Formal yet Human-Readable Proofs in Isabelle

Clemens Ballarin

Technische Universität München

Outline

Isabelle, Isar

Locales

Algebraic Library

Possible interaction with the Semantic Web

Isabelle

Interactive Proof Assistant

Generic

- Main Logics: ZF Set Theory, Higher-Order Logic

Highlights

- Newton's Proof of Kepler's Law
- Security Properties of the Internet Protocol TLS
- Formal Semantics of Java

Traditional Tactic-Style Proof

theorem $\bigwedge A\ B.\ A \wedge B \Longrightarrow B \wedge A$
  apply $(\mathit{rule\ conjI})$
  apply $(\mathit{drule\ conjunct2})$ **apply** $\mathit{assumption}$
  apply $(\mathit{drule\ conjunct1})$ **apply** $\mathit{assumption}$
  done

Hard to read — unless you are familiar with natural deduction!

Isar-Style Proof

theorem $\bigwedge A\ B.\ A \wedge B \Longrightarrow B \wedge A$
proof $-$
  fix $A\ B$
  assume ab: $A \wedge B$
  from ab **have** a: A **by** $(rule\ conjunct1)$
  from ab **have** b: B **by** $(rule\ conjunct2)$
  from $b\ a$ **show** $B \wedge A$ **by** $(rule\ conjI)$
qed

Isar-Style Proof

- Inspired by the Mizar prover.
- Proofs are more verbose.
- Proofs are structured.
- Context of fixed variables and assumptions.
- Context contains further information, like local lemmas, simpsets etc.
- Contexts build hierarchical proof environments.
- Isar proofs capture important features of informal proofs.

Locales

It is often useful to fix a context shared by a series of lemmas.
Common practice in informal proof.

Locales:

Named proof contexts with additional features.

Example: Groups

locale *monoid* = *struct* G +
  assumes *m-assoc*:
    $[\![\ x \in \mathit{carrier}\ G;\ y \in \mathit{carrier}\ G;\ z \in \mathit{carrier}\ G\ ]\!] \Longrightarrow$
    $(x \otimes y) \otimes z = x \otimes (y \otimes z)$
   and *l-one* [*simp*]: $x \in \mathit{carrier}\ G \Longrightarrow \mathbf{1} \otimes x = x$
   and *r-one* [*simp*]: $x \in \mathit{carrier}\ G \Longrightarrow x \otimes \mathbf{1} = x$

$\vdots$

locale *group* = *monoid* +
  assumes *Units*: $\mathit{carrier}\ G \subseteq \mathit{Units}\ G$

Example: Groups

Locales

- Abbreviate frequently used contexts.
- Can extend other Locales.
- Provide syntax.
- Modify the context of proof methods.

Example: Groups

Entering a Locale context:

$$\textbf{lemma}\ (\textbf{in}\ \mathit{group})\ \mathit{l\text{-}inv}:$$
$$x \in \mathit{carrier}\ G \Longrightarrow \mathit{inv}\ x \otimes x = \mathbf{1}$$

Exporting from a Locale context:

$$\mathit{group.l\text{-}inv}:$$
$$[\![\mathit{group}\ ?G;\ ?x \in \mathit{carrier}\ ?G]\!] \Longrightarrow \mathit{mult}\ ?G\ (\mathit{m\text{-}inv}\ ?G\ ?x)\ ?x = \mathit{one}\ ?G$$

Example: Sylow's Theorem

Let G be a group of order $p^a m$, p prime.
There exists a subgroup of order p^a.

Proof considers the subsets of G of order p^a and their right-cosets.

Example: Sylow's Theorem

$$
\begin{array}{l}
\textbf{locale } \mathit{sylow} = \mathit{coset} + \\
\quad \textbf{fixes } p \textbf{ and } a \textbf{ and } m \textbf{ and } M \textbf{ and } \mathit{RelM} \\
\quad \textbf{assumes } \mathit{prime\text{-}p}\text{: } p \in \mathit{prime} \\
\quad\quad \textbf{and } \mathit{order\text{-}G}\text{: } \mathit{order}\ G = (p\ \hat{}\ a) * m \\
\quad\quad \textbf{and } \mathit{finite\text{-}G}\ [\mathit{iff}]\text{: } \mathit{finite}\ (\mathit{carrier}\ G) \\
\quad \textbf{defines } M \equiv \{s.\ s \subseteq \mathit{carrier}\ G \wedge \mathit{card}\ s = p\ \hat{}\ a\} \\
\quad\quad \textbf{and } \mathit{RelM} \equiv \{(N1,N2).\ N1 \in M \wedge N2 \in M \wedge \\
\qquad\qquad\qquad\qquad (\exists\, g \in \mathit{carrier}\ G.\ N1 = (N2\ \#{>}\ g))\}
\end{array}
$$

Local definition of frequently used terms.

Example: Sylow's Theorem

Prove Sylow's Theorem in Locale context:

$$\mathbf{lemma}\ (\mathbf{in}\ \mathit{sylow})\ \mathit{sylow\text{-}thm}\colon \exists H.\ \mathit{subgroup}\ H\ G \wedge \mathit{card}\ H = p\,\hat{}\,a$$

Then export to global context:

$$\begin{aligned}&\mathbf{theorem}\ \mathit{sylow\text{-}thm}\colon\\ &\quad [\![\ p \in \mathit{prime};\ \mathit{group}\ G;\ \ \mathit{order}\ G = (p\,\hat{}\,a) * m;\ \mathit{finite}\ (\mathit{carrier}\ G)\ ]\!]\\ &\quad \Longrightarrow \exists H.\ \mathit{subgroup}\ H\ G \wedge \mathit{card}\ H = p\,\hat{}\,a\end{aligned}$$

Example: Group Homomorphisms

— $hom\ G\ H$ is the set of group homomorphisms from G to H.

locale $group\text{-}hom = group\ G + group\ H + var\ h\ +$
  assumes $homh$: $h \in hom\ G\ H$

Operations on Locales:

- Renaming of parameters
- Merging of Locales

Algebraic Library in Isabelle

Foundation for any algebraic development in Isabelle

- Reason in algebraic structures.
- Reason about algebraic structures.
- Reusable.

Used in formalisation of Homological Algebra

- Basic Perturbation Lemma (with Rubio, Aransay)

Available with Isabelle2003

- Released earlier today!
- http://isabelle.in.tum.de

Content of the Algebraic Library

Group theory

- Foundations: subgroup, homomorphism, direct product
- Sylow's theorem (by Kammüller)
- Bijection group (by Kammüller)

Ring theory

- Normalisation method
- Sums and products over finite sets
- Univariate polynomials, universal property

Contributions are welcome!

Possible Interaction with the Semantic Web

Where can Isabelle benefit from the Semantic Web?

- Import proofs!
- Import proof tools.
- Sophisticated theory browsing?

Where can the Semantic Web benefit from Isabelle?

- Library.
- Context-based representation of proofs.