Certifying Higher-Order Polynomial Interpretations

Niels van der Weide
Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands

Deivid Vale
Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands

Cynthia Kop
Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands

Abstract

Higher-order rewriting is a framework in which one can write higher-order programs and study their properties. One such property is termination: the situation that for all inputs, the program eventually halts its execution and produces an output. Several tools have been developed to check whether higher-order rewriting systems are terminating. However, developing such tools is difficult and can be error-prone. In this paper, we present a way of certifying termination proofs of higher-order term rewriting systems. We formalize a specific method that is used to prove termination, namely the polynomial interpretation method. In addition, we give a program that processes proof traces containing a high-level description of a termination proof into a formal Coq proof script that can be checked by Coq. We demonstrate the usability of this approach by certifying higher-order polynomial interpretation proofs produced by Wanda, a termination analysis tool for higher-order rewriting.

2012 ACM Subject Classification Theory of computation → Logic and verification; Theory of computation → Equational logic and rewriting

Keywords and phrases higher-order rewriting, Coq, termination, formalization

Digital Object Identifier 10.4230/LIPIcs.ITP.2023.30


Supplementary Material Software (Coq Formalization): github.com/nmvdw/Nijn [31]

Funding Niels van der Weide: This research was supported by the NWO project “The Power of Equality” OCENW.M20.380, which is financed by the Dutch Research Council (NWO).
Deivid Vale: Author supported by NWO Top project “Implicit Complexity through Higher-Order Rewriting”, NWO 612.001.803/7571.
Cynthia Kop: Author supported by NWO Top project “Implicit Complexity through Higher-Order Rewriting”, NWO 612.001.803/7571 and the NWO VIDI project “Constrained Higher-Order Rewriting and Program Equivalence”, NWO VI.Vidi.193.075.

Acknowledgements The authors thank Dan Frumin for his help with understanding and using Ltac.

1 Introduction

Automatically proving termination is an important problem in term rewriting, and numerous tools have been developed for this purpose, such as AProVE [10], NaTT [35], MatchBox [33], Mu-Term [12], SOL [13], TTT2 [21] and Wanda [16], which compete against each other in an annual termination competition [11]. Aside from basic (first-order) term rewriting, this includes tools analyzing for instance string, conditional, and higher-order rewriting.

Developing termination tools is a difficult and error-prone endeavor. On the one hand, the termination techniques that are implemented may contain errors. This is particularly relevant in higher-order term rewriting, where the proofs are often very intricate due to
partial application, type structure, beta-reduction, and techniques often not transferring perfectly between different formalisms of higher-order rewriting. Hence, it should come as no surprise that errors have been found even in published papers on higher-order rewriting. On the other hand, it is very easy for a tool developer to accidentally omit a test whether some conditions to apply specific termination techniques are satisfied, or to incorrectly translate a method between higher-order formalisms.

To exacerbate this issue, termination proofs are usually complex and technical in nature, which makes it hard to assess the correctness of a prover’s output by hand. Not only do many benchmarks contain hundreds of rules, modern termination tools make use of various proof methods that have been developed for decades. Indeed, a single termination proof might, for instance, make use of a combination of dependency pairs [9, 19, 3], recursive path orders [20, 5], rule removal, and multiple kinds of interpretations [8, 23, 34, 18]. This makes bugs very difficult to find.

Hence, there is a need to formally certify the output of termination provers, ideally automatically. There are two common engineering strategies to provide such certification. In the first, one builds the certifier as a library in a proof assistant along with tools to read the prover’s output and construct a formal proof, which we call proof script. The proof script is then verified by a proof assistant. Examples of this system design are the combinations Cochinelle/CIME3 [7] and CoLoR/Rainbow [6]. In the second, the formalization includes certified algorithms for checking the correctness of the prover’s output. This allows for the whole certifier to be extracted, using code extraction, and be used as a standalone program. Hence, the generation of proof scripts by a standalone tool is not needed in this approach, but it comes with a higher formalization cost. IsaFoR/CeTA [28] utilizes this approach.

When it comes to higher-order rewriting, however, the options are limited. Both Cochinelle [7] and IsaFoR/CeTA [28] only consider first-order rewriting. CoLoR/Rainbow [6] does include a formalization of an early definition of HORPO [20]. Since here we use a different term formalism compared to that of [20], our results are not directly compatible. See for instance [2, 25] for more formalization results in rewriting.

In this paper, we introduce a new combination Nijn/ONijn for the certification of higher-order rewriting termination proofs. We follow the first aforementioned system design: Nijn is a Coq library providing a formalization of the underlying higher-order rewriting theory and ONijn is a proof script generator that given a minimal description of a termination proof (which we call proof trace), outputs a Coq proof script. The proof script then utilizes results from Nijn for checking the correctness of the traced proof. The schematic below depicts the basic steps to produce proof certificates using Nijn/ONijn.

![Figure 1 Nijn/ONijn schematics.](image)
While $\text{Nijn}$ is the certified core part of our tool since it is checked by Coq, the proof script generation implemented in OCaml ($\text{ONijn}$) is not currently certified and must be trusted. For this reason, we deliberately keep $\text{ONijn}$ as simple as possible and no checking or computation is done by it. The only task delegated to $\text{ONijn}$ is that of parsing the proof trace given by the termination prover to a Coq proof script. Additionally, checking the correctness of polynomial termination proofs in Coq is an inherently incomplete task, since it would require a method to solve inequalities over arbitrary polynomials, which is undecidable in general.

**Contributions.** The main contribution of this paper can be summarized as follows:
- we provide a formalization of higher-order algebraic functional systems (Definition 2.6);
- a formal proof of the interpretation method using weakly monotonic algebras (Theorem 3.11);
- a formalization of the higher-order polynomial method (Theorem 4.7);
- a tactic that automatically solves the constraints that arise when using the higher-order polynomial method (Section 4.3);
- an OCaml program that transforms the output of a termination prover into a Coq script that represents the termination proof (Section 5).

**Technical Overview.** This paper orbits $\text{Nijn}$, a Coq library formalizing higher-order rewriting [31]. The formalization is based on intensional dependent type theory extended with two axioms: function extensionality and uniqueness of identity proofs [14]. Currently, the termination criterion formalized in the library is the higher-order polynomial method, introduced in [8]. The tool $\text{coqwc}$ counts the following amount of lines of code:

```
spec    proof   comments
5497    1985    272 total
```

The higher-order interpretation method roughly works as follows. First, types are interpreted as well-ordered structures (Definition 3.3), compositionally. For instance, we interpret base types as natural numbers (with the usual ordering). Then we interpret a functional type $A \Rightarrow B$ as the set of weakly monotonic functions from $\langle A \rangle$ to $\langle B \rangle$ where $\langle A \rangle$, $\langle B \rangle$ denote the interpretations of $A$, $B$ respectively. The second step is to map inhabitants of a type $A$ to elements of $\langle A \rangle$, which is expressed here by Definition 3.9.

This interpretation, called extended monotonic algebras in [8], alone does not suffice for termination. To guarantee termination, we interpret both term application (Definition 4.6) and function symbols as strongly monotonic functionals. In addition, terms must be interpreted in such a way that the rules of the system are strictly oriented, i.e., $[\ell] > [r]$, for all rules $\ell \rightarrow r$. This means that whenever a rewriting is fired in a term, the interpretation of that term strictly decreases. As such, termination is guaranteed. Here we use termination models (Definition 3.10) to collect these necessary conditions.

The main result establishing the correctness of this technique in the higher-order case is expressed by Theorem 3.11. To the reader familiar with the interpretation method in first-order rewriting, Theorem 4.7 would be no surprise. It is essentially the combination of the Manna–Ness criterion with higher-order polynomials and the additional technicalities that are needed for the higher-order case.
2 The Basics of Higher-Order Rewriting in Coq

In this section, we introduce the basic constructs needed to formalize algebraic functional systems (AFSs) like types, contexts, variables, terms, and rewriting rules. We end the section with an exposition on how to express termination constructively in Coq.

2.1 Terms and Rewrite Rules

Let us start by defining simple types.

**Definition 2.1** (ty). Simple types over a type $B$ are defined as follows:

\[
\text{Inductive ty} \ (B : \text{Type}) : \text{Type} := \\
\quad \mid \text{Base} : B \to ty B \\
\quad \mid \text{Fun} : ty B \to ty B \to ty B.
\]

Elements of $B$ are called base types. Every inhabitant $b : B$ gives rise to a simple type $\text{Base } b$ and if $A_1, A_2$ are simple types then so is $\text{Fun } A_1 A_2$. We write $A_1 \to A_2$ for $\text{Fun } A_1 A_2$.

We need (variable) contexts in order to type terms that may contain free variables. Conceptually, a context is a list of variables with their respective types. For instance, $[x_0 : A_0 ; \ldots ; x_n : A_n]$ is the context with variables $x_0$ of type $A_0$, $\ldots$, $x_n$ of type $A_n$. However, we use nameless variables in our development, so we do not keep track of their names. Consequently, a context is represented by a list of types. Then we only consider the list $[A_0 ; \ldots ; A_n]$. However, we still need to refer to the free variables in terms. In order to do so, we represent them through indexing positions in the context. For instance, in the context $[A_0 ; \ldots ; A_n]$ we have $n + 1$ position indexes $0, 1, \ldots, n$, which we use as variables.

**Definition 2.2** (con). The type of variable contexts over a type $B$ is defined as follows.

\[
\text{Inductive con} \ (B : \text{Type}) : \text{Type} := \\
\quad \mid \text{Empty} : \text{con } B \\
\quad \mid \text{Extend} : ty B \to \text{con } B \to \text{con } B.
\]

We write $\bullet$ for $\text{Empty}$ and $A \cdot, C$ for $\text{Extend } A C$.

**Definition 2.3** (var). We define the type $\text{var } C A$ of variables of type $A$ in context $C$ as

\[
\text{Inductive var} \ {\{B : \text{Type}\}} : \text{con } B \to ty B \to \text{Type} := \\
\quad \mid \text{Vz} : \forall C \ {\{\text{con } B\}} \ A : ty B, \text{var} (A \cdot, C) A \\
\quad \mid \text{Vs} : \forall C \ {\{\text{con } B\}} \ (A_1 A_2 : ty B), \text{var } C A_2 \to \text{var } (A_1 \cdot, C) A_2.
\]

Let us consider an example of a context and some variables. Suppose that we have a base type denoted by $b$. Then we can form the context $\text{Base } b$, $\text{Base } b \to \text{Base } b$, $\text{Empty}$. In this context, we have two variables. The first one, which is $\text{Vz}$, has type $\text{Base } b$, and the second variable, which is $\text{Vs} \text{Vz}$, has type $\text{Base } b \to \text{Base } b$. The context that we discussed corresponds to $[x_0 : b; x_1 : b \to b]$. The variable $\text{Vz}$ represents $x_0$, while $\text{Vs} \text{Vz}$ represents $x_1$.

In Definition 2.4 below we define the notion of well-typed terms-in-context which consists of those expressions such that there is a typing derivation. We use dependent types to ensure well-typedness of such expressions. The type of terms depends on a simple type $A : ty B$ (which represents the object-level type of the expression) and context $C : \text{con } B$ that carries the types of all free variables in the term. We also need to type function symbols. Hence, we require a type $F : \text{Type}$ of function symbols and $\text{ar} : F \to ty B$, which maps $f : F$ to a simple type $\text{ar } f$. 
As usual, every AFS induces a rewrite relation on the set of terms, which we denote by $\sim$. The formal definition is found in RewritingSystem.v. The rewrite relation $\sim$ is defined to be the closure of the one-step relation under transitivity and compatibility with the term constructors. In Coq, we use an inductive type to define this relation. Each rewrite step is represented by a constructor. More specifically, we have a constructor for rewriting the left-hand and the right-hand side of an application, we have a constructor for $\beta$-reduction, and we have a constructor for the rewrite rules of the AFS.

Example 2.7 (map_afs). Let us encode $R_{\text{map}}$ in Coq. It is composed of two rules: $\text{map } F \text{ nil } \rightarrow \text{ nil}$ and $\text{map } F (\text{cons } x \text{ xs }) \rightarrow \text{cons } (F x) (\text{map } F \text{ xs })$. We start with base types.

Example 2.7 (map_afs). Let us encode $R_{\text{map}}$ in Coq. It is composed of two rules: $\text{map } F \text{ nil } \rightarrow \text{ nil}$ and $\text{map } F (\text{cons } x \text{ xs }) \rightarrow \text{cons } (F x) (\text{map } F \text{ xs })$. We start with base types.
30:6 Certifying Higher-Order Polynomial Interpretations

The abbreviations \texttt{Btype} and \texttt{List} is to smoothen the usage of the base types. There are three function symbols in this system:

\begin{verbatim}
Inductive fun_symbols := TNil | TCons | TMap.
\end{verbatim}

The arity function \texttt{map_ar} maps each function symbol in \texttt{fun_symbols} to its type.

\begin{verbatim}
Definition map_ar f : ty base_types :=
  match f with
  | TNil ⇒ List
  | TCons ⇒ Btype → List → List
  | TMap ⇒ (Btype → Btype) → List → List
  end.
\end{verbatim}

So, \texttt{TNil} is a list and given an inhabitant of \texttt{Btype} and \texttt{List}, the function symbol \texttt{TCons} gives a \texttt{List}. Again we introduce some abbreviations to simplify the usage of the function symbols.

\begin{verbatim}
Definition Nil {C} : tm map_ar C _ := BaseTm TNil.
Definition Cons {C} x xs : tm map_ar C _ := BaseTm TCons · x · xs.
Definition Map {C} f xs : tm map_ar C _ := BaseTm TMap · f · xs.
\end{verbatim}

The first rule, \texttt{map F nil → nil}, is encoded as the following Coq construct:

\begin{verbatim}
Program Definition map_nil :=
  make_rewrite (\_, \_, \_ · \_) \_ (let f := TmVar Vz in Map · f · Nil) Nil.
\end{verbatim}

Notice that we only defined the \texttt{pattern} of the first two arguments of \texttt{make_rewrite}, leaving the types in the context (\_, \_, \_ · \_) and the type of the rule unspecified. Coq can fill in these holes automatically, as long as we provide a context pattern of the correct length. In this particular rewrite rule, there is only one free variable. As such, the variable \texttt{TmVar Vz} refers to the only variable in the context. In addition, we use iterated \texttt{let}-statements to imitate variable names. For every position in the context, we introduce a variable in Coq, which we use in the left- and right-hand sides of the rule. This makes the rules more human-readable. Indeed, the lhs \texttt{map F nil} of this rule is represented as \texttt{Map · f · Nil} in code. The second rule for \texttt{map} is encoded following the same ideas.

\begin{verbatim}
Program Definition map_cons :=
  make_rewrite (\_ · \_ · \_ · \_ · \_ · \_) \_ (let f := TmVar Vz in let x := TmVar (Vs Vz) in let xs := TmVar (Vs (Vs Vz)) in Map · f · (Cons · x · xs))
  (let f := TmVar Vz in let x := TmVar (Vs Vz) in let xs := TmVar (Vs (Vs Vz)) in Cons · (f · x) · (Map · f · xs)).
\end{verbatim}

Putting this all together, we obtain an AFS, which we call \texttt{map_afs}.

\begin{verbatim}
Definition map_afs := make_afs map_ar (map_nil :: map_cons :: nil).
\end{verbatim}

2.2 Termination

Strong normalization is usually defined as the absence of infinite rewrite sequences. Such a definition is sufficient in a classical setting where the law of excluded middle holds. However, we work in a constructive setting, and thus we are interested in a stronger definition.
Therefore, we need a constructive predicate, formulated positively, which implies there are no infinite rewrite sequences. This idea is captured by the following definition

\[\text{Definition 2.8} \text{(WellfoundedRelation.v). The well-foundedness predicate for a relation } R \text{ is defined as follows}\]

\[
\begin{align*}
\text{Inductive isWf} &\{X : \text{Type}\} (R : X \to X \to \text{Type}) (x : X) : \text{Prop} := \\
&\mid \text{acc} : (\forall y : X. R x y \to \text{isWf} R y) \to \text{isWf} R x.
\end{align*}
\]

A relation is well-founded if the well-foundedness predicate holds for every element.

\[\text{Definition Wf} \{X : \text{Type}\} (R : X \to X \to \text{Type}) := \forall (x : X), \text{isWf} R x.\]

Note that this definition has been considered numerous times before, for example in [4] and in ColoR [6]. An element \(x\) is well-founded if all \(y\) such that \(R x y\) are well-founded. Note that if there is no \(y\) such that \(R x y\), then \(x\) is vacuously well-founded. From the rewriting perspective, this definition properly captures the notion of strong normalization. Indeed, a term \(s\) is strongly normalizing iff every \(s'\) such that \(s\) rewrites to \(s'\) is strongly normalizing.

Well-foundedness contradicts the existence of infinite rewrite sequences, even in a constructive setting. As such, it indeed gives a stronger condition.

\[\text{Proposition 2.9} \text{(no_infinite_chain). If } R \text{ is well-founded, then there is no infinite sequence } s_0, s_1, \ldots \text{ such that } R(s_n, s_{n+1}), \text{ for all } n.\]

Next, we define strong normalization using well-founded predicates.

\[\text{Definition 2.10} \text{(is_SN). An algebraic functional system is strongly normalizing if for every context } C \text{ and every type } A \text{ the rewrite relation for terms of type } A \text{ in context } C \text{ is well-founded. We formalize that as follows:}\]

\[
\text{Definition isSN} \{B F : \text{Type}\} \{X : \text{afs} B F\} : \text{Prop} := \\
\forall (C : \text{con} B) (A : \text{ty} B), \text{Wf} \text{(fun (t1 t2 : tm X C A) } \Rightarrow t1 \sim > t2).\]

3 Higher-Order Interpretation Method

In this section, we formalize the method of weakly monotonic algebras for algebraic functional systems. We proceed by providing type-theoretic semantics for the syntactic constructions introduced in the last section and a sufficient condition for which such semantics can be used to establish strong normalization.

3.1 Interpreting types and terms

In weakly monotonic algebras, types are interpreted as sets along with a well-founded ordering and a quasi-ordering [24, 8]. For that reason, we start by defining compatible relations. Intuitively, these are the domain for our semantics.

\[\text{Definition 3.1} \text{(CompatibleRelation.v). Compatible relations are defined as follows}\]

\[
\text{Record CompatRel} := \{ \\
\text{carrier : Type} ; \\
gt : \text{carrier} \to \text{carrier} \to \text{Prop} ; \\
ge : \text{carrier} \to \text{carrier} \to \text{Prop} \}.
\]

We write \(x > y\) and \(x >= y\) for \(gt x y\) and \(ge x y\) respectively.
The record `CompatRel` consists of the data needed to express compatibility between \( > \) and \( \geq \). The conditions it needs to satisfy, are in the type class `isCompatRel`, defined below.

\[
\text{Class isCompatRel} \ (X : \text{CompatRel}) := \\
\hspace{1em} \text{gt_trans} : \forall \{x y z : X\}, \ x > y \rightarrow y > z \rightarrow x > z ; \\
\hspace{1em} \text{ge_trans} : \forall \{x y z : X\}, \ x \geq y \rightarrow y \geq z \rightarrow x \geq z ; \\
\hspace{1em} \text{ge_refl} : \forall \{x : X\}, \ x \geq x ; \\
\hspace{1em} \text{compat} : \forall \{x y : X\}, \ x > y \rightarrow x \geq y ; \\
\hspace{1em} \text{ge_gt} : \forall \{x y z : X\}, \ x \geq y \rightarrow y > z \rightarrow x > z ; \\
\hspace{1em} \text{gt_ge} : \forall \{x y z : X\}, \ x > y \rightarrow y \geq z \rightarrow x > z .
\]

Note that the field `gt_trans` in `isCompatRel` follows from `compat` and `ge_gt`. The type `nat` of natural numbers with the usual orders is a first example of data that satisfies `isCompatRel`. We denote this one by `nat_CompatRel`. This type class essentially models the notion of extended well-founded set introduced in [18]. An extended well-founded set is a set together with compatible orders \( >, \geq \) such that \( > \) is well-founded and \( \geq \) is a quasi-ordering. This compatibility requirement corresponds to the axiom `compat` in the type class `isCompatRel`. However, since we do not require \( > \) to be well-founded in this definition, we instead call it a compatible relation. More specifically, \( X \) is a compatible relation if it is of type `CompatRel` and satisfies the constraints in the type class `isCompatRel`.

In order to interpret simple types (Definition 2.1), we start by fixing a type \( B : \text{Type} \) of base types and an interpretation \( \text{semB} : B \rightarrow \text{CompatRel} \) such that each \( \text{semB} b \) is a compatible relation. Whenever \( \text{semB} \) satisfies such property we call it an interpretation key for \( B \). We interpret arrow types as functional compatible relations, i.e., compatible relations such that the inhabitants of their carrier are functional. The class of functionals we are interested in is that of weakly-monotone maps.

\[\textbf{Definition 3.2 (MonotonicMaps.v).} \textbf{Weakly monotone maps} are defined as follows\]

\[
\text{Class weakMonotone \{X Y : \text{CompatRel}\} \ (f : X \rightarrow Y) :=} \\
\hspace{1em} \text{map_ge} : \forall \{x y : X\}, \ x \geq y \rightarrow f x \geq f y .
\]

\[
\text{Record weakMonotoneMap \{X Y : \text{CompatRel}\} :=} \\
\hspace{1em} \text{make_monotone} \{ \\
\hspace{2em} \text{fun_carrier} := X \rightarrow Y ; \\
\hspace{2em} \text{is_weak_monotone} : \text{weakMonotone} \text{fun_carrier} \}.
\]

The class `weakMonotone` says when a function is weakly monotonic, and an inhabitant of the record `weakMonotoneMap` consists of a function together with proof of its weak monotonicity. Then we define `fun_CompatRel` which is of type `CompatRel` and represents the functional compatible relations from \( X \) to \( Y \). It is defined as follows:

\[\text{Definition \hspace{1em}} \text{fun_CompatRel} \ (X Y : \text{CompatRel}) : \text{CompatRel} :=\{ |} \\
\hspace{2em} \text{carrier} := \text{weakMonotoneMap} X Y ; \\
\hspace{2em} \text{gt_f_g := forall} \ (x : X), \ f x > g x ; \\
\hspace{2em} \text{ge_f_g := forall} \ (x : X), \ f x \geq g x |} .\]
In what follows, we write \( X \rightarrow \text{wm} \ Y \) for \( \text{fun}_\text{CompatRel} \ X \ Y \). The semantics for a type is parametrized by an interpretation key \text{sem}B. It is defined as follows:

\[ \text{Definition 3.3 (sem_Ty).} \] Assume \( A : \text{ty} \ B \) and \text{sem}B is an interpretation key for \( B \). Then Fixpoint \( \text{sem}_\text{Ty} (A : \text{ty} \ B) : \text{CompatRel} := \)
\[
\text{match} \ A \text{ with}
\begin{align*}
| \text{Base} \ b & \Rightarrow \text{sem}B b \\
| A1 \rightarrow A2 & \Rightarrow \text{sem}_\text{Ty} \ A1 \rightarrow \text{wm} \ \text{sem}_\text{Ty} \ A2
\end{align*}
\]
end.

We also show how to interpret contexts, and to do so, we need to interpret the empty context and context extension. For those, we define the unit and product of compatible relations.

\[ \text{Definition 3.4 (Examples.v).} \] The \text{unit} and \text{product} compatible relations:

\[
\begin{align*}
\text{Definition unit}_\text{CompatRel} : \text{CompatRel} := |
\end{align*}
\]
\[
\begin{align*}
\text{carrier} := \text{unit} ;
\text{gt} _ _ := \text{False} ;
\text{ge} _ _ := \text{True} ;
\text{end}.
\end{align*}
\]

Note that \text{unit}_\text{CompatRel} is the compatible relation on the type with only one element, for which the ordering is trivial. In addition, \text{prod}_\text{CompatRel} is the compatible relation on the product, for which we compare elements coordinate-wise. We write \( X \ast Y \) for \text{prod}_\text{CompatRel} \ X \ Y.

\[ \text{Definition 3.5 (sem_Con).} \] Contexts are interpreted as follows

\[
\begin{align*}
\text{Fixpoint sem}_\text{Con} (C : \text{con} \ B) : \text{CompatRel} := \)
\[
\text{match} \ C \text{ with}
\begin{align*}
| \bullet & \Rightarrow \text{unit}_\text{CompatRel} \\
| A , \ C & \Rightarrow \text{sem}_\text{Ty} \ A \ast \text{sem}_\text{Con} \ C
\end{align*}
\]
end.

Next, we give semantics to variables and terms. The approach we use here is slightly different from what is usually done in higher-order rewriting. In [8, 18, 24], for instance, context information is lifted to the meta-level and variables are interpreted using the notion of valuations. In contrast, in our setting, the typing context lives at the syntactic level and variables are interpreted as weakly monotonic functions. Consequently, to every term \( t : \text{tm} \ C \ A \), we assign a map from \text{sem}_\text{Con} \ C \ to \text{sem}_\text{Ty} \ A \). In the remainder, we need the following weakly monotonic functions.

\[ \text{Definition 3.6 (Examples.v).} \] We define the following weakly monotonic functions.

\= Given \( y : \ Y \), we write \( \text{const}_\text{wm} \ y : X \rightarrow \text{wm} \ \ Y \) for the constant function.
\= Given \( f : X \rightarrow \text{wm} \ Y \text{ and } g : Y \rightarrow \text{wm} \ Z \), we define \( \text{g}_\text{wm} \ f : X \rightarrow \text{wm} \ Z \) to be their composition.
\= We have the first projection \( \text{fst}_\text{wm} : X \ast Y \rightarrow \text{wm} \ X \), which sends a pair \( (x, \ y) \) to \( x \), and the second projection \( \text{snd}_\text{wm} : X \ast Y \rightarrow \text{wm} \ Y \), which sends \( (x, \ y) \) to \( y \).
\= Given \( f : X \rightarrow \text{wm} \ Y \text{ and } g : X \rightarrow \text{wm} \ Z \), we have a function \( (f, \ g) : X \rightarrow \text{wm} \ (Y + Z) \). For \( x : X \), we define \( (f, \ g) \ X \ x \) to be \( (f \ X, \ g \ x) \).
\= Given \( f : Y = X \rightarrow \text{wm} \ Z \), we get \( \text{lam}_\text{wm} \ f : X \rightarrow \text{wm} \ (Y \rightarrow \text{wm} \ Z) \). For every \( x : X \text{ and } \ y : Y \), we define \( \text{lam}_\text{wm} \ f \ X \ y \ x \) to be \( f \ (X, \ y, \ x) \).
\= Given \( f : X \rightarrow \text{wm} \ (Y \rightarrow \text{wm} \ Z) \) and \( x : X \rightarrow \text{wm} \ Y \), we obtain \( f \ \text{wm} \ x : X \rightarrow \text{wm} \ Z \), which sends every \( a : X \) to \( f \ a \ (x, a) \).
\= Given \( x : X \), we have a weakly monotonic function \( \text{apply}_\text{el}_\text{wm} \ x : (X \rightarrow \text{wm} \ Y) \rightarrow \text{wm} \ Y \) which sends \( f : X \rightarrow \text{wm} \ Y \) to \( f \ x \).
Recall that variables are represented by positions in a context which in turn is interpreted as a weakly monotonic product (Definition 3.5). This allows us to interpret the variable at a position in a context as the corresponding interpretation of the type in that position.

**Definition 3.7 (\(\text{sem}_\text{Var}\)).** We interpret variables with the following function

\[
\text{Fixpoint } \text{sem}_\text{Var} \{C : \text{con} B\} \{A : \text{ty} B\} (v : \text{var} C A) : \text{sem}_\text{Con} C \twoheadrightarrow \text{wm } \text{sem}_\text{Ty} A \\
:= \text{match } v \text{ with} \\
| Vz \Rightarrow \text{fst}_\text{wm} \\
| Vs v \Rightarrow \text{sem}_\text{Var} v \circ \text{wm } \text{snd}_\text{wm} \\
\text{end}.
\]

We need the following data in order to provide semantics to terms. An arity function \(\text{ar} : F \rightarrow \text{ty} B\), together with its interpretation \(\text{semF}: \forall (f : F), \text{sem}_\text{Ty} (\text{ar } f)\), and an application operator given by

\[
\text{semApp}: \forall (A_1 A_2 : \text{ty} B), (\text{sem}_\text{Ty} A_1 \twoheadrightarrow \text{wm } \text{sem}_\text{Ty} A_2) * (\text{sem}_\text{Ty} A_1 \twoheadrightarrow \text{wm } \text{sem}_\text{Ty} A_2)
\]
to interpret term application.

**Remark 3.8.** A first, but incorrect, guess to interpret application would have been by interpreting the application of \(f : \text{sem}_\text{Ty} A_1 \twoheadrightarrow \text{wm } \text{sem}_\text{Ty} A_2\) to \(x : \text{sem}_\text{Ty} A_1\) by \(f x\). However, there is a significant disadvantage of this interpretation. Ultimately, we want to deduce strong normalization from the interpretation, and the main idea is that if we have a rewrite \(x \rightsquigarrow x'\), then we have \(\text{sem}_\text{Tm} x > \text{sem}_\text{Tm} x'\). This requirement would not be satisfied if we interpret application of our terms as actual applications as functions. Indeed, if we have \(x < x'\), then one is not guaranteed that we also have \(f x < f x'\), because \(f\) is only weakly monotone.

There are two ways to deal with this. One way is by interpreting function types as strictly monotonic maps [18]. In this approach, this interpretation of application is valid. However, it comes at a price, because the interpretation of lambda abstraction becomes more difficult.

Another approach, which we use here, is also used in [8]. We add a parameter to our interpretation method, namely \(\text{semApp}\), which abstractly represents the interpretation of application. To deduce strong normalization in this setting, we add requirements about \(\text{semApp}\) in Section 3.2. As a result, in concrete instantiations of this method, we need to provide an actual definition for \(\text{semApp}\). We see this in Section 4.2.

**Definition 3.9 (\(\text{sem}_\text{Tm}\)).** Given a function \(\text{semF}: \forall (f : F), \text{sem}_\text{Ty} (\text{ar } f)\), the semantics of terms is given by

\[
\text{Fixpoint } \text{sem}_\text{Tm} \{C : \text{con} B\} \{A : \text{ty} B\} \{t : \text{tm ar} C A\} : \text{sem}_\text{Con} C \twoheadrightarrow \text{wm } \text{sem}_\text{Ty} A := \\
\text{match } t \text{ with} \\
| \text{BaseTm } f \Rightarrow \text{const}_\text{wm} (\text{semF } f) \\
| \text{TmVar } v \Rightarrow \text{sem}_\text{Var} v \\
| \lambda f \Rightarrow \lambda \text{wm } (\text{sem}_\text{Tm } f) \\
| f \cdot t \Rightarrow \text{semApp }_\twoheadrightarrow \text{wm } (\text{sem}_\text{Tm } f, \text{sem}_\text{Tm } t) \\
\text{end}.
\]

Notice that we could have chosen a fixed way of interpreting application. We follow the same approach used by Fuhs and Kop [8] in our formalization and leave \(\text{semApp}\) abstract. This choice is essential if we want to use the interpretation method for both rule removal and the dependency pair approach. See [15, Chapters 4 and 6] for more detail.
3.2 Termination Models for AFSs

Now we have set up everything that is necessary to define the main notion of this section: *termination models*. From a termination model of an algebraic functional system, one obtains an interpretation of the types and terms. In addition, every rewrite rule is “satisfied” in this interpretation.

▶ **Definition 3.10 (Interpretation).** Let \( R \) be an algebraic functional system with base type \( B \) and function symbols \( F \). A **termination model** of \( R \) consists of

- an interpretation key \( \text{sem}B \);
- a function \( \text{sem}F : \forall (f : F), \text{sem}_{Ty}(\text{ar} f) \);
- a function \( \text{semApp} : \forall (A1 A2 : \text{ty} B), (\text{sem}_{Ty}A1 \rightarrow \text{wm sem}_{Ty}A2) \times \text{sem}_{Ty}A1 \rightarrow \text{wm sem}_{Ty}A2 \)

such that the following axioms are satisfied

- each \( \text{sem}B b \) is well-founded and inhabited;
- if \( f > f' \), then \( \text{semApp} _ _ (f, x) > \text{semApp} _ _ (f', x) \);
- if \( x > x' \), then \( \text{semApp} _ _ (f, x) > \text{semApp} _ _ (f, x') \);
- we have \( \text{semApp} _ _ (f, x) \geq f x \) for all \( f \) and \( x \);
- for every rewrite rule \( r \), substitution \( s \), and element \( x \), we have

\[
\text{semTm}(\text{lhs} r \ [\ s\ ] \ x) > \text{semTm}(\text{rhs} r \ [\ s\ ] \ x).
\]

Whereas the left-hand side of every rewrite rule is greater than its right-hand side, this does not hold for \( \beta \)-reduction in our interpretations. Since rewrite sequences can contain both rewrite rules and \( \beta \)-reduction, such sequences are not guaranteed to strictly decrease. As such, we need more to actually conclude strong normalization, and we follow the method used by Kop [15]. More specifically, Kop uses rule removal to show that strong normalization follows from the strong normalization of \( \beta \)-reduction, which is a famous theorem proven by Tait [27]. The strong normalization of \( \beta \)-reduction has been formalized numerous times and an overview can be found in [1]. Now we deduce the main theorem of this section.

▶ **Theorem 3.11 (afs_is_SN_from_2terpretation).** Let \( R \) be an algebraic functional system. If we have a termination model of \( X \), then \( X \) is strongly normalizing.

4 The Higher-Order Polynomial Method

4.1 Polynomials

In this section, we instantiate the material of Section 3 to a concrete instance, namely the polynomial method [8]. For that reason, we define the notation of higher-order polynomial.

▶ **Definition 4.1 (Polynomial.v).** We define the type \( \text{base poly} \) of base polynomials and \( \text{poly} \) of higher-order polynomials by mutual induction as follows:
We can make expressions of base polynomials using \( \text{from}_\text{poly} \) and \( \text{from}_\text{poly} \) with \( \text{from}_\text{poly} \) and \( \text{from}_\text{poly} \) respectively. Note that every polynomial \( \text{base}_\text{poly} \) is a polynomial in context \( \text{base}_\text{poly} \) and \( \text{base}_\text{poly} \). Our \( \text{base}_\text{poly} \) and \( \text{base}_\text{poly} \) are a type of base polynomials that does not depend on the actual base type. This is the role of \( \text{base}_\text{poly} \), which only depends on the variables being used. We can freely add and multiply inhabitants of \( \text{base}_\text{poly} \), and if we were to use a constant, then we do not explicitly need to mention the base type. In addition, we are able to transfer between \( \text{base}_\text{poly} \) and \( \text{base}_\text{poly} \), and that is what \( \text{base}_\text{poly} \) and \( \text{from}_\text{poly} \) enable us to do.

Let us make some remarks about the design choices we made and how they affected the definition of polynomials. One of our requirements is that we are able to add and multiply polynomials on different base types. This is frequently used in actual examples, such as Example 4.2. Function symbols might use arguments from different base types, and we would like to use both of them in polynomial expressions.

One possibility would have been to only work with the type \( \text{poly} \) and to add a constructor

\[
\text{P}_\text{plus} : \forall \{ C : \text{con} \} \, \{ b1 : B \} \, \{ b2 : B \},
\text{poly} \, C \, (\text{Base} \, b1) \rightarrow \text{poly} \, C \, (\text{Base} \, b2) \rightarrow \text{poly} \, C \, (\text{Base} \, b1)
\]

However, we refrained from doing so: if we were to use \( \text{P}_\text{const} \), then the elaborator would be unable to determine the actual type if we do not tell the base type explicitly. Instead, we used a type of base polynomials that does not depend on the actual base type. This is the role of \( \text{base}_\text{poly} \), which only depends on the variables being used. We can freely add and multiply inhabitants of \( \text{base}_\text{poly} \), and if we were to use a constant, then we do not explicitly need to mention the base type. In addition, we are able to transfer between \( \text{base}_\text{poly} \) and \( \text{poly} \), and that is what \( \text{base}_\text{poly} \) and \( \text{from}_\text{poly} \) enable us to do.

Note that our definition of higher-order polynomials is rather similar to the one given by Fuhs and Kop [8, Definition 4.1]. They define a set \( \text{Pol}(X) \), which consists of polynomial expressions, and for every type \( A \) a set \( \text{Pol}^A(X) \). The set \( \text{Pol}^A(X) \) is defined by recursion: for base type, it is the set of polynomials over \( X \) and \( A \) for function types \( A_1 \rightarrow A_2 \), it consists of expressions \( \lambda y : A_1 \, P \) where \( P \) is a polynomial of type \( A_2 \) using an extra variable \( y : A_1 \). Our \( \text{base}_\text{poly} \) and \( \text{poly} \) correspond to \( \text{Pol}(X) \) and \( \text{Pol}^A(X) \) respectively. However, there are some differences. First of all, Fuhs and Kop require variables to be fully applied, whereas we permit partially applied variables. Secondly, Fuhs and Kop define polynomials in such a way that for every two base types \( b_1, b_2 \) the types \( \text{Pol}^{b_1}(X) \) and \( \text{Pol}^{b_2}(X) \) are equal. This is not the case in our definition: instead we use constructors \( \text{from}_\text{poly} \) and \( \text{base}_\text{poly} \) to relate \( \text{base}_\text{poly} \) and \( \text{poly} \).

In the polynomial method, the interpretation key sends every base type to \( \text{nat}_\text{CompatRel} \), and in what follows, we write \([ C \text{con}] \) and \([ A \text{ty}] \) for the interpretation of contexts and types respectively. Note that every polynomial \( \text{P} : \text{poly} \, C \, A \) gives rise to a weakly monotonic
function \textit{sem\_poly} : \texttt{C \rightarrow \textit{wm} \texttt{A \texttt{ty}}} and that every base polynomial \textit{P} : \textit{base\_poly} \texttt{C} gives rise to \textit{sem\_base\_poly} : \texttt{C \rightarrow \textit{wm} nat\_CompatRel}. These two functions are defined using mutual recursion and every constructor is interpreted in the expected way: \textit{sem\_poly}.

In order to actually use \textit{base\_poly} \texttt{C} and \textit{poly} \texttt{C A}, we provide convenient notations for operations on polynomials. More concretely, we define notations +, *, and \texttt{·} that represent addition, multiplication, and application respectively. These operations must be overloaded since we need to be able to add polynomials of different types. To do so, we similarly use type classes to \textit{Math\_Classes} [26]. For details, we refer the reader to the formalization.

\section*{Example 4.2 (map\_fun\_poly)}

We continue with Example 2.7 and provide a polynomial interpretation to the system \textit{map\_afs} as follows:

\begin{verbatim}
Definition map\_fun\_poly fn\_symbols : poly \texttt{•} (arity trs fn\_symbols) :=
  match fn\_symbols with
  | Tnil \rarr; to\_Poly (P\_const 3)
  | Tcons \rarr; \lambda P \lambda \lambda P let y1 := P\_var Vz in
to\_Poly (P\_const 3 + P\_const 2 \ast y1)
  | Tmap \rarr; \lambda P let y0 := P\_var (Vs Vz) in \lambda P let G1 := P\_var Vz in
to\_Poly (P\_const 3 \ast y0 + P\_const 3 \ast y0 \ast (G1 \texttt{·} P (y0)))
end.
\end{verbatim}

Informally, the interpretation of \texttt{nil} is the constant 3. The interpretation of \texttt{cons} is the function that sends \texttt{y1 : N} to \texttt{3 + 2 y1}, and \texttt{map} is interpreted as the function that sends \texttt{y0 : N} and \texttt{G1 : N \rightarrow \textit{wm} N} to \texttt{3y0 + 3y0G1(y0)}.

\section{4.2 Polynomial Interpretation}

Using polynomials, we deduce strong normalization under certain circumstances using Theorem 3.11. Suppose that for all function symbols \texttt{f} we have a polynomial \textit{J} : \texttt{poly \texttt{•} (arity X f)}, and now we need to provide the interpretation for application. Following Fuhs and Kop [8], we use a general method to interpret application. We start by constructing a minimal element in the interpretation of every type.

\section*{Definition 4.3 (min\_el\_ty)}

For every simple type \texttt{A} we define a minimal element of \texttt{J A} as follows

\begin{verbatim}
Fixpoint min\_el\_ty \{ A : ty B \} : minimal\_element \texttt{[A \texttt{ty}]}
:=
  match A with
  | Base _ \rarr; nat\_minimal\_element
  | A1 \rightarrow A2 \rarr; min\_el\_fun\_space (min\_el\_ty A2)
end.
\end{verbatim}

Here \texttt{nat\_minimal\_element} is defined to be 0, and \texttt{min\_el\_fun\_space (min\_el\_ty A2)} is the constant function on \texttt{min\_el\_ty A2}.

In order to define the semantics of application, we need several operations involving \texttt{J A ty}. First, we consider \textit{lower value functions}.

\section*{Definition 4.4 (lvf)}

We define the \textit{lower value function} as follows

\begin{verbatim}
Fixpoint lvf \{ A : ty B \} : \texttt{[A \texttt{ty} \rightarrow \textit{wm} nat\_CompatRel} :=
  match A with
  | Base _ \rarr; id\_wm
  | A1 \rightarrow A2 \rarr; lvf \texttt{·} wm\_apply\_el\_wm (min\_el\_ty A1)
end.
\end{verbatim}
Note that we construct \( lvf \) directly as a weakly monotonic function. In addition, we reuse the combinators defined in Definition 3.6. As such, we do not need to prove separately that this function is monotonic.

In Kop and Fuhs [8], this definition is written down in a different, but equivalent, way. Instead of defining \( lvf_A \) recursively, they look at full applications, which would be more complicated in our setting. More specifically, since we are working with simple types, we must have that \( A = A_1 \rightarrow \ldots \rightarrow A_n \rightarrow B \). Then they define \( lvf_A(f) := f(\bot_{A_1}, \ldots, \bot_{A_n}) \), where \( \bot_A \) is the minimum element of the interpretation of \( A \). Next, we define two addition operations on \( \uplus A \).

- **Definition 4.5** (\( \text{plus}_\text{ty}_\text{nat} \)). Addition of natural numbers and elements on \( \uplus A \) is defined as follows

  \[
  \text{Fixpoint} \; \text{plus}_\text{ty}_\text{nat} \{ A : \text{ty} \} : \uplus A \rightarrow \uplus A \rightarrow \uplus A \\
  := \text{match} \; A \text{ with} \\
  | \text{Base} \_ \Rightarrow \text{plus}_\uplus \\
  | A1 \rightarrow A2 \Rightarrow \\
  \quad \text{let} \; f := \text{fst}_\uplus \text{owm} \text{snd}_\uplus \text{in} \\
  \quad \text{let} \; x := \text{fst}_\uplus \text{in} \\
  \quad \text{let} \; n := \text{snd}_\uplus \text{owm} \text{snd}_\uplus \text{in} \\
  \quad \lambda \text{wm} \left( \text{plus}_\text{ty}_\text{nat} \text{owm} (f \cdot \text{wm} x, n) \right) \\
  \text{end} 
  \]

  The function \( \text{plus}_\text{ty}_\text{nat} \) allows us to add arbitrary natural numbers to elements of the interpretation of types. Note that there are two cases in Definition 4.5. First of all, the type \( A \) could be a base type. In that case, we are adding two natural numbers, and we use the usual addition operation. In the second case, we are working with a functional type \( A1 \rightarrow A2 \). The resulting function is defined using pointwise addition with the relevant natural number. Now we have everything in place to define the interpretation of application.

- **Definition 4.6** (\( \text{p_app} \)). Application is interpreted as the following function

  \[
  \text{Definition} \; \text{p_app} \{ A1, A2 : \text{ty} \} \rightarrow \uplus \text{ty} \\
  := \text{let} \; f := \text{fst}_\uplus \text{in} \\
  \quad \text{let} \; x := \text{snd}_\uplus \text{in} \\
  \quad \text{plus}_\text{ty}_\text{nat} \text{owm} (f \cdot \text{wm} x, lvf \text{owm} x) 
  \]

  If both \( A1 \) and \( A2 \) are base types, then \( \text{p_app} (f, x) \) reduces to \( f \cdot x + x \). Note that \( \text{p_app} \) satisfies the requirements from Theorem 3.11. Hence, we obtain the following.

- **Theorem 4.7** (\( \text{poly}_\text{Interpretation} \)). Let \( R \) be an AFS. Suppose that for every function symbol \( f \) we have a polynomial \( \text{p_fun_sym} f \) such that for all rewrite rules \( l \leadsto r \) in \( R \) we have \( \text{semTm} l x > \text{semTm} r x \) for all \( x \). Then \( R \) has a termination model.

### 4.3 Constraint Solving Tactic

Notice that in order to formally verify a proof of termination of a system using Theorem 4.7, we need to provide a polynomial interpretation and show that \( \uplus l > \uplus r \) holds for all rules \( l \rightarrow r \). This will introduce inequality proof goals into the Coq context that must be solved.
The tactic is able to verify strong normalization.

Finding witnesses for such inequalities is tedious, and we would like to automate this task. For that reason, we developed a tactic (solve_poly) that automatically solves the inequalities coming from Theorem 4.7. Essentially, this tactic tries to mimic how one would solve those goals in a pen-and-paper proof, and the same method is used by Wanda.

Example 4.9. We show how to solve the constraint arising from map_cons mentioned in Example 4.8. The first step is to find matching terms on both sides of the inequality and subtract them. In our example, $3 + y_0 + 12y_1 + G_0(0)$ occurs on both sides, and after subtraction, we obtain the following constraint:

$$9 + 3y_0 + 9y_1 + (3y_0 + 9y_1 + 9)G_0(3 + y_0 + 3y_1) > 2G_0(0) + G_0(y_0) + 9y_1G_0(y_1).$$

The second step is combining the arguments for the higher-order variable $G_0$ use its monotonicity. Note that each of $0$, $y_0$, and $y_1$ is lesser than or equal to $3 + y_0 + 3y_1$, because they are natural numbers. Since $G_0$ is weakly monotonic, we get

$$2G_0(0) + G_0(y_0) + 9y_1G_0(y_1) \leq (9y_1 + 3)G_0(3 + y_0 + 3y_1).$$

Now we can simplify our original constraint to

$$9 + 3y_0 + 9y_1 + (3y_0 + 9y_1 + 9)G_0(3 + y_0 + 3y_1) > (9y_1 + 3)G_0(3 + y_0 + 3y_1).$$

Since $3y_0 + 9y_1 + 9 \geq y_1 + 3$, we have

$$(3y_0 + 9y_1 + 9)G_0(3 + y_0 + 3y_1) \geq (9y_1 + 3)G_0(3 + y_0 + 3y_1).$$

This is sufficient to conclude that the constraints for map_cons are satisfied.

The tactic solve_poly (solve_poly) follows the steps described above. Note that we use the tactic nia, which is a tactic in Coq that can solve inequalities and equations in nonlinear integer arithmetic. More specifically, solve_poly works as follows:

- First, we generate a goal for every rewrite rule, and we destruct the assumptions so that each variable in the context is either a natural number or a function.
- For every variable $f$ that has a function type, we look for pair $(x, y)$ such that $f(x)$ on the left hand side and $f(y)$ occurs on the right-hand side. We try using nia whether we can prove $x < y$ from our assumptions. If so, we add $x < y$ to the assumptions, and otherwise, we continue.
- The resulting goals with the extra assumptions are solved using nia.

Note that solve_poly is not complete, because nia is incomplete. As such, if a proof using this tactic is accepted by Coq, then that proof is correct. However, if the proof is not accepted, then it does not have to be the case that the proof is false. With the material discussed in this section, we can write down the polynomials given in Example 4.2, and the tactic is able to verify strong normalization.

Example 4.8. Let us consider a concrete example. We use the polynomials given in Example 4.2 to show strong normalization of Example 2.7. This example introduces two inequalities, one for each rule. Let $G_0 : \mathbb{N} \rightarrow \mathbb{N}$ be weakly monotonic. For rule map_nil, we need to prove that for all $G_0$, the constraint $12 + G_0(0) + 9G_0(3) > 3$ holds. For the second rule, map_cons, the constraint is: $12 + 4y_0 + 12y_1 + G_0(0) + (3y_0 + 9y_1 + 9)G_0(3 + y_0 + 3y_1) > 3 + y_0 + 12y_1 + 3G_0(0) + G_0(y_0) + 9y_1G_0(y_1)$, for all $y_0, y_1 \in \mathbb{N}$ and $G_0$.
5 Generating Proof Scripts

In this section, we discuss the practical aspects of our verification framework. In principle, one can manually encode rewrite systems as Coq files and use the formalization we provide to verify their own termination proofs. However, this is cumbersome to do. Indeed, in Example 2.7 we used abbreviations to make the formal description of \( R_{\text{map}} \) more readable. A rewrite system with many more rules would be difficult to encode manually. Additionally, to formally establish termination we also need to encode proofs. We did this in Example 4.2. The full formal encoding of \( R_{\text{map}} \) and its termination proof is found in the file Map.v.

5.1 Proof traces for polynomial interpretation

This difficulty of manual encoding motivates the usage of proof traces. A proof trace is a human-friendly encoding of a TRS and the essential information needed to reconstruct the termination proof as a Coq script. Let us again consider \( R_{\text{map}} \) as an example. The proof trace for this system starts with YES to signal that we have a termination proof for it. Then we have a list encoding the signature and the rules of the system.

YES
Signature: [cons : a -> list -> list ;
    map : list -> (a -> a) -> list ;
    nil : list
]
Rules: [
    map nil F => nil ;
    map (cons X Y) G => cons (G X) (map Y G)
]

Notice that the free variables in the rules do not need to be declared nor their typing information provided. Coq can infer this information automatically. The last section of the proof trace describes the interpretation of each function symbol in the signature.

Interpretation: [
    \( J(\text{cons}) = \text{Lam}[y0;y1].3 + 2*y1; \)
    \( J(\text{map}) = \text{Lam}[y0;G1].3*y0 + 3*y0 * G1(y0); \)
    \( J(\text{nil}) = 3 \)
]

We can fully reconstruct a formal proof of termination for \( R_{\text{map}} \), which uses Theorem 4.7, with the information provided in the proof trace above. The full description of proof traces can be found in [29], the API for ONijn. Proof traces are not Coq files. So we need to further compile them into a proper Coq script. The schematics in Figure 1 describe the steps necessary for it. We use ONijn to compile proof traces to Coq script. It is invoked as follows:

\texttt{onijn path/to/proof/trace.onijn -o path/to/proof/script.v}

Here, the first argument is the file path to a proof trace file and the -o option requires the file path to the resulting Coq script. The resulting Coq script can be verified by Nijn as follows:

\texttt{coqc path/to/proof/script.v}

Instructions on how to locally install ONijn/Nijn can be found at [29].
5.2 Verifying Wanda’s Polynomial Interpretations

It is worth noticing that the termination prover is abstract in our certification framework. This means that we are not bound to a specific termination tool. So we can verify any termination tool that implements the interpretation method described here and can output proof traces in ONijn format.

Since Wanda [16] is a termination tool that implements the interpretation method in [8], it is our first candidate for verification. We added to Wanda the runtime argument \textit{--formal} so it can output proof traces in ONijn format. In [16] one can find details on how to invoke Wanda. For instance, we illustrate below how to run Wanda on the map AFS.

```bash
./wanda.exe -d rem --formal Mixed_HO_10_map.afs
```

The setting \textit{-d rem} sets Wanda to disable rule removal. The option \textit{--formal} sets Wanda to only use polynomial interpretations and output proofs to ONijn proof traces. Running Wanda with these options gives us the proof trace we used for $R_{\text{map}}$ above. The latest version of Wanda, which includes this parameter, is found at [17].

The table below describes our experimental evaluation on verifying Wanda’s output with the settings above. The benchmark set consists of those 46 TRSs that Wanda outputs YES while using only polynomial interpretations and no rule removal. The time limit for certification of each system is set to 60 seconds.

The experiment was run in a machine with M1 Pro 2021 processor with 16GB of RAM. Memory usage of Nijn during certification ranges from 400MB to 750MB. We provide the experimental benchmarks at https://github.com/deividrvale/nijn-coq-script-generation.

<table>
<thead>
<tr>
<th>Technique</th>
<th>Wanda</th>
<th>Nijn/ONijn</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>46</td>
<td>23%</td>
</tr>
</tbody>
</table>

Hence, we can certify all TRSs proven SN by Wanda using only polynomial interpretations.

6 Conclusions and Future Work

We presented a formalization of the polynomial method in higher-order rewriting. This not only included the basic notions, such as algebraic functional systems, but also the interpretation method and the instantiation of this method to polynomials. In addition, we showed how to generate Coq scripts from the output of termination provers. This allowed us to certify their output and construct a formal proof of strong normalization. We also applied our tools to a concrete instance, namely to check the output of Wanda.

There are numerous ways to extend this work. First, one could formalize more techniques from higher-order rewriting, such as tuple interpretations [18] and dependency pairs [19, 22]. One could also integrate HORPO into our framework [20]. Second, in the current formalization, the interpretation of application is fixed for every instance of the polynomial method. One could also provide the user with the option to select their own interpretation. Third, currently, only Wanda is integrated with our work. This could be extended so that there is direct integration for other tools as well.
References


René Thiemann and Christian Sternagel. Certification of Termination Proofs Using CeTA. In Stefan Berghofer, Tobias Nipkow, Christian Urban, and Makarius Wenzel, editors, Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich,
30:20  Certifying Higher-Order Polynomial Interpretations


