Theorem and proof transfer for a universal collaborative repository of formal proofs

Théo Zimmermann

\(\pi r^2\) project-team, Inria
&
IRIF, Paris Diderot University

Logipedia meeting
Tuesday, 22 January 2019
Concepts have multiple definitions (and multiple names)

- Equivalent characterizations
- Different foundations
- Varied levels of efficiency
- Invented by different people

Why try to select a canonical one?
Theorems have multiple statements (and zero, one, or several names)

- Order of hypotheses
- Equivalent formulation of hypotheses
- Associativity, commutativity, symmetry...
- Specializations, generalizations

Why try to eliminate duplicates?
Duplication is unavoidable (and sometimes good), so we need instead:

- Good search
- Good automation
- Concept alignment
Finding concept alignments

- Automation should automatically find potential alignments.
- Try to prove transfer properties.
- Ask humans to prove other transfer properties (or rate the likelihood of the conjecture).
Using concept alignments

- To transfer theorems: the proof still depends on the transferred theorem, and its dependencies.
- To transfer proofs: more difficult but can avoid complex dependencies.

\[
\begin{align*}
(\mathbb{N}, |) & \text{ is isomorphic to multisets of prime numbers equipped with multiset inclusion.} \\
\mathbb{n} | \mathbb{m} & \iff \exists p, p \cdot \mathbb{n} = \mathbb{m} \\
\mathbb{n} \sqsubseteq \mathbb{m} & \iff \forall x \in \mathbb{n}, x \in \mathbb{m}
\end{align*}
\]
Using concept alignments

- To transfer theorems: the proof still depends on the transferred theorem, and its dependencies.

- To transfer proofs: more difficult but can avoid complex dependencies.

Sometimes a theorem can be transferred but not its proof. For instance, if the statement contains two related operators but the proof needs to unfold them and they do not unfold in the same way.

\((\mathbb{N}, |)\) is isomorphic to multisets of prime numbers equipped with multiset inclusion.

\[ n|m \triangleq \exists p, p \cdot n = m \text{ while } n \sqsubseteq m \triangleq \forall x \in n, x \in m \]
How to transfer

[1999] C. Dubois, M. Jaume, *Reuse of formal developments: some experiments within Coq*

[2000] N. Magaud, Y. Bertot, *Changing Data Structures in Type Theory: A Study of Natural Numbers*

[2001] G. Barthe, O. Pons, *Type Isomorphisms and Proof Reuse in Dependent Type Theory*


[2013] P. Lammich, *Automatic Data Refinement*


[2015] T. Zimmermann, H. Herbelin, *Automatic and Transparent Transfer of Theorems along Isomorphisms in the Coq Proof Assistant*

[2017] R. Cauderlier, C. Dubois, *Focalize and dedukti to the rescue for proof interoperability*


Sorry to those I forgot…
How to relate the first line to the second?

\[ \forall x : A, \ A.eq \ (A.add \ x \ A.zero) \ x \]

\[ \forall x : B, \ B.eq \ (B.add \ x \ B.zero) \ x \]
Transfer 101

How to relate the first line to the second?

\[ \forall x : A, \ A.\text{eq} \ (A.\text{add} \ x \ A.\text{zero}) \ x \]

\[ \forall x : B, \ B.\text{eq} \ (B.\text{add} \ x \ B.\text{zero}) \ x \]

First transformation:

\[ \text{A.all} \ (\lambda x. \ A.\text{eq} \ (A.\text{add} \ x \ A.\text{zero}) \ x) \]

\[ \rightarrow \]

\[ \text{B.all} \ (\lambda x. \ B.\text{eq} \ (B.\text{add} \ x \ B.\text{zero}) \ x) \]
Transfer 101

(from Huffman and Kunčar)

\[
\Gamma \vdash (A \Rightarrow B) \ f \ g \quad \Gamma \vdash A \ x \ y
\]

\[
\frac{}{\Gamma \vdash B \ (f \ x) \ (g \ y)}_{\text{APP}}
\]

\[
\Gamma, A \ x \ y \vdash B \ (f \ x) \ (g \ y)
\]

\[
\frac{}{(\Gamma \vdash A \Rightarrow B) \ (\lambda x. f \ x) \ (\lambda y. g \ y)}_{\text{ABS}}
\]

\[
A \ x \ y \in \Gamma
\]

\[
\frac{}{\Gamma \vdash A \ x \ y}_{\text{VAR}}
\]
Thanks to:

\[(\sim \Rightarrow \Rightarrow) \Rightarrow \Rightarrow) A.\text{all} B.\text{all}\]

we get down to:

\[x, x', x \sim x' \vdash A.\text{eq} (A.\text{add} x A.\text{zero}) x\]
\[\Rightarrow B.\text{eq} (B.\text{add} x' B.\text{zero}) x'\]

Transfer 101
Transfer 101

Thanks to:

\[(\sim \Rightarrow \rightarrow) \Rightarrow \rightarrow\] A.all B.all

we get down to:

\[x, x', x \sim x' \vdash A.\text{eq} (A.\text{add} x A.\text{zero}) x \ni B.\text{eq} (B.\text{add} x' B.\text{zero}) x'\]

Thanks to:

\[(\sim \Rightarrow \sim \Rightarrow \rightarrow)\] A.eq B.eq

we get down to:

\[x, x', x \sim x' \vdash A.\text{add} x A.\text{zero} \sim B.\text{add} x' B.\text{zero}\]

\[x, x', x \sim x' \vdash x \sim x'\]
Transfer 101

Thanks to:

\((\sim \Rightarrow \sim \Rightarrow \sim) \text{ A.add B.add} \)

we get down to:

\[
x, x', x \sim x' \mid \vdash x \sim x' \\
x, x', x \sim x' \mid \vdash \text{A.zero} \sim \text{B.zero}
\]