Convenient Reasoning about Substructures
—
Towards Instantiation of Locales

Clemens Ballarin

Technische Universität München

Locales — What Happened Last Year?

- Locales: modular reasoning in the Isabelle theorem prover
- First release of algebra library (May 2003)
  - Sylow's Theorem
  - Universal Property of Polynomial Rings
- Locales can be used with both
  - old-style tactic proofs and structured Isar proofs
- Tutorial to appear
  - In proceedings of Types 2003 workshop (LNCS)

What Next?

Extend library by substantial material about substructures.

- Uniform treatment of subgroups, subrings etc.
- Also normal subgroups, monomorphic embeddings.

Mathematical texts casually switch to what is needed.

Needed: Lattice Theory

Get powerful results by instantiation, e.g.:

Subgroups of a group form a lattice.

Hence if K, L and M are subgroups of G then

$$K \cap (L \cap M) = (K \cap L) \cap M$$

This is modular reasoning!

- Natural to mathematicians.
- But no explicit use of a module system.

Locales

- Designed to support modular reasoning in Isabelle.
- Abbreviate contexts (specifications).
- Hierarchic (including multiple inheritance).
- Isabelle's logical kernel not modified.

Example — Specification of Groups

record $'a$ *group* $=$
  carrier $::$ $'a$ *set*
  mult $::$ $['a,\ 'a] \Rightarrow\ 'a$ (**infixl** $\cdot\imath$ *85*)
  one $::$ $'a$ ($\mathbf{1}\imath$)
  m-inv $::$ $'a \Rightarrow\ 'a$ ($inv\imath$ - [*86*] *85*)

locale *magma* $=$
  fixes G (**structure**)
  assumes *closed*: $[\![\ x \in carrier\ G;\ y \in carrier\ G\ ]\!] \Longrightarrow x \cdot y \in carrier\ G$

locale *semigroup* $=$ *magma* $+$
  assumes *assoc*:
    $[\![\ x \in carrier\ G;\ y \in carrier\ G;\ z \in carrier\ G\ ]\!] \Longrightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$

locale *monoid* $=$ *semigroup* $+$
  assumes *one-closed*: $\mathbf{1} \in carrier\ G$
    and *l-one*: $x \in carrier\ G \Longrightarrow \mathbf{1} \cdot x = x$
    and *r-one*: $x \in carrier\ G \Longrightarrow x \cdot \mathbf{1} = x$

Use of Locales

Specify locale target when stating a theorem.

- Locale assumptions are present in the context.

After the theorem is proved:

- Local version is added to the locale as a fact.
- May also specify attributes — for example,
  fact is marked as a default rewrite rule for the simplifier.
- Exported version contains additional premise.

In order to use a locale it must be specified like a premise.

Example

Show that subgroups form a complete lattice.

$$\mathcal{L} = (\{H \mid \text{subgroup}\, H\, G\}, \text{subgroup})$$

Therefore show

$$I = (\bigcap_{H \in \mathcal{H}} \text{carrier}\, H, \cdot_G, 1_G, \text{inv}_G)$$

is infimum of an arbitrary set of subgroups $\mathcal{H}$.

Therefore show

$$\text{subgroup}\, I\, H$$

for any $H \in \mathcal{H}$.

Example — Continued

Therefore show

$$x, y \in \bigcap_{K \in \mathcal{H}} \text{carrier } K \implies x \cdot_H y \in \bigcap_{K \in \mathcal{H}} \text{carrier } K$$

or, since H subgroup of G, show that

$$x \cdot_G y \in \bigcap_{K \in \mathcal{H}} \text{carrier } K$$

For any $K \in \mathcal{H}$ have $x, y \in K$.

Since K subgroup of G we have finally

$$x \cdot_G y \in K.$$

Example — Continued

Therefore show

$$x, y \in \bigcap_{K \in \mathcal{H}} \text{carrier } K \implies x \cdot_H y \in \bigcap_{K \in \mathcal{H}} \text{carrier } K$$

or, since H submagma of G, show that

$$x \cdot_G y \in \bigcap_{K \in \mathcal{H}} \text{carrier } K$$

For any $K \in \mathcal{H}$ have $x, y \in K$.

Since K submagma of G we have finally

$$x \cdot_G y \in K.$$

Example — Continued

Similarly, need to show

$$1_H \in \bigcap_{K \in \mathcal{H}} \text{carrier } K$$

Involves instantiating that H and K are submonoids of G.

Discussion

The proof contains various examples of instantiation.

At these points reasoning switches from abstract to concrete.

Manual instantiation of (exported) locale lemmas is possible but not convenient:

- Does not take advantage of default tool setup.
- Requires explicit reasoning about inheritance hierarchy.

Solution

Introduce instantiation command:

Given a proof of, say

$$\text{subgroup}\,(\bigcap_{H \in \mathcal{H}} \text{carrier } H, \cdot_G, \ldots)\, G$$

- Instantiate add all facts from locale subgroup.
- Add to current context.

Syntax

Important feature of locales.

Instantiation involves two structures.

- Both may provide their own syntax!
- Prefer syntax of the abstract structure?
- User may want to use both!

Conclusion

Instantiation simplifies switching from abstract to concrete reasoning.

More examples:

$$\text{group } G \implies \text{complete\_lattice}\,(\{H \mid \text{subgroup } H\, G\}, \text{subgroup})$$
$$\text{prime}\, n \Longrightarrow \text{field}(M\text{OD}\, n)$$
$$\text{ring}\, R \Longrightarrow \text{ring}(\text{UP}\, R)$$

Conjecture:

Instantiation makes Locales a full module system!

The Isar Structured Proof Language

State mode:
build context

$$\sigma \left\{ \begin{array}{l} \text{fix <vars>} \\ \text{assume <assms>} \\ \text{have <intermediate>}\ \varphi \\ \text{show <goal>}\ \varphi \end{array} \right.$$

Corresponds to

$$\forall <\text{vars}> . <\text{assms}> \Longrightarrow <\text{goal}>$$

Prove mode:
refine/discharge goals

$$\varphi \left\{ \text{apply <method>}^{+}\ \text{done} \right.$$

$$\varphi \left\{ \begin{array}{l} \text{proof <method>} \\ \quad \sigma\ \text{next}\ \sigma\ \ \ldots\ \text{next}\ \sigma \\ \text{qed <method>} \end{array} \right.$$