Working Principles of Proof Assistants and Formalization of some proofs in Agda

Bishesh Bohora, Supreme Chaudhary, Ashwot Acharya
Kathmandu University

July 4, 2025

Abstract

Contents

1 Introduction

2 Foundations

This section sheds light upon some fundamental concept on which Proof Assistants work along with how a proof should be written so that it can be mechanically verified.

2.1 Logic Foundations

This works assumes prior knowledge of Propositional and Predicate Logic. And we refer to both together as **Classical**.

2.1.1 Natural Deduction

The propositions or formulas in Propositional Logic can be verified or proved simply by constructing their truth tables. But for logically complex propositions or propositions with many atomic statements, it becomes difficult to construct a truth table. With predicates, this becomes impossible. Therefore, to mitigate this we adhere to a basic set of inference rules with which we derive conclusions from assumptions in step by step, structured manner. The rule based system which allows us to reason about logical structure of propositions is known as **Natural Deduction**.
With the rules in Section 2.3 of [Alrubyli and Yazeed, 2021] we now present examples on how a proof is carried out with Natural Deduction for Classical Logic.

Example 2.1 $(A \wedge \neg A) \to \bot$
By negation introduction we can write $\neg A$ *as* $A \to \bot$
$(A \wedge (A \to \bot)) \to \bot$

$$\dfrac{[A] \qquad [A \to \bot]}{\bot}\,{\scriptstyle \to E}$$

Example 2.2 *Proof for Law of Excluded Middle* $(P \vee \neg P)$
Note that Example 2.1's result is used here.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[P]}{P \vee \neg P}\,{\scriptstyle \vee I} \qquad [\neg(P \vee \neg P)]}{\bot}\,{\scriptstyle \bot}}{\neg P}\,{\scriptstyle \neg I}}{P \vee \neg P}\,{\scriptstyle \vee I} \qquad [\neg(P \vee \neg P)]}{\bot}\,{\scriptstyle \bot}}{\neg\neg(P \vee \neg P)}\,{\scriptstyle \neg I}}{P \vee \neg P}\,{\scriptstyle \neg\neg E}$$

Example 2.3

$$\forall x(A(x) \to B(x)), A(s) \vdash \exists x B(x)$$

$$\dfrac{\dfrac{\dfrac{[\forall x(A(x) \to B(x))] \qquad [A(s)]}{A(s) \to B(s)}\,{\scriptstyle \forall E}}{B(s)}\,{\scriptstyle \to E}}{\exists x B(x)}\,{\scriptstyle \exists I}$$

The **soundness** and **completeness** of this system are discussed in Section 3.1 and 3.2 [Alrubyli and Yazeed, 2021].

2.1.2 Intuitionstic Logic

Intuitionstic Logic was introduced to formalize the constructive method to do mathematics. Unlike in Classical Logic a statement is True if we can construct a proof for it and to claim a statement is False, again a proof of its falsity is required. This allows the case that some statements are not provable. To show something exists one must provide an method or algorithm to construct it. Proof Assistants leverage this fact. The constructive view of doing mathematics gives a stricter criteria. Intuitionstic Logic can be obtained by restricting certain parts of Classical Logic, like the Law of Excluded Middle.

For inference rules for Natural Deduction in Intuitionstic Logic See 2.1 [Pfenning, 2004], here the language is slightly different from above, we have
Terms $t ::= x \mid a \mid f(t_1, \ldots, t_n)$
Propositions $A ::= P(t_1, \ldots, t_n) \mid A_1 \wedge A_2 \mid A_1 \supset A_2 \mid A_1 \vee A_2 \mid \neg A \mid \bot \mid \top \mid \forall x.A \mid \exists x.A$

The main focus is that this new set of rules does not contain the double negation rule which is present in what we introduced in Section 2.1.1. **Example 2.2** uses the Double negation rule in its proof, which we don't have now. This agrees to that Law of Excluded Middle does not work in Intuitionstic Logic. The method of proof by contradiction also relies on this rule, so constructivists omit it.
These rules are revised with localized hypotheses i.e we use the above rules under a set of premises, and refer the derivation as "derived under a context". With introduction of contexts

$$\textit{Contexts}\ \Gamma ::= .|\Gamma, u : A$$

[See 2.3 [Pfenning, 2004]]

2.2 Type Theory

3 General Architecture of Proof Assistants

4 Upon Some Proof Assistants and Comparative Study

4.1 Coq

4.2 Lean

4.3 Isabelle

4.4 Agda

5 Agda

6 Formalization of Some Proofs

7 Challenges and Workarounds

References

[Alrubyli and Yazeed, 2021] Alrubyli and Yazeed (2021). Natural deduction calculus for first-order logic.

[Pfenning, 2004] Pfenning, F. (2004). This includes revised excerpts from the course notes on linear logic (spring 1998) and computation and deduction. Technical report.