

Proof Explainer Project

Advancing Proof Comprehension

Vadim Zaliva | vadim@zaliva.org

The Problem

Formal proofs using Proof Assistants such as Coq, Lean, and Isabelle have become important design artefacts of modern high-assurance software systems. Along with the traditional source code base, proof scripts must be reviewed, documented, and maintained. As different groups of proof engineers work on them over time, proof scripts' documentation and overall readability become crucial.

Unfortunately, proof scripts are generally not easily human-readable. Consider the following example of a textbook [3] proof of Gauss' Formula in Coq, and compare it with the explanation generated by the LLM, shown in Appendix A, and the proof from a classical mathematics textbook [5], shown in Appendix B.

```
Example gauss n :  
  \sum_ (0 <= i < n.+1) i = n * n.+1 %/ 2.  
Proof.  
  elim: n =>[|n IHn|]; first by apply: big_nat1.  
  rewrite big_nat_recr // = IHn addnC -divnMD1 //.  
  by rewrite mulnS muln1 -addnA -mulSn -mulnS.  
Qed.
```

The difficulty of human comprehensibility goes beyond the obscure syntax and is inherent to tactic languages. Each tactic operates on an implicit proof state, which is invisible unless you step through the script in the proof assistant. Even if the proof state is available, it could be large, making it difficult to focus on the relevant part of each step. Some features of proof assistants allow for writing more human-readable proofs, but proof writers often ignore them in favour of brevity and expediency. One example is automatic variable naming. While tactic languages support some structuring of the proof script to reflect the branching of the proof tree, these features are not always rigorously used by human proof writers, and their expressivity is limited.

Proposal

We propose to develop a tool to explain and document Coq proofs with the help of LLMs. When applied to an already proven lemma, the Proof Explainer will produce standalone documentation or annotated and restructured for readability proof script. It could be made accessible via a simple web interface or integrated into the proof assistant's IDE (e.g. as a VS Code plugin). The command line version could be used in a build or continuous integration process to generate online documentation or to annotate proof scripts.

It would be immediately helpful to a wide array of users. Professional proof engineers could use it to examine and understand existing proof code bases. The generated documentation could be used to onboard new team members and conduct code reviews. It would immediately benefit students of formal methods and proof engineering by allowing to break down and understand the intricacies of existing proofs. It could be an invaluable educational tool for learning best practices and building confidence in engaging with real-world proof codebases.

The approach

The key observation is that proof explanation requires insight into the proof state, as maintained by a proof assistant. Our tool will integrate a proof assistant to access this information. We can use proof assistant APIs to disambiguate syntax and access the per-step proof state, definitions, and types. When proof automation is used, we can unroll the automation steps to access their intermediate results.

The second insight is that current LLMs have a limit on a LLM's context window, and feeding the whole proof along with all related definitions is impractical. This calls for carefully curating the

information supplied to the model at each reasoning step. We can supply only necessary definitions, strip irrelevant parts of the proof context, or the calculated proof stated diffs between the steps.

Additionally, we can leverage different models and arbitrage or verify their results. Using the well-established “AI agents” approach, we can split reasoning into several steps and process each via separate LLM queries.

Finally, we can perform multi-pass elaboration for projects containing reusable lemmas, first processing the auxiliary lemmas and later using AI-generated summaries of already processed lemmas accessible via retrieval-augmented generation (RAG) or similar techniques.

In the initial project stage, we would focus first on the Rocq proof assistant, which is mature and has good automation means (LSP protocol server, plugin API, and command-line tools). Many Rocq proofs are published as open source, which we can use for training, testing, and validation. Our preliminary experiments show that popular LLM models like OpenAI o1 and Anthropic Claude 3.5 Sonnet can perform basic Rocq proof elaboration, which we can use as a baseline.

Key Differentiators and Related Work

Several recent projects have used LLMs for formal proofs. For example, [2, 7, 8, 1, 9, 6]. Most attempt to synthesise proofs from scratch or aid in repairing existing proofs. Given the current early state of LLMs, these are ambitious goals. We believe that to reach the ultimate goal of fully automated proof synthesis, merely promoting or guiding existing models is insufficient, and a deeper integration into the LLM reasoning process is required, as, for example, proposed in [4]. The required approaches would likely be costly, with prices comparable to training new LLMs. Our goals are more modest, and we are trying to play on the strength of existing models in knowledge summarisation and presentation, where they are already showing promising results.

Budget & Estimates

This is a relatively small-scale project. We estimate 6-8 months with a budget of approximately \$20K, covering the salary of one full-time research engineer and LLM usage fees. The involvement of the PI (and potentially a co-PI) is provided at no cost.

A Appendix: Explained Coq Proof of Gauss's Summation Formula

The following explanation is produced by ChatGPT *o3-mini-high* model using the following prompt.

Explain this proof. In addition to explaining the mathematical proof, provide a step-by-step explanation of the proof script. Give me the explanation in LaTeX format. [proof script text]

The models' output is included verbatim below.

In this appendix we explain the following Coq/SSReflect proof of the formula

$$\sum_{0 \leq i < n+1} i = \frac{n(n+1)}{2},$$

which is the well-known result for the sum of the first n natural numbers.

Proof Script

```
Example gauss n :  
  \sum_(0 <= i < n.+1) i = n * n.+1 %/ 2.  
Proof.  
  elim: n =>[|n IHn|]; first by apply: big_nat1.  
  rewrite big_nat_recr // = IHn addnC -divnMD1 //.  
  by rewrite mulnS muln1 -addnA -mulSn -mulnS.  
Qed.
```

Step-by-Step Explanation

1. Statement of the Theorem: The goal is to prove that

$$\sum_{0 \leq i < n+1} i = \frac{n(n+1)}{2}.$$

Here, the notation $n.+1$ denotes the successor of n (i.e. $n+1$), and the summation $\sum_{(0 \leq i < n.+1)} i$ is taken over the integers $0, 1, \dots, n$.

2. Proof by Induction: The proof proceeds by induction on n , as initiated by the command:

```
elim: n =>[|n IHn|];
```

This command splits the proof into two cases:

- The *base case* where $n = 0$.
- The *inductive step* where one assumes the statement for n (captured by the identifier IHn) and then proves it for $n+1$.

3. Base Case ($n = 0$): For $n = 0$, the summation becomes

$$\sum_{0 \leq i < 0.+1} i = \sum_{i=0}^0 i = 0.$$

The right-hand side is

$$\frac{0 \times 1}{2} = 0.$$

Thus, the equality holds. The tactic:

```
first by apply: big_nat1.
```

applies the lemma `big_nat1`, which establishes that the sum over a singleton range is equal to the sole element in that range (here, 0).

4. Inductive Step: Assuming the induction hypothesis (IHn):

$$\sum_{0 \leq i < n.+1} i = \frac{n(n+1)}{2},$$

we must show that

$$\sum_{0 \leq i < (n.+1).+1} i = \frac{(n+1)(n+2)}{2}.$$

5. Decomposing the Sum: The tactic:

```
rewrite big_nat_recr // = IHn addnC -divnMD1 //.
```

performs several operations:

- `big_nat_recr` rewrites the extended summation

$$\sum_{0 \leq i < (n.+1).+1} i$$

as the sum of the previous range plus the final term:

$$\left(\sum_{0 \leq i < n.+1} i \right) + (n+1).$$

- The `// =` notation triggers automatic simplification.
- `IHn` replaces $\sum_{0 \leq i < n.+1} i$ with $\frac{n(n+1)}{2}$ by the induction hypothesis.
- `addnC` utilises the commutativity of addition to rearrange terms.
- `-divnMD1` manages the division by 2, preparing the expression for the subsequent algebraic manipulation.

6. Algebraic Simplification: The final rewriting step is given by:

```
by rewrite mulnS muln1 -addnA -mulSn -mulnS.
```

This step uses a series of algebraic rewrite rules:

- `mulnS` rewrites multiplication involving the successor, for instance, expressing $(n+1)(n+1)$ as $n(n+1) + (n+1)$.
- `muln1` emphasises that multiplying by 1 does not change a number.
- `-addnA` applies the associativity of addition.
- `-mulSn` and `-mulnS` further manipulate the multiplicative structure.

Together, these rewrites confirm that:

$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

which is exactly the form required to complete the inductive step.

7. Conclusion: Since both the base case and the inductive step have been established, by the principle of mathematical induction the formula

$$\sum_{0 \leq i < n+1} i = \frac{n(n+1)}{2}$$

holds for all natural numbers n .

B Textbook proof of Gauss' Summation Formula

Example 6.1.1 Prove for all $n \in \mathbf{N}$ that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Proof: Let $P(n)$ be the statement $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ and let

$$S = \{n \in \mathbf{N} \mid P(n) \text{ is true}\}.$$

(i) *Remark:* First we prove that $1 \in S$. For $n = 1$, the left-hand side of the statement $P(1)$ is 1 and the right-hand side is $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Consequently, $P(1)$ is true and $1 \in S$.

(ii) *Remark:* Next, we prove that for $n \in \mathbf{N}$, $n \in S \Rightarrow n+1 \in S$. Let $n \in \mathbf{N}$ and assume that $n \in S$. Hence, $P(n)$, which is

$$(1) \quad 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

is assumed to be true. The statement $P(n+1)$, which we must prove to be true using (1), is

$$(2) \quad 1 + 2 + \cdots + n + (n+1) = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

Grouping the summands on the left-hand side of (2) as shown below and then substituting from (1), we find

$$\begin{aligned} (1 + 2 + \cdots + n) + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1) \left(\frac{n}{2} + 1 \right) = \frac{(n+1)(n+2)}{2}. \end{aligned}$$

That is, if (1) is true, it follows that (2) is true and therefore $n+1 \in S$.

Since the hypotheses (i) and (ii) of the Fundamental Theorem of Mathematical Induction are true, the conclusion $S = \mathbf{N}$ is true. Consequently, the statement $P(n)$ is true for all $n \in \mathbf{N}$ —that is, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbf{N}$. ■

Figure 1: A textbook proof of Gauss' Summation Formula from [5]

References

- [1] KOZYREV, A., SOLOVEV, G., KHRAMOV, N., AND PODKOPAEV, A. Coqpilot, a plugin for llm-based generation of proofs. *CoRR abs/2410.19605* (2024).
- [2] LU, M., DELAWARE, B., AND ZHANG, T. Proof automation with large language models. *CoRR abs/2409.14274* (2024).
- [3] MAHBOUBI, A., AND TASSI, E. Mathematical components. *Online book* (2021).
- [4] PARK, K., WANG, J., BERG-KIRKPATRICK, T., POLIKARPOVA, N., AND D’ANTONI, L. Grammar-aligned decoding, 2024.
- [5] ROBERTS, C. *Introduction to Mathematical Proofs*. CRC Press, 2014.
- [6] WANG, R., ZHANG, J., JIA, Y., PAN, R., DIAO, S., PI, R., AND ZHANG, T. Theoremllama: Transforming general-purpose llms into lean4 experts. *CoRR abs/2407.03203* (2024).
- [7] WU, Y., JIANG, A. Q., LI, W., RABE, M. N., STAATS, C., JAMNIK, M., AND SZEGEDY, C. Autoformalization with large language models. *CoRR abs/2205.12615* (2022).
- [8] YANG, K., AND DENG, J. Learning to prove theorems via interacting with proof assistants. *CoRR abs/1905.09381* (2019).
- [9] YANG, K., SWOPE, A. M., GU, A., CHALAMALA, R., SONG, P., YU, S., GODIL, S., PRENGER, R., AND ANANDKUMAR, A. Leandojo: Theorem proving with retrieval-augmented language models. *CoRR abs/2306.15626* (2023).