Autogenerating Natural Language Proofs for Proof Education

Seth Poulsen, Matthew West, and Talia Ringer
University of Illinois at Urbana-Champaign

GRAINGER ENGINEERING

Presentation Overview

1. Proof Blocks
2. Generating Natural Language Proofs from Coq
3. (WIP) Generating Proof Blocks from Coq

CSB Proof

Recall that the interval $(0,1) = \{r \in \mathbb{R} \mid 0 < r < 1\}$ and $[0,1] = \{r \in \mathbb{R} \mid 0 \le r \le 1\}$. Drag and drop a subset of the blocks below to create a proof of the following statement. **Note, not all blocks are needed in the proof.**

$$|(0,1)| = |[0,1]|$$

We will prove this result by showing $|(0,1)| \le |[0,1]|$ and $|[0,1]| \le |(0,1)|$ and using the Cantor-Schroeder-Bernstein theorem.

Drag from here:

- Since f is injective, $|[0,1]| \le |(0,1)|$.
- Consider the function $f : [0,1] \to (0,1)$ where for any $r \in [0,1]$, $f(r) = \frac{r+1}{4}$.
- f is injective because if $f(r) = r = s = f(s)$ then $r = s$.
- f is injective because if $f(r) = \frac{r+1}{4} = \frac{s+1}{4} = f(s)$ then $r = s$.
- Result follows from the Cantor-Schroeder-Bernstein theorem. (End of Proof)
- f is surjective because for any $r \in (0,1)$, $f(r) = r$.

Construct your solution here:

- Consider the function $id : (0,1) \to [0,1]$ where for any $r \in (0,1)$, $id(r) = r$.
- id is injective because if $id(r) = r = s = id(s)$ then $r = s$.
- Since id is injective, $|(0,1)| \le |[0,1]|$.
- Consider the function $f : [0,1] \to (0,1)$ where for any $r \in [0,1]$, $f(r) = r$.

Related Work

- Educational Proof Tools
- Proof Understanding
  - “more intervention-oriented studies in the area of proof are sorely needed” (Stylianides et al. 2017)
- Parson’s Problems

CSB Proof

Recall that the interval $(0,1) = \{r \in \mathbb{R} \mid 0 < r < 1\}$ and $[0,1] = \{r \in \mathbb{R} \mid 0 \leq r \leq 1\}$. Drag and drop a subset of the blocks below to create a proof of the following statement. **Note, not all blocks are needed in the proof.**

$$|(0,1)| = |[0,1]|$$

We will prove this result by showing $|(0,1)| \leq |[0,1]|$ and $|[0,1]| \leq |(0,1)|$ and using the Cantor-Schroeder-Bernstein theorem.

Drag from here:

6 Since f is injective, $|[0,1]| \leq |(0,1)|$.

4 Consider the function $f : [0,1] \to (0,1)$ where for any $r \in [0,1]$, $f(r) = \frac{r+1}{4}$.

f is injective because if $f(r) = r = s = f(s)$ then $r = s$.

5 f is injective because if $f(r) = \frac{r+1}{4} = \frac{s+1}{4} = f(s)$ then $r = s$.

7 Result follows from the Cantor-Schroeder-Bernstein theorem. (End of Proof)

f is surjective because for any $r \in (0,1)$, $f(r) = r$.

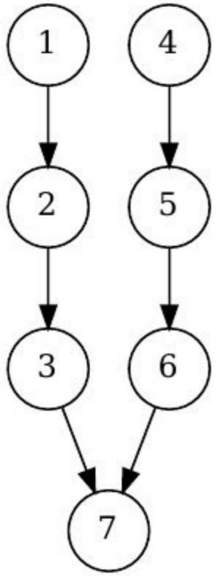
Construct your solution here:

1 Consider the function $id : (0,1) \to [0,1]$ where for any $r \in (0,1)$, $id(r) = r$.

2 id is injective because if $id(r) = r = s = id(s)$ then $r = s$.

3 Since id is injective, $|(0,1)| \leq |[0,1]|$.

Consider the function $f : [0,1] \to (0,1)$ where for any $r \in [0,1]$, $f(r) = r$.



```
<pl-order-blocks feedback="first-wrong" answers-name="csb-v1" grading-method="dag">
  <pl-answer correct="true" tag="1" depends="">Consider the function $id: (0,1) \to [0,1]$ where for any $r \in (0,1)$,
    $id(r) = r$.</pl-answer>
  <pl-answer correct="true" tag="2" depends="1">$id$ is injective because if $id(r) = r = s = id(s)$ then $r=s$.</pl-answer>
  <pl-answer correct="true" tag="3" depends="2">Since $id$ is injective, $|(0,1)| \leq |[0,1]|$.</pl-answer>
  <pl-answer correct="true" tag="4" depends="" >Consider the function $f: [0,1] \to (0,1)$ where for any $r \in [0,1]$,
    $f(r) = \frac{r+1}{4}$.</pl-answer>
  <pl-answer correct="true" tag="5" depends="4">$f$ is injective because if $f(r) = \frac{r+1}{4} = \frac{s+1}{4} = f(s)$
    then $r=s$.</pl-answer>
  <pl-answer correct="true" tag="6" depends="5">Since $f$ is injective, $|[0,1]| \leq |(0,1)|$.</pl-answer>
  <pl-answer correct="true" tag="7" depends="3,6">Result follows from the Cantor-Schroeder-Bernstein theorem.
    (End of Proof)</pl-answer>

  <!-- Distractors -->
  <pl-answer correct="false" tag="" depends="">Consider the function $f: [0,1] \to (0,1)$ where for any $r \in [0,1]$,
    $f(r) = r$.</pl-answer>
  <pl-answer correct="false" tag="" depends="">$f$ is injective because if $f(r) = r = s = f(s)$ then $r=s$.</pl-answer>
  <pl-answer correct="false" tag="" depends="">$f$ is surjective because for any $r \in (0,1)$, $f(r) = r$.</pl-answer>
</pl-order-blocks>
```

Challenges of Coq -> Proof Blocks

1. Translate the formal proof to a natural language proof
2. Extract the dependency graph of parts of the proof

Translating Formal Proofs to Natural Language

1. First Attempt: naively translate low-level logic to natural language
   - EXPOUND: Chester, 1976
   - Coq: Coscoy, Kahn, Théry, 1995

$\lambda A, B : Prop.\ \lambda h : A \vee B.$

$(\vee elim\ A\ B\ (B \vee A\ )(\lambda i : A.\ \vee intro_r\ B\ A\ i)\ (\lambda j : B.\ \vee intro_l\ B\ A\ j)\ h)$

Let $A, B : Prop$

Assume $A \vee B$ (h)

Assume A (i)

From i and the definition of $\vee$, we have $B \vee A$

-We have proved $A \rightarrow B \vee A$

Assume B (j)

From j and the definition of $\vee$, we have $B \vee A$

-We have proved $B \rightarrow B \vee A$

-We have h

Applying $\vee elim$ we get $B \vee A$

We have proved $A \vee B \rightarrow B \vee A$

We have proved $\vee A, B : Prop.A \vee B \rightarrow B \vee A$

Translating Formal Proofs to Natural Language

2. Further Work: Aggregate logical steps into higher level statements, or translate directly from the tactics
   - Coq: Coscoy, 1997
   - LF Type Theory: Huang and Fiedler, 1997
   - NuPRL: Holland-Minkley, Barzilay, Constable, 1999

Theorem: Trans_R imp_Trans_Inv_R.

Statement : ∀ U: Set. ∀ R: (Rel U). (Trans U R) (Trans U (Inv U R)).

Proof:

Consider a set U and a R of type (Rel U) such that
∀ x, y,z: U. (R x y) (R y z) (R x z) (trans') and consider three elements x,
y and z of U such that (Inv U R x y) (h1) and (Inv U R y z) (h2).
-Using definition of Inv with hypothesis h2 we get (R z y)
-Using definition of Inv with hypothesis h1 we get (R y x)
Applying hypothesis trans' to these two results we get (R z x)
So, applying definition of Inv, we get (Inv U R x z).
Q.E.D.

Translating Formal Proofs to Natural Language

3. More recent: Only allow certain Tactics
   - Robotone: Ganesalingam and Gowers, 2017

Consider the following proof that if $f : X \to Y$ is continuous and U is an open subset of Y, then $f^{-1}(U)$ is an open subset of X:

> Let x be an element of $f^{-1}(U)$. Then $f(x) \in U$. Therefore, since U is open, there exists $\eta > 0$ such that $u \in U$ whenever $d(f(x), u) < \eta$. We would like to find $\delta > 0$ s.t. $y \in f^{-1}(U)$ whenever $d(x, y) < \delta$. But $y \in f^{-1}(U)$ if and only if $f(y) \in U$. We know that $f(y) \in U$ whenever $d(f(x), f(y)) < \eta$. Since f is continuous, there exists $\theta > 0$ such that $d(f(x), f(y)) < \eta$ whenever $d(x, y) < \theta$. Therefore, setting $\delta = \theta$, we are done.

Robotone

- Benefits:
  - Clear natural language output
- Drawbacks:
  - Supports only very few kinds of proofs

Can we reap the benefits of using an established theorem proving environment *and* the benefits of a restricted tactic set?

Tactic Category	Robotone Tactic	Coq Tactic
Deletion	`deleteDone`	Done automatically
	`deleteDoneDisjunct`	Done automatically
	`deleteDangling`	N/A
	`deleteUnmatchable`	N/A
Tidying	`peelAndSplitUniversalConditionalTarget`	`intros`
	`splitConjunctiveTarget`	`split`
	`peelBareUniversalTarget`	`intro/intros`
	`removeTarget`	`exists/reflexivity/assumption`
	`collapseSubtableauTarget`	Done automatically
Applying	`forwardsReasoning`	`rewrite/apply`
	`forwardsLibraryReasoning`	`rewrite/apply`
	`expandPreExistentialHypothesis`	Done automatically
	`elementaryExpansionOfHypothesis`	Done automatically
	`backwardsReasoning`	`rewrite/apply`
	`backwardsLibraryReasoning`	`rewrite/apply`
	`elementaryExpansionOfTarget`	`unfold`
	`expandPreUniversalTarget`	`unfold`
	`solveBullets`	`auto/ring/field`, etc.
	`automaticRewrite`	Done automatically
Suspension	`expandPreExistentialTarget`	Done automatically
	`convertDiamondToBullet`	N/A
	`unlockExistentialUniversalConditionalTarget`	`eexists`
	`unlockExistentialTarget`	`eexists`
Equality Substitution	`rewriteVariableVariableEquality`	`rewrite`
	`rewriteVariableTermEquality`	`rewrite`

Robottwo

- Coq plugin that outputs natural language proofs
- Only allow tactics that have a clear natural language translation

```
Lemma divide_refl: forall a: Z, (a | a).
Proof.
    intro x.
    unfold divide.
    exists 1.
    ring.
Qed.
```

```
Lemma divide_refl_inst: forall a: Z, (a | a).
Proof.
    PreExplain intro x.
    intro x.
    PostExplain intro x.

    PreExplain unfold divide.
    unfold divide.
    PostExplain unfold divide.

    PreExplain exists 1.
    exists 1.
    PostExplain exists 1.

    PreExplain ring.
    ring.
    PostExplain ring.
Qed.
```

Let x be an arbitrary element of $\mathbb{Z}$. Now we must show that $(x|x)$. Which by the definition of divide means we need to show that $\exists q \in \mathbb{Z}, x = q * x$. Choose q to be 1. Now we must show that $x = 1 * x$. By algebraic simplification, this is clearly true.

Challenges

- Decision Procedures Hiding Behind Tactics
- Use of non-standard definitions
- Excessive proof term manipulation

What’s next?

Links

- https://proofblocks.org
- https://prairielearn.org
- https://github.com/SethPoulsen/robottwo

Contact

- sethp3@illinois.edu