Chapter 5

Sets, Functions, Relations, and Fixpoints

Sets, Functions, Relations

see IHT 6.1, 6.2, 6.3

- Finite Set Notation
- Set Comprehension
- Binding Operators
- Finiteness and Cardinality
- Function update, Range, Injective - Surjective
- Relations, Predicates

Overview

- Set notation
- Inductively defined sets

Set notation

Sets

Sets over type *'a*:

'a set

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

Sets

Sets over type *'a*:

$$'a\ set \quad = \quad 'a \Rightarrow bool$$

- $\{\}$, $\{e_1,\ldots,e_n\}$, $\{x.\ P\ x\}$

Sets

Sets over type *'a*:

$$\text{'a set} \quad = \quad \text{'a} \Rightarrow \mathit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1,\ldots,e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, A - B, - A

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1,\ldots,e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, A - B, - A
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $-A$
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$
- $\{i..j\}$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $-A$
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$
- $\{i..j\}$
- $\textit{insert} :: \textit{'a} \Rightarrow \textit{'a set} \Rightarrow \textit{'a set}$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, A - B, - A
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$
- $\{i..j\}$
- *insert* :: *'a* $\Rightarrow$ *'a set* $\Rightarrow$ *'a set*
- ...

Proofs about sets

Natural deduction proofs:

- `equalityI`: $[\![A \subseteq B; B \subseteq A]\!] \Longrightarrow A = B$

Proofs about sets

Natural deduction proofs:

- `equalityI`: $[\![A \subseteq B; B \subseteq A]\!] \Longrightarrow A = B$
- `subsetI`: $(\bigwedge x.\ x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$

Proofs about sets

Natural deduction proofs:

- `equalityI`: $[\![A \subseteq B; B \subseteq A]\!] \Longrightarrow A = B$
- `subsetI`: $(\bigwedge x.\ x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$
- ... (see Tutorial)

Demo: proofs about sets

Bounded quantifiers

- $\forall x \in A.\ P\ x$

Bounded quantifiers

- $\forall x{\in}A.\ P\ x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\ x$

Bounded quantifiers

- $\forall x{\in}A.\ P\,x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\,x$
- $\exists x{\in}A.\ P\,x$

Bounded quantifiers

- $\forall x{\in}A.\ P\,x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\,x$
- $\exists x{\in}A.\ P\,x \quad \equiv \quad \exists x.\ x{\in}A \wedge P\,x$

Bounded quantifiers

- $\forall x{\in}A.\ P\ x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\ x$
- $\exists x{\in}A.\ P\ x \quad \equiv \quad \exists x.\ x{\in}A \wedge P\ x$
- `ballI`: $(\bigwedge x.\ x \in A \Longrightarrow P\ x) \Longrightarrow \forall x{\in}A.\ P\ x$
- `bspec`: $[\![\forall x{\in}A.\ P\ x;\ x \in A]\!] \Longrightarrow P\ x$

Bounded quantifiers

- $\forall x{\in}A.\ P\ x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\ x$
- $\exists x{\in}A.\ P\ x \quad \equiv \quad \exists x.\ x{\in}A \wedge P\ x$
- `ballI`: $(\bigwedge x.\ x \in A \Longrightarrow P\ x) \Longrightarrow \forall x{\in}A.\ P\ x$
- `bspec`: $[\![\forall x{\in}A.\ P\ x;\ x \in A]\!] \Longrightarrow P\ x$
- `bexI`: $[\![P\ x;\ x \in A]\!] \Longrightarrow \exists x{\in}A.\ P\ x$
- `bexE`: $[\![\exists x{\in}A.\ P\ x;\ \bigwedge x.\ [\![x \in A;\ P\ x]\!] \Longrightarrow Q]\!] \Longrightarrow Q$

Inductively defined sets

Example: even numbers

Informally:

Example: even numbers

Informally:

- 0 is even

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n+2$

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$
- These are the only even numbers

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$
- These are the only even numbers

In Isabelle/HOL:

inductive_set *Ev :: nat set* — The set of all even numbers

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$
- These are the only even numbers

In Isabelle/HOL:

inductive_set *Ev :: nat set* — The set of all even numbers
where
0 $\in$ *Ev* |
n $\in$ *Ev* $\Longrightarrow$ *n + 2* $\in$ *Ev*

Format of inductive definitions

inductive_set $S :: \tau\ set$

Format of inductive definitions

inductive_set $S :: \tau$ *set*

where

$[\![\, a_1 \in S; \ldots ; a_n \in S; A_1; \ldots ; A_k \,]\!] \Longrightarrow a \in S \mid$

$\vdots$

Format of inductive definitions

inductive_set $S :: \tau$ *set*

where

$\llbracket\ a_1 \in S; \ldots\ ; a_n \in S; A_1; \ldots ; A_k\ \rrbracket \Longrightarrow a \in S \ \ |$

$\vdots$

where $A_1; \ldots ; A_k$ are side conditions not involving S.

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m+m \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$
Idea: induction on the length of the derivation of $m \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m+m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$
- rule $n \in Ev \Longrightarrow n{+}2 \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$
- rule $n \in Ev \Longrightarrow n{+}2 \in Ev$
  $\Longrightarrow m = n{+}2$ and $n{+}n \in Ev$ (ind. hyp.!)

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$
- rule $n \in Ev \Longrightarrow n{+}2 \in Ev$
  $\Longrightarrow m = n{+}2$ and $n{+}n \in Ev$ (ind. hyp.!)
  $\Longrightarrow m{+}m = (n{+}2){+}(n{+}2) = ((n{+}n){+}2){+}2 \in Ev$

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\,n$$

by *rule induction* on $n \in Ev$ we must prove

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

- $P\ 0$

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

- $P\ 0$
- $P\ n \Longrightarrow P(n{+}2)$

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

- $P\ 0$
- $P\ n \Longrightarrow P(n{+}2)$

Rule `Ev.induct`:

$$[\![\ n \in Ev;\ P\ 0;\ \bigwedge n.\ P\ n \Longrightarrow P(n{+}2)\ ]\!] \Longrightarrow P\ n$$

Rule induction in general

Set S is defined inductively.

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\,x$$

by *rule induction* on $x \in S$

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\,x$$

by *rule induction* on $x \in S$
we must prove for every rule

$$[\![\, a_1 \in S; \ldots ; a_n \in S \,]\!] \Longrightarrow a \in S$$

that P is preserved:

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\,x$$

by *rule induction* on $x \in S$
we must prove for every rule

$$[\![\, a_1 \in S; \ldots ; a_n \in S \,]\!] \Longrightarrow a \in S$$

that P is preserved:

$$[\![\, P\,a_1; \ldots ; P\,a_n \,]\!] \Longrightarrow P\,a$$

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\,x$$

by *rule induction* on $x \in S$
we must prove for every rule

$$[\![\ a_1 \in S; \dots ; a_n \in S\ ]\!] \Longrightarrow a \in S$$

that P is preserved:

$$[\![\ P\,a_1; \dots ; P\,a_n\ ]\!] \Longrightarrow P\,a$$

In Isabelle/HOL:

apply *(induct rule: S.induct)*

Demo: inductively defined sets

Inductive predicates

$$x \in S \quad \rightsquigarrow \quad S\,x$$

Inductive predicates

$$x \in S \quad \rightsquigarrow \quad S\,x$$

Example:

inductive $Ev :: nat \Rightarrow bool$

where

$Ev\ 0 \quad |$

$Ev\ n \Longrightarrow Ev\ (n + 2)$

Inductive predicates

$$x \in S \quad \rightsquigarrow \quad S\,x$$

Example:

inductive $Ev :: nat \Rightarrow bool$

where

$Ev\ 0 \quad |$

$Ev\ n \Longrightarrow Ev\ (n + 2)$

Comparison:

predicate: simpler syntax

set: direct usage of $\cup$ etc

Inductive predicates

$$x \in S \quad \rightsquigarrow \quad S\,x$$

Example:

inductive *Ev :: nat ⇒ bool*
where
Ev 0 |
Ev n ⟹ Ev (n + 2)

Comparison:

predicate:	simpler syntax
set:	direct usage of ∪ etc

Inductive predicates can be of type $\tau_1 \Rightarrow \ldots \Rightarrow \tau_n \Rightarrow bool$

Automating it

simp and auto

simp rewriting and a bit of arithmetic

auto rewriting and a bit of arithmetic, logic & sets

simp and auto

simp rewriting and a bit of arithmetic

auto rewriting and a bit of arithmetic, logic & sets

- Show you where they got stuck

simp and auto

simp rewriting and a bit of arithmetic

auto rewriting and a bit of arithmetic, logic & sets

- Show you where they got stuck
- highly incomplete wrt logic

blast

- A complete (for FOL) tableaux calculus implementation

blast

- A complete (for FOL) tableaux calculus implementation
- Covers logic, sets, relations, . . .

blast

- A complete (for FOL) tableaux calculus implementation
- Covers logic, sets, relations, ...
- Extensible with intro/elim rules

blast

- A complete (for FOL) tableaux calculus implementation
- Covers logic, sets, relations, . . .
- Extensible with intro/elim rules
- Almost no “=”

Demo: blast

Well founded relations

see IHT 6.4

- Well founded orderings: Induction
- Complete Lattices Fixpoints
- Knaster-Tarski Theorem

Fixpoints

Importance

- Inductive definitions of sets and relations
- Reminder: relations are sets in Isabelle/HOL
- E.g.: $0 \in$ even
- $n \in$ even ==> $n+2 \in$ even

Properties of Orderings and Functions

Definition 5.1. *Monotone Function*
Let D be a set with an ordering relation $\leq$. A function $f : D \rightarrow D$ is called monotone, if $x \leq y \longrightarrow f(x) \leq f(y)$

Remark

The inductive definition above induces a monotone function on sets with the subset relation as ordering:

- f_even :: nat set -> nat set
- f_even $(A) = A \cup \{0\} \cup \{n+2 | n \in A\}$
-
-

Well-founded Orderings

- Partial-order $\leq \subseteq X \times X$ well-founded iff

$$(\forall Y \subseteq X : Y \neq \emptyset \rightarrow (\exists y \in Y : y \text{ minimal in } Y \text{ in respect of } \leq))$$

- Quasi-order $\lesssim$ well-founded iff strict part of $\lesssim$ is well-founded.
- Initial segment: $Y \subseteq X$, left-closed i.e.

$$(\forall y \in Y : (\forall x \in X : x \lesssim y \rightarrow x \in Y))$$

- Initial section of x: $\mathrm{sec}(x) = \{y : y < x\}$

Supremum

- Let $(X, \leq)$ be a partial-order and $Y \subseteq X$
- $S \subseteq X$ is a chain iff elements of S are linearly ordered through $\leq$.
- y is an upper bound of Y iff

$$\forall y' \in Y : y' \leq y$$

- Supremum: y is a supremum of Y iff y is an upper bound of Y and

$$\forall y' \in X : ((y' \text{ upper bound of } Y) \rightarrow y \leq y')$$

- Analog: lower bound, Infimum $\inf(Y)$

CPO

- A Partial-order $(D, \sqsubseteq)$ is a complete partial ordering (CPO) iff
  - $\exists$ the smallest element $\perp$ of D (with respect of $\sqsubseteq$)
  - Each chain S has a supremum $\sup(S)$.

Example

Example 5.2. .

- $(\mathcal{P}(X), \subseteq)$ is CPO.
- $(D, \sqsubseteq)$ is CPO with
  - $D = X \nrightarrow Y$: set of all the partial functions f with $\mathrm{dom}(f) \subseteq X$ and $\mathrm{cod}(f) \subseteq Y$.
  - Let $f, g \in X \nrightarrow Y$.

$$f \sqsubseteq g \text{ iff } \mathrm{dom}(f) \subseteq \mathrm{dom}(g) \wedge (\forall x \in \mathrm{dom}(f) : f(x) = g(x))$$

Monotonous, continuous

- $(D, \sqsubseteq)$, $(E, \sqsubseteq')$ CPOs
- $f : D \to E$ monotonous iff

$$(\forall d, d' \in D : d \sqsubseteq d' \to f(d) \sqsubseteq' f(d'))$$

- $f : D \to E$ continuous iff f monotonous and

$$(\forall S \subseteq D : S \text{ chain } \to f(\sup(S)) = \sup(f(S)))$$

- $X \subseteq D$ is admissible iff

$$(\forall S \subseteq X : S \text{ chain } \to \sup(S) \in X)$$

Fixpoint

- $(D, \sqsubseteq)$ CPO, $f : D \to D$
- $d \in D$ fixpoint of f iff
$$f(d) = d$$
- $d \in D$ smallest fixpoint of f iff d fixpoint of f and
$$(\forall d' \in D : d' \text{ fixpoint } \to d \sqsubseteq d')$$

Fixpoint-Theorem

Theorem 5.3 (Fixpoint-Theorem:). *$(D, \sqsubseteq)$ CPO, $f : D \to D$ continuous, then f has a smallest fixpoint μf and*

$$\mu f = \sup\{f^i(\bot) : i \in \mathbb{N}\}$$

Proof: (Sketch)

- $\sup\{f^i(\bot) : i \in \mathbb{N}\}$ fixpoint:

$$\begin{aligned} f(\sup\{f^i(\bot) : i \in \mathbb{N}\}) &= \sup\{f^{i+1}(\bot) : i \in \mathbb{N}\} \\ &\ \text{(continuous)} \\ &= \sup\{\sup\{f^{i+1}(\bot) : i \in \mathbb{N}\}, \bot\} \\ &= \sup\{f^i(\bot) : i \in \mathbb{N}\} \end{aligned}$$

Fixpoint-Theorem (Cont.)

Fixpoint-Theorem: $(D, \sqsubseteq)$ CPO, $f : D \to D$ continuous, then f has a smallest fixpoint μf and

$$\mu f = \sup\{f^i(\bot) : i \in \mathbb{N}\}$$

Proof: (Continuation)

- $\sup\{f^i(\bot) : i \in \mathbb{N}\}$ smallest fixpoint:
  1. d' fixpoint of f
  2. $\bot \sqsubseteq d'$
  3. f monotonous, d' FP: $f(\bot) \sqsubseteq f(d') = d'$
  4. Induction: $\forall i \in \mathbb{N} : f^i(\bot) \sqsubseteq f^i(d') = d'$
  5. $\sup\{f^i(\bot) : i \in \mathbb{N}\} \sqsubseteq d'$

Induction over $\mathbb{N}$

Induction's principle:

$$(\forall X \subseteq \mathbb{N} : ((0 \in X \land (\forall x \in X : x \in X \to x+1 \in X))) \to X = \mathbb{N})$$

Correctness:

1. Let's assume no, so $\exists X \subseteq \mathbb{N} : \mathbb{N} \setminus X \neq \emptyset$
2. Let y be minimum in $\mathbb{N} \setminus X$ (with respect to $<$).
3. $y \neq 0$
4. $y - 1 \in X \land y \notin X$
5. Contradiction

Induction over $\mathbb{N}$ (Alternative)

Induction's principle:

$$(\forall X \subseteq \mathbb{N} : (\forall x \in \mathbb{N} : \mathrm{sec}(x) \subseteq X \rightarrow x \in X) \rightarrow X = \mathbb{N})$$

Correctness:

1. Let's assume no, so $\exists X \subseteq \mathbb{N} : \mathbb{N} \setminus X \neq \emptyset$
2. Let y be minimum in $\mathbb{N} \setminus X$ (with respect to $<$).
3. $\mathrm{sec}(y) \subseteq X, y \notin X$
4. Contradiction

Well-founded induction

Induction's principle: Let $(Z, \leq)$ be a well-founded partial order.

$$(\forall X \subseteq Z : (\forall x \in Z : \mathrm{sec}(x) \subseteq X \to x \in X) \to X = Z)$$

Correctness:

1. Let's assume no, so $Z \setminus X \neq \emptyset$
2. Let z be a minimum in $Z \setminus X$ (in respect of $\leq$).
3. $\mathrm{sec}(z) \subseteq X, z \notin X$
4. Contradiction

FP-Induction: Proving properties of fixpoints

Induction's principle: Let $(D, \sqsubseteq)$ CPO, $f : D \to D$ continuous.

$$(\forall X \subseteq D \text{ admissible} : (\perp \in X \wedge (\forall y : y \in X \to f(y) \in X)) \to \mu f \in X)$$

Correctness: Let $X \subseteq D$ admissible.

$$\begin{array}{lcll}
\mu f \in X & \Leftrightarrow & \sup\{f^i(\perp) : i \in \mathbb{N}\} \in X & \text{(FP-theorem)} \\
& \Leftarrow & \forall i \in \mathbb{N} : f^i(\perp) \in X & (X \text{ admissible }) \\
& \Leftarrow & \perp \in X \wedge (\forall n \in \mathbb{N} : f^n(\perp) \in X \to f(f^n(\perp)) \in X) & \\
& & & \text{(Induction } \mathbb{N}) \\
& \Leftarrow & \perp \in X \wedge (\forall y \in X \to f(y) \in X) & \text{(Ass.)}
\end{array}$$

Problem

Exercise 5.4. Let $(D, \sqsubseteq)$ CPO with

- $X = Y = \mathbb{N}$
- $D = X \nrightarrow Y$: set all partial functions f with $\mathrm{dom}(f) \subseteq X$ and $\mathrm{cod}(f) \subseteq Y$.
- Let $f, g \in X \nrightarrow Y$.

$$f \sqsubseteq g \text{ iff } \mathrm{dom}(f) \subseteq \mathrm{dom}(g) \wedge (\forall x \in \mathrm{dom}(f) : f(x) = g(x))$$

Consider

$$\begin{array}{llll} F: & D & \rightarrow & \mathcal{P}(\mathbb{N} \times \mathbb{N}) \\ & g & \mapsto & \begin{cases} \{(0,1)\} & g = \emptyset \\ \{(x, x \cdot g(x-1)) : x - 1 \in \mathrm{dom}(g)\} \cup \{(0,1)\} & \text{otherwise} \end{cases} \end{array}$$

Problem

Prove:

1. $\forall g \in D : F(g) \in D$, i.e. $F : D \rightarrow D$
2. $F : D \rightarrow D$ continuous
3. $\forall n \in \mathbb{N} : \mu F(n) = n!$

Note:

- μF can be understood as the semantics of a function's definition

$$\begin{array}{l}\text{function}\,\text{Fac}(n : \mathbb{N}_\perp) : \mathbb{N}_\perp =_{\text{def}}\\ \qquad \text{if } n = 0 \text{ then } 1\\ \qquad \text{else } n \cdot \text{Fac}(n-1)\end{array}$$

- Keyword: ' functions' in Isabelle

Problem

Exercise 5.5. Prove: Let $G = (V, E)$ be an infinite directed graph with

- G has finitely many roots (nodes without incoming edges).
- Each node has finite out-degree.
- Each node is reachable from a root.

There exists an infinite path that begins on a root.

Complete Lattices and Existence of Fixpoints

Definition 5.6. *Complete Lattice*
A partially ordered set $(L, \leq)$ is a complete lattice if every subset A of L has both a greatest lower bound (the infimum, also called the meet) and a least upper bound (the supremum, also called the join) in $(L, \leq)$. The meet is denoted by $\bigwedge A$, and the join by $\bigvee A$.

Lemma 5.7. *Complete lattices are non empty.*

Theorem 5.8. *Knaster-Tarski*
Let $(L, \leq)$ be a complete lattice and let $f : L \to L$ be a monotone function. Then the set of fixed points of f in L is also a complete lattice.

Consequence 5.9. *The Knaster-Tarski theorem guarantees the existence of least and greatest fixpoints.*

Proof of the Knaster-Tarski theorem

Reformulation

For a complete lattice $(L, \leq)$ and a monotone function $f : L \rightarrow L$ on L, the set of all fixpoints of f is also a complete lattice $(P, \leq)$, with:

- $\bigvee P = \bigvee\{x \in L | x \leq f(x)\}$ as the greatest fixpoint of f
- $\bigwedge P = \bigwedge\{x \in L | f(x) <= x\}$ as the least fixpoint of f

Proof: We begin by showing that P has least and greatest elements.
Let $D = \{y \in L | y \leq f(y)\}$ and $x \in D$. Then, because f is monotone, we have $f(x) \leq f(f(x))$, that is $f(x) \in D$.
Now let $u = \bigvee D$. Then $x \leq u$ and $f(x) \leq f(u)$, so $x \leq f(x) \leq f(u)$. Therefore $f(u)$ is an upper bound of D, but u is the least upper bound, so $u \leq f(u)$, i.e. $u \in D$. Then $f(u) \in D$ (from above) and $f(u) \leq u$ hence $f(u) = u$. Because every fixpoint is in D we have that u is the greatest fixpoint of f.

Proof of the Knaster-Tarski theorem (cont.)

The function f is monotone on the dual (complete) lattice $(L^{op}, \geq)$. As we have just proved, its greatest fixpoint there exists. It is the least one on L, so P has least and greatest elements, or more generally that every monotone function on a complete lattice has least and greatest fixpoints.

If $a \in L$ and $b \in L, a \leq b$, we'll write $[a, b]$ for the closed interval with bounds a and b : $\{x \in L | a \leq x \leq b\}$. The closed intervals are also complete lattices.

It remains to prove that P is complete lattice.

Proof of the Knaster-Tarski theorem (cont.)

Let $W \subset P$ and $w = \bigvee W$. We construct a least upper bound of W in P. (The reasoning for the greatest lower bound is analogue.)
For every $x \in W$, we have $x = f(x) \leq f(w)$, i.e., $f(w)$ is an upper bound of W. Since w is the least upper bound of W, $w \leq f(w)$.
Furthermore, for $y \in [w, \bigvee L]$, we have $w \leq f(w) \leq f(y)$. Thus, $f([w, \bigvee L]) \subset [w, \bigvee L]$, and we can consider f to be a monotone function on the complete lattice $[w, \bigvee L]$. Then,
$v = \bigwedge\{x \in [w, \bigvee L] | f(x) \leq x\}$ is the least fixpoint of f in $[w, \bigvee L]$.
We show that v is the least upper bound of W in P.
a) v is in P.
b) v is an upper bound of W, because $v \in [w, \bigvee L]$, i.e., $w \leq v$.
c) v is least. Let z be another upper bound of W in P. Then,
$w \leq z, z \in [w, \bigvee L], z$ is fixpoint, hence $v \leq z$

Lattices in Isabelle

Monotony and Fixpoints

- mono $f \equiv \forall AB.\ A \leq B \longrightarrow f\ A \leq f\ B$ (mono_def)
- Usually subset relation as ordering
- lfp $f \equiv Inf\{u|\ f\ u \leq u\}$ (lfp_def)
- $mono\ f \Longrightarrow lfp\ f = f\ (lfp\ f)$ (lfp_unfold)
- $[|mono\ ?f; ?f\ (inf\ (lfp\ ?f)\ ?P) \leq\ ?P|] \Longrightarrow lfp ?f \leq\ ?P$ (lfp_induct)
- gfp $f \equiv Sup\{u|\ u \leq f\ u\}$ (gfp_def)
- $mono\ f \Longrightarrow gfp\ f = f\ (gfp\ f)$ (gfp_unfold)
- $[|mono\ ?f; ?X\ \leq\ ?f\ (sup\ ?X\ (gfp\ ?f))|] \Longrightarrow ?X \leq\ gfp\ ?f$ (coinduct)