follow your nose!

Let A and B be arbitrary sets.

Let x be element of $(A \cup B) \setminus B$.

So $(x \in A \vee x \in B) \wedge \neg x \in B$.

Therefore $x \in A$.

Therefore $x \in (A \cup B) \setminus B \rightarrow x \in A$.

Therefore $((A \cup B) \setminus B) \subseteq A$.

This semi-formal proof combines forward reasoning (first step) with backward reasoning. This is common in practice and usually easy to unscramble.

Extending Set Comprehensions

Recall set comprehensions $\{x \mid P(x)\}$.

Extending Set Comprehensions

Recall set comprehensions $\{x|P(x)\}$.

Now what do you think this is?

$$\{f(x)|P(x)\}$$

Extending Set Comprehensions

Recall set comprehensions $\{x|P(x)\}$.

Now what do you think this is?

$$\{f(x)|P(x)\} \equiv \{y|\exists x. P(x) \wedge y = f(x)\}$$

Extending Set Comprehensions

Recall set comprehensions $\{x|P(x)\}$.

Now what do you think this is?

$$\{f(x)|P(x)\} \equiv \{y|\exists x. P(x) \wedge y = f(x)\}$$

Example: $t \in \{x^2|x > 5\}$ equivalent to

Extending Set Comprehensions

Recall **set comprehensions** $\{x|P(x)\}$.

Now what do you think this is?

$$\{f(x)|P(x)\} \equiv \{y|\exists x. P(x) \wedge y = f(x)\}$$

Example: $t \in \{x^2|x > 5\}$ **equivalent to** $\exists x. x > 5 \wedge t = x^2$.

True for $t \in \{36, 49, \dots\}$

Indexing

Sometimes, it is natural to view and denote a function f applied to an argument x as “ f indexed by x ”, so f_x , rather than $f(x)$.

Indexing

Sometimes, it is natural to view and denote a function f applied to an argument x as “ f indexed by x ”, so f_x , rather than $f(x)$.

Example: let S = set of students and let m_s stand for “the mother of s ”, for s a student. Call S an **index set**. Define $M = \{m_s | s \in S\}$

$$x \in M \iff x \in \{y | \exists s. s \in S \wedge y = m_s\}$$

$$\iff \exists s. s \in S \wedge x = m_s$$

$$\iff \exists s \in S. x = m_s$$

Logical Forms of the New Notation

Question: what is the logical form of $\{x_i | i \in I\} \subseteq A$?

Logical Forms of the New Notation

Question: what is the logical form of $\{x_i | i \in I\} \subseteq A$?

$$\forall x. x \in \{x_i | i \in I\} \rightarrow x \in A, \quad \text{i.e.,}$$

$$\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A.$$

Logical Forms of the New Notation

Question: what is the logical form of $\{x_i | i \in I\} \subseteq A$?

$$\forall x. x \in \{x_i | i \in I\} \rightarrow x \in A, \quad \text{i.e.,}$$

$$\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A.$$

Intuition suggests that $\forall i \in I. x_i \in A$ is also correct, i.e.,

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A).$$

Proof

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

Proof

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

- “ \rightarrow ”

Let $i \in I$ be given. Now from assumption (for instance x_i) we have $(\exists j \in I. x_i = x_j) \rightarrow x_i \in A$. But premise is true for $i = j$, so $x_i \in A$.

Proof

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

- “ \rightarrow ”

Let $i \in I$ be given. Now from assumption (for instance x_i) we have $(\exists j \in I. x_i = x_j) \rightarrow x_i \in A$. But premise is true for $i = j$, so $x_i \in A$.

- “ \leftarrow ”

Let x be given and assume $\exists i \in I. x = x_i$. So for some $i \in I$, we have $x = x_i$. Now $\forall i \in I. x_i \in A$. Hence $x \in A$.

Indexed Families

Can formulate sets as **indexed families**.

Let S = set of students, C_s = courses taken by student s .
 $\{C_s | s \in S\}$ is set whose elements are those sets of courses taken by some student.

Logical Forms of Powersets

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

What is the logical form of:

1. $x \in \mathcal{P}(A)$?

Logical Forms of Powersets

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

What is the logical form of:

1. $x \in \mathcal{P}(A)$?

$$x \subseteq A, \text{ i.e., } \forall y. (y \in x \rightarrow y \in A)$$

2. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$?

Logical Forms of Powersets

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

What is the logical form of:

1. $x \in \mathcal{P}(A)$?

$$x \subseteq A, \text{ i.e., } \forall y. (y \in x \rightarrow y \in A)$$

2. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$?

$$\forall x. x \in \mathcal{P}(A) \rightarrow x \in \mathcal{P}(B), \text{ i.e.,}$$

$$\forall x. (\forall y. y \in x \rightarrow y \in A) \rightarrow (\forall y. y \in x \rightarrow y \in B)$$

Logical Forms of Powersets

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

What is the logical form of:

1. $x \in \mathcal{P}(A)$?

$$x \subseteq A, \text{ i.e., } \forall y. (y \in x \rightarrow y \in A)$$

2. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$?

$$\forall x. x \in \mathcal{P}(A) \rightarrow x \in \mathcal{P}(B), \text{ i.e.,}$$

$$\forall x. (\forall y. y \in x \rightarrow y \in A) \rightarrow (\forall y. y \in x \rightarrow y \in B)$$

Exercise: prove that the last answer is equivalent to $A \subseteq B$, i.e., $\forall x. x \in A \rightarrow x \in B$.

Problems in Paradise?

Sets can have other sets as elements.

Implicitly assume that universe of discourse is **collection** of all sets.

Russell's Paradox

Suppose $U := \{x \mid \top\}$. Then $U \in U$.

Quite strange but no contradiction yet.

Russell's Paradox

Suppose $U := \{x \mid \top\}$. Then $U \in U$.

Quite strange but no contradiction yet.

Now split sets into two categories:

1. unusual sets like U that are elements of themselves, and
2. more typical sets that are not.

Russell's Paradox

Suppose $U := \{x \mid \top\}$. Then $U \in U$.

Quite strange but no contradiction yet.

Now split sets into two categories:

1. unusual sets like U that are elements of themselves, and
2. more typical sets that are not.

Let $R := \{A \mid A \notin A\}$.

Logical characterization is: $\forall A. (A \in R \leftrightarrow A \notin A)$

Russell's Paradox

Suppose $U := \{x \mid \top\}$. Then $U \in U$.

Quite strange but no contradiction yet.

Now split sets into two categories:

1. unusual sets like U that are elements of themselves, and
2. more typical sets that are not.

Let $R := \{A \mid A \notin A\}$.

Logical characterization is: $\forall A. (A \in R \leftrightarrow A \notin A)$

Substituting R for A (\forall -E) yields $R \in R \leftrightarrow R \notin R$, which is a logical contradiction. **What does this tell us about sets?**

Where Do We Go from here?

- Automation: lifting the level of argumentation up from individual ND steps to larger “natural” ND steps.

Where Do We Go from here?

- Automation: lifting the level of argumentation up from individual ND steps to larger “natural” ND steps.
- Formalization: less naive \implies take extensions seriously!

Where Do We Go from here?

- Automation: lifting the level of argumentation up from individual ND steps to larger “natural” ND steps.
- Formalization: less naive \implies take extensions seriously!

Metatheory: The theory of formalization

HOL: Higher-order logic and conservative extensions thereof

Where Do We Go from here?

- Automation: lifting the level of argumentation up from individual ND steps to larger “natural” ND steps.
- Formalization: less naive \implies take extensions seriously!

Metatheory: The theory of formalization

HOL: Higher-order logic and conservative extensions thereof

- Modeling and reasoning in action!

References

[Vel94] Daniel J. Velleman. *How to Prove It*. Cambridge University Press, 1994.

More Detailed Explanations

Logical vs. Non-logical Symbols

In logic languages, it is common to distinguish between **logical** and **non-logical** symbols. We explain this for first-order logic.

Recall that there isn't just **the** language of first-order logic, but rather defining a particular signature gives us **a** first-order language. The **logical** symbols are those that are part of **any** first-order language and whose meaning is “hard-wired” into the formalism of first-order logic, like \wedge or \forall . The **non-logical** symbols are those given by a particular **signature**, and whose meaning must be defined “by the user” by giving a **structure**.

Above we say “mathematical” instead of “non-logical” because we assume that mathematics is our domain of discourse, so that the **signature** contains the symbols of “mathematics”.

Now what status should the equality symbol $=$ have? We will assume

that $=$ is a symbol whose meaning is hard-wired into the formalism. One then speaks of **first-order logic with equality**.

Alternatively, one could regard $=$ as an ordinary (binary infix) predicate. However, even if one does not give $=$ a special status, anyone reading $=$ has a certain expectation. Thus it would be very confusing to have a structure that defines $=$ as a, say, non-reflexive relation.

Three Different Uses of Equality

$$I_{\mathcal{A}}(s=t) = \begin{cases} 1 & I_{\mathcal{A}}(s)=I_{\mathcal{A}}(t) \\ 0 & \text{otherwise} \end{cases}$$

The first $=$ is a predicate symbol.

Three Different Uses of Equality

$$I_{\mathcal{A}}(s=t) = \begin{cases} 1 & I_{\mathcal{A}}(s)=I_{\mathcal{A}}(t) \\ 0 & \text{otherwise} \end{cases}$$

The first $=$ is a predicate symbol.

The second $=$ is a **definitional** occurrence: The expression on the left-hand side is **defined** to be equal to the value of the right-hand side.

Three Different Uses of Equality

$$I_{\mathcal{A}}(s=t) = \begin{cases} 1 & I_{\mathcal{A}}(s) = I_{\mathcal{A}}(t) \\ 0 & \text{otherwise} \end{cases}$$

The first $=$ is a predicate symbol.

The second $=$ is a **definitional** occurrence: The expression on the left-hand side is **defined** to be equal to the value of the right-hand side.

The third $=$ is **semantic** equality, i.e., **the identity relation on the domain**.

Why Rules?

Since $=$ is a logical symbol in the formalism of first-order logic with equality, there should be **derivation rules** for $=$ to derive which formulas $a = b$ are true.

What is an Equivalence Relation?

In general mathematical terminology, a relation \equiv is an **equivalence relation** if the following three properties hold:

Reflexivity: $a \equiv a$ for all a ;

Symmetry: $a \equiv b$ implies $b \equiv a$;

Transitivity: $a \equiv b$ and $b \equiv c$ implies $a \equiv c$.

Example: being equal modulo 6.

“ a is equal b modulo 6” is often written $a \equiv b \pmod{6}$.

What is a Congruence?

In general mathematical terminology, a relation \cong is a **congruence w.r.t.** (or: **on**) f , where f has arity n , if $a_1 \cong b_1, \dots, a_n \cong b_n$ implies $f(a_1, \dots, a_n) \cong f(b_1, \dots, b_n)$.

Example: being equal modulo 6 is congruent w.r.t. multiplication.

$14 \equiv 8 \pmod{6}$ and $15 \equiv 9 \pmod{6}$, hence $14 \cdot 15 \equiv 8 \cdot 9 \pmod{6}$.

This can be defined in an analogous way for a property (relation) P .

Example: being equal modulo 6 is congruent w.r.t. divisibility by 3.

$15 \equiv 9 \pmod{6}$ and 15 is divisible by 3, hence 9 is divisible by 3.

$14 \equiv 8 \pmod{6}$ and 14 is not divisible by 3, hence 8 is not divisible by 3.

What Does this Notation Mean?

Why did we use letters t and A here?

Recall the rules for building **terms** and **atoms**.

Is $t(x_1, \dots, x_n)$ a term, and $A(x_1, \dots, x_n)$ an atom, obtained by one application of such a rule, i.e.: is t a function symbol in \mathcal{F} , applied to x_1, \dots, x_n , and is A a predicate symbol in \mathcal{P} , applied to x_1, \dots, x_n ?

What Does this Notation Mean?

Why did we use letters t and A here?

Recall the rules for building **terms** and **atoms**.

Is $t(x_1, \dots, x_n)$ a term, and $A(x_1, \dots, x_n)$ an atom, obtained by one application of such a rule, i.e.: is t a function symbol in \mathcal{F} , applied to x_1, \dots, x_n , and is A a predicate symbol in \mathcal{P} , applied to x_1, \dots, x_n ?

In general, no! The notations $t(x_1, \dots, x_n)$ and $A(x_1, \dots, x_n)$ are **metanotations**. $t(x_1, \dots, x_n)$ stands for any term in which x_1, \dots, x_n occur, and $A(x_1, \dots, x_n)$ stands for any atom in which x_1, \dots, x_n occur.

This is why we used letters t (term) and A (atom) here instead of f (function) and P (predicate).

And in this context, the notation $t(y_1, \dots, y_n)$ stands for the term obtained from $t(x_1, \dots, x_n)$ by replacing all occurrences of x_1 with y_1

and so forth. In analogy the notation $A(y_1, \dots, y_n)$ is defined.

Note that in the schematic formulation of the rule, we use letters x and y to suggest variables, but the rule applies to arbitrary terms.

This description is not very formal, but this is not too problematic since we will be more formal once we have some useful machinery for this at hand.

Soundness of Equivalence Rules

On the semantic level, two things are equal if they are identical. Semantic equality is an **equivalence relation**. This semantic fact is so fundamental that we cannot explain it any further.

So one can prove that $I_{\mathcal{A}}(s = s) = 1$ for all all terms s , because $I_{\mathcal{A}}(s) = I_{\mathcal{A}}(s)$ for all terms, and likewise for symmetry and transitivity.

Soundness of Congruence Rules

If $t(x)$ is a term containing x and $t(y)$ is the term obtained from $t(x)$ by replacing all occurrences of x with y , and moreover $I_{\mathcal{A}}(x = y) = 1$, then $I_{\mathcal{A}}(x) = I_{\mathcal{A}}(y)$. One can show by induction on the structure of t that $I_{\mathcal{A}}(t(x)) = I_{\mathcal{A}}(t(y))$.

So by “truth-functional” we mean that the value $I_{\mathcal{A}}(t(x))$ depends on $I_{\mathcal{A}}(x)$, not on x itself.

This can be generalized to n variables as in the rule.

An analogous proof can be done for rule $cong_2$.

Replacing Some Occurrences

The notation $t[x_1, \dots, x_n/z_1, \dots, z_n]$ stands for the term obtained from t by simultaneously replacing each z_i ($i \in \{1, \dots, n\}$) with x_i .

$[x_1, \dots, x_n/z_1, \dots, z_n]$ is called a **substitution**.

To have an unambiguous notation for “replacing some occurrences of x_1, \dots, x_n ”, we start from a term t containing variable occurrences z_1, \dots, z_n . On the LHS, these are replaced with x_1, \dots, x_n , on the RHS they are replaced with y_1, \dots, y_n . So on the RHS we have a term obtained from the one on the LHS by replacing some occurrences of x_1, \dots, x_n with y_1, \dots, y_n .

One can say that the z_1, \dots, z_n are introduced to **mark** the occurrences of x_1, \dots, x_n that should be replaced by y_1, \dots, y_n .

Note that in the schematic formulation of the rule, we use letters x and

y to suggest variables, but the rule applies to arbitrary terms. The z 's however are variables (substitutions replace variables, not arbitrary terms).

Example: $x^2 + y^2 > 12x$

The atom $x^2 + y^2 > 12x$ contains two occurrences of x . There are four ways to choose some occurrences of x in $x^2 + y^2 > 12x$.

Each of those ways corresponds to an atom obtained from $x^2 + y^2 > 12x$ by replacing some occurrences of x with z . That is, there are four different A 's such that $A[x/z] = x^2 + y^2 > 12x$. Now the atom above the line in the examples is obtained by substituting x for z , and the atom below the line is obtained by substituting y for z .

Isabelle Rule

The Isabelle FOL rule is:

$$\frac{x = y \quad P(x)}{P(y)} \textit{subst}$$

In this rule, P is an Isabelle [metavariable](#).

Why doesn't the Isabelle rule contain a z to [mark](#) which occurrences should be replaced?

We cannot understand this yet, but think of P as a formula where some positions are marked in such a way that once we apply P to t (we write $P(t)$), t will be inserted into all those positions. This is why $P(x)$ is a formula and $P(y)$ is a formula obtained by replacing some occurrences of x with y .

Why Are All Functions in a Structure Total?

If we allowed functions in a **structure** not to be total, then for some terms t , $\mathcal{A}(t)$ would be undefined.

For such a term, $\exists x. t = x$ would not be true.

Theories

Recall our [intuitive explanation of theories](#).

A theory involves certain function and/or predicate symbols for which certain “laws” hold.

Depending on the context, these symbols may co-exist with other symbols.

Technically, the laws are added as rules (in particular, axioms) to the [proof system](#).

A [structure](#) in which these rules are true is then called a [model](#) of the rules.

Partial Orders

A partial order is a binary relation that is reflexive, transitive, and anti-symmetric: $a \leq b$ and $b \leq a$ implies $a = b$.

A Language Consisting of \leq ?

\leq is (by convention) a binary infix predicate symbol.

The theory of **partial orders** involves only this symbol, but that does not mean that there could not be any other symbols in the context.

What Is an Axiom?

An **axiom** is a rule without premises.

We call a rule with premises **proper**.

Antisymmetry and Reflexivity

Note that $\forall x, y. x \leq y \wedge y \leq x \leftrightarrow x = y$ encodes both antisymmetry (\rightarrow) and reflexivity (\leftarrow). Recall that $A \leftrightarrow B$ as shorthand for $A \rightarrow B \wedge B \rightarrow A$.

Axioms vs. Rules

One can see that using $\rightarrow-I$ and $\rightarrow-E$, one can always convert a proof using the axioms to one using the **proper** rules.

More generally, an axiom of the form $\forall x_1, \dots, x_n. A_1 \wedge \dots \wedge A_n \rightarrow B$ can be converted to a rule

$$\frac{A_1 \quad \dots \quad A_n}{B} .$$

Linear and Dense Orders

We define these notions in a usual mathematical terminology.

A partial order \leq is **linear** or **total** if for all a, b , either $a \leq b$ or $b \leq a$.

A partial order \leq is **dense** if for all a, b where $a < b$, there exists a c such that $a < c$ and $c < b$.

“Pure” Rule Formulation

The axiom $\forall x, y. x \leq y \vee y \leq x$ cannot be phrased as a **proper** rule in the style of, for example, the **transitivity axiom**.

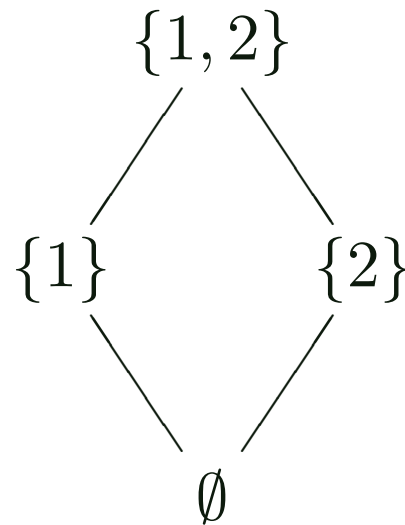
$<$

We use $s < t$ as shorthand for $s \leq t \wedge \neg s = t$.

We say that $<$ is the **strict** part of the **partial order** \leq .

The \subseteq -Relation

The \subseteq -relation is partial but not total. As an example, consider the \subseteq -relation on the set of subsets of $\{1, 2\}$.



Depicting **partial orders** by a such a graph is quite common. Here, node a is below node b and connected by an arc if and only if $a < b$ and there exists no c with $a < c < b$.

In this example, we have the **partial order**

$$\{(\emptyset, \emptyset), (\{1\}, \{1\}), (\{1\}, \{1\}), (\{1, 2\}, \{1, 2\}), (\emptyset, \{1\}), (\emptyset, \{1\}), (\{1\}, \{1, 2\}), (\{1\}, \{1, 2\})\}.$$

Group Language

$_ \cdot _$ is a binary infix function symbol (in fact, only \cdot is the symbol, but the notation $_ \cdot _$ is used to indicate the fact that the symbol stands between its arguments).

$_^{-1}$ is a unary function symbol written as superscript. Again, the $_$ is used to indicate where the argument goes.

e is a **nullary function symbol (= constant)**.

Note that groups are very common in mathematics, and many different notations, i.e., function names and fixity (infix, prefix. . .) are used for them.

Groups

In general mathematical terminology, a **group** consists of three function symbols \cdot , $^{-1}$, e , obeying the following laws:

Associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c ,

Right neutral $a \cdot e = a$ for all a ,

Right inverse $a \cdot a^{-1} = e$ for all a .

A Model a Group?

A **model** of the group axioms is a **structure** in which the group axioms are true.

However, when we say something like, “this model **is** a group”, then this is a slight abuse of terminology, since there may be other function symbols around that are also interpreted by the structure.

So when we say “this model **is** a group”, we mean, “this model is a model of the group axioms for function symbols \cdot , $^{-1}$, and e clear from the context”.

“Eureka” terms

By “eureka” terms we mean terms that have to be guessed in order to find a proof. At least at first sight, it seems like these terms simply fall from the sky.

The Greek **Heureka** is 1st person singular perfect of **heuriskō**, “to find”. It was exclaimed by Archimedes upon discovering how to test the purity of Hiero’s crown.

The Word Problem

The word problem w.r.t. a theory (here: the group axioms) is the problem of deciding whether two terms s and t are equal in the theory, that is to say, whether the formula $s = t$ is true in any **model** of the theory.

Equational Proofs

An equational proof consists simply of a sequence of equations, written as $t_1 = t_2 = \dots = t_n$, where each t_{i+1} is obtained from t_i by replacing some subterm s with a term s' , provided the equality $s = s'$ holds.

This style of proof can be justified by the rules given for equality, in particular the [congruences](#). However, it looks very different from the [natural deduction style](#).

Proof of Theorem 2 by Natural Deduction

$$e \cdot x = x$$

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 by Natural Deduction

$$x \cdot e = x$$

$$e \cdot x = x \cdot e$$

$$e \cdot x = x$$

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 by Natural Deduction

r-neutr

$$x \cdot e = x$$

$$e \cdot x = x \cdot e$$

$$e \cdot x = x$$

Most steps use the congruence rule $cong_2$.

Proof of Theorem 2 by Natural Deduction

r-neutr	$x^{-1} \cdot x = e$	$e \cdot x = x \cdot (x^{-1} \cdot x)$
$x \cdot e = x$	$e \cdot x = x \cdot e$	
	$e \cdot x = x$	

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 by Natural Deduction

	<u>Theorem 1</u>	
$r\text{-neutr}$	$x^{-1} \cdot x = e$	$e \cdot x = x \cdot (x^{-1} \cdot x)$
$x \cdot e = x$	$e \cdot x = x \cdot e$	
	$e \cdot x = x$	

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 by Natural Deduction

	Theorem 1	$(x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x)$	$e \cdot x = (x \cdot x^{-1}) \cdot x$
r-neutr	$x^{-1} \cdot x = e$	$e \cdot x = x \cdot (x^{-1} \cdot x)$	
$x \cdot e = x$		$e \cdot x = x \cdot e$	
	$e \cdot x = x$		

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 by Natural Deduction

$$\begin{array}{c}
 \boxed{\text{r-neutr}} \\
 \hline
 x \cdot e = x \\
 \hline
 \text{Theorem 1} \\
 \hline
 x^{-1} \cdot x = e \\
 \hline
 \boxed{\text{assoc}} \\
 \hline
 \frac{(x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) \quad e \cdot x = (x \cdot x^{-1}) \cdot x}{e \cdot x = x \cdot (x^{-1} \cdot x)} \\
 \hline
 \frac{x \cdot e = x \quad e \cdot x = x \cdot e}{e \cdot x = x}
 \end{array}$$

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 by Natural Deduction

	assoc	next slide
r-neutr	Theorem 1	$(x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x)$
$x \cdot e = x$	$x^{-1} \cdot x = e$	$e \cdot x = (x \cdot x^{-1}) \cdot x$
$x \cdot e = x$	$e \cdot x = x \cdot (x^{-1} \cdot x)$	$e \cdot x = x \cdot e$
$x \cdot e = x$	$e \cdot x = x \cdot e$	$e \cdot x = x$

Most steps use the congruence rule *cong*₂.

Proof of Theorem 2 (Cont.)

$$e \cdot x = (x \cdot x^{-1}) \cdot x$$

Proof of Theorem 2 (Cont.)

$$\frac{\frac{}{e = x \cdot x^{-1}} \text{sym} \quad \frac{}{e \cdot x = e \cdot x} \text{refl}}{e \cdot x = (x \cdot x^{-1}) \cdot x}$$

Proof of Theorem 2 (Cont.)

$$\frac{\boxed{\text{r-inv}}}{x \cdot x^{-1} = e} \quad \frac{}{e \cdot x = e \cdot x} \text{ refl}$$
$$\frac{}{e = x \cdot x^{-1}} \text{ sym} \quad \frac{}{e \cdot x = e \cdot x} \text{ refl}$$
$$\frac{}{e \cdot x = (x \cdot x^{-1}) \cdot x}$$

Proof of Theorem 2 by Natural Deduction, Complete

$$\begin{array}{c}
 \boxed{\text{r-neutr}} \\
 \hline
 x \cdot e = x \\
 \hline
 \boxed{\text{r-neutr}} \\
 \hline
 x^{-1} \cdot x = e \\
 \hline
 \text{Theorem 1} \\
 \hline
 (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) \\
 \hline
 \boxed{\text{assoc}} \\
 \hline
 (x \cdot x^{-1}) \cdot x = x \cdot (x^{-1} \cdot x) \\
 \hline
 \boxed{\text{r-inv}} \\
 \hline
 (x \cdot x^{-1}) = e \\
 \hline
 e = (x \cdot x^{-1}) \quad \text{sym} \quad \hline
 e \cdot x = e \cdot x \quad \text{refl} \\
 \hline
 e \cdot x = (x \cdot x^{-1}) \cdot x \\
 \hline
 e \cdot x = x \cdot (x^{-1} \cdot x) \\
 \hline
 e \cdot x = x \cdot e \\
 \hline
 e \cdot x = x
 \end{array}$$

Axioms

Each framed box in the derivation tree stands for a sub-tree consisting of a **group axiom** and possibly several applications of \forall - E .

Set Comprehension

Set comprehension is a way of defining sets. $\{x|P(x)\}$ stands for the set of elements of the universe for which $P(x)$ (some formula usually containing x) holds.

Is a Set a Term?

It is more adequate to regard a set as a term than as a formula. A set is a “thing”, not a statement about “things”.

After all, we have the predicate \in expecting a set on the RHS (and even the LHS may be a set!), and predicates take terms as arguments.

However, the syntax used in set comprehensions is not legal syntax for terms, since $P(x)$ is a formula.

This is why we introduce a special syntactic category for sets.

Extensional Equality

Two things are **extensionally equal** if they are “equal in their effects”. Thus two sets are equal if they have the same members, regardless of what syntactic expressions are used to define those sets. Note that extensional equality may be undecidable.

Deriving Equivalence for Comprehensions

$$\begin{array}{c}
 \frac{[P(x)]^1}{x \in \{y|P(y)\}} \text{ compr_I} \qquad \frac{[x \in \{y|P(y)\}]^2}{P(x)} \text{ compr_E} \\
 \hline
 \frac{P(x) \rightarrow x \in \{y|P(y)\}}{\rightarrow\text{-I}^1} \qquad \frac{x \in \{y|P(y)\} \rightarrow P(x)}{\rightarrow\text{-I}^2} \\
 \hline
 \frac{P(x) \rightarrow x \in \{y|P(y)\} \wedge x \in \{y|P(y)\} \rightarrow P(x)}{\wedge\text{-I}} \\
 \hline
 \frac{P(x) \leftrightarrow x \in \{y|P(y)\}}{\text{iff}} \\
 \hline
 \frac{P(x) \leftrightarrow x \in \{y|P(y)\}}{\forall x. P(x) \leftrightarrow x \in \{y|P(y)\}} \forall\text{-I}
 \end{array}$$

Rules $\wedge\text{-I}$, $\rightarrow\text{-I}$, $\forall\text{-I}$ were defined in previous lectures. The step marked with **iff** is not a proof step in the technical sense. We only make the expansion of a shorthand notation explicit.

Universes

We already know what a **universe** or **domain** is. To interpret a particular language, we have a **structure** interpreting all function symbols as functions on the universe.

However, it is often adequate to subdivide the universe into several “sub-universes”. Those are called **sorts**. Note that a sort is a set.

For example, in a usual mathematical context, one may distinguish \mathcal{R} (the real numbers) and \mathcal{N} (the natural numbers) to say that \sqrt{x} requires x to be of sort \mathcal{R} and $x!$ requires x to be of sort \mathcal{N} .

Avoiding Ambiguity

We want to make explicit the sort of the variable in question. So we do not want the set of all x such that $P(x)$ holds, but only the ones of the right sort, so the ones for which $x \in U$ (U being the sort/universe) holds. Note there is a certain confusion here, since we write $x \in U$ in one place (so U should be a set) and $U(x)$ in another (so U should be a predicate). This confusion is deliberate and quite common. One can identify a set (sort) U with a unary predicate U such that $U(t)$ is interpreted as *True* iff t is a member of U .

The whole expression $\{x \in U | P(x)\}$ is a special kind of syntax. Therefore, you must look at it as a whole: it makes no sense to see any meaning just in, say, the bit $x \in U$ in this expression. It is called **set**

comprehension, and it is defined by

$$\{x \in U \mid P(x)\} \equiv \{x \mid U(x) \wedge P(x)\}.$$

Sorted Logic

In sorted logic, sorts are part of the syntax. So the **signature** contains a fixed set of sorts. For each constant, it is specified what its sort is. For each function symbol, it is specified what the sort of each argument is, and what the sort of the result is. For each predicate symbol, it is specified what the sort of each argument is.

Terms and formulas that do not respect the sorts are not well-formed, and so they are not assigned a meaning.

In contrast, our logic is unsorted. The special syntax we provide for sorted reasoning is just **syntactic sugar**, i.e., we use it as shorthand and since it has an intuitive reasoning, but it has no impact on how expressive our logic is.

Syntactic Sugar

For any formal language (programming language, logic, etc.), the term “syntactic sugar” refers to syntax that is provided for the sake of readability and brevity, but which does not affect the expressiveness of the language.

It is usually a good idea to consider the language without the syntactic sugar for any theoretical considerations about the language, since it makes the language simpler and the considerations less error-prone. However, the correspondence between the syntactic sugar and the basic syntax should be stated formally.

Sorted Quantification

So $\forall x \in U. P(x)$ is simply a shorthand or **syntactic sugar** for $\forall x. x \in U \rightarrow P(x)$, and analogously for $\exists x \in U. P(x)$.

Set Functions

\cap is called **intersection**.

\cup is called **union**.

\setminus is called **set difference**.

\subseteq is called **inclusion**.

Is a Venn Diagram a Proof?

A **Venn diagram** draws sets as bubbles. Intersecting sets are drawn as overlapping bubbles, and the overlapping area is meant to depict the intersection of the sets.

A Venn diagram is not a proof in the sense defined [earlier](#).

Moreover, it would not even be acceptable as a proof according to usual mathematical practice. If it is unknown whether two sets have a non-empty intersection, how are we supposed to draw them? Trying to make a case distinctions (drawing several diagrams depending on the cases) is error-prone.

Venn diagrams are useful for illustration purposes, but they are not proofs.

Natural Language

We intersperse formal notation with natural language here in order to give an intuitive and short proof.

We can also do this more formally in Isabelle.

Explanations for Each Step

Let A and B be arbitrary sets.

$(\forall\text{-I})$

Explanations for Each Step

Let A and B be arbitrary sets.

(\forall -I)

Let x be an element of $(A \cup B) \setminus B$

(Temporary assumption)

Explanations for Each Step

Let A and B be arbitrary sets.

(\forall -I)

Let x be an element of $(A \cup B) \setminus B$

(Temporary assumption)

So $(x \in A \vee x \in B) \wedge \neg x \in B$

(equivalent proposition)

Explanations for Each Step

Let A and B be arbitrary sets. (\forall -I)

Let x be an element of $(A \cup B) \setminus B$ (Temporary assumption)

So $(x \in A \vee x \in B) \wedge \neg x \in B$ (equivalent proposition)

Therefore $x \in A$ (P follows from $(P \vee Q) \wedge \neg Q$)

Explanations for Each Step

Let A and B be arbitrary sets. (\forall -I)

Let x be an element of $(A \cup B) \setminus B$ (Temporary assumption)

So $(x \in A \vee x \in B) \wedge \neg x \in B$ (equivalent proposition)

Therefore $x \in A$ (P follows from $(P \vee Q) \wedge \neg Q$)

Therefore $x \in (A \cup B) \setminus B \rightarrow x \in A$ (\rightarrow -I)

Explanations for Each Step

Let A and B be arbitrary sets.	(\forall -I)
Let x be an element of $(A \cup B) \setminus B$	(Temporary assumption)
So $(x \in A \vee x \in B) \wedge \neg x \in B$	(equivalent proposition)
Therefore $x \in A$	(P follows from $(P \vee Q) \wedge \neg Q$)
Therefore $x \in (A \cup B) \setminus B \rightarrow x \in A$	(\rightarrow -I)
Therefore $((A \cup B) \setminus B) \subseteq A$	(def of \subseteq)

Explanations for Each Step

Let A and B be arbitrary sets.	(\forall -I)
Let x be an element of $(A \cup B) \setminus B$	(Temporary assumption)
So $(x \in A \vee x \in B) \wedge \neg x \in B$	(equivalent proposition)
Therefore $x \in A$	(P follows from $(P \vee Q) \wedge \neg Q$)
Therefore $x \in (A \cup B) \setminus B \rightarrow x \in A$	(\rightarrow -I)
Therefore $((A \cup B) \setminus B) \subseteq A$	(def of \subseteq)

Definition of \subseteq

$$\{x_i | i \in I\} \subseteq A \equiv \forall x. x \in \{x_i | i \in I\} \rightarrow x \in A$$

follows from the definition of \subseteq .

Details of Logical Form

We want to show

$$\forall x. x \in \{x_i | i \in I\} \rightarrow x \in A \equiv \forall x. (\exists i \in I. x = x_i) \rightarrow x \in A$$

$$\begin{aligned} x \in \{x_i | i \in I\} &\equiv \text{(def. of notation)} \\ x \in \{y | \exists i. i \in I \wedge y = x_i\} &\equiv \text{(Compr. elim.)} \\ \exists i. i \in I \wedge x = x_i &\equiv \text{(Sorted quantification)} \\ \exists i \in I. x = x_i & \end{aligned}$$

Intuition for Indexed Sets

It may be helpful to pronounce both forms out loud in natural language to get an intuitive feeling that they are equivalent.

→ in More Detail

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

→ in More Detail

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

We show $\forall i \in I. x_i \in A$ assuming $\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A$.

So we show that for **arbitrary** $i \in I$, assuming

$\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A$, we have $x_i \in A$. So let $i \in I$ be arbitrary.

Since we have $\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A$, by rule **\forall -E** we can

specialize to $(\exists j \in I. x_i = x_j) \rightarrow x_i \in A$. But premise $(\exists j \in I. x_i = x_j)$ is true for $i = j$, and so $x_i \in A$, which is what was to be proven.

This proof could be made more formal by drawing a proof tree or using Isabelle.

← in More Detail

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

← in More Detail

Want to prove

$$(\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A) \leftrightarrow (\forall i \in I. x_i \in A)$$

We show $\forall x. (\exists i \in I. x = x_i) \rightarrow x \in A$, assuming $\forall i \in I. x_i \in A$.

So we show that for **arbitrary** x , assuming $\forall i \in I. x_i \in A$, we have

$(\exists i \in I. x = x_i) \rightarrow x \in A$. So let x be arbitrary.

To show $(\exists i \in I. x = x_i) \rightarrow x \in A$, assume $\exists i \in I. x = x_i$. So for some $i \in I$, we have $x = x_i$. Now by our earlier assumption $\forall i \in I. x_i \in A$,

and so it follows that $x \in A$. thus we have shown $x \in A$ under the

assumption $(\exists i \in I. x = x_i)$, thus we have shown

$(\exists i \in I. x = x_i) \rightarrow x \in A$, which is what was to be proven.

This proof could be made more formal by drawing a proof tree or using

Isabelle.

Families

The word **family** is sometimes used for a set of sets [Vel94].

Collections and Sets

We speak of **collection** of all sets rather than **set** of all sets in order to pretend that we are being careful since we are not sure if there is such a thing as a **set of all sets**. Therefore we use the “neutral” word **collection** whose meaning is obvious. . .

Collections and Sets

We speak of **collection** of all sets rather than **set** of all sets in order to pretend that we are being careful since we are not sure if there is such a thing as a **set of all sets**. Therefore we use the “neutral” word **collection** whose meaning is obvious. . .

Is it?

Collections and Sets

We speak of **collection** of all sets rather than **set** of all sets in order to pretend that we are being careful since we are not sure if there is such a thing as a **set of all sets**. Therefore we use the “neutral” word **collection** whose meaning is obvious. . . .

Is it?

Recall that we have defined **set** as **collection of objects** in the first place. So it is rather futile to suggest now that there should be some difference between collections and sets.

The fact of the matter is: the approach of allowing arbitrary collections of “objects” and regarding such collections as “objects” themselves is **naive**. We will see this shortly.

Logical Characterization

Recall $R := \{A \mid A \notin A\}$.

Let A be arbitrary (for the formal reasoning applied here, **arbitrary** means: it could be a set, a number, a dog, the pope, anything whatsoever).

By the **rules for set comprehension**, we can prove

$A \in \{A \mid A \notin A\} \rightarrow A \notin A$ and $A \notin A \rightarrow A \in \{A \mid A \notin A\}$, and so by **definition of \leftrightarrow** , we have $A \in R \leftrightarrow A \notin A$, and since A was arbitrary, by **\forall -I**, we have $\forall A. (A \in R \leftrightarrow A \notin A)$.

What does this tell us about sets?

It tells us that there can be no such thing as the set of all sets.

The fundamental flaw of naive set theory is in saying that a set is a **collection of “objects”** without worrying what an object is. If we make no restriction as to what an object is, then a set is obviously also an object. But then we effectively base the definition of the new concept **set** on the existence of sets, so the definition is circular.

The intuition for the solution to this dilemma is not difficult: A set is a collection of objects of which we are already sure that they exist. In particular, since we are only just about to define sets, these objects may not themselves be sets.

Once we have such sets, we can introduce “sets of second order”, that is, sets that contain sets of the first kind. This process can be continued

ad infinitum.

The formal details will come later.

True

Assume that \top is syntactic sugar for a proposition that is always true, say $\top \equiv \perp \rightarrow \perp$. We have not introduced this, but it is convenient.

So **semantically**, we have $I_{\mathcal{A}}(\top) = 1$ for all $I_{\mathcal{A}}$.

A Strange Set Comprehension

Recall that a **set comprehension** has the form $\{x \mid P(x)\}$, where $P(x)$ is a formula usually containing x .

The set comprehension $U := \{x \mid \top\}$ is strange since \top does not contain x .

But by the **introduction rule for set comprehensions**, this means that $x \in U$ for **any** x . Thus in particular, $U \in U$.

Higher-Order Logic

Higher-order logic is a solution to the dilemma posed by Russell's paradox.

It is a surprisingly simple formalism which can be extended conservatively: this means that it can be ensured that the extensions cannot compromise the truth or falsity of statements that were already expressible before the extension.