The new rewriting engine of Dedukti

Gabriel Hondet
Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria
Laboratoire Spécification et Vérification, 94235, Cachan, France

Frédéric Blanqui
Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria
Laboratoire Spécification et Vérification, 94235, Cachan, France

Abstract

Dedukti is a type-checker for the λΠ-calculus modulo rewriting, an extension of Edinburgh's logical framework LF where functions and type symbols can be defined by rewriting rules. It therefore contains an engine for rewriting LF terms and types according to the rewriting rules given by the user. A key component of this engine is the matching algorithm to find which rules can be fired. In this paper, we describe the class of rewriting rules supported by Dedukti and the new implementation of the matching algorithm. Dedukti supports non-linear rewriting rules on terms with binders using higher-order pattern-matching as in Combinatory Reduction Systems (CRS). The new matching algorithm extends the technique of decision trees introduced by Luc Maranget in the OCaml compiler to this more general context.

2012 ACM Subject Classification Theory of computation → Equational logic and rewriting; Theory of computation → Operational semantics

Keywords and phrases rewriting, higher-order pattern-matching, decision trees

Digital Object Identifier 10.4230/LIPIcs.FSCD.2020.?

Related Version [10]

Supplement Material https://github.com/deducteam/lambdapi.git

Acknowledgements The authors thank Bruno Barras and Rodolphe Lepigre for their help in developing the new rewriting engine of Dedukti.

1 Introduction

Dedukti is primarily a type-checker for the so-called λΠ-calculus modulo rewriting, λΠ/R, an extension of Edinburgh’s logical framework LF [9] where function and type symbols can be defined by rewrite rules. This means that Dedukti takes as input type declarations and rewrite rules, and check that expressions are well typed modulo these rewrite rules and the β-reduction of λ-calculus.

The λΠ-calculus is the simplest type system on top of the pure untyped λ-calculus combining both the usual simple types of (functional) programming (e.g. the type \( \mathbb{N} \Rightarrow \mathbb{N} \) of functions from natural numbers to natural numbers) with value-dependent types (e.g. the type \( \forall n : \mathbb{N}, V(n) \) of vectors of some given dimension). In fact, a simple type \( A \Rightarrow B \) is just a particular case of dependent type \( \forall x : A, B \) where \( x \) does not occur in \( B \). Syntactically, this means that types are not defined prior to terms as usual, but that terms and types are mutually defined.

Moreover, in λΠ/R, a term of type \( A \) is also seen as a term of type \( B \) if \( A \) and \( B \) are equivalent not only modulo β-reduction but also modulo some user-defined rewrite rules \( R \). Therefore, to check that a term \( t \) is of type \( A \), one has to be able to check when two expressions are equivalent modulo β-reduction and rewrite rules. This is why there is a rewriting engine in Dedukti.
The new rewriting engine of Dedukti

Thanks to the Curry-Howard correspondence between λ-terms and proofs on the one hand, and (dependent) types and formulas on the other hand, Dedukti can be used as a proof checker. Hence, in recent years, many satellite tools have been developed in order to translate to Dedukti proofs generated by automated or interactive theorem provers: Krajono for Matita, Coqine for Coq, Holide of OpenTheory (HOL Light, HOL4), Focalide for Focalize, Isabelle, Zenon, iProverModulo, ArchSAT, etc. [1].

By unplugging its type verification engine to only retain its rewriting engine, Dedukti can also be used as a programming language. Thanks to its rewriting capabilities, Dedukti can be used to apply transformation rules on terms and formulas with binders [18, 4].

A rewrite rule is nothing but an oriented equation [2]. Rewriting consists in applying some set of rewrite rules $R$ (and β-reduction) as long as possible so as to get a term in (weak head) normal form. At every step it is therefore necessary to check whether a term matches some left-hand side of a rule of $R$. It is therefore important to have an efficient algorithm to know whether a rule is applicable and select one:

Example 1. Consider the following rules in the new Dedukti syntax (pattern variables are prefixed by & to avoid name clashes with other symbols):

```plaintext
rule f (c (c &x)) a → &x
and f &x b → &x
```

To select the correct rule to rewrite a term, the naive algorithm matches the term against each rule left-hand side from the top rule to the bottom one. Let us apply the algorithm on the matching of the term $t = f (c (c e)) b$.

The first argument of $t$ is matched against the first argument of the first left-hand side $c (c &x)$. As $c (c e)$ matches $c (c &x)$, it succeeds. However, when we pass to the second argument, $b$ does not match the pattern $a$. So the second rule is tried. Pattern &x filters successfully $c (c e)$, and $b$ matches $b$, so it succeeds.

Yet, matching $c (c e)$ against $c (c &x)$ can be avoided. Indeed, if we start by matching the second argument of $f$, then the first rule is rejected in one comparison. The only remaining work is to match $c (c e)$ against &x.

In [14], Maranget introduces a domain-specific language of so-called decision trees for describing matching algorithms, and a procedure for compiling some set of rewrite rules into this language. But his language and compilation procedure handle rewrite systems whose left-hand sides are linear constructor patterns only. In Dedukti, as we are going to see it soon, we use a more general class of patterns. Dedukti patterns can contain defined symbols and λ-abstractions. They can also be non-linear and contain variable-occurrence conditions as in Klop’s Combinatory Reduction Systems (CRS) [11].

In this paper, we describe an extension of Maranget’s work to this more general setting, and present some benchmark.

Outline of the paper In Section 2, we start by giving examples of the kind of rewrite rules that can be handled by Dedukti, before giving a more formal definition. In Section 3, we present our extension of Maranget’s decision trees, their syntax and semantics, and how to compile a set of rewrite rules into this language. In Section 4, we compare this new implementation with previous ones and other tools implementing rewriting. Finally, in Section 5, we discuss some related work and conclude.
We will start by providing the reader with various examples of rewrite rules accepted by Dedukti before giving a formal definition. To this end, we will use the new Dedukti syntax (see https://github.com/Deducteam/lambdapi). In this new syntax, one can use Unicode characters, some function symbols can be written in infix positions and, in rewrite rules, pattern variables need to be prefixed by & to avoid name clashes with function symbols. Note however that, for the sake of simplicity, we may omit some declarations.

Dedukti can of course handle the “Hello world!” example of first-order rewriting, the addition on unary natural numbers, as follows:

```
symbol N:: TYPE
symbol 0:: N
symbol s:: N⇒N
symbol +:: N⇒N⇒N

rule 0 + &m → &m
and (s &n) + &m → s (&n + &m)
```

More interestingly is the fact that, in constrast to functional programming languages like OCaml, Haskell or Coq, rule left-hand sides can overlap each other. Consequently, in Dedukti, addition on unary numbers can be more interestingly defined as follows:

```
rule 0 + &m → &m
and (s &n) + &m → s (&n + &m)
and &m + 0 → &m
and &m + (s &n) → s (&m + &n)
```

With the first definition, one has 0 + t equivalent to t modulo rewriting, written 0 + t ≃ t, for all terms t (of type N), but not t + 0 ≃ t. Hence, the interest of the second definition.

It is also possible to match on defined symbols and not just on constructors like in usual functional programming languages. Hence, for instance, one can add the following associativity rule on addition:

```
rule (&x + &y) + &z → &x + (&y + &z)
```

Moreover, one can use non-linear patterns, that is, require the equality of some subterms to fire a rule like in:

```
rule &x + (- &x) → 0
```

Therefore, Dedukti can handle any first-order rewriting system [2]. But it can also handle higher-order rewriting in the style of Combinatory Reduction Systems (CRS) [11].

The simplest example of higher-order rewriting is given by the map function on lists, which applies an argument function to every element of a list:

```
symbol map:: (N⇒N)⇒List⇒List

rule map &f (cons &x &l) → cons (&f &x) (map &f &l)
```

Unlike first-order rewriting, function symbols can be partially applied, including in patterns. Hence, in Dedukti, one can write the following:

```
symbol id:: N⇒N

rule id &x → &x
```
The new rewriting engine of Dedukti

\begin{verbatim}
rule plus 0 → id and plus (s &n) &m → s (plus &n &m)
rule map id &l → &l
\end{verbatim}

It is also possible to match \(\lambda\)-abstractions as follows:

\begin{verbatim}
symbol cos: R ⇒ R
symbol sin: R ⇒ R
symbol *: (R ⇒ R) ⇒ (R ⇒ R) ⇒ (R ⇒ R)
symbol diff: (R ⇒ R) ⇒ (R ⇒ R)
rule diff (λx, sin(&v[x])) → diff (λx, &v[x]) * cos
\end{verbatim}

Following the definition of CRS, in a rule left-hand side, a higher-order pattern variable can only be applied to distinct bound variables (this condition could be slightly relaxed though [13]). A similar condition appears in \(\lambda\)Prolog [15]. It ensures the decidability of matching.

It can also be used to check variable-occurrence conditions. The differential of a constant function can thus be simply defined as follows in Dedukti:

\begin{verbatim}
rule diff (λx, &v) → λx, 0
\end{verbatim}

While in the rule for \(\sin\), we had \&v[x], meaning that the term matching \&v[x] may depend on \(x\), here we have \&v applied to no bound variables, meaning that the term matching \&v cannot depend on \(x\).

2.1 Terms, patterns, rewrite rules and matching, formally

We now define more formally terms, patterns, rewrite rules and rewriting. Following [3], the terms of the \(\lambda\Pi\)-calculus are inductively defined as follows:

\begin{verbatim}
t, u ::= TYPE | KIND | x | f | tu | λx : t, u | ∀x : t, u
\end{verbatim}

where \(x\) is a term variable, \(f\) is a function symbol, \(tu\) is the application of the function \(t\) to the value \(u\), \(λx : t, u\) is the function mapping \(x\) of type \(t\) to \(u\), which type is the dependent product type \(∀x : t, u\) (often written \(\Pi x : t, u\) as well). The simple type \(t ⇒ u\) is syntactic sugar for \(∀x : t, u\) where \(x\) is any fresh term variable not occurring in \(u\).

In \(λx : t, u\) and \(∀x : t, u\), the occurrences of \(x\) in \(u\) are bound, and terms equivalent modulo renaming of their bound variables are identified, as usual. In Dedukti, this is implemented by using the Bindlib library [12].

A (possibly empty) ordered sequence of terms \(t_1, \ldots, t_n\) is written \(\vec{t}\) for short.

Patterns are inductively defined as follows:

\begin{verbatim}
p ::= &x [\vec{y}] | fj | λy, p
\end{verbatim}

where \&x is a pattern variable, and \vec{y} is a sequence of distinct bound variables.

A rewrite rule is a pair of terms, written \(l → r\), such that \(l\) is a pattern of the form \(fj\) and every pattern variable occurring in \(r\) also occurs in \(l\).

In the following, we will assume given a set of user-defined rewrite rules \(R\).
Matching a term $t$ against a pattern $p$ whose bound variables are in the set $V$, written $p \prec_V t$ is inductively defined as follows:

$$x[y] \prec_V t \quad \text{iff } \text{FV}(t) \cap V \subseteq \{y\} \quad \text{(MatchFv)}$$

$$f p_1 \ldots p_n \prec_V f t_1 \ldots t_n \quad \text{iff } (p_1 \ldots p_n) \prec_V (t_1 \ldots t_n) \quad \text{(MatchSymb)}$$

$$\lambda y . p \prec_V \lambda y : A, t \quad \text{iff } p \prec_{V \cup \{y\}} t \quad \text{(MatchAbst)}$$

$$(p_1 \ldots p_n) \prec_V (t_1 \ldots t_n) \quad \text{iff } \forall i, p_i \prec_V t_i \land \forall j, p_j = p_i \Rightarrow t_i = t_j \quad \text{(MatchTuple)}$$

and we say that the term $t$ matches the pattern $p$ or that the pattern $p$ filters the term $t$.

The indexing set $V$ of variables is used to record which binders have been traversed, which is necessary to perform variable-occurrence tests.

The condition in the (MatchTuple) rule translates non-linearity conditions: if a variable occurs twice in a pattern, then the matching values must be equal.

### 3 Implementing matching with decision trees

The rewriting engine described in this paper is based on the work of Maranget [14]. Maranget introduces a domain-specific language for matching and an algorithm to transform a (ordered) list of first-order linear constructor patterns into a program in this language. In this section, we explain how we extend Maranget’s language and compilation procedure to our more general setting with non-linear higher-order patterns, partially applied function symbols, and no order on patterns.

We start by defining the language of decision trees $D$ and switch case lists:

$$D, E ::= \text{Leaf}(r) \mid \text{Fail} \mid \text{Swap}(D) \mid \text{Store}(D) \mid \text{Switch}(L)$$

$$L ::= (s, D)::L \mid (\lambda, D)::L_{\lambda} \mid T$$

$$L_{\lambda} ::= (s, D)::L_{\lambda} \mid T$$

$$T ::= (s, D)::\text{nil} \mid \text{nil}$$

where $r$ is a rule right-hand side, $i, j$ and $n$ are integers, $X$ is a finite set of variables. For case lists, $s$ is a function symbol annotated with the number of arguments it is applied to, :: is the cons operator on lists and \text{nil} is the empty list.

An element of a switch case list is a pair mapping:
- a function symbol $s$ to a tree for matching its arguments,
- a $\lambda$ to a tree for matching the body of an abstraction,
- a default case * to a tree for matching the other arguments.

Note that a list $L_{\lambda}$ has no element $(\lambda, D)$ and, in a list $L$, there is at most one element of the form $(\lambda, D)$. Finally, in both cases, there is at most one element of the form $(s, D)$ and, if so, it is the last one (default case).

#### Semantics

Decision trees are evaluated along with a stack of terms $\vec{v}$ to filter and an array $\vec{s}$ used by the decision tree to store elements. Informally, the semantics of each tree constructor is as follows:

- \text{Leaf}(r) matching succeeds and yields right-hand side $r$.
- \text{Fail} matching fails.
- \text{Swap}(D) moves the $i$th element of $\vec{v}$ to the top of $\vec{v}$ and carries on with $D$.
- \text{Store}(D) stores the top of the stack into $\vec{s}$ and continues with $D$.
- \text{Switch}(L) branches on a tree in $L$ depending on the term on top of $\vec{v}$.
BinNl\((D, \{i, j\}, E)\) checks whether \(s_i\) and \(s_j\) are equal and continues with \(D\) if this is the case, and \(E\) otherwise.

BinCl\((D, (n, X), E)\) checks whether \(\text{FV}(s_n) \subseteq X\) and continues with \(D\) if this is the case, and with \(E\) otherwise.

Example 2. The matching algorithm described in Example 1 can be represented by the following decision tree:

\[
\begin{array}{c}
\text{Swap}_2(\text{Switch}([b_0, \text{Leaf}(\&x)]);
(a_0, \text{Switch}([c_0, \text{Switch}([c_0, \text{Leaf}(\&x)])])))
\end{array}
\]

which can be graphically represented as follows:

![Graphical representation of the decision tree of Example 2](image)

where leaves are the right-hand sides of the rewrite rules and a path from the root to a leaf is a successful matching. The tree of Figure 1 can be used to rewrite any term of the form \(f \bar{t}\). The sequence of operations to filter the term \(f (f a) b\) can be read from the tree. The initial vector \(\vec{v}\) is \(\vec{v} = ((f a) b)\) and the array \(\vec{s}\) won’t be necessary here.

1. The \(\text{Swap}_2\) transforms \(\vec{v}\) into \((b, (f a))\), so the next operations will be carried out on \(b\).
2. The \(\text{Switch}\) node with the case list \([([b_0, D], (a_0, E))]\) allows to branch on \(D\) or \(E\) depending on the term on top of \(\vec{v}\), that is, \(b\). Since \(b\) is applied to no argument, it matches \(b_0\) and filtering continues on \(D\). The stack is now \(\vec{v} = (f a)\).
3. Node \(D\) is in fact a \(\text{Leaf}\) and so the matching succeeds.

The formal semantics is given in Figure 2. An evaluation is written as a judgement \(\vec{v}, \vec{s}, V \vdash D \rightarrow r\) which can be read as follows: “stack \(\vec{v}\), store \(\vec{s}\) and abstracted variables \(V\) yield the term \(r\) when matched against tree \(D\)”.

3.1 Matrix representation of rewrite systems

In order to compile a set of rewrite rules into this language, it is convenient to represent rewrite systems as matrices with lines of different lengths (because function symbols can be partially applied). Hence, a rewrite system for a function symbol \(f\), that is, a set of rewrite rules \(fp^i \rightarrow r^1, \ldots, fp^m \rightarrow r^m\) is represented by:

\[
\begin{pmatrix}
\begin{array}{c}
p_1^1 & \cdots & p_{n_1}^1 \\
p_1^2 & \cdots & p_{n_2}^2 \\
\vdots & & \vdots \\
p_1^m & \cdots & p_{n_m}^m
\end{array}
\end{pmatrix}
\begin{pmatrix}
N_1 \\
N_2 \\
\vdots \\
N_m
\end{pmatrix}
\begin{pmatrix}
C_1 \\
C_2 \\
\vdots \\
C_m
\end{pmatrix}
\begin{pmatrix}
r_1 \\
r_2 \\
\vdots \\
r_m
\end{pmatrix}
\]

where \(C_i\) encodes the variable-occurrence constraints in \(p^i\) and \(N_i\) encodes non-linearity constraints in \(p^i\).

A variable-occurrence constraint given by a pattern variable \(\&x[\bar{y}]\) is encoded as a pair \((a, \bar{y})\) where \(a\) is the position of the variable in the main term.
Figure 2 Evaluation of decision trees
The new rewriting engine of Dedukti

Convertibility constraints between two terms at positions \(a\) and \(b\) are encoded by the unordered pair \(\{a, b\}\).

In the above matrix, we can then replace a pattern of the form \(kx[y]\) or \(kx\) by \(_\).

For the sake of completeness, we recall the definition of positions:

**Definition 3** (Positions in a term). The set of positions of a term \(t\) is the set of words over the alphabet of positive integers inductively defined as follows:

\[
\text{Pos}(x) \doteq \{\varepsilon\}
\]

\[
\text{Pos}(f t_1 \cdots t_n) \doteq \{\varepsilon\} \cup \bigcup_{i=1}^{n} \{ia \mid a \in \text{Pos}(t_i)\}
\]

\[
\text{Pos}(\lambda x, t) \doteq \{\varepsilon\} \cup \{ia \mid a \in \text{Pos}(t)\}
\]

The position \(\varepsilon\) is called the root position of the term \(t\) and the symbol at this position is called the root symbol of \(t\).

For \(a \in \text{Pos}(t)\), the subterm of \(t\) at position \(a\), denoted by \(t|_a\), is defined by induction on the length of \(a\):

\[
t|_\varepsilon \doteq t
\]

\[
f t_1 \cdots t_n|_ia \doteq t_i|_a
\]

The notion of position is extended to sequences of terms by taking \(\vec{t}\mid|_ia \doteq t_i|_a\).

**Example 4.** The rewrite system

\[
\text{rule } f a (\lambda x, \lambda y, &g[x]) \rightarrow 0
\]

\[
\text{and } f &x &x \rightarrow 1
\]

\[
\text{and } f a b \rightarrow 2
\]

is represented by the following matrix:

\[
\begin{pmatrix}
\varepsilon & \lambda x, \lambda y, &_ & \varepsilon \\
_ & _ & _ & \{1, 2\} \\
\lambda x, & & & \{211, (x)\}
\end{pmatrix}
\]

\[
\begin{pmatrix}
\varepsilon & 0 \\
_ & 0 \\
\lambda x, & 1
\end{pmatrix}
\]

The variable-occurrence constraint of the first rule is encoded by \(211, (x)\) since only the variable \(x\) among the \(\lambda x, \lambda y, &g[x]\) is authorised. The non-linearity constraint \(f &x &x\) is translated by \(\{1, 2\}\), hence the constraints set \(\{\{1, 2\}\}\).

### 3.2 Compiling a rewrite system into a decision tree

We now describe the compilation process as a non-deterministic recursively defined relation \(\succ\) between matrices and decision trees.

To this end, we use the transformations on matrices defined in Table 1.

\(\text{Spec}(f, a, (P, \vec{N}, \vec{C}, \vec{r}))\) keeps rows whose first pattern is the function \(f\) applied to \(a\) arguments:

**Example 5.** Let \(P = \begin{pmatrix}
kx & q \\
r & f & kx \\
kx & r \\
\lambda x, & kx & \lambda x, & r
\end{pmatrix}\). Then,

\[
\text{Spec}\left(r, 1, \left(P, \vec{N}, \vec{C}, \vec{r}\right)\right) = \left(\begin{pmatrix}
\varepsilon & q \\
r & f & kx \\
kx & r \\
\lambda x, & kx & \lambda x, & r
\end{pmatrix}, \vec{N}, \vec{C}, \begin{pmatrix}r_1 \end{pmatrix}\right)
\]

\(\text{Spec}_\lambda\left(\left(P, \vec{N}, \vec{C}, \vec{r}\right)\right)\) keeps rows whose first pattern is a \(\lambda\)-abstraction:

**Example 6.** Let \(P\) be the same as in Example 5.

\[
\text{Spec}_\lambda\left(P, \vec{N}, \vec{C}, \vec{r}\right) = \left(\begin{pmatrix}
\varepsilon & r \\
kx & \lambda x, & r \\
\lambda x, & \lambda x, & r
\end{pmatrix}, \vec{N}, \vec{C}, \begin{pmatrix}r_3 \end{pmatrix}\right)
\]
### Table 1 Decomposition operators

<table>
<thead>
<tr>
<th>Pattern $p^j$</th>
<th>Rows of $\text{Spec}(f, a, P \rightarrow A)$</th>
<th>Rows of $\text{Spec}_\lambda(P \rightarrow A)$</th>
<th>Rows of $\text{Def}(P \rightarrow A)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f \ q_1 \cdots q_a$</td>
<td>$q_1 \cdots q_a \ p^j_2 \cdots p^j_n$</td>
<td>No row</td>
<td>No row</td>
</tr>
<tr>
<td>$f \ q_1 \cdots q_b$</td>
<td>No row, $a \neq b$</td>
<td>No row</td>
<td>No row</td>
</tr>
<tr>
<td>$\lambda x, q$</td>
<td>No row</td>
<td>$q \ p^j_2 \cdots p^j_n$</td>
<td>No row</td>
</tr>
</tbody>
</table>

The same idea is used for constraints:

- $\text{csucc}(k, (P, \vec{N}, \vec{C}, \vec{r}))$ keeps all the rows and simplify the constraint sets
  
  $\text{csucc}(k, (\vec{p}, N, C, r)) \triangleq (\vec{p}, N\{k\}, C\{k\}, r)$

- $\text{cfail}(k, (P, \vec{N}, \vec{C}, \vec{r}))$ keeps rows that don’t have $k$ in their constraint sets
  
  $\text{cfail}(k, (\vec{p}, N, C, r)) \triangleq \begin{cases} 
  \text{No row} & \text{if } k \in N \cup C \\
  (\vec{p}, N\{k\}, C\{k\}, r) & \text{if } k \notin N \cup C
  \end{cases}$

A compilation process consists in reducing the matrix step by step, compiling the sub-matrices and aggregating the sub-trees obtained using the node that corresponds to the sub-matrices computed (e.g. a $\text{Switch}$ if the $\text{Spec}$, $\text{Def}$ and $\text{Spec}_\lambda$ sub-matrices have been computed).

To say that the matrix $(P, \vec{N}, \vec{C}, \vec{r})$ compiles to the decision tree $D$, we write

$$(\vec{p}, (P, \vec{N}, \vec{C}, \vec{r}), n, \mathcal{E}) \triangleright D$$

where:

- $\vec{p}$ are the positions in the term that will be matched against during evaluation.
- $\mathcal{E}$ is a map from positions to integers such that $\mathcal{E}(\rho)$ is the index in $\vec{s}$ of the subterm at position $\rho$ used during the evaluation of decision trees. The empty map is denoted $\emptyset$.
- $n$ is the size of the store, which is incremented each time an element is added.

We can now describe the compilation process:

**Definition 8 (Compilation).** 1. If the matrix $P$ has no row ($m = 0$), then matching always fails, since there is no rule to match,

$$(\vec{p}, (\emptyset, \vec{N}, \vec{C}, \vec{r}), n, \mathcal{E}) \triangleright \text{Fail} \quad (2)$$
The new rewriting engine of Dedukti

2. If there is a row \( k \) in \( P \) composed of unconstrained variables, matching succeeds and yields right-hand side \( r \)

\[
\begin{pmatrix}
(p_1^1 \cdots p_{n_1}^1) & N_1 & C_1 & \rightarrow & r_1 \\
\vdots \\
(p_1^m \cdots p_{n_m}^m) & N_m & C_m & \rightarrow & r_m \\
\end{pmatrix}
\]

\[\triangleright \text{Leaf}(r_k) \quad (3)\]

3. Otherwise, there is at least one row with either a symbol or a constraint or an abstraction.

We can choose to either specialise on a column or solve a constraint.

a. Consider a specialisation on the first column, assuming it contains at least a symbol or an abstraction.

If \( \rho_1 \) is constrained in some \( N_i \) or \( C_i \), then define \( n' = n + 1 \) and \( E' = E \cup \{ \rho_1 \mapsto n \} \).

Otherwise, let \( n' = n \) and \( E' = E \).

Let \( \Sigma \) be the set of root symbols of the terms of the first column and \( k \) the number of arguments \( f \) is applied to. Then for each \( f \in \Sigma \), we compile

\[
\left( (\rho_1 |_1 \cdots \rho_1 |_k \rho_2 \cdots \rho_n), \text{Spec} \left( f, k, \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n', E' \right) \triangleright D_{f_k}
\]

Let \( L \) be the switch case list defined as (we use the bracket notation for list comprehension as the order is not important here)

\[
L \triangleq [(f, D_{f_k}) | f \in \Sigma]
\]

If there is an abstraction in the column, the \( \text{Spec}_\lambda \) sub-matrix is computed and compiled to \( D_\lambda \), and an abstraction case is added to the mapping

\[
\left( (\rho_1 |_1 \rho_2 \cdots \rho_n), \text{Spec}_\lambda \left( \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n', E' \right) \triangleright D_\lambda
\]

\[
L \triangleq [(s, D_{f_k}) | f \in \Sigma]:(:, \lambda, D_\lambda):\text{nil}
\]

Similarly, if the column contains a variable, the \( \text{Def} \) sub-matrix is computed and compiled to \( D_* \), and the mapping is completed with a default case, (the abstraction case may or may not be present)

\[
\left( (\rho_2 \cdots \rho_n), \text{Def} \left( \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n', E' \right) \triangleright D_*
\]

\[
L \triangleq [(f_k, D_{f_k}) | s \in \Sigma]:(:, \lambda, D_\lambda):(:, *, D_*):\text{nil}
\]

Now that the switch case list \( L \) is complete (all the symbols, the abstractions and the pattern variables are handled) and the sub-trees are defined and related to their pattern matrix, we can create the top node \( \text{Switch}(L) \).

Furthermore, if \( \rho_1 \) is constrained, the term must be saved during evaluation. In that case, we add a \text{Store} node,

\[
\left( \vec{\rho}, \left( P, \vec{N}, \vec{C}, \vec{r} \right), n, E \right) \triangleright \text{Store} (\text{Switch}(L)).
\]

Otherwise,

\[
\left( \vec{\rho}, \left( P, \vec{N}, \vec{C}, \vec{r} \right), n, E \right) \triangleright \text{Switch}(L).
\]
b. If a term has been stored and is subject to a closedness constraint, then this constraint can be checked. That is, for any position \( \mu \) such that \( \mathcal{E}(\mu) \) is defined and there is a constraint set \( C_i \) and a variable set \( V \) such that \( (\mu, V) \in C_i \), we compute the sub-matrices \( c_{\text{succ}} \) and \( c_{\text{fail}} \) and we compile them to \( D_s \) and \( D_f \),

\[
\left( \vec{\rho}, c_{\text{succ}} \left( \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n, \mathcal{E} \right) \triangleright D_s
\]

\[
\left( \vec{\rho}, c_{\text{fail}} \left( \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n, \mathcal{E} \right) \triangleright D_f
\]

with \( (\mu, X) \in F^j \) for some row number \( j \) and we finally define

\[
\left( \vec{\rho}, \left( P, \vec{N}, \vec{C}, \vec{r} \right), n, \mathcal{E} \right) \triangleright \text{BinCl}(D_s, (\mathcal{E}(\mu), X), D_f)
\]

c. A non linearity constraints can be enforced when the two terms involved in the constraint have been stored, that is, when there is a couple \( \{\mu, \nu\} \) \( (\mu \neq \nu) \) such that \( \mathcal{E}(\mu) \) and \( \mathcal{E}(\nu) \) are defined and there is a row \( j \) such that \( \{\mu, \nu\} \in N_j \). If it is the case, then compute \( c_{\text{succ}} \), \( c_{\text{fail}} \) and compile them,

\[
\left( \vec{\rho}, c_{\text{succ}} \left( \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n, \mathcal{E} \right) \triangleright D_s
\]

\[
\left( \vec{\rho}, c_{\text{fail}} \left( \left( P, \vec{N}, \vec{C}, \vec{r} \right) \right), n, \mathcal{E} \right) \triangleright D_f
\]

and define

\[
\left( \vec{\rho}, \left( P, \vec{N}, \vec{C}, \vec{r} \right), n, \mathcal{E} \right) \triangleright \text{BinNl}(D_s, \{\mathcal{E}(i), \mathcal{E}(j)\}, D_f)
\]

4. If column \( i \) contain either a symbol, an abstraction or a constraint, and each pattern vector of \( P \) is at least of length \( i \), then compile \( \vec{\mu}, \left( P', \vec{N}, \vec{C}, \vec{r} \right), n, \mathcal{E} \) \( \triangleright D' \) where \( \vec{\mu} = (\rho_1, \rho_2, \ldots, \rho_n) \) and \( P' \) is \( P \) with column \( i \) moved to the front; to build

\[
\left( \vec{\rho}, \left( P, \vec{N}, \vec{C}, \vec{r} \right), n, \mathcal{E} \right) \triangleright \text{Swap}_i(D')
\]
Then we compute $D_a$ and $D_b$ such that $(2, (P_a, \emptyset, \emptyset, \vec{r}), 0, \emptyset) \triangleright D_a$ and $(2, (P_b, \emptyset, \emptyset, \vec{r}), 0, \emptyset) \triangleright D_b$. The switch case list $L \triangleq [(a_0, D_a), (b_0, D_b)]$ can be defined and so the compilation step produces

$$((21), (P', \emptyset, \emptyset, \vec{r}), 0, \emptyset) \triangleright \text{Switch}(L).$$

3. Since $P_b$ contains only unconstrained variables, we are in the case item 2 and so we have $(1, (P'_b, \emptyset, \emptyset, \&x), 0, \emptyset) \triangleright \text{Leaf}(\&x)$.

4. A specialisation on $P_a$ with respect to $c$ can be performed, let $Q_a \triangleq \text{Spec}(c, 0, P_a) = [c \_]$ and define $E$ such that $(1, (Q_a, \emptyset, \emptyset, \&x), 0, \emptyset) \triangleright E$. The compilation step produces

$$(1, (P_a, \emptyset, \emptyset, \&x), 0, \emptyset) \triangleright \text{Switch}([c, E]).$$

5. Similarly, we can specialise $Q_a$ on $c$ yielding the matrix $[\_]$ which compiles to $\text{Leaf}$. We thus have,

$$(1, (Q_a, \emptyset, \emptyset, \&x), 0, \emptyset) \triangleright \text{Switch}([c, \text{Leaf}(\&x)]).$$

The soundness and completeness proofs for this compilation process can be found in [10].

We have seen that at each compilation step, several options are possible. The stack can be swapped with $\text{Swap}$ to orient the filtering, if a constraint can be solved, either is solved with a $\text{BinNL}$ or $\text{BinCl}$ node, or a $\text{Switch}$ can be performed. These possibilities make the compilation process undeterministic. Therefore, a given matrix can be compiled to several decision trees. Maranget compares different heuristics based on the shape of patterns as well as some more complex ones. In DEDUKTI, since verifying constraints can involve non-trivial operations (convertibility and variable occurrence tests), constraint checking is postponed as much as possible. Regarding $\text{Swap}$, we process in priority columns that have many constructors and few constraints.

## 4 Results

This section compares the performance of the new rewriting engine with previous implementations of DEDUKTI, and other tools as well.

### 4.1 Hand-written examples

We consider 3 different implementations of DEDUKTI:

- **DEDUKTI2.6** is the latest official release of DEDUKTI available on opam. Its matching algorithm also implements decision trees but non-linearity and variable-occurrence constraints are not integrated in decision trees. Its implementation, primarily due to Ronan Saillard [17], is available on https://github.com/Deducteam/dedukti.

- **LAMBDAPI1.0** is an alternative implementation of DEDUKTI due to Rodolphe Lepigre [12]. It implements a naive algorithm for matching. It is available on https://github.com/Deducteam/lambdapi/tree/fix_ho.

- **DEDUKTI3.0** is our new implementation of DEDUKTI. It adds to LAMBDAPI1.0 the decision trees described in this paper. It is available on https://github.com/Deducteam/lambdapi.

The git repository https://github.com/Deducteam/libraries contains several hand-written DEDUKTI examples, including a Sudoku solver with 3 examples labelled easy, medium and hard respectively, and a DPLL-based SAT solver to decide the satisfiability of propositional logic formulae in conjunctive normal form with two example files:
Table 2 Time needed to solve sudokus and SAT formulae in seconds.

<table>
<thead>
<tr>
<th></th>
<th>Sudoku</th>
<th>DPLL-SAT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>easy</td>
<td>med</td>
</tr>
<tr>
<td>DEDUKTI2.6</td>
<td>0.7</td>
<td>7.7</td>
</tr>
<tr>
<td>LAMBDAPI1.0</td>
<td>1.2</td>
<td>13</td>
</tr>
<tr>
<td>DEDUKTI3.0</td>
<td>0.5</td>
<td>5.2</td>
</tr>
</tbody>
</table>

2_ex contains a function that when given an integer \( n \), produces \( n \) literals named \( v_n \) and the formula \( p(0) = v_0 \land \land_{k=1}^{n} (p(k) = p(k-1) \land (v_{k-1} \neq v_k)) \). ok_50x80 contains a formula with 50 literals and 80 clauses of the form \( \neg x \lor \neg y \lor \neg z \).

Because of the nature of the problems, they require a substantial amount of rewriting steps to be solved.

Table 2 shows the performance of each tool on these examples. Using decision trees increases significantly performance on Sudoku since LAMBDAPI1.0 is twice as slow as DEDUKTI2.6 which is slower than DEDUKTI3.0. SAT problems confirm that DEDUKTI3 is more efficient than LAMBDAPI1.0 and DEDUKTI2.

More benchmarks are described in [10].

### 4.2 Rewriting Engine Competition (REC)

The Rewriting Engine Competition\(^1\) (REC), first organized in 2009, aims to compare rewriting engines. F. Durán and H. Garavel revived the competition in 2018, and another study has been done in 2019 \[^5\]. There are 14 rewriting engines tested, among which Haskell’s GHC and OCAML.

REC problems are written in a specific REC syntax which is then translated into one of the 14 target languages with Awk scripts. To use REC benchmarks with DEDUKTI, a translation from HASKELL benchmarks to DEDUKTI has been implemented\(^2\).

Our rewriting engine has been compared on the problems that do not use conditional rewriting with OCAML and HASKELL. For each language, we have measured both the interpretation time with ocaml and runghc, and the compiling and running time with ocamlopt and ghc. The results are in Table 3.

We can divide our observations on classes of problems. There are 43 problems, among which 19 are solved in less that one second by DEDUKTI. On these problems, our rewriting engine performs as well as others, and even better in some cases. On two problems, add8 and benchtree10, DEDUKTI performs better that ocaml. On all other problems, DEDUKTI is slower than the other rewrite engines. Interestingly, ocamlopt has more memory overflows than DEDUKTI (six against five).

### 5 Conclusion & related work

This article describes the implementation of the new rewriting engine of DEDUKTI. It extends Maranget’s techniques of decision trees used in the OCaml compiler \[^{14}\] to the class of

---

\(^1\) http://rec.gforge.inria.fr

\(^2\) https://raw.githubusercontent.com/Deducteam/lambdapi/master/tools/rec_to_lp/rec_hs_to_lp.awk
Table 3 Performance on REC benchmark in seconds. N/A is for out of memory. T/O is for timeout (30 minutes). The first line indicates that on the add32 problem, Dedukti timed out, the command \texttt{runghc add32.hs} took 19.7 seconds to finish, \texttt{ocaml add32.ml} took 8.6 seconds, \texttt{ghc add32.hs} \& \& \texttt{./a.out} failed because of a memory overflow.
non-linear higher-order patterns used in Combinatory Reduction Systems (CRS) [11]. We
define the language of decision trees and how to compile a set of rewrite rules into a decision
tree. We finally present some benchmarks showing good performances.

A similar algorithm had been implemented in Dedukti2.6 by Ronan Saillard [17].
However, Saillard’s rewriting engine used decision trees for first-order linear matching and
handled non-linearity and variable-occurrence constraints afterwards in a naive way. In the
new implementation, these constraints are fully integrated in decision trees.

Other rewriting engine uses decision trees as well like CRSX, which is a rewrite engine for
an extension of Combinatory Reduction Systems [16], and Maude under certain conditions
[8], but Maude considers first-order terms only.

Other pattern-matching algorithm are also possible, in particular using backtracking
automata instead of trees, which allow to have smaller data structures. The interested reader
can look at Prolog implementations or Egison (see [6] and, more particularly on the question
of pattern matching, [7]).

Further useful extensions would be interesting: conditional rewrite rules (the REC data-
base contains many files with conditional rewrite rules) and matching modulo associativity and
commutativity (AC). Conditional rewriting could be implemented without too much difficulty
since it would consist in extending the constraints mechanism which is modular. A prototype
implementation of matching modulo AC has already been developed for Dedukti2.6 by
Gaspard Férey but performances are not very good yet. This new implementation could
provide a better basis to implement matching modulo AC.

References

1 A. Assaf, G. Burel, R. Cauderlier, D. Delahaye, G. Dowek, C. Dubois, F. Gilbert, P. Hal-
magrand, O. Hermant, and R. Saillard. Dedukti: a logical framework based on the \( \lambda \Pi \)-calculus
3 H. Barendregt. Lambda calculi with types. In S. Abramsky, D. M. Gabbay, and T. S. E.
Maibaum, editors, Handbook of logic in computer science. Volume 2. Background: computa-
4 R. Cauderlier. Tactics and Certificates in Meta Dedukti. In Proceedings of the 9th International
5 Francisco Durán and Hubert Garavel. The rewrite engines competitions: A retrospecti
ve. In TACAS, 2019.
6 Satoshi Egi. Egison: Non-linear pattern-matching against non-free data types. ArXiv,
abs/1506.04498, 2015.
7 Satoshi Egi and Yuichi Nishiwaki. Non-linear pattern matching with backtracking for non-free
8 S. Eker. Fast matching in combinations of regular equational theories. Electronic Notes in
Theoretical Computer Science, 4:90 – 109, 1996. RWLIW96, First International Workshop on Re-
writing Logic and its Applications. URL: http://www.sciencedirect.com/science/article/
pii/S1571066104000350, doi:https://doi.org/10.1016/S1571-0661(04)00035-0.

3 https://github.com/Deducteam/Dedukti/tree/acu-state
The new rewriting engine of Dedukti


