Doing Mathematics with the Rodin Platform

Jean-Raymond Abrial

- To present difficult proofs in pure mathematics.

- To figure out that such proofs are highly polymorphic.

- To propose a systematic mathematical methodology.

- To show that such proofs can be mechanized.

- To use them as benchmarks for Event-B mathematical extension.

- Some mathematical concepts in computer science and modeling:

    - Well-founded sets and relations

    - Fixpoint and recursion

    - Transitive closure

    - Graphs, trees, rings, connectivity, ...

- I shall present another difficult theorem.

Reference: J.R. Abrial, D. Cansell, G. Laffitte.

Higher Order Mathematics in B. ZB-2002

Every set can be well-ordered

Refresher on Orders

- Partial order

- Well-order

- Transporting well-orders

Partial Order q on a set S

- Relation: $\boldsymbol{q \in S \leftrightarrow S}$

- Reflexive: $\mathbf{id} \subseteq \boldsymbol{q}$

- Transitive: $\boldsymbol{q \mathbin{;} q \subseteq q}$

- Anti-symmetric: $\boldsymbol{q \cap q^{-1}} \subseteq \mathbf{id}$

- Example: the set inclusion relation is a partial order

  Reflexivity: $\boldsymbol{A \subseteq A}$

  Transitivity: $\boldsymbol{A \subseteq B \land B \subseteq C \;\Rightarrow\; A \subseteq C}$

  Anti-symmetry: $\boldsymbol{A \subseteq B \land B \subseteq A \;\Rightarrow\; A = B}$

Well-order q on a set S

- Partial order: q is a partial order on S

- Each non-empty subset A of S has a smallest element x:

$$\forall A \cdot A \subseteq S \land A \neq \varnothing \Rightarrow (\exists x \cdot x \in A \land A \subseteq q[\{x\}])$$

Example: $\leq$ on $\mathbb{N}$

1 is the smallest number x in $\{1, 3, 7\}$: $\{1, 3, 7\} \subseteq \{ y \mid 1 \leq y \}$

Transporting a Well-order q by Means of an Injection f

- We are given two sets S and T

- We suppose that a relation q is a well-order on T

- We are given a total injection f from S to T: $f \in S \rightarrowtail T$

- **Theorem 1**: $f \, ; q \, ; f^{-1}$ is a well-order on S

- Proof: Rodin demo (3)

- Mind the polymorphism on S and T.

Example of Transportation

$$f \in SEGMENT \rightarrowtail \mathbb{N}$$

$$\forall s \cdot s \in SEGMENT \;\Rightarrow\; f(s) = \min(\{\, x \mid x \notin s \,\})$$

$$\begin{aligned} f = \{ \;& \varnothing \mapsto 0, \\ & \{0\} \mapsto 1, \\ & \{0,1\} \mapsto 2, \\ & \{0,1,2\} \mapsto 3, \\ & \ldots \\ \} \end{aligned}$$

Hence, $SEGMENT$ is well-ordered by transportation of $\leq$

- We apply **Theorem 1**

- For this:

  (1) We construct a well-order q on a certain set T

  (2) We construct a total injection f from S to T

- This is done by:

  (1) Using some **Assumptions** and **Definitions**

  (2) Later proving the **Assumptions**

Constructing the Set T (More Later)

- T is a set of subsets of S: $T \subseteq \mathbb{P}(S)$

- T is partially ordered by set inclusion. This is relation q

- **Assumption 1**: $\forall A \cdot A \subseteq T \wedge A \neq \varnothing \Rightarrow \mathrm{inter}(A) \in A$

- **Theorem 2**: q is a well-order on T

- Proof: Rodin demo (2)

Constructing a Total Function f from S to T

- **Definition 1**:

$$\begin{cases} f \in S \to \mathbb{P}(S) \\ \forall x \cdot z \in S \;\Rightarrow\; f(z) = \mathrm{union}(\{\, x \mid x \in T \;\wedge\; z \notin x \,\}) \end{cases}$$

- **Assumption 2** : $\mathrm{union}[\mathbb{P}(T)] \subseteq T$

- **Theorem 3**: $f \in S \to T$

- Proof: Rodin demo (1)

Proving that f is Injective. Introducing the choice function c

- **Definition 2** : $$\begin{cases} c \in \mathbb{P}1(S) \rightarrow S \\ \forall A \cdot A \subseteq S \;\wedge\; A \neq \varnothing \;\Rightarrow\; c(A) \in A \end{cases}$$

- **Definition 3**: $$\begin{cases} n \in \mathbb{P}(S) \rightarrow \mathbb{P}(S) \\ n(S) = S \\ \forall A \cdot A \subset S \;\Rightarrow\; n(A) = A \cup \{c(S \setminus A)\} \end{cases}$$

- **Assumption 3** : $n[T] \subseteq T$

- **Theorem 4** : $f \in S \rightarrowtail T$

- Proof: Rodin demo (1)

Proving Assumption 1

- **Assumption 4**: $\forall x, y \cdot x \in T \wedge y \in T \Rightarrow x \subseteq y \vee y \subseteq x$

- **Theorem 5**:

Definition 2	$c \in \mathbb{P}1(S) \rightarrow S \ldots$
Definition 3	$n \in \mathbb{P}(S) \rightarrow \mathbb{P}(S) \ldots$
Assumption 2	$\mathrm{union}[\mathbb{P}(T)] \subseteq T$
Assumption 3	$n[T] \subseteq T$
Assumption 4	$\forall x, y \cdot x \in T \wedge y \in T \Rightarrow x \subseteq y \vee y \subseteq x$
$\vdash$	
Assumption 1	$\forall A \cdot A \subseteq T \wedge A \neq \varnothing \Rightarrow \mathrm{inter}(A) \in A$

- Proof: Rodin demo (0)

Proving Assumptions 2 and 3

- **Definition 4**: $\begin{cases} g \in \mathbb{P}(\mathbb{P}(S)) \rightarrow \mathbb{P}(\mathbb{P}(S)) \\ \forall A \cdot A \subseteq \mathbb{P}(S) \;\Rightarrow\; g(A) = n[A] \cup \mathrm{union}[\mathbb{P}(A)] \end{cases}$

- **Assumption 5**: $g[T] \subseteq T$

- **Theorem 6**:

Definition 4	$g \in \mathbb{P}(\mathbb{P}(S)) \rightarrow \mathbb{P}(\mathbb{P}(S)) \ldots$
Assumption 5	$g[T] \subseteq T$
$\vdash$	
Assumption 2	$\mathrm{union}[\mathbb{P}(T)] \subseteq T$
Assumption 3	$n[T] \subseteq T$

- Proof: trivial

- **Definition 5**: $T = \text{fix}(g)$

- **Theorem 7**: $\forall A, B \cdot A \subseteq B \Rightarrow g(A) \subseteq g(B)$

- **Theorem 8**:

Definition 5	$T = \text{fix}(g)$
Theorem 7	$\forall A, B \cdot A \subseteq B \Rightarrow g(A) \subseteq g(B)$
$\vdash$	
Assumption 5	$g[T] \subseteq T$

- Proof: trivial

Proving Assumption 4. Introducing Transfinite Induction

- **Theorem 9**:

$$\begin{array}{l} \forall p \cdot p \subseteq T \\ \qquad \forall a \cdot a \in p \Rightarrow n(a) \in p \\ \qquad \forall b \cdot b \subseteq p \Rightarrow \text{union}(b) \in p \\ \quad \Rightarrow \\ \qquad T \subseteq p \end{array}$$

- **Theorem 10**:

Definition 3 $\quad n \in \mathbb{P}(S) \rightarrow \mathbb{P}(S) \ldots$

Theorem 9 $\quad \ldots$

$\vdash$

Assumption 4 $\quad \forall x, y \cdot x \in T \wedge y \in T \Rightarrow x \subseteq y \vee y \subseteq x$

- Proof: Rodin demo (4)

Re-wording Zermelo's Theorem

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

Structure of the Proof