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

\text{theorem } \bigwedge A B. A \land B \implies B \land A

\text{apply (rule conjI)}

\text{apply (drule conjunct2) apply assumption}

\text{apply (drule conjunct1) apply assumption}

done

Hard to read — unless you are familiar with natural deduction!
Isar-Style Proof

theorem $\bigwedge A \ B. \ A \land B \implies B \land A$

proof –
  fix $A \ B$
  assume $ab: \ A \land B$
  from $ab$ have $a: \ A$ by (rule conjunct1)
  from $ab$ have $b: \ B$ by (rule conjunct2)
  from $b \ a$ show $B \land A$ 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:
  \[
  \left[ \ x \in \text{carrier } G; \ y \in \text{carrier } G; \ z \in \text{carrier } G \ \right] \Rightarrow
  \ (x \otimes y) \otimes z = x \otimes (y \otimes z) \\
  \text{and l-one [simp]: } x \in \text{carrier } G \implies 1 \otimes x = x \\
  \text{and r-one [simp]: } x \in \text{carrier } G \implies x \otimes 1 = x \\
  \]

locale group = monoid +
  assumes Units: carrier $G$ $\subseteq$ 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:

**lemma (in group) l-inv:**
\[ x \in \text{carrier } G \implies \text{inv } x \otimes x = 1 \]

Exporting from a Locale context:

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

locale sylow = coset +
  fixes p and a and m and M and RelM
  assumes prime-p: p ∈ prime
    and order-G: order G = (p^a) * m
    and finite-G [iff]: finite (carrier G)
  defines M ≡ { s. s ⊆ carrier G ∧ card s = p^a }
    and RelM ≡ { (N1,N2). N1 ∈ M ∧ N2 ∈ M ∧
    (∃ g ∈ carrier G. N1 = (N2 #> g))}

Local definition of frequently used terms.
Example: Sylow's Theorem

Prove Sylow's Theorem in Locale context:

\text{lemma (in sylow) sylow-thm: } \exists H. \text{ subgroup } H \ G \land \text{ card } H = p^a

Then export to global context:

\text{theorem sylow-thm: }
\begin{array}{l}
[ \ p \in \text{ prime}; \ \text{ group } G; \ \text{ order } G = (p^a) \ast m; \ \text{ finite } (\text{ carrier } G) \ ] \\
\implies \exists H. \ \text{ subgroup } H \ G \land \text{ card } H = p^a
\end{array}
Example: Group Homomorphisms

— $\text{hom } G \times H$ is the set of group homomorphisms from $G$ to $H$.

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

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.