Verifying Atelier B's Predicate Prover[1]

Ciarán Dunne Guillaume Burel
SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris
ciaran-matthew.dunne@telecom-sudparis.eu guillaume.burel@ensiie.fr

April 2026

The Predicate Prover (PP) is an automated theorem prover used by Atelier B to discharge first-order proof obligations arising from B-method developments. Because PP's source code is not publicly available, its results must be trusted without independent verification. We address this gap with `pp2lp`, an OCaml tool that reconstructs PP proofs in LambdaPi, a proof assistant based on the $\lambda\Pi$-calculus modulo rewriting.

We first encode PP's inference rules (conjunction, disjunction, implication, negation, quantification, equality, normalisation, arithmetic, booleans) as LambdaPi symbols whose types capture each rule's antecedents and consequent, and whose bodies are proofs of soundness (Figure 1). PP can be instrumented to record a compact *trace* listing the inference rules applied during a proof; a companion Atelier B utility expands this trace into a *replay* recording, for each step, the rule applied and the intermediate goal (Figure 2, left). Given a replay, `pp2lp` parses it, reconstructs a proof tree, and emits a LambdaPi script that composes the encoded rules following the tree structure, yielding a complete, independently checkable proof (Figure 2, right). We currently encode 126 of PP's 140 inference rules and successfully verify over 100 proof goals.

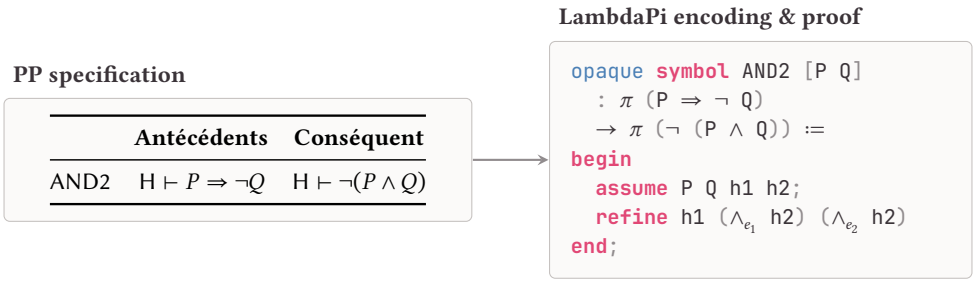

Figure 1: PP rule AND2 and its LambdaPi encoding. The antecedent becomes a function parameter and the consequent the return type; the proof body witnesses soundness using conjunction eliminators $\wedge_{e_1}$, $\wedge_{e_2}$ from LambdaPi's standard library.

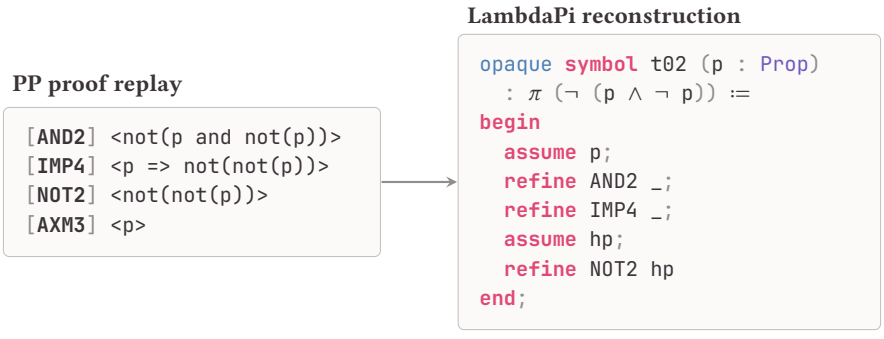

Figure 2: Automated reconstruction of a PP proof of $\neg(p \wedge \neg p)$. Each line in the replay maps to a `refine` tactic that applies the corresponding rule; LambdaPi type-checks the composed proof against the goal type.

[1]This work is supported by the ANR project ICSPA in collaboration with CLEARSY.