Note on the operational semantics of Dedukti 2.5

Frédéric Blanqui (Inria) and Guillaume Genestier (LSV)

5 March 2018

Abstract. In this note, we describe an over-approximation of the operational semantics actually implemented in Dedukti [3, 2] and study some of its properties wrt confluence and termination.

Let $\mathcal{R}$ be a set of rules $l \to r$.

Let $\to_{\mathcal{R}}$ be the smallest rewrite relation (*i.e.* stable by substitution and context) containing $\mathcal{R}$, $\downarrow_{\mathcal{R}} = \to^*_{\mathcal{R}}\leftarrow^*_{\mathcal{R}}$ be the joinability relation, and $\leftrightarrow^*_{\mathcal{R}}$ be the reflexive, symmetric and transitive closure. $\leftrightarrow^*_{\mathcal{R}}$ is the equational theory defined by $\mathcal{R}$ when rules are seen as equations.

As we are going to see that, to decide $\leftrightarrow^*_{\mathcal{R}}$, Dedukti does not use $\to_{\mathcal{R}}$ but an extension of it that we are going to describe.

Conditional rewriting

Let a *condition* be a set C of disjoint non-empty lists of variables X, and a *conditional rule* be a triple (l, r, C) where l and r are terms and C is a condition such that $\bigcup C \subseteq \mathrm{Var}(l)$.

A condition checker c maps every relation R and every non-empty list of variables X to a set of substitutions $c(R, X)$ so that, for all families of relations $(R_k)_{k\in\mathbb{N}}$, $c(\bigcup_{k\in\mathbb{N}} R_k, X) = \bigcup_{k\in\mathbb{N}} c(R_k, X)$. Examples of condition checkers are:

- the reflexivity checker: $\sigma \in r(R, X)$ if there is t such that, for all $x \in X$, $x\sigma = t$;
- the joinability checker: $\sigma \in j(R, X)$ if there is t such that, for all $x \in X$, $x\sigma R^* t$;
- the Dedukti checker: $\sigma \in d(R, y :: X)$ if, for all $x \in X$, there is t such that $y\sigma R^* t$ and $x\sigma R^* t$;
- the equivalence checker: $\sigma \in e(R, X)$ if there is t such that, for all $x \in X$, $x\sigma(R \cup R^{-1})^* t$.

Given a set $\mathcal{S}$ of conditional rewrite rules and a condition checker c, let $\to_{\mathcal{S}c}$ be the smallest rewrite relation such that, for all $(l, r, C) \in \mathcal{S}$ and substitution σ, $l\sigma \to_{\mathcal{S}c} r\sigma$ if $\sigma \in \bigcap_{X\in C} c(\to_{\mathcal{S}c}, X)$.

Note that $\rightarrow_{\mathcal{S}c}$ is defined as a fixpoint reachable by ω-iteration, that is, $\rightarrow_{\mathcal{S}c} = \bigcup_{i\in\mathbb{N}} \rightarrow_{\mathcal{S}c,i}$ where $\rightarrow_{\mathcal{S}c,0}= \emptyset$ and $\rightarrow_{\mathcal{S}c,i+1}$ is the smallest rewrite relation such that, for all $(l,r,C) \in \mathcal{S}$ and substitution σ, $l\sigma \rightarrow_{\mathcal{S}c,i+1} r\sigma$ if $\sigma \in \bigcap_{X\in C} c(\rightarrow_{\mathcal{S}c,i}, X)$.

Operational semantics of Dedukti 2.5

The operational semantics relative to $\mathcal{R}$ actually implemented in Dedukti can be defined as follows.

Wlog we assume that the set of variables $\mathbb{V}$ is made of two disjoint subsets $\mathbb{V}_1$ and $\mathbb{V}_2$, every variable of $\mathcal{R}$ belonging to $\mathbb{V}_1$, and that there is an injection x from words on $\mathbb{N}$ (positions in terms) to $\mathbb{V}_2$.

Thanks to this injection, a term t whose variables are all in $\mathbb{V}_1$ can be transformed into a *linear* term t' whose variables are all in $\mathbb{V}_2$: replace each variable x at position p by x_p.

Now, for each term t, we assume given a substitution γ_t mapping every variable x of t to the variable x_p where p is the smallest position in the lexicographic order of the positions where x occurs in t.

Then, Dedukti implements the rewrite relation $\rightarrow_{\mathcal{S}d}$ where $\mathcal{S}$ is the set of conditional rewrite rules $(l', r\gamma_l, C(l))$ such that $l \rightarrow r \in \mathcal{R}$ and $C(l) = \{X(l,x) \mid x \in \mathrm{Var}(l)\}$ where $X(l,x)$ is the list of variables x_p such that $p \in \mathrm{Pos}(x,l)$, ordered lexicographically wrt. p.

For instance, if $\mathsf{f}xxx \rightarrow \mathsf{a} \in \mathcal{R}$, then $(\mathsf{f}xx'x'', \mathsf{a}, \{[x,x',x'']\}) \in \mathcal{S}$. So, Dedukti will reduce $\mathsf{f}tuv$ to a if, on the one hand, t and u have a common reduct wrt. $\rightarrow_{\mathcal{S}d}$, and on the other hand, t and v have a common reduct wrt. $\rightarrow_{\mathcal{S}d}$.

Lemma 1

1. If $r \subseteq c$, then $\rightarrow_{\mathcal{R}} \subseteq \rightarrow_{\mathcal{S}c}$.
2. If $c \subseteq e$, then $\rightarrow_{\mathcal{S}c} \subseteq \leftrightarrow^*_{\mathcal{R}}$.

Proof.

1. Immediate.
2. We prove that, for all i, $\rightarrow_{\mathcal{S}c,i} \subseteq \leftrightarrow^*_{\mathcal{R}}$, by induction on i. For $i = 0$, this is immediate since $\rightarrow_{\mathcal{S}c,0} = \emptyset$. Assume now that $l'\sigma \rightarrow_{\mathcal{S}c,i+1} r\gamma_l\sigma$. For all $x \in \mathrm{Var}(l)$, there is t such that, for all $p \in \mathrm{Pos}(x,l)$, $x_p\sigma \leftrightarrow^*_{\mathcal{S}c,i} t$. So, there is σ' such that $l'\sigma \leftrightarrow^*_{\mathcal{S}c,i} l\sigma' \rightarrow_{\mathcal{R}} r\sigma' \leftarrow^*_{\mathcal{S}c,i} r\gamma_l\sigma$. By induction hypothesis, $\rightarrow_{\mathcal{S},i} \subseteq \leftrightarrow^*_{\mathcal{R}}$. Therefore, $l'\sigma \leftrightarrow^*_{\mathcal{R}} r\gamma_l\sigma$. ∎

Corollary 2 If $r \subseteq c \subseteq e$, then $\leftrightarrow^*_{\mathcal{S}c} = \leftrightarrow^*_{\mathcal{R}}$.

Proof. Since we have $\rightarrow_{\mathcal{R}} \subseteq \rightarrow_{\mathcal{S}c} \subseteq \leftrightarrow^*_{\mathcal{R}}$. ∎

This is in particular the case for $c \in \{r,d,j,e\}$ since $r \subseteq j \subseteq d \subseteq e$.

Lemma 3 If $\to_{\mathcal{R}}$ has unique normal forms and $r \subseteq c \subseteq e$, then $\to_{\mathcal{S}c}$ has unique normal forms too and the same normal forms as $\to_{\mathcal{R}}$.

Proof. Since $r \subseteq c$, we have $\to_{\mathcal{R}} \subseteq \to_{\mathcal{S}c}$ and every term in $\to_{\mathcal{S}c}$ normal form is in $\to_{\mathcal{R}}$ normal form too.

Conversely, assume that $l'\sigma$ is in $\to_{\mathcal{R}}$ normal form and $l'\sigma \to_{\mathcal{S}c} r\gamma_l\sigma$. Let $X \in C(l)$. Since $c \subseteq e$, there is t such that, for all $x \in X$, $x\sigma \leftrightarrow^*_{\mathcal{R}} t$. Since every $x\sigma$ is in $\to_{\mathcal{R}}$ normal form and $\to_{\mathcal{R}}$ has unique normal forms, there is u such that, for all $x \in X$, $x\sigma = u$. Thus, $l'\sigma$ is not in $\to_{\mathcal{R}}$-normal form. Contradiction.

Assume now that t and u are two $\to_{\mathcal{S}c}$ normal forms such that $t \leftrightarrow^*_{\mathcal{S}c} u$. Then, t and u are two $\to_{\mathcal{R}}$ normal forms such that $t \leftrightarrow^*_{\mathcal{R}} u$. Hence, $t = u$. ■

Lemma 4 If $\to_{\mathcal{R}}$ is confluent and $r \subseteq c \subseteq j$, then $\to_{\mathcal{S}c}$ is confluent too and $\downarrow_{\mathcal{S}c} = \downarrow_{\mathcal{R}}$.

Proof. First, $\leftrightarrow^*_{\mathcal{S}c} = \leftrightarrow^*_{\mathcal{R}} = \downarrow_{\mathcal{R}}$ since $\to_{\mathcal{R}}$ is confluent. Second $\downarrow_{\mathcal{R}} \subseteq \downarrow_{\mathcal{S}c}$ since $r \subseteq c$. Therefore, $\to_{\mathcal{S}c}$ is confluent. Moreover, $\downarrow_{\mathcal{S}c} \subseteq \leftrightarrow^*_{\mathcal{S}c} = \downarrow_{\mathcal{R}}$. ■

Here is an example of a non-confluent system $\mathcal{R}$ such that $\downarrow_{\mathcal{S}j} \not\subseteq \downarrow_{\mathcal{R}}$:

Example 1 Take $\mathcal{R} = \{\mathsf{a} \to \mathsf{b}, \mathsf{a} \to \mathsf{c}, \mathsf{f}xx \to \mathsf{g}x\}$. Then, on the one hand, $\mathsf{fab} \to_{\mathcal{S}} \mathsf{ga} \to_{\mathcal{S}} \mathsf{gc}$ and, on the other hand, $\mathsf{fab} \to_{\mathcal{R}} \mathsf{fcb}$ and $\mathsf{fab} \to_{\mathcal{R}} \mathsf{fbb} \to_{\mathcal{R}} \mathsf{gb}$, which are in normal form wrt $\to_{\mathcal{R}}$.

Note also that we may not have $\downarrow_{\mathcal{S}d} \subseteq \downarrow_{\mathcal{R}}$ if $\to_{\mathcal{R}}$ is not confluent as shown by the following example:

Example 2 Take $\mathcal{R} = \{\mathsf{f}xxx \to \mathsf{a}, \mathsf{a} \to \mathsf{b}, \mathsf{a} \to \mathsf{c}\}$. Then, $\mathsf{fabc} \to_{\mathcal{S}d} \mathsf{a}$ but $\mathsf{fabc} \not\downarrow_{\mathcal{R}} \mathsf{a}$.

Finally, note that the termination of $\to_{\mathcal{R}}$ does not imply the termination of $\to_{\mathcal{S}c}$ as shown by the following example:

Example 3 Take $\mathcal{R} = \{\mathsf{ga} \to \mathsf{fab}, \mathsf{a} \to \mathsf{b}, \mathsf{f}xx \to \mathsf{g}x\}$. We have $\mathsf{fab} \to_{\mathcal{S}c} \mathsf{ga} \to_{\mathcal{R}} \mathsf{fab}$. On the other hand, $\to_{\mathcal{R}}$ terminates as shown by AProVE [1] as follows:

- The rule $\mathsf{a} \to \mathsf{b}$ can be eliminated by using the following monotone polynomial interpretation on $\mathbb{N}$: $\mathsf{a} = 1$, $\mathsf{b} = 0$, $\mathsf{f}(x, y) = 2x + 2y + 2$, $\mathsf{g}(x) = 2x + 2$.
- Then, the rule $\mathsf{ga} \to \mathsf{fab}$ can be eliminated by taking the following polynomial interpretation on $\mathbb{N}$: $\mathsf{a} = 1$, $\mathsf{b} = 0$, $\mathsf{f}(x, y) = x + 2y + 2$, $\mathsf{g}(x) = 2x + 2$.
- Finally, $\mathsf{f}xx \to \mathsf{g}x$ is proved terminating by taking MPO with $\mathsf{f} > \mathsf{g}$.

References

[1] `http://aprove.informatik.rwth-aachen.de/`, 2018.

[2] A. Assaf, G. Burel, R. Cauderlier, D. Delahaye, G. Dowek, C. Dubois, F. Gilbert, P. Halmagrand, O. Hermant, and R. Saillard. Dedukti: a Logical Framework based on the $\lambda\Pi$-Calculus Modulo Theory, 2016. Draft.

[3] `https://deducteam.github.io/`, 2018.