IsarMathLib - a formalized mathematics library for Isabelle/ZF

Sławomir Kołodyński

Abstract

We present the current state of the IsarMathLib project.

1 Overview and statistics

IsarMathLib [Kol2005] started as a hobby formalized mathematics project in 2005. Isabelle [Isa1986] was chosen as the theorem proving environment for the project. There were several reasons for that. The most important one was that Isabelle supported the familiar setting of Zermelo-Fraenkel (untyped) set theory encoded in one of its object logics (Isabelle/ZF, [IsaZF1995]). The second reason for the choice was Isabelle's declarative style Isar formal proof language that was "both like and unlike Mizar" [Wen2007]. Lastly, the Isabelle's document preparation system allowed interleaving of formalized mathematical text and informal commentary which was in line with the project's goals.

IsarMathLib does not have any specific goal of formalizing a single result, but aims to be a general-purpose collection of definitions and facts and a playground for experimenting with different ways of creating readable presentations of formalized mathematics. The current release from Nov. 5th 2017 contains 235 definitions and 3301 theorems and lemmas in 82 theory files. The following Table 1 summarizes the distribution of the material over different subprojects and areas of mathematics.

Table 1: Some statistics on IsarMathLib

	definitions	theorems	lines
Basics	85	755	14496
Algebra - monoids, groups, rings, fields	30	479	10149
General Topology	92	413	18313
Algebraic Topology	1	54	1657
Construction of real numbers	15	290	6596
AC in topology	3	14	563
Metamath translation	9	1296	26420

IsarMathLib is hosted on the Savannah software forge. All sources including the Metamath translation tool and isarmathlib.org site generator are available from the SVN repository there.

The main focus areas in the formalization that are not specific to subprojects (discussed below) are Algebra and General and Algebraic Topology. The Topology part starts with the basics: interior, closure, boundary, compact sets, separation axioms and continuous functions. Properties preserved by continuous functions are studied and as an application it is shown, for example that quotient topological spaces of compact (or connected) spaces are

In: A. Editor, B. Coeditor (eds.): Proceedings of the XYZ Workshop, Location, Country, DD-MMM-YYYY, published at http://ceur-ws.org

compact (or connected, resp.). In Algebra the notions and properties of group quotient, conjugate of subgroup, simple groups, endomorphisms of groups etc. are included. In Algebraic topology a couple of basic properties are shown, like that the closure of a subgroup is a subgroup, the closure of a normal subgroup is normal and the property that every locally-compact subgroup of a T_0 group is closed. Some statements about separation properties of topological groups are proven like that if a topology of a group is T_0, then it must be T_3, and that the topology in a topological group is always regular.

Currently IsarMathLib is in maintenance mode. It gets updated for new Isabelle releases, but no new formalized mathematics has been added to it since July 2013.

2 Subprojects

IsarMathLib never had any specific goal of formalizing a particular result, but over the years as my interests changed various subprojects have emerged. The following sections describe some of them.

2.1 Construction of real numbers

The construction formalized in IsarMathLib is relatively less known. It defines real numbers based only on the additive group of integer numbers (although ring properties of integers are used in the proofs). The construction can be summarized as follows: Let $(G, +)$ be an abelian group. We say that a function $f : G \longrightarrow G$ is an *almost homomorphism* if the set $\{f(m+n) - f(m) - f(n) : m, n \in G\}$ is finite. Almost homomorphisms form an abelian group under pointwise addition. We say that two almost homomorphisms f, g are almost equal if the set $\{f(n) - g(n) : n \in G\}$ is finite. This defines an equivalence relation and the corresponding projected abelian group structure on the set of almost homomorphisms. We can then define another operation "$\cdot$" on the equivalence classes of this relation by setting $[f] \cdot [g] = [f \circ g]$, i.e. as the projection of composition of almost homomorphisms on the quotient. In this general setting we can show that the classes of almost homomorphisms with these operations form a ring. If we now specialize setting G to the group of integers we can show the resulting structure is in fact a complete ordered field, i.e. a model of real numbers. The construction does not use any form of the Axiom of Choice in definitions or proofs (a fact that is always difficult to ascertain without formalization).

The formalization was based on a paper by Rob Arthan [Art2004].

2.2 Metamath translation

Metamath [Meg2007] is a language and proof checker for formalized mathematic created by Norman Megill. At the time of the translation project the part of Metamath theorem database that was based on ZFC contained over 8000 theorems (it is more than 20000 now and still in active development). The translation was semiautomatic and done on purely syntactic level. One of Metamath proof checker commands generates a (somewhat) human - readable form of the theorems and proofs. This form was parsed by a tool created for that purpose and converted to Isabelle proof language Isar. Some manual editing was usually necessary for the proofs to get successfully verified by Isabelle. This way about 1300 assertions and 600 proofs have been translated to Isabelle/Isar (the difference coming from the fact that many basic theorems Isabelle/ZF was accepting without an explicit proof based on it's own ZF libraries added to the simplifier).

2.3 The isarmathlib.org web site

It is quite common to present formalized mathematics divided into two parts: an informal discussion and a separate file with source written in a formal proof language. There are two main reasons for that split. The first one is that some proof languages are syntacticly very different from how standard (not machine-checkable) proofs are written. This is especially true for imperative proof scripts that consist of a series of commands that manipulate the "proof state". It is then indeed better to hide the formal part from the view so that fewer people see its ugliness. This concern does not apply to Isabelle's Isar proof language that was designed to be (possible to) read by mathematicians familiar only with mathematical vernacular language.

The second main reason that such division is often done is that formal proofs typically carry and provide much more information content than their informal counterparts. In my view this is not in itself a problem and only becomes one when it is assumed that paper is a natural medium for presenting formal proofs. Indeed, in such case formal proofs, even if written in a well designed language take lots of space and overwhelm the reader with details obstructing the big picture. However, this problem can be easily overcome if one accepts that the

best medium for presenting formal proofs is not paper, but dynamic web pages. The isarmathlib.org web site is an attempt to illustrate that idea.

As an example let's look at a theorem characterizing closure in topological groups, taken from IsarMathLib's TopologicalGroup_ZF.thy theory file. By default only the informal description and the formal statement of the theorem is presented.

The next theorem provides a characterization of closure in topological groups in terms of neighborhoods of zero.

theorem (in topgroup**)** cl_topgroup:

assumes $A \subseteq G$

shows $cl(A) = (\bigcap H \in \mathcal{N}_0.\ A + H)$ proof

A reader interested in the proof may click on the `proof` keyword to see the basic outline of the proof.

The next theorem provides a characterization of closure in topological groups in terms of neighborhoods of zero.

theorem (in topgroup**)** cl_topgroup:

assumes $A \subseteq G$

shows $cl(A) = (\bigcap H \in \mathcal{N}_0.\ A + H)$ proof

from assms **show** $cl(A) \subseteq (\bigcap H \in \mathcal{N}_0.\ A + H)$ **using** zneigh_not_empty , cl_contains_zneigh

next

{ }

thus $(\bigcap H \in \mathcal{N}_0.\ A + H) \subseteq cl(A)$

qed

This shows the reader that the equality between two sets that is claimed in the assertion is proven by showing two inclusions, one of them proven in a separate lemma (whose statement is available by clicking on the reference) and the other one proven locally by some kind or reasoning. Further details can be obtained by clicking on the opening brace {:

The next theorem provides a characterization of closure in topological groups in terms of neighborhoods of zero.

theorem (in topgroup**)** cl_topgroup:

assumes $A \subseteq G$

shows $cl(A) = (\bigcap H \in \mathcal{N}_0.\ A + H)$ proof

from assms **show** $cl(A) \subseteq (\bigcap H \in \mathcal{N}_0.\ A + H)$ **using** zneigh_not_empty , cl_contains_zneigh

next

{

fix x

assume $x \in (\bigcap H \in \mathcal{N}_0.\ A + H)$

then have $x \in A + G$ **using** zneigh_not_empty

with assms **have** $x \in G$ **using** interval_add

have $\forall U \in T.\ x \in U \longrightarrow U \cap A \neq 0$ proof

with assms, $x \in G$ **have** $x \in cl(A)$ **using** inter_neigh_cl

}

thus $(\bigcap H \in \mathcal{N}_0.\ A + H) \subseteq cl(A)$

qed

This process can continue until the reader reaches her desired level of detail or until entire proof is displayed.

Technically, the isarmathlib.org web site is generated by a tool (written in Haskell) which parses IsarMathLib theory files and converts them to HTML. The dynamic aspects of the pages are implemented in about a 100 lines of the Haxe language that compile to about 400 lines of JavaScript.

2.4 Weak forms of AC in topology research

In the first half of 2013 IsarMathLib received a large (10 theory files, 155 theorems) contribution of formalized material from Daniel de la Concepción Sáez. Part of that was original research on equivalence of some purely topological statements to certain weak versions of the Axiom of Choice.

Namely, for a given cardinal Q we say that the axiom of Q-choice holds for subsets of K if we can find a choice function for every family of subsets of K whose (that family's) cardinality does not exceed Q. If the axiom of Q-choice holds for subsets of K for every set K we simply say that the axiom of Q-choice holds.

It is known that some statements in topology aren't just derived from choice axioms, but also equivalent to them. For example the following are known to be equivalent:

- Every topological space of second cardinality csucc(Q) is separable of cardinality csucc(Q).
- The axiom of Q-choice holds.

Here the csucc(Q) is the successor cardinal of Q and we say that T *is of second type of cardinal* Q if there exist B such that B is a base for T and $B \prec Q$ and T *is separable of cardinal* Q if there exist $U \subseteq \bigcup T$ such that $\overline{U} = \bigcup T$ and $U \prec Q$.

In his contribution Daniel de la Concepción Sáez built on existing material on General Topology and formalized a number of new statements of this kind.

In 2015 Daniel made the informal description of the results available on arXiv.org [Conc2015]. Unfortunately due to limitations of the tool generating the HTML presentation of the IsarMathLib theories only a subset of Daniel's contribution is presented on the isarmathlib.org we site. The complete version can be found in the Isabelle generated IsarMathLib's proof document [Kol2017].

Besides the results related to the subject of relation between axiom(s) of choice and topology Daniel de la Concepción Sáez' contribution concerns a study of notion of properties of topological spaces. Turns out given a property of a topological space one can define a local version of a property in general. This is applied to

local versions of the property of being finite or compact or Hausdorff (i.e. locally finite, locally compact, locally Hausdorff). There are a couple of applications formalized as well, like one-point compactification that allows showing that every locally compact Hausdorff space is regular. Also there are some results on the interplay between hereditability of a property and local properties.

It is well-known that automorphisms of a topological space form a group. This fact is proven and automorphism groups for co-cardinal, included-set, and excluded-set topologies are identified. For order topologies it is shown that order isomorphisms are homeomorphisms of the topology induced by the order.

2.4.1 Acknowledgements

I would like to thank my wife for proofreading this document.

References

[Art2004] R. D. Arthan "The Eudoxus Real Numbers", 2004

[Conc2015] Daniel de la Concepción "New equivalences to axioms weaker than AC in topology", arXiv:1510.09139

[Isa1986] http://isabelle.in.tum.de

[IsaZF1995] http://isabelle.in.tum.de/dist/library/ZF

[Kol2005] Sławomir Kołodyński http://www.nongnu.org/isarmathlib/

[Kol2017] Sławomir Kołodyński, Daniel de la Concepción http://www.nongnu.org/isarmathlib/IsarMathLib/document.pdf

[Meg2007] Norman Megill "Metamath: A Computer Language for Pure Mathematics", 2007 Lulu Press, Morrisville, North Carolina. ISBN 978-1-4116-3724-5

[Wen2007] Makarius Wenzel "Isabelle/Isar a Generic Framework for Human-Readable Proof Documents" Studies in Logic, Grammar and Rhetoric 10 (23) 2007