

“Higher-Order” Mathematics in B

Jean-Raymond Abrial Dominique Cansell Guy Laffitte

January 24, 2002

Summary

- A structure language to encode theorems
- A tool (in Logic-Solver)
- A tricky proof (Thm. Zermelo)

The talk presents our structure language using Zermelo's example

Why structure?

- To put together data and theorems (with a proof) which accompany these data
 - To prove High-order theorems mechanically, using Atelier B's prover
 - To Distribute the difficulties of the proof
 - To re-use proof (for free or cheap) by instantiation
 - To instantiate structure and use the instantiated theorems
 - To improve explanation (a communication act)
-

How to do it?

Define two kinds of mathematical devices

- **structure** like predicate
 - **construct** like term (and associated predicate)
-

A tricky theorem

Every set, equipped with a “choice function”, can be well-ordered

A tricky theorem

Inter

Partial_order

Fixpoint

Well_order

Transfinite

Zermelo

Transport_w_o

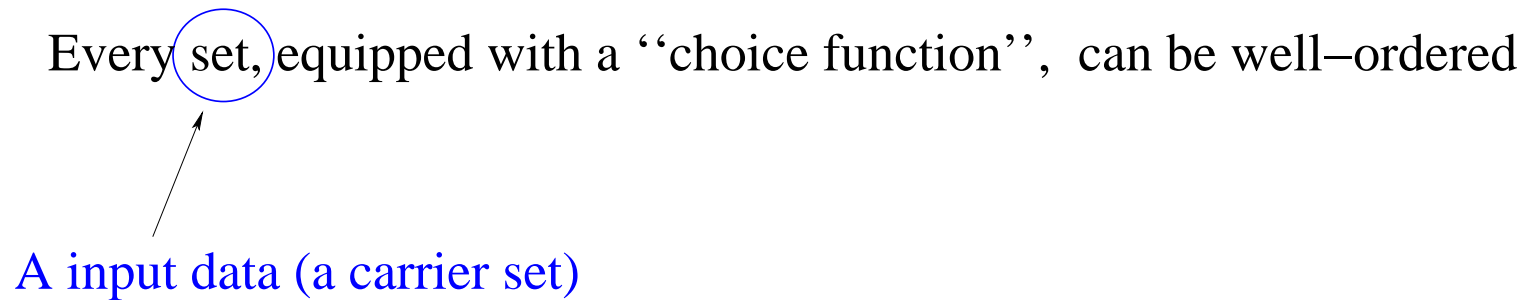
Progression to a structure (and a proof)

Every set, equipped with a “choice function”, can be well-ordered

Progression to a structure (and a proof)

Every set, equipped with a “choice function”, can be well-ordered

A input data (a carrier set)



Progression to a structure (and a proof)

Every set, equipped with a “choice function”, can be well-ordered

A input data (a carrier set)

A theorem (another structure)

A structure *Partial_order*

structure

Partial_order

sets

s

components

r

axioms

$r \in s \leftrightarrow s$;

$\text{id}(s) \subseteq r$; /* injectivity */

$r \cap r^{-1} \subseteq \text{id}(s)$; /* antisymetry */

$r \circ r \subseteq r$ /* transitivity */

end

- A structure like predicate (definition)
 r is a partial order on s
“Let s be a set and r a partial order on s ”
- a clause **axioms** to define r
- No proof obligation.

A structure *Well_order*

structure

Well_order

sets

s

components

r

axioms

Partial_order(s, r) ;

$\forall t \cdot (t \in \mathbb{P}_1(s)$

\Rightarrow

$\exists x \cdot (x \in t \wedge t \subseteq r[\{x\}]))$

end

- a use of a structure
- No proof obligation for this use

Progression to a construct (and a proof)

A CONSTRUCT (when a result)
A STRUCTURE (else)

Every set, equipped with a 'choice function', can be well-ordered

A input data (a carrier set)

A theorem (with a result)

A component (defined with axiom)

A first construct *Zermelo*

construct

Zermelo

sets

s

components

c

returns

r

axioms

$c \in \mathbb{P}_1(s) \rightarrow s ;$

$\forall a \cdot (a \in \mathbb{P}_1(s) \Rightarrow c(a) \in a)$

...

definition

$r \in s \leftrightarrow s ;$

$r = \dots$

theorems

Well_order(s, r)

end

- a clause **return** for the result of the construct
- a clause **definition** to define the result
- we can also define local constant (see next)
- a clause **theorem** (to prove)

Moving the Problem

$$\{\emptyset, n(\emptyset), n(n(\emptyset)), n(n(n(\emptyset))), \dots\}$$

if $\forall x.(x \in \mathcal{P}(s) \Rightarrow x \subseteq n(x))$

we can perhaps find an injection between s and this new set ordered by inclusion.

\rightsquigarrow transport the order using the injection

The construct *Transport_w_o*

construct

Transport_w_o

sets

t, s

components

q, f

returns

r

axioms

Well_order(t, q) ;

f ∈ s ↦ t ;

definition

r ∈ s ↔ s ;

r = f⁻¹ ∘ q ∘ f

theorems

Well_order(s, r)

end

- a theorem to prove
- to prove with axioms

The construct *Transport_w_o*

construct

Transport_w_o

sets

t, s

components

q, f

returns

r

axioms

$Well_order(t, q) ;$

$f \in s \mapsto t ;$

definition

$r \in s \leftrightarrow s ;$

$r = f^{-1} \circ q \circ f$

theorems

$Well_order(s, r) \quad \checkmark$

end

- a theorem to prove
 - to prove with axioms
 - easy to prove (mechanically)
-

Associated Proof Obligations

structure *or* **construct**

S

sets

s

components

c

axioms

$A(s, c)$

theorems

$T(s, c)$

end

$$A(s, c) \Rightarrow T(s, c)$$

$$A(s, c) \Rightarrow T1(s, c)$$

$$A(s, c) \wedge T1(s, c) \Rightarrow T2(s, c)$$

We have a **lemmas** clause (internal theorems)

Instantiate a structure

```
structure
   $\mathcal{T}$ 
sets
   $t$ 
components
   $d$ 
  ...
   $\mathcal{S}(\sigma(t, d), \gamma(t, d))$ 
  ...
end
```

$$\begin{array}{l} A(\sigma(t, d), \gamma(t, d)) \\ \Rightarrow \\ T(\sigma(t, d), \gamma(t, d)) \end{array}$$

- in an axiom clause we have, for free, $A(\sigma(t, d), \gamma(t, d)) \wedge T(\sigma(t, d), \gamma(t, d))$
 - in a theorem clause we have $A(\sigma(t, d), \gamma(t, d)) \wedge T(\sigma(t, d), \gamma(t, d))$ after proving $A(\sigma(t, d), \gamma(t, d))$
-

Proof Obligations for a call

- a structure in an axiom clause \rightsquigarrow no PO
 - a structure in a theorem or lemma \rightsquigarrow instantiated axioms
 - a construct in a definition \rightsquigarrow instantiated axioms
 - a definition of a constant \rightsquigarrow existence and unicity (well-defined)
 - No circularity in structure or construct.
-

Hypothesis of Proof Obligations

- the axioms of the structure or construct,
- the previous definitions,
- the previous theorems or lemmas,
- the instantiated axioms and theorems of the structures or constructs previously called.

Converting into B

sets \rightsquigarrow **sets**

components \rightsquigarrow **constants**

axioms \rightsquigarrow **properties**

definition \rightsquigarrow **constants** and **properties**

theorems \rightsquigarrow **assertions**

lemmas \rightsquigarrow **assertions**

instantiated (axioms imply theorems) \rightsquigarrow **properties**

A “little” tool exists

quickly written using Logic-Solver from Atelier B

Moving the Problem

construct

Zermelo

...

constants

t, q, f

definition

$t \in \mathbb{P}(\mathbb{P}(s)) ;$

$t = \dots$

definition

$q \in t \leftrightarrow t ;$

$\forall (a, b) \cdot (a, b \in t \times t \Rightarrow (a, b \in q \Leftrightarrow a \subseteq b))$

definition

$f \in s \rightarrow t ;$

$f = \dots$

lemmas

$Well_order(t, q) ;$

$f \in s \mapsto t$

definition

$r \in s \leftrightarrow s ;$

$r = Transport_w_o(t, s, q, f) \quad \checkmark$

theorems

$Well_order(s, r) \quad \checkmark$

end

Proving the Well-ordering on t

construct

Zermelo

...

lemmas

$\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a) ;$

$Well_order(t, q) ; \quad \checkmark$

$f \in s \rightsquigarrow t$

definition

$r \in s \leftrightarrow s ;$

$r = Transport_w_o(t, s, q, f) \quad \checkmark$

theorems

$Well_order(s, r) \quad \checkmark$

end

Defining the Injection Between s and t

constants n, t, q, f **definition** $n \in \mathbb{P}(s) \rightarrow \mathbb{P}(s) ;$ $n(s) = s ;$ $\forall a \cdot (a \in \mathbb{P}(s) \wedge a \neq s \Rightarrow n(a) = a \cup \{c(s-a)\})$

...

 $t \in \mathbb{P}(\mathbb{P}(s)) ;$ $t = \dots$

...

definition $f \in s \rightarrow t ;$ $\forall z \cdot (z \in s \Rightarrow f(z) = \text{union}(\{x \mid x \in t \wedge z \notin x\}))$

$n(f(z))$ will then necessarily contain z ,

$c(s-f(z))$ is equal to z .

construct

Zermelo

...

lemmas

$\forall x \cdot (x \in t \Rightarrow n(x) \in t) ;$
 $\forall a \cdot (a \in \mathbb{P}(t) \Rightarrow \text{union}(a) \in t) ;$
 $\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a) ;$
 $\text{Well_order}(t, q) ; \quad \checkmark$
 $f \in s \rightsquigarrow t \quad \checkmark$

definition

$r \in s \leftrightarrow s ;$
 $r = \text{Transport_w_o}(t, s, q, f) \quad \checkmark$

theorems

$\text{Well_order}(s, r) \quad \checkmark$

end

- the first three lemmas must be given by the construct which defines the set t

Finalizing the Construct *Zermelo*

construct

Zermelo

sets

s

components

c

returns

r

axioms

$c \in \mathbb{P}_1(s) \rightarrow s ;$

$\forall a \cdot (a \in \mathbb{P}_1(s) \Rightarrow c(a) \in a)$

constants

n, t, q, f

definition

$n \in \mathbb{P}(s) \rightarrow \mathbb{P}(s) ;$

$n(s) = s ;$

$\forall a \cdot (a \in \mathbb{P}(s) \wedge a \neq s \Rightarrow n(a) = a \cup \{c(s-a)\})$

Finalizing the Construct *Zermelo*

definition

$t \in \mathbb{P}(\mathbb{P}(s)) ;$
 $t = \text{Transfinite}(s, n)$

definition

$q \in t \leftrightarrow t ;$
 $\forall (a, b) \cdot (a, b \in t \times t \Rightarrow (a, b \in q \Leftrightarrow a \subseteq b))$

definition

$f \in s \rightarrow t ;$
 $\forall z \cdot (z \in s \Rightarrow f(z) = \text{union}(\{x \mid x \in t \wedge z \notin x\}))$

lemmas

$\forall x \cdot (x \in t \Rightarrow n(x) \in t) ; \quad \checkmark$
 $\forall a \cdot (a \in \mathbb{P}(t) \Rightarrow \text{union}(a) \in t) ; \quad \checkmark$
 $\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a) ; \quad \checkmark$
 $\text{Well_order}(t, q) ; \quad \checkmark$
 $f \in s \mapsto t \quad \checkmark$

definition

$r \in s \leftrightarrow s ;$
 $r = \text{Transport_w_o}(t, s, q, f) \quad \checkmark$

theorems

$\text{Well_order}(s, r) \quad \checkmark$

end

Finalizing the Construct *Zermelo*

definition

$t \in \mathbb{P}(\mathbb{P}(s)) ;$
 $t = \text{Transfinite}(s, n)$

definition

$q \in t \leftrightarrow t ;$
 $\forall (a, b) \cdot (a, b \in t \times t \Rightarrow (a, b \in q \Leftrightarrow a \subseteq b))$

definition

$f \in s \rightarrow t ;$
 $\forall z \cdot (z \in s \Rightarrow f(z) = \text{union}(\{x \mid x \in t \wedge z \notin x\}))$

lemmas

$\text{Well_order}(t, q) ; \quad \checkmark$
 $f \in s \mapsto t \quad \checkmark$

definition

$r \in s \leftrightarrow s ;$
 $r = \text{Transport_w_o}(t, s, q, f) \quad \checkmark$

theorems

$\text{Well_order}(s, r) \quad \checkmark$

end

First shape of construct *Transfinite*

construct

Transfinite

sets

s

components

n

returns

t

axioms

$n \in \mathbb{P}(s) \rightarrow \mathbb{P}(s) ;$

...

definition

$t \in \mathbb{P}(\mathbb{P}(s)) ;$

$t = \dots$

theorems

$\forall x \cdot (x \in t \Rightarrow n(x) \in t) ;$

$\forall a \cdot (a \in \mathbb{P}(t) \Rightarrow \text{union}(a) \in t) ;$

$\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a)$

end

construct *Transfinite*

construct

Transfinite

sets

s

components

n

returns

t

axioms

$n \in \mathbb{P}(s) \rightarrow \mathbb{P}(s) ;$

...

definition

$t \in \mathbb{P}(\mathbb{P}(s)) ;$

$t = \dots$

theorems

$\forall x \cdot (x \in t \Rightarrow n(x) \in t) ;$

$\forall a \cdot (a \in \mathbb{P}(t) \Rightarrow \text{union}(a) \in t) ;$

$\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a)$

end

construct

Transfinite

...

constants

g

definition

$g \in \mathbb{P}(\mathbb{P}(s)) \rightarrow \mathbb{P}(\mathbb{P}(s)) ;$

$\forall a \cdot (a \in \mathbb{P}(\mathbb{P}(s)))$

\Rightarrow

$g(a) = n[a] \cup \text{union}[\mathbb{P}(a)]$

...

lemmas

$g(t) \subseteq t$

theorems

$\forall x \cdot (x \in t \Rightarrow n(x) \in t) ; \quad \checkmark$

$\forall a \cdot (a \in \mathbb{P}(t) \Rightarrow \text{union}(a) \in t) ; \quad \checkmark$

$\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a)$

end

Constructing *Fixpoint*

construct

Fixpoint

sets

s

components

h

returns

t

axioms

$h \in \mathbb{P}(s) \rightarrow \mathbb{P}(s) ;$

$\forall (a, b) \cdot (a \in \mathbb{P}(s) \wedge b \in \mathbb{P}(s) \wedge a \subseteq b \Rightarrow h(a) \subseteq h(b))$

constants

a

definition

$a \in \mathbb{P}(\mathbb{P}(s)) ; a = \{x \mid x \in \mathbb{P}(s) \wedge h(x) \subseteq x\}$

definition

$t \in \mathbb{P}(s) ; t = \text{inter}(a)$

lemmas

$\text{Inter}(s, a) \quad \checkmark$

theorems

$h(t) \subseteq t ; \quad \checkmark$

$\forall p \cdot (p \in \mathbb{P}(s) \wedge h(p) \subseteq p \Rightarrow t \subseteq p) \quad \checkmark$

end

Constructing *Inter*

structure

Inter

sets

s

components

a

axioms

$a \in \mathbb{P}_1(\mathbb{P}(s))$

theorems

$\forall n \cdot (n \in a \Rightarrow \text{inter}(a) \subseteq n) ; \quad \checkmark$

$\forall m \cdot (m \subseteq s \wedge \forall n \cdot (n \in a \Rightarrow m \subseteq n) \Rightarrow m \subseteq \text{inter}(a)) \quad \checkmark$

end

Revisiting the Construct *Transfinite*

We must prove $\forall a \cdot (a \in \mathbb{P}_1(t) \Rightarrow \text{inter}(a) \in a)$

axioms

$$n \in \mathbb{P}(s) \rightarrow \mathbb{P}(s) ;$$

$$n(s) = s ;$$

$$\forall a \cdot (a \in \mathbb{P}(s) \wedge a \neq s \Rightarrow \exists x \cdot (x \in s - a \wedge n(a) = a \cup \{x\}))$$

...

$a \in \text{inter}(a)$

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$a \in \text{inter}(a)$

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$a \in \text{inter}(a)$

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$a \in \text{inter}(a)$

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$$\neg \forall y \cdot (y \in a \Rightarrow n(\text{union}(b)) \subseteq y)$$

$a \in \text{inter}(a)$

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$$\neg \forall y \cdot (y \in a \Rightarrow n(\text{union}(b)) \subseteq y)$$

$$\exists y \cdot (y \in a \wedge \neg n(\text{union}(b)) \subseteq y)$$

$a \in \text{inter}(a)$ if \subseteq is a total order on t

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$$\neg \forall y \cdot (y \in a \Rightarrow n(\text{union}(b)) \subseteq y)$$

$$\exists y \cdot (y \in a \wedge \neg n(\text{union}(b)) \subseteq y)$$

$$y \subset n(\text{union}(b))$$

$a \in \text{inter}(a)$ if \subseteq is a total order on t

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$$\neg \forall y \cdot (y \in a \Rightarrow n(\text{union}(b)) \subseteq y)$$

$$\exists y \cdot (y \in a \wedge \neg n(\text{union}(b)) \subseteq y)$$

$$y \subset n(\text{union}(b))$$

$$\text{union}(b) \subseteq \text{inter}(a) \subseteq y \subset \text{union}(b) \cup \{x\}$$

$a \in \text{inter}(a)$ if \subseteq is a total order on t

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$$\neg \forall y \cdot (y \in a \Rightarrow n(\text{union}(b)) \subseteq y)$$

$$\exists y \cdot (y \in a \wedge \neg n(\text{union}(b)) \subseteq y)$$

$$y \subset n(\text{union}(b))$$

$$\text{union}(b) \subseteq \text{inter}(a) \subseteq y \subset \text{union}(b) \cup \{x\}$$

$$\text{union}(b) = \text{inter}(a) = y \subset \text{union}(b) \cup \{x\}$$

$a \in \text{inter}(a)$ if \subseteq is a total order on t

$$b = \{x \mid x \in t \wedge x \subseteq \text{inter}(a)\}$$

$$\text{union}(b) \subseteq \text{inter}(a)$$

$$\neg n(\text{union}(b)) \subseteq \text{inter}(a)$$

$$\neg \forall y \cdot (y \in a \Rightarrow n(\text{union}(b)) \subseteq y)$$

$$\exists y \cdot (y \in a \wedge \neg n(\text{union}(b)) \subseteq y)$$

$$y \subset n(\text{union}(b))$$

$$\text{union}(b) \subseteq \text{inter}(a) \subseteq y \subset \text{union}(b) \cup \{x\}$$

$$\text{union}(b) = \text{inter}(a) = y \subset \text{union}(b) \cup \{x\}$$

Proving the Total Ordering of t

We have proved a transfinite induction lemma

construct

Transfinite

...

definition

$t \in \mathbb{P}(\mathbb{P}(s))$;

$t = \text{Fixpoint}(\mathbb{P}(s), g)$ \checkmark

lemmas

$g(t) \subseteq t$; \checkmark

$\forall p \cdot \left(\begin{array}{l} p \in \mathbb{P}(\mathbb{P}(s)) \wedge \\ \forall a \cdot (a \in p \Rightarrow n(a) \in p) \wedge \\ \forall b \cdot (b \in \mathbb{P}(p) \Rightarrow \text{union}(b) \in p) \\ \Rightarrow \\ t \subseteq p \end{array} \right) ; \checkmark$

$\forall (x, y) \cdot (x \in t \wedge y \in t \Rightarrow x \subseteq y \vee y \subseteq x)$

...

end

Transfinite induction lemma

$$\forall p \cdot \left(\begin{array}{l} p \in \mathbb{P}(\mathbb{P}(s)) \quad \wedge \\ \forall a \cdot (a \in p \Rightarrow n(a) \in p) \quad \wedge \\ \forall b \cdot (b \in \mathbb{P}(p) \Rightarrow \text{union}(b) \in p) \\ \Rightarrow \\ t \subseteq p \end{array} \right) ; \quad \checkmark$$

Proving the Total Ordering of t

An idea of the proof:

two inductions one on x and inside the next part one on y

and many proof by cases

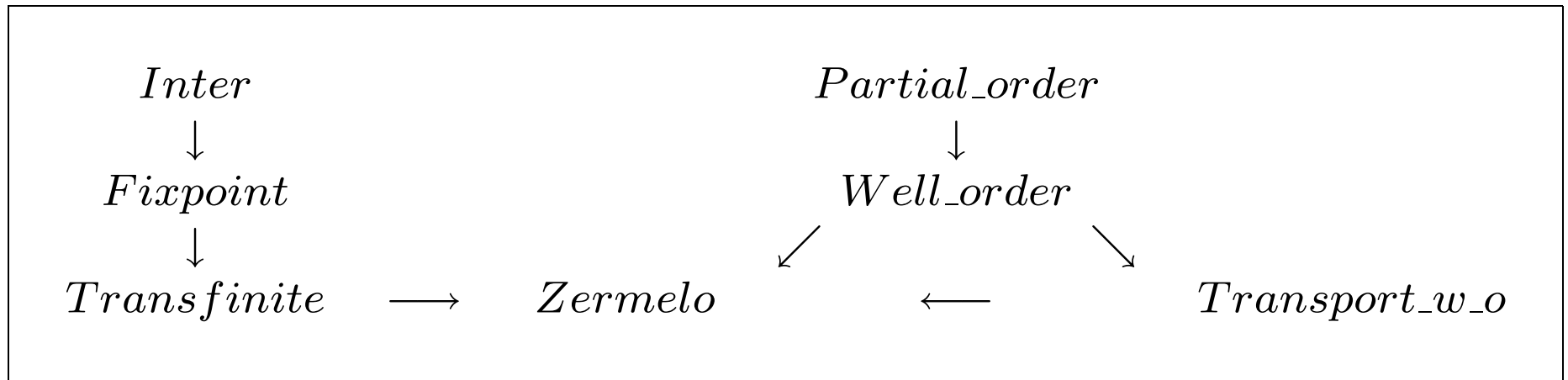
- $x \subseteq y$ or $y \subseteq x$
 - $n(x) \subseteq y$ or $y \subseteq n(x)$
 - $x = s$ or not and $y = s$ or not
-

The two inductions in Atelier B

```
ph({xx | xx: tt & !yy.(yy: tt => xx <: yy or yy <: xx)},  
  !pp.(pp <: POW(ss) &  
  !aa.(aa: pp => nn(aa): pp) &  
    !bb.(bb <: pp => union(bb): pp)  
  => tt <: pp)) &
```

```
ph({yy | yy: tt & (nn(aa) <: yy or yy <: nn(aa))},  
  !pp.(pp <: POW(ss) &  
  !aa.(aa: pp => nn(aa): pp) &  
    !bb.(bb <: pp => union(bb): pp)  
  => tt <: pp)) &
```

The Overall Structure of the Proof



Other approaches

- PVS
- Isabelle

Conclusion

- A structure language (soon in a B machine)
 - Generic (allows mechanical proof and re-use by instantiation)
 - A tool (in Logic-Solver)
 - A tricky mechanical proof
-

Mechanically proven using Atelier B

Project status

COMPONENT	TC	POG	Obv	nPO	nUn	%Pr
Fix	OK	OK	3	7	0	100
Inter	OK	OK	1	2	0	100
TF	OK	OK	4	8	0	100
Zer	OK	OK	19	19	0	100
po	OK	OK	1	0	0	100
two	OK	OK	2	7	0	100
wo	OK	OK	1	0	0	100
TOTAL	OK	OK	31	48	0	100

BZermelo Theorem