A Rewrite System for Proof Constructivization
Raphaël Cauderlier

To cite this version:

HAL Id: hal-01420634
https://inria.hal.science/hal-01420634
Submitted on 20 Dec 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A Rewrite System for Proof Constructivization

Raphaël Cauderlier  
Inria, CNAM  
raphael.cauderlier@inria.fr

Abstract

Proof constructivization is the problem of automatically extracting constructive proofs out of classical proofs. This process is required when classical theorem provers are integrated in intuitionistic proof assistants. We use the ability of rewrite systems to represent partial functions to implement heuristics for proof constructivization in Dedukti, a logical framework based on rewriting in which proofs are first-class objects which can be the subject of computation. We benchmark these heuristics on the proofs output by the automated theorem prover Zenon on the TPTP library of problems.

1. Introduction

Intuitionistic logic is usually presented as the fragment of classical logic obtained by removing the Law of Excluded Middle (or equivalent principles such as the Law of Double Negation) from the primitive axioms. Interestingly, it can also be seen as a supersystem of classical logic in the sense that classical formulae and proofs can be translated in intuitionistic logic thanks to double-negation translations (Kolmogorov 1925, Gödel 1933, Gentzen 1934, Kreisel 1951, Krivine 1990, Boudard and Hermant 2013, Dowek 2015, Gilbert 2015).

Unfortunately, neither point of view is very practical when we want to use a classical theorem prover together with a constructive proof assistant. In the first interpretation, the classical prover is only usable if the Law of Excluded Middle is added as an axiom in the proof assistant thus limiting the interpretation of the proof as an algorithm. In the second interpretation, the classical prover is seen as only able to produce proofs for formulae belonging to a fragment of the syntax where double-negations are mandatory at certain positions.

In practice, classical provers often use the refutation method which consists in adding the negation of the goal as hypothesis and trying to prove the inconsistency of the set of hypotheses. The justification for this simplification is exactly the Law of Double Negation, hence every proof coming from a refutation-based theorem prover contains at least one occurrence of a classical principle. However, a lot of automatically generated classical proofs are believed to be only accidentally classical in the sense that they use classical principles at non-critical places so constructive proofs can be extracted from them; we call this proof constructivization. One goal of this article is to give an experimental lower-bound on the number of proofs which can be constructivized.

Proof constructivization is an inherently incomplete activity. It obviously has to fail when the classically proved formula is not constructively provable but also when intuitionistic proofs of the formula require ingredients which are not present in the classical proof.

Type theory usually attaches no computational behaviour to axioms. We propose however to interpret axioms such as the Law of Excluded Middle as partial functions defined by a set of rewrite rules; normalizing a proof relying on some axiom with respect to this rewrite system may (or not) lead to an axiom-free proof of the same theorem. Such rewrite systems can be defined in the $\lambda I$-calculus modulo (Saillard 2015), an extension of the Logical Framework $\lambda I$-calculus with rewriting. Concretely, we use Dedukti, an implementation of the $\lambda I$-calculus modulo which can be used to check proofs coming from the classical provers Zenon (Cauderlier and Halmagrand 2015) and iProver (Burel 2013).

This article starts with a short presentation of Dedukti in Section 2 then our notations for Natural Deduction proofs are given in Section 3. In Section 4 and 5 we define rewrite systems for proof constructivization. In Section 6 we show how they can be combined in Dedukti. An example of a successful constructivization by normalization is shown in Section 7. The article ends with experimental results on Zenon proofs for the TPTP library in Section 8 and a comparison with related works in Section 9.

2. Dedukti

Dedukti (Saillard 2015) is a type-checker for the $\lambda I$-calculus modulo, a logical framework based on rewriting closely related to Martin-Löf’s Logical Framework (Nordström et al. 1992). The typing rules for the $\lambda I$-calculus modulo are presented in Figure 1. It extends the $\lambda I$-calculus (Harper et al. 1993) (also known as $\lambda P$ and LF) by adding rewrite rules in the context and by replacing the congruence used in the conversion rule (which is $\beta$ equivalence in the $\lambda I$-calculus) by the congruence $\equiv_{\beta I}$ induced by $\beta$-reduction together with the rewrite rules which are present in the context.

In order for type-checking to be decidable, a few assumptions are to be made:

- Left-hand sides of rewrite rules are restricted to linear higher-order patterns (Miller 1991). This constraint makes rewrite rule matching decidable. Dedukti checks this purely syntactic constraint.
- For each rewrite rule, a most general unifier must be computable by unification for the verification of the condition in the typing rule for rewrite rules. Thanks to this constraint, which is also checked by Dedukti, typing of rewrite rules is decidable.
- The congruence $\equiv_{\beta I}$ is approximated by syntactic comparison of $\beta I$ normal forms. So Dedukti might not terminate if $\beta I$-reduction is not terminating and it might be incomplete if $\beta I$-reduction is not confluent. Confluence is also a sufficient condition for subject reduction. These conditions are not decid-
3. Natural Deduction in Dedukti

Natural Deduction is a standard formalism for intuitionistic and classical proofs in Predicate logic. It is very close to type systems for the $\lambda$-calculus so it is a convenient proof system for a logical framework based on type theory such as Dedukti.

3.1 Syntax

We use the standard notations for formulae of Predicate logic (see Figure 2). Our basic connectives are constants, conjunction, disjunction, implication, and quantifiers. Negation and equivalence are seen as derived connectives defined by $\neg A := A \Rightarrow \bot$ and $A \Leftrightarrow B := (A \Rightarrow B) \land (B \Rightarrow A)$ respectively.

3.2 Intuitionistic Natural Deduction in Dedukti

In Dedukti, Intuitionistic Natural Deduction is easy to define following the Curry-Howard correspondence and the proposition-as-
4.2 A rewrite system for the Law of Double Negation

We can do the same job for other classical axioms such as the Law of Double Negation. Let \( \text{LDN}(A) \) abbreviate \( \neg
\neg A \Rightarrow A \), the following are constructive theorems proved in Figure 5:

\[
\begin{align*}
\text{l}_0 : & \text{LEM}(\top) := \text{left}(\top) \\
\text{l}_1 : & \text{LEM}(\bot) := \text{right}(\lambda H \bot. H \bot) \\
\text{l}_2^A (H \Rightarrow B) : & \text{LEM}(A \land B) := \text{right}(\lambda H A \land B. H \Rightarrow \text{fst}(H A \land B)) \\
\text{l}_2^2 (H \Rightarrow B) : & \text{LEM}(A \land B) := \text{right}(\lambda H A \land B. H \Rightarrow \text{snd}(H A \land B)) \\
\text{l}_2 (H \text{LEM}(A), H \text{LEM}(B)) : & \text{LEM}(A \land B) := \\
\text{\forall}_E^{(A \land B)} (\lambda H A, \text{left}(H A), H \text{LEM}(B)) \\
\text{\lambda H \neg A. \text{\forall}_E^{(A \land B)} (\lambda H B, \text{right}(H B)),} \\
\text{\lambda H \neg A. \text{\forall}_E^{(A \lor B)} (\lambda H B, \text{left}(H B), H \text{LEM}(B))} \\
\text{l}_3^A (H \Rightarrow B) : & \text{LEM}(A \Rightarrow B) := \text{left}(\lambda H A. H \Rightarrow B) \\
\text{l}_3^2 (H \Rightarrow B) : & \text{LEM}(A \Rightarrow B) := \text{right}(\lambda H A \Rightarrow B. H \Rightarrow (H A \Rightarrow B)) \\
\text{l}_4 (H \text{LEM}(A), H \text{LEM}(B)) : & \text{LEM}(A \Rightarrow B) := \\
\text{\forall}_E^{(A \Rightarrow B)} (\lambda H A, \text{right}(H B), H \text{LEM}(B)) \\
\text{\lambda H \neg A. \text{\forall}_E^{(A \Rightarrow B)} (\lambda H B, \text{left}(H B), H \text{LEM}(B))} \\
\text{H \text{LEM}(A))} \\
\text{H \text{LEM}(A))} \\
\text{H \text{LEM}(A))} \\
\text{H \text{LEM}(A))}
\end{align*}
\]

Figure 4. Constructive instances of the Law of Excluded Middle

5. Inspecting the proof

Seen as a function symbol in type theory, the symbol \( \text{ldn} \) is a function of two parameters; the first one is a formula \( A \), the second one is a proof of the formula \( \neg \neg A \). The rewrite system that we have just presented only inspects the first argument \( A \) and acts independently of the second one. Thanks to higher-order rewriting, it is also possible to inspect the second one.

5.1 Two trivial special cases

Regardless of the shape of \( A \), there are two trivial ways in which a proof \( \pi \Rightarrow \neg \neg A \) can be constructivized into a proof of \( A \):

- seen as a function from \( \neg \neg A \) to \( \bot \), \( \pi \Rightarrow \neg \neg A \) does not use its argument, hence the current context is inconsistent so we can build a proof of \( A \)
- \( \pi \Rightarrow \neg \neg A \) is an instance of the canonical constructive proof of \( A \Rightarrow \neg \neg A \) (which is \( \lambda H A \Rightarrow \neg \neg A. H A \)

These two special cases can be written in Dedukti as higher-order rewrite rules:

\[
\begin{align*}
\text{ldn}(A, \lambda H \neg A. H A) & \Rightarrow \bot E (H A) \quad (R_1) \\
\text{ldn}(A, \lambda H \neg A. H \neg - A) & \Rightarrow \bot E (H A) \quad (R_2)
\end{align*}
\]

The second rule can be generalized by allowing any proof of \( \neg \neg A \) depending on \( H \Rightarrow A \) (instead of exactly \( H \Rightarrow A \)).

\[
\text{ldn}(A, \lambda H \neg A. (H \Rightarrow \neg \neg A - A) H A) \Rightarrow H A \quad (R_2')
\]

These rules restrict the positions in which \( H \Rightarrow A \) is allowed to appear; in order to favor their application, we consider proof transformations which make some proofs of \( \neg \neg A \) disappear.

5.2 Eliminating negation proofs

The typical case where a proof of \( \neg A \) is useless is when it is eliminated to build a proof of \( A \):

\[
\bot E (H \neg A - A) H A \Rightarrow H A \quad (R_3)
\]

In turn, to favor the application of this rewrite rule, we can give \( \bot E \) some freedom by adding the usual rewrite rules which interpret elimination of \( \bot \) as error propagation:

\[
\begin{align*}
\bot E (H \bot) & \Rightarrow \bot E (H \bot) \quad (R_{\text{abort-\bot}}) \\
\lambda H A. \bot E (H \bot) & \Rightarrow \bot E (H \bot) \quad (R_{\text{abort-\bot}})
\end{align*}
\]

Similar rewrite rules for all introduction and elimination rules can be added this way.
Another option for eliminating ldn is to make it progress toward the leaves in the hope that \( R_1 \) will be applicable in some branches and \( R_2 \) in others; this is the topic of next subsection.

5.3 Exchanging elimination rules

We further inspect the proof of \( \bot \) that missed to be captured by the pattern \( H \) in \( R_1 \) and the pattern \( H \) in \( R_2 \) by looking at where it does use the hypothesis \( H \). \( \bot \) has no introduction rule so it can only be proved by an elimination rule. Elimination rules for disjunction and existential can be traversed by \( \text{ldn} \) if the required proof of \( B \lor C \) and \( \exists x.P(x) \) respectively do not use the assumption \( H \).

\[
\begin{align*}
\text{ldn}(A, \lambda H \Rightarrow_A. \forall \beta (H \Rightarrow_B. H \Rightarrow_A \Rightarrow_C H \Rightarrow_A H_B \lor C)) & \iff \\
\text{ldn}(A, \lambda H \Rightarrow_A. \forall \beta (H \Rightarrow_B. H \Rightarrow_A \Rightarrow_B H \Rightarrow_A H_B), \\
\lambda H_C. \text{ldn}(A, \lambda H \Rightarrow_A. H \Rightarrow_A \Rightarrow_C H \Rightarrow_A H_C), \\
H_B \lor C)
\end{align*}
\]

\[
\begin{align*}
\text{ldn}(A, \lambda H \Rightarrow_A. \exists \beta (H \Rightarrow_x \lor P(x) \Rightarrow A, H \Rightarrow_x P(x)))) & \iff \\
\exists \beta (\lambda H \Rightarrow_A. \text{ldn}(A, \lambda H \Rightarrow_A. H \Rightarrow_x \lor P(x) \Rightarrow H \Rightarrow_A H_B), \\
\lambda H_x. P(x) \Rightarrow H \Rightarrow_A H_B)
\end{align*}
\]

To ease triggering of these new rules, we want to push elimination rules for disjunction and existential toward the root of the formula in the hope that they will meet the \( \text{ldn} \) symbol and help it progress toward the leaves of the proof.

We avoid commuting with introduction rules because it goes a long against cut-elimination and does not seem useful in practice for normal forms with respect to the rewrite system \( \text{ldn} \). Commuting with other elimination rules is however achieved easily:

\[
\begin{align*}
\text{fst}(\forall \beta (H \Rightarrow A, \forall \beta (H \Rightarrow B, H \Rightarrow A \lor B))) & \iff \\
\forall \beta (\text{fst}(H \Rightarrow A), \forall \beta (H \Rightarrow B, H \Rightarrow A \lor B))
\end{align*}
\]

\[
\begin{align*}
\text{snd}(\forall \beta (H \Rightarrow A, \forall \beta (H \Rightarrow B, H \Rightarrow A \lor B))) & \iff \\
\forall \beta (\text{snd}(H \Rightarrow A, \forall \beta (H \Rightarrow B, H \Rightarrow A \lor B))
\end{align*}
\]

7. Example: Zenon classical proof of \( A \Rightarrow A \)

Once translated to Classical Natural Deduction, the classical proof of \( A \Rightarrow A \) that comes out of Zenon is the following term:

\[
\begin{align*}
\text{ldn}(A, A) & \iff \\
\lambda H \Rightarrow (A \Rightarrow A). H \Rightarrow (A \Rightarrow A) \\
(\lambda A. \bot \Rightarrow \bot)(\lambda H \Rightarrow (A \Rightarrow A). (H_A, H_A'))(H_A)
\end{align*}
\]

Two rules apply here, the rule for implication from system \( \text{ldn} \) and the rule \( R_3 \) for elimination of \( \bot \). Following the heuristic strategy of Section 6 the first step \( (R_1 \cup R_2) \) is skipped and we apply the rule in \( \text{ldn} \) leading to the following term:

\[
\begin{align*}
d_3 (\text{ldn}(A), \lambda H \Rightarrow (A \Rightarrow A). H \Rightarrow (A \Rightarrow A)) & \iff \\
(\lambda A. \bot \Rightarrow \bot)(\lambda H \Rightarrow (A \Rightarrow A). (H_A, H_A'))(H_A)
\end{align*}
\]

We now need to unfold the definition of \( d_3 \):

\[
\begin{align*}
d_3 (H \text{ldn}(B), H \Rightarrow (A \Rightarrow B)) & := H_A \cdot H \text{ldn}(B) \cdot (H \Rightarrow B, H \Rightarrow (A \Rightarrow B)) \\
\end{align*}
\]

so our proof of \( A \Rightarrow A \) is now

\[
\begin{align*}
H_A & \cdot \lambda H \Rightarrow (A \Rightarrow A) \\
(\lambda A. \bot \Rightarrow \bot)(\lambda H \Rightarrow (A \Rightarrow A). (H_A, H_A'))(H_A)
\end{align*}
\]

Now we perform elimination of \( \bot \) (\( R_3 \)), which has priority over \( \beta \)-reduction:

\[
\begin{align*}
\lambda H_A & \cdot \text{ldn}(A, A) \cdot (\lambda H \Rightarrow (A \Rightarrow A). (H_A, H_A'))(H_A)
\end{align*}
\]
we now β-reduce:

\[ \lambda H_A. \text{ldn}(A, \lambda H_{\leadsto A}. H_{\leadsto A} H_A) \]

and finally apply \( R_2 \), getting rid of the classical axiom:

\[ \lambda H_A. H_A \]

As we can see, the translation to natural deduction has introduced a fortunate β-redex \((\lambda H'_{\leadsto A}. H_{\leadsto (A \Rightarrow A)}(\lambda H''_{\leadsto A}. H''_{\leadsto A})) H_A\). Reducing this cut would forbid to fire \( R_3 \) but we need β-reduction to simplify the resulting proof so that \( R_2 \) can in turn be fired.

8. Experimental results

We have performed tests on the latest version (v6.3.0) of the reference library for first-order problems: TPTP. This library contains 6528 problems for first-order logic (TPTP FOF format). We filtered these problems by running Zenon with a short timeout\(^1\) Zenon claimed to have proved 1371 problems which form our starting benchmark. For every problems in this benchmark but two, Zenon provided a proof in Classical Sequence Calculus that we type-checked in Dedukti. Among these 1369 proofs, 1258 (91.9%) were translated to classical natural deduction. Among these natural deduction proofs, 1237 (98.3%) were normalized by the combination of rewrite systems presented in Section 6. All these normalized natural deduction proofs were rechecked in Dedukti and 778 (62.9% of the normalized classical proofs) were checked in intuitionistic natural deduction.

As a constructivization tool for natural deduction, our approach succeeded for 61.8% of the classical proofs. We can distinguish four sources of failure:

1. normalization reaches memory or time limits because matching of higher-order patterns can be costly;
2. some TPTP problems are classical theorems but have no constructive proofs;
3. some problems have constructive proofs but these proofs require ingredients that are not present in the classical proof provided by Zenon, a typical example would be a formula of the form \( \varphi \lor P \lor \neg P \) where \( \varphi \) has a complex intuitionistic proof, finding such proofs would require intuitionistic proof search and is out of the scope of our approach;
4. because our approach is heuristic, it is fundamentally incomplete so other proofs are missed, these problems are a good source of inspiration for further improving our heuristics.

The first source of failure affects only 21 proofs (1.7% of the proofs in classical natural deduction). The second source is very hard to count: one goal of the ILTP library (Raths et al. 2005) was to associate a constructive status to TPTP problems but the majority of them (69.7% for ILTP v1.1) remains unsolved or open. Finally, when an intuitionistically valid problem fails to be constructivized by our approach, it is not always clear whether the failure comes from the third or the fourth source because we did not formalize the notion of ingredient present in a classical proof; for example, the formula \( P \Rightarrow (P \lor \neg P) \) has two classical proofs, a constructive one and a non-constructive one, our technique fails to constructivize the non-constructive one \( \lambda H_A. \text{lem}(A) \) as it requires to query the proof context, an operation which can be seen as a very limited form of proof search.

Each line of a TPTP category of problems:

- the \( \text{LK} \) column contains the number of problems proved by Zenon in classical sequent calculus
- the \( \text{NK} \) column contains the number of proofs translated in classical natural deduction
- the \( \text{Normalized} \) column contains the number of classical proofs which have been normalized with respect to our rewrite systems
- the \( \text{NJ} \) column contains the number of proofs for which constructivization has succeeded in a proof in intuitionistic natural deduction

<table>
<thead>
<tr>
<th></th>
<th>LK</th>
<th>NK</th>
<th>Normalized</th>
<th>NJ</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGT</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>ALG</td>
<td>23</td>
<td>13</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>CAT</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>COM</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>CSR</td>
<td>91</td>
<td>91</td>
<td>87</td>
<td>57</td>
</tr>
<tr>
<td>GEO</td>
<td>213</td>
<td>210</td>
<td>210</td>
<td>184</td>
</tr>
<tr>
<td>GRA</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>GRP</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>HWV</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>KLE</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>KRS</td>
<td>62</td>
<td>62</td>
<td>62</td>
<td>12</td>
</tr>
<tr>
<td>LAT</td>
<td>9</td>
<td>9</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>LCL</td>
<td>28</td>
<td>8</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>MED</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>MGT</td>
<td>39</td>
<td>38</td>
<td>35</td>
<td>22</td>
</tr>
<tr>
<td>MSC</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>NLP</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>NUM</td>
<td>101</td>
<td>92</td>
<td>92</td>
<td>78</td>
</tr>
<tr>
<td>PUZ</td>
<td>11</td>
<td>11</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>RNG</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>16</td>
</tr>
<tr>
<td>SCT</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>SET</td>
<td>135</td>
<td>135</td>
<td>135</td>
<td>102</td>
</tr>
<tr>
<td>SEU</td>
<td>84</td>
<td>80</td>
<td>78</td>
<td>60</td>
</tr>
<tr>
<td>SWB</td>
<td>21</td>
<td>21</td>
<td>21</td>
<td>20</td>
</tr>
<tr>
<td>SWC</td>
<td>43</td>
<td>43</td>
<td>43</td>
<td>1</td>
</tr>
<tr>
<td>SWV</td>
<td>132</td>
<td>132</td>
<td>131</td>
<td>75</td>
</tr>
<tr>
<td>SWW</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>SYN</td>
<td>264</td>
<td>201</td>
<td>194</td>
<td>62</td>
</tr>
<tr>
<td>SYO</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>TOP</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Total | 1369 | 1258 | 1237 | 778

Example 6. Per-category results

The details for each TPTP category of problem are summarized in Figure 6.

The experimental conditions for this study were the following:

- Processor: Intel Core i5-4310M @ 2.70GHz
- Timeouts: 10 seconds for Zenon filtering phase, 10 minutes for each Dedukti call
- Tools versions: We used development versions of the tools built from their respective git repositories (git://scm.gforge.inria.fr/dedukti/dedukti.git for Dedukti and git://scm.gforge.inria.fr/zenon/zenon.git for Zenon). More precisely, Dedukti was built from branch develop (latest commit: April 11th 2016), Zenon was built from branch modulo_intuit (latest commit: February 5th 2016).

\(^1\)The choice of this timeout does not affect much the results because the number of proofs found by Zenon in more than a few seconds is very low. It has however a direct impact on the time needed for running the benchmark since this timeout is reached on most TPTP problems.
9. Related Work

The differences between classical and intuitionistic logic have been deeply studied since the early days of intuitionistic logic leading to the discovery of double-negation translations and extensions of the Curry-Howard correspondence to classical logic. Concretely, a few automated theorem provers, iLeanCoP in particular, can be used for intuitionistic logic but their integration in intuitionistic proof assistants is far from easy because they do not yet provide proof certificates in a checkable format. We know only one exception to this rule: a constructivization module for Zenon called Zenonide which is able to produce proofs in Dedukti format.

9.1 Double-negation translations

It is usually easy to test whether a formula is in the image of a given double-negation translation. Since for such formulæ intuitionistic provability corresponds to classical provability, this provides a simple criterion for proof constructivization which does not depend on the classical proof but only on the proven formula. This criterion is not very powerful but it is very efficient: typically in linear time and finite memory.

Our first rewrite system for the Law of Double Negation $R_{dn}$ is related to the way one can replace a double-negation translation by another one. Because the right-hand side of the rule for $ldn(A \Rightarrow B)$ uses $ldn(B)$ but not $ldn(A)$, the correct way to look at $R_{dn}$ is as a transformer for polarized double-negation translations (Boudard and Hermant [2013]).

In the particular case of Zenon proofs in Classical Sequent Calculus and their translation to Classical Natural Deduction, the Law of Double Negation is used at the head of the proof and after introduction of universal quantification only. Because Zenon finds cut-free proofs in Sequent Calculus, the subformula property guarantees that all double negations corresponding to these classical axioms appear in positions where the polarized version of Gödel-Gentzen double-negation translation would also have added a double-negation. After normalization by our rewrite system $R_{dn}$, they are placed at positions where a lighter translation, Gilbert’s double-negation translation (Gilbert [2015]), would also put double-negations.

9.2 Intuitionistic provers

A few automated theorem provers for intuitionistic logic have been developed. The ILTP library (Raths et al. [2005]) is a benchmark constructed from the TPTP problems in FOF format (non-clausal first-order formulæ) to evaluate intuitionistic provers. The most performant intuitionistic prover for predicate logic on this benchmark is by far the iLeanCoP prover. It is noticeable that iLeanCoP is built as a constructivization extension of a classical prover, LeanCoP.

The main difference between our work and an intuitionistic prover such as iLeanCoP is that, in case of failure, iLeanCoP can ask LeanCoP to provide another classical proof. For example, our technique fails to constructivize the following proof of $A \Rightarrow A \Rightarrow \lambda x.\, \text{term}(A)$. Backtracking makes however iLeanCoP complete for first-order intuitionistic logic. According to Oten [2005], this backtracking feature is rarely used because the first classical proof is usually constructive.

Unfortunately, intuitionistic provers such as iLeanCoP do not produce certificates so we can not easily integrate them in intuitionistic proof assistants.

9.3 Zenonide

Zenonide is a constructivization module for Zenon developed by Frédéric Gilbert. Because Zenonide has access to the internal representation of proofs in Zenon, it has access to the proof context for each proof node so the constructivization of Zenon proof of $A \Rightarrow A$ is trivial for Zenonide whereas we have seen in Section 7 that it required some work in our case.

Zenonide is however not able to backtrack to another classical proof as iLeanCoP so it is an interesting middle point between our approach to constructivization and intuitionistic proof search.

Zenonide does not need to translate the classical proof to Natural Deduction, it tries to transform a proof in Classical Sequent Calculus to a proof in Intuitionistic Sequent Calculus so it avoids the combinatorial explosion appearing with some problems of the syntactic category of TPTP which have been especially designed to have no small proof in Natural Deduction. The price to pay for using Sequent Calculus is that more commutations of deduction rules have to be taken into account.

Zenon, as many theorem provers, searches for cut-free proofs; this is a very good point for Zenonide since the cut rule in Sequent Calculus behaves very badly with proof constructivization. Our input proofs do however use natural deduction cuts and these cuts are, as we have seen, sometimes welcomed.

For all these reasons, Zenonide globally performs better than our rewrite systems but also fails on some proofs that we manage to constructivize: on the set of 1371 problems proved by Zenon, Zenonide proves 915 problems constructively but a very fair amount of proofs (113) was constructivized by our rewrite systems despite Zenonide lacks to prove it. If we use our rewrite systems together with Zenonide, we obtain a total constructivization rate of 81.7%.

9.4 Extensions of the Curry-Howard correspondence for Classical Logic

The Curry-Howard correspondence, which is at the heart of the use of logical frameworks such as Dedukti for checking proofs, has been extended to classical reasoning in several ways.

Minimal logic can be extended to a classical logic of implication by Pierce Law $(A \Rightarrow B) \Rightarrow A$ which is a possible type for the call-cc control operator found in the Scheme programming language for example. This remark lead to Parigot’s $\lambda \mu$-calculus which corresponds to a classical extension of Minimal Natural Deduction where several formulæ are allowed at the right side of sequents (Parigot [1992]).

Classical Sequent Calculus has also been the subject of interpretations through the Curry-Howard correspondence leading to Curien and Herbelin’s $\lambda \mu \mu$-calculus for minimal classical sequent calculus (Curien and Herbelin [2000]).

An interpretation of classical logic in terms of stack manipulations is also investigated in the context of classical realizability (Krivine [2001]).

All these systems suffer, as we do, from a lack of confluence but this is directly connected with non-confluence of classical cut elimination whereas we do not even need to consider cut-elimination to loose confluence.

As extensions of typed $\lambda$-calculus, it is possible to ask in these systems whether a given term (that is, a classical proof) reduces to a pure $\lambda$-term (that is, a constructive proof). Conversely, the rewrite systems that we have proposed can be seen as alternative semantics or program transformations in these systems.

We believe that Dedukti is a good framework for studying extensions of these systems to predicate logic.

10. Conclusion

By combining relatively naïve rewrite rules, we constructivized automatically a good proportion of the classical proofs that were found by the theorem prover Zenon.

Our approach can easily be generalized to extensions of Predicate Logic such as polymorphism and Deduction Modulo which are implemented in Zenon. These two extensions would allow the
constructivization of program verification proofs. We expect these proofs to be particularly easy to constructivize because the user is often encouraged in this context to define decidable predicates as functions to type \texttt{bool} and $\forall b: \texttt{bool}. b \lor \neg b$ is constructively provable so even the very simple rewrite system $R_{\text{int}}$ together with a rewrite rule for atoms of type \texttt{bool} should successfully constructivize a lot of problems.

We can also improve our handling of failure by trying to reach an intermediate logic, an extension of intuitionistic logic with an axiom scheme which is classically provable, not intuitionistically provable but not strong enough to prove the Law of Excluded Middle either. Such an intermediate axiom scheme is $\neg A \lor \neg \neg A$ which allows some De Morgan simplification rules. Other axioms of interest would be decidability of equality and decidability of atoms.

We use Dedukti in a very different context than its common usage as a universal proof checker. We hope this new use, especially the usage of non-confluent intermediate rewrite systems producing proofs to be checked in a safe rewrite system (in this case, the signature for intuitionistic natural deduction, which contains no rewrite rule), will be a fruitful source for further automatic elimination of axioms. This topic is not only important for benefiting from the witness property of constructive proofs but also from a reverse mathematics point of view and for interoperating proofs in theories whose union is inconsistent.

References


