Equational Reasoning in Algebraic Structures: a Complete Tactic

Luís Cruz-Filipe[1,2] and Freek Wiedijk[1]

[1]NIII, University of Nijmegen, Netherlands and [2]CLC, Lisbon, Portugal

Abstract

We present rational, a Coq tactic for equational reasoning in abelian groups, commutative rings, and fields. We give an mathematical description of the method that this tactic uses, which abstracts from Coq specifics.

We prove that the method that rational uses is correct, and that it is complete for groups and rings. Completeness means that the method succeeds in proving an equality if and only if that equality is provable from the the group/ring axioms. Finally we characterize in what way our method is incomplete for fields.

Contents

1 Introduction

One of the main aims of the Foundations group at the University of Nijmegen is to help making formalization of mathematics practical and attractive. For this reason a library of formal mathematics for the Coq system [3] – called the C-CoRN library [4] – has been developed to exercise the technology of proof formalization. This library started as a formalization of the Fundamental Theorem of Algebra in the so-called FTA project, but then was extended with a formalization of basic analysis up to the Fundamental Theorem of Calculus, and currently other subjects are being added to it as well.

To support the formalization work for the C-CoRN library, a tactic called rational was implemented. It automatically proves equations from the field axioms. Later this tactic was generalized to prove equations in rings and groups as well. The tactic uses the approach of *reflection* from [1], in particular the variant of reflection called *partial reflection* described in [7]. The generalization to rings and groups uses the application of partial reflection called *hierarchical reflection* in [5].

The tactic has two parts: the first part is a Coq formalization of normalization of polynomial expressions over a field, and the second part is an ML program that constructs a proof term for a given equation. This means that the tactic contains two – quite different – programs. On the one hand there is the program that computes the normal form of a polynomial expression. This program is written in the Coq type theory, and is proved correct as part of the Coq formalization. On the other hand there is the program that calculates a proof term from an equation, which is written in ML.

The correctness of the rational tactic is guaranteed by the way that it works: if it finds a proof of an equation, then that proof is automatically checked by Coq. Failure, however, can arise from two different situations:

(1) the ML program cannot find a term that corresponds to the problem.

(2) the ML program returns a term that does not have the expected behavior.

In turn, the second situation can arise in two cases:

(2a) although the original terms are provably equal, the normalization procedure cannot determine that;

(2b) the original terms are in fact not provably equal.

This paper studies the behavior of rational from a theoretical point of view.

- It gives a mathematical description of the algorithm implicit in the ML part of the rational tactic, and proves that this algorithm is correct.
- It describes under what conditions the tactic is complete.

  Now completeness can mean two things here: either one can consider the set of equations that hold in all fields, or one can consider the equations that can be proved from the field axioms. It happens to be the case that both sets of equations are the same [2].

The first point means that situation (1) cannot occur. In the second point, we establish completeness for groups and rings, excluding also situation (2a). Unfortunately this result only extends partially to fields, but we can still give a simple condition which, if fulfilled, also excludes this situation.

As a consequence, when a call to rational fails no proof of the goal exists that follows exclusively from the structure's axioms. This is extremely useful in interactive proof development, since it enables the user to detect wrong paths much earlier.

The mathematics in this paper has not been formalized. Formalizing takes an order of a magnitude more work than just doing the proofs in the informal – old style – way, and it is not clear what the benefit of formalization would be in this case (apart from the fact that one then would be *certain* that the proofs are correct).

The description in this paper of the rational tactic is kept as independent of Coq as possible. The algorithms and results that we describe are not specific to Coq or even to type theory, they can be used with any proof assistant.

This paper is self-contained in the sense that everything that is used is defined as well. However, it does not go into detail about partial/hierarchical reflection or the details of the rational tactic. For this we refer to two earlier papers, [7] and [5].

We begin by describing the mechanism of rational in more detail. Then we discuss the several layers of expressions we need to study this mechanism.

Section 3 formally describes the ML part of the tactic and proves a number of results about it, among which the correctness of the code. In Section 4 we introduce the normalization function for rings and prove its completeness. This proof generalizes almost directly to groups, as explained in Section 5. Finally, Section 6 analyzes the more complex case of fields, focusing on why the previous proof cannot be adapted to this situation, and presents an alternative completeness result.

The tactic described here is a simplified version of that in [5], and in Section 7 we explain how the same theorems can be generalized to the implemented tactic. We conclude with an overview of what was achieved in Section 8.

1.1 Related work

Most proof assistants have automation tools that provide the functionality of rational for rings, and many also have them for fields (for instance, the standard library of Coq provides both these functionalities with the ring and field tactics, see [3]). This automation is always implemented (like rational is) by putting polynomials into a normal form.

The main difference between our approach and these other implementations of the same idea is that we do the normalization in a very structured and systematic way. We define addition and multiplication functions that are meant to operate on monomials and polynomials that are already in normal form. These functions are then the 'building blocks' of our normalization function. This enables us to easily prove the correctness of the normalization function, which we need to use the reflection method.

2 Background

In this section we lay the bricks for the work we propose to do. We begin by describing the way rational works in detail, after which we summarize the parts of [6], [7] and [5] that are essential for the remainder of the paper.

2.1 The mechanism of rational

The rational tactic proves equalities in an algebraic structure A through the use of a type of *syntactic expressions* E together with an *interpretation relation.*

$$]\!]_\rho \subseteq E \times A$$

In this, ρ is a *valuation* that maps the variables in the syntactic expressions to values in A. The relation $e \;]\!]_\rho \; a$ means that the syntactic expression e is interpreted under the valuation ρ by the object a.

The type E is an inductive type, and therefore it is possible to recursively define a *normalization function* $\mathcal{N}$ on the type of syntactic expressions:

$$\mathcal{N} : E \to E$$

One can prove the following two lemmas

$$e \rrbracket_\rho a \ \Rightarrow\ \mathcal{N}(e) \rrbracket_\rho a$$

$$e \rrbracket_\rho a \ \wedge\ e \rrbracket_\rho b \ \Rightarrow\ a =_A b$$

and together these lemmas give a method to prove equalities between terms that denote elements of A.

For instance, suppose that one wants to prove $a =_A b$. One finds e, f and ρ with $e \rrbracket_\rho a$ and $f \rrbracket_\rho b$, and one checks whether $\mathcal{N}(e) = \mathcal{N}(f)$. If this is the case then it follows that $a =_A b$.

For from the first lemma we find that $\mathcal{N}(e) \rrbracket_\rho a$ and $\mathcal{N}(f) \rrbracket_\rho b$, and then the second lemma gives this desired equality.

2.2 Object level and meta-level

To describe the behavior of rational we need to look at terms of several kinds. This section explains these different kinds of terms in turn, so that the remainder of the paper can be easily understood.

Throughout this paper we deal with algebraic structures (groups, rings and fields). And, as we are working with formal systems, we also have *terms* that are interpreted in these algebraic structures. To complicate things, we use the method of *reflection* which means that the notion of 'term' both occurs on the meta-level as well as on the object level. In this section we will clarify this. We will identify various instances of 'number zero' as an example to explain the situation.

Let us start with the *object level.* We have three kinds of objects that have a 'zero'.

- *The natural numbers and the integers.* First of all, we have the natural numbers $\mathbb{N}$. In the natural numbers there is a unique object which is the natural number zero.

  The equality that one uses for the natural numbers is *Leibniz equality.* This means that the zero of the natural numbers does not have different representations: there is only one zero.

  The integers are like the natural numbers: there is exactly one integer zero, and one uses Leibniz equality to compare integers.

- *The elements of the algebraic structures.* Each group, ring, or field A has a zero as well. However, as we use *setoids* for these algebraic structures (so we can model quotients in a constructively valid way), an algebraic structure can have more than one object that *represents* the zero of that structure. In other words, for an algebraic structure we use *setoid equality* instead of Leibniz equality.

  For instance, suppose we construct the real numbers as Cauchy sequences of rational numbers. Then *every* Cauchy sequence that converges to zero represents the zero of these 'Cauchy reals'. These sequences are then all 'setoid equal' to each other, but can be distinguished using Leibniz equality.

- *Field expressions.* Finally we have the set E of terms generated by the field operations: $+$, $-$, $\times$ and $/$. This is an inductively generated set of syntactic objects. In this set there is a unique term for 'zero'. For these 'field expressions' we also use Leibniz equality.

  Note that although these objects that we call field expressions are terms, they exist on the object level (as a set of mathematical objects, like the natural numbers) and not on the meta-level (as linguistic constructions).

We also have the *meta-level.* In the formal language that we use to talk about all these objects, we have terms denoting these objects. This means there is still another kind of zero:

- *Terms on the meta-level.* For the integers there is a constant in the language that denotes the integer zero. This symbol is a linguistic construction that differs from the integer zero itself, in that it exists on the meta-level instead of at the object level.

  Similarly, there is a function in the language that maps each algebraic structure to a zero element of that structure. Again, the symbol for this function is different from those zero elements itself, in that it exists on the meta-level. Note that this function denotes one specific zero of the structure among all the elements that are setoid equal to it.

Finally, in the case of the field expressions, the basic terms denoting them on the meta-level are very similar to the objects themselves. Still one should distinguish the two.

On the terms of the language there are two notions of equality. There is *syntactic identity*, and there is *$\beta\delta\iota$-equality* or *convertibility.* (These equalities are used to talk about the language, and cannot be expressed in the language itself.)

Consider the function 'zring' that maps the integers into a given ring. Then if one applies this function to the integer zero, one gets a term that is syntactically different from the term that denotes the zero of the ring. However it is convertible to this term, by $\beta\delta\iota$-reduction (δ-reduction means unfolding the definition of a function, and ι-reduction means unfolding of a recursive definition.)

We will almost everywhere use syntactic identity in this paper. The only conversion that we will refer to is $\beta\delta\iota$-reduction of a few basic functions: subtraction, the zring function and exponentiation with a constant natural number. Of all other functions the definition will never be unfolded.

We also have two kinds of 'terms', which are quite different. There are the 'field expressions' on the object level, and there are the terms denoting elements of a field on the meta-level. In both cases one builds these terms with the field operations: +, −, × and /. However they exist on different levels (the method of mimicking part of the meta-level on the object level is called *reflection*). Also, the field expressions are very trivial: they can *only* involve variables and the field operations. But the meta-level terms can involve any type of sub-term, as long as the full term denotes an element of the field. For instance in the field of real numbers $\sqrt{\mathrm{zring}(2)}$ is an acceptable meta-level term, but there is nothing like a square root in field expressions.

The distinction between these two different kinds of terms can be illustrated with two relations that are defined in this paper. The relation $<_E$ is defined on the field expressions in Definition 2.17. The relation $\prec_A$ is defined on meta-level terms denoting elements of the field A in Definition 2.12. Note that this second relation does not respect convertibility: ${1_A}^0$ ('one to the power zero') is convertible with 1_A, but $1_A \prec_A {1_A}^0$ while $1_A \not\prec_A 1_A$.

To summarize, we have three quite different kinds of objects that have a zero (integers, elements in an algebraic structure, and field expressions), and we should distinguish between these objects on the object level and terms denoting them on the meta-level.

Also we have four kinds of equality: between the objects on the object level we have *Leibniz equality* and *setoid equality* (and we can write those equalities in our language), while between the terms on the meta-level we have *syntactic identity* and *$\beta\delta\iota$-equality* (and those two relations are not in the language).

2.3 The semantic level

We now summarize the Algebraic Hierarchy of C-CoRN [6], on top of which rational works.

Definition 2.1 A *setoid structure* over A is a relation $=_A$: $A \to A \to \mathsf{Prop}$ (denoted infix) satisfying:

$$\begin{array}{lll}
\mathbf{Set_1} & : & \forall_{x:A}.x =_A x \\
\mathbf{Set_2} & : & \forall_{x,y:A}.x =_A y \to y =_A x \\
\mathbf{Set_3} & : & \forall_{x,y,z:A}.x =_A y \to y =_A z \to x =_A z
\end{array}$$

Furthermore, we distinguish subtypes $[A \to A]$ and $[A \to A \to A]$ of $A \to A$ and $A \to A \to A$, respectively, satisfying

$$\mathbf{Set_4} \quad : \quad \forall_{f:[A\to A]}.\forall_{x,x':A}.x =_A x' \to f(x) =_A f(x')$$

$$\mathbf{Set_5} \quad : \quad \forall_{f:[A\to A\to A]}.\forall_{x,x',y,y':A}.x =_A x' \to y =_A y' \to f(x,y) =_A f(x',y')$$

We will speak of a setoid A to mean a type A with a setoid structure over A.

Definition 2.2 A *group structure* over A is a setoid structure over A together with a tuple $\langle 0_A, +_A, -_A\rangle$ where $0_A : A$, $+_A : [A \to A \to A]$ and $-_A : [A \to A]$ (we will write $+_A$ using the usual infix notation) satisfying:

$$\begin{array}{rcl}
\mathbf{SG} & : & \forall_{x,y,z:A}.(x +_A y) +_A z =_A x +_A (y +_A z)\\
\mathbf{M_1} & : & \forall_{x:A}.x +_A 0 =_A x\\
\mathbf{M_2} & : & \forall_{x:A}.0 +_A x =_A x\\
\mathbf{G_1} & : & \forall_{x:A}.x +_A (-_A x) =_A 0\\
\mathbf{G_2} & : & \forall_{x:A}.(-_A x) +_A x =_A 0\\
\mathbf{AG} & : & \forall_{x,y:A}.x +_A y =_A y +_A x
\end{array}$$

Notice that axiom $\mathbf{M_2}$ (respectively $\mathbf{G_2}$) can be proved from $\mathbf{M_1}$ (resp. $\mathbf{G_1}$) and $\mathbf{AG}$. But in the construction of the Algebraic Hierarchy $\mathbf{AG}$ is introduced last.

By a group A we mean a type A with a group structure over it.

Definition 2.3 Let A be a group. We define $-_A : A \to A \to A$ by

$$x -_A y := x +_A (-_A y).$$

The following is trivial, and allows us to write $-_A : [A \to A \to A]$.

Proposition 2.4 $-_A$ satisfies $\mathbf{Set_5}$.

Definition 2.5 A *ring structure* over A is a group structure over A together with a tuple $\langle 1_A, \times_A\rangle$ where $1_A : A$, $\times_A : [A \to A \to A]$ (we will write $\times_A$ using the usual infix notation) satisfying the following.

$$\begin{array}{rcl}
\mathbf{R_1} & : & \forall_{x,y,z:A}.(x \times_A y) \times_A z =_A x \times_A (y \times_A z)\\
\mathbf{R_2} & : & \forall_{x:A}.x \times_A 1 =_A x\\
\mathbf{R_3} & : & \forall_{x:A}.1 \times_A x =_A x\\
\mathbf{R_4} & : & \forall_{x,y:A}.x \times_A y =_A y \times_A x\\
\mathbf{R_5} & : & \forall_{x,y,z:A}.x \times_A (y +_A z) =_A (x \times_A y) +_A (x \times_A z)
\end{array}$$

As before, axiom $\mathbf{R_3}$ can be proved from $\mathbf{R_2}$ and $\mathbf{R_4}$.

By a ring A we mean a type A with a ring structure over it.

Definition 2.6 Let A be a ring. We define two functions $\mathrm{zring}_A : \mathbb{Z} \to A$ and $\mathrm{nexp}_A : A \to \mathbb{N} \to A$ inductively as follows:

$$\begin{array}{rcll}
\mathrm{zring}_A(0) & := & 0_A & (1)\\
\mathrm{zring}_A(n+1) & := & \mathrm{zring}_A(n) +_A 1_A, \text{ for } n \geq 0 & (2)\\
\mathrm{zring}_A(n-1) & := & \mathrm{zring}_A(n) -_A 1_A, \text{ for } n \leq 0 & (3)
\end{array}$$

$$\begin{array}{rcll}
\mathrm{nexp}_A(x,0) & := & 1_A & (4)\\
\mathrm{nexp}_A(x,n+1) & := & x \times_A \mathrm{nexp}_A(x,n) & (5)
\end{array}$$

We denote $\mathrm{zring}_A(n)$ by $\underline{n}_A$ and $\mathrm{nexp}_A(x,n)$ by x^n.

The following is again trivial to prove.

PROPOSITION 2.7 For every n, the function $\cdot^n : A \to A$ satisfies $\mathbf{Set_4}$.

Based on this result, we will often see x^n as the application of $\cdot^n : [A \to A]$ to x.

DEFINITION 2.8 A *field structure* over A is a ring structure over A together with an operation $\cdot^{-1} : \Pi_{x:A}.x \neq 0 \to A$ (we denote $(\cdot^{-1}\ x\ H)$ simply by x^{-1}, leaving the proof term implicit) satisfying

$$\mathbf{F} : x \neq 0 \to x \times_A x^{-1} =_A 1_A.$$

By a field A we mean a type A with a field structure over it.

DEFINITION 2.9 Let A be a field. We define $/_A : A \to \Pi_{y:A}.y \neq 0 \to A$ by

$$x/_A y := x \times_A (y^{-1}).$$

The following is trivial:

PROPOSITION 2.10 $/_A$ satisfies $\mathbf{Set'_5}$:

$$\mathbf{Set'_5} \quad : \quad \forall_{x,x',y,y':A}.y \neq 0 \to y' \neq 0 \to x =_A x' \to y =_A y' \to x/_A y =_A x'/_A y'$$

We will sometimes abuse notation and refer to $\mathbf{Set'_5}$ as an instance of $\mathbf{Set_5}$, and refer to $/_A$ as an operation of type $[A \to A \to A]$.

DEFINITION 2.11 A *proof* of $t_1 =_A t_2$ from the field axioms in an environment Γ is a sequence $\varphi_1, \ldots, \varphi_n$ of equalities such that φ_n is $t_1 =_A t_2$ and, for $i = 1, \ldots, n$, one of the following holds.

- φ_i is an instance of one of the axioms $\mathbf{Set_1}$, $\mathbf{SG}$, $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{G_1}$, $\mathbf{G_2}$, $\mathbf{AG}$ or $\mathbf{R_1}$–$\mathbf{R_5}$.
- φ_i is an instance of axiom $\mathbf{F}$ and the hypothesis of this axiom is in Γ.
- φ_i is an instance of one of the axioms $\mathbf{Set_2}$–$\mathbf{Set_5}$ and the hypothesis(es) of the axiom are included in $\{\varphi_1, \ldots, \varphi_{i-1}\}$.

We will often not mention Γ explicitly, but assume that all the proofs are done in an environment containing all the necessary inequalities. The reason for this (and for choosing the term "environment" rather than "context") is that rational only looks at the equality being proved and assumes all needed inequalities hold anyway.

DEFINITION 2.12 Let A be a type. We define the relation $\prec_A$ on the terms of type A as the least relation satisfying:

1. $t \prec_A f(t)$ for $f : [A \to A]$ (in particular, in a group one has $t \prec_A -_A t$ and in a ring $t \prec_A t^n$ for $n : \mathbb{N}$);
2. $t_i \prec_A f(t_1, t_2)$ for $f : [A \to A \to A]$ and $i = 1, 2$ (in particular, f can be one of $+_A$, $-_A$ or $\times_A$ in a group or ring);
3. if A is a field, then $t_i \prec_A t_1/_A t_2$ for $i = 1, 2$.

(Notice the implicit requirement $t_2 \neq 0$ in the clause $t_i \prec_A t_1/_A t_2$.)

PROPOSITION 2.13 $\prec_A$ is a well founded relation.

PROOF. By definition, if $t_1 \prec_A t_2$ then t_1 is a subterm of t_2; since "being a subterm of" is a well founded relation, so is $\prec_A$. □

NOTATION 2.14 From now on, we will omit the subscript A in the symbols denoting the algebraic operations, since no ambiguity is introduced. However, we will write $=_A$ to emphasize the distinction between this defined equality and the one induced by $\beta\delta\iota$-reduction on the set of lambda terms of type A.

2.4 The syntactic level

We now introduce the syntactic counterpart to the type of fields, which is the type of expressions that rational works with.

Definition 2.15 The syntactic type E of expressions is the inductive type generated by the following grammar:

$$E ::= \mathbb{Z} \mid \mathbb{V}_0 \mid \mathbb{V}_1(E) \mid E + E \mid E \times E \mid E/E$$

where $\mathbb{V}_i = \{v^i_j | j \in \mathbb{N}\}$ for $i = 0, 1$.

Definition 2.16 We define the following *abbreviations* on expressions:

$$-e \quad := \quad e \times (-1) \tag{6}$$

$$e_1 - e_2 \quad := \quad e_1 + (-e_2) \tag{7}$$

$$e^0 \quad := \quad 1 \tag{8}$$

$$e^{n+1} \quad := \quad e \times e^n \tag{9}$$

Notice that these abbreviations are done only on the meta-level; when we write e.g. $e_1 - e_2$ we are speaking about the expression $e_1 + (e_2 \times (-1))$.

At some stage we will need an order on E.

Definition 2.17 The *order* on E is defined as follows, where $\star$ stands for $+$, $\times$ or $/$.

(i) $v^0_i <_E v^0_j$ if $i < j$;

(ii) $v^0_i <_E e$ whenever e is $i : \mathbb{Z}$, $e_1 \star e_2$ or $v^1_i(e')$;

(iii) $i <_E j$ if $i < j$ $(i, j : \mathbb{Z})$;

(iv) $i <_E e$ whenever e is $e_1 \star e_2$ or $v^1_i(e')$;

(v) $e_1 \star e_2 <_E e'_1 \star e'_2$ whenever $e_1 <_E e'_1$ or $e_1 = e'_1$ and $e_2 <_E e'_2$ (lexicographic ordering);

(vi) $e_1 + e_2 <_E e$ whenever e is $e'_1 \times e'_2$, e'_1/e'_2 or $v^1_i(e')$;

(vii) $e_1 \times e_2 <_E e$ whenever e is e'_1/e'_2 or $v^1_i(e')$;

(viii) $e_1/e_2 <_E e$ whenever e is $v^1_i(e')$;

(ix) $v^1_i(e_1) <_E v^1_j(e_2)$ whenever $i < j$ or $i = j$ and $e_1 <_E e_2$.

In other words, expressions are recursively sorted by first looking at their outermost operator

$$x <_E i <_E e + f <_E e \times f <_E e/f <_E v(e)$$

and then sorting expressions with the same operator using a lexicographic ordering. For example, if $x <_{\mathbb{V}_0} y$ and $u <_{\mathbb{V}_1} v$, then

$$x <_E y <_E 2 <_E 34 <_E x/4 <_E u(x + 3) <_E u(2 \times y) <_E v(x + 3).$$

2.5 The interpretation relation

The correspondence between the syntactic and the semantic levels is made via an interpretation relation, described in detail in [7] and [5]. It is this relation that allows us to speak of correctness and completeness of rational, which is what we want to do.

Substitutions

The definition of E includes families of variables so that we can speak about arbitrary expressions in a field, and not only about those that only mention the field operations. Therefore, the interpretation of an expression is dependent on an assignment of values to the variables, which we will call a substitution.

Definition 2.18 A *substitution* from a type of variables $\mathbb{V}$ to a type T is a finite (partial) function from $\mathbb{V}$ to T.

Notation 2.19 The domain of a substitution ρ will be denoted by $\mathrm{dom}(\rho)$ or simply by $\mathrm{dom}\rho$. We will use the usual notation $[v := t]$ for the substitution that replaces v with t.

The following definitions and results are standard from the theory of finite functions.

Definition 2.20 Let ρ, σ be substitutions from $\mathbb{V}$ to T. If ρ and σ coincide on the intersection of their domains (in particular, if their domains are disjoint), we define the *union* $\rho \cup \sigma$ to be the only substitution θ with domain $\mathrm{dom}\rho \cup \mathrm{dom}\sigma$ such that $\theta(v) = \rho(v)$, for $v \in \mathrm{dom}\rho$, and $\theta(v) = \sigma(v)$ for $v \in \mathrm{dom}\sigma$.

Definition 2.21 Let ρ, σ be substitutions from $\mathbb{V}$ to T. We say that ρ *is contained* in σ, denoted by $\rho \subseteq \sigma$, if there is a substitution θ from $\mathbb{V}$ to T such that $\sigma = \rho \cup \theta$.

Proposition 2.22 For all $\mathbb{V}$ and T, $\subseteq$ is a partial order on the set of substitutions from $\mathbb{V}$ to T.

Proof. Trivial. □

Proposition 2.23 Let ρ, σ be substitutions from $\mathbb{V}$ to T such that $\rho \subseteq \sigma$. Then $\sigma(v) = \rho(v)$ for every $v \in \mathrm{dom}\rho$.

Proof. By definition of $\subseteq$, there is a substitution θ such that $\sigma = \rho \cup \theta$; by definition of $\cup$, since $v \in \mathrm{dom}\rho$, $\sigma(v) = (\rho \cup \theta)(v) = \rho(v)$. □

Definition 2.24 A substitution ρ is *injective* if, for any two distinct variables x and y in $\mathbb{V}$, the terms $\rho(x)$ and $\rho(y)$ are syntactically distinct.

From now on, we assume a fixed field A.

Definition 2.25 A *substitution pair over* A is a pair $\rho = \langle \rho_0, \rho_1 \rangle$ where ρ_0 and ρ_1 are injective substitutions from, respectively, $\mathbb{V}_0$ to A and $\mathbb{V}_1$ to $[A \to A]$.

The results about substitutions generalize in the obvious way to substitution pairs.

Definition 2.26 Let ρ be a substitution pair over A. We say that ρ *is contained* in σ, denoted by $\rho \subseteq \sigma$, if $\rho_i \subseteq \sigma_i$ for $i = 0, 1$.

Proposition 2.27 $\subseteq$ is a reflexive and transitive relation on the set of substitution pairs over A.

Proposition 2.28 Let ρ, σ be substitution pairs over A such that $\rho \subseteq \sigma$. Then $\sigma_i(v^i_k) = \rho_i(v^i_k)$ for $i = 0, 1$ and $v^i_k \in \mathrm{dom}\rho_i$.

Interpretation of expressions

Definition 2.29 Let ρ be a substitution pair over A. The *interpretation relation* $\rrbracket_\rho \subseteq E \times A$ is defined inductively by:

$$
\begin{array}{rcll}
\rho_0(v_i^0) =_A t & \rightarrow & v_i^0 \rrbracket_\rho t & (10)\\
\underline{k} =_A t & \rightarrow & k \rrbracket_\rho t & (11)\\
e_1 \rrbracket_\rho t_1 \wedge e_2 \rrbracket_\rho t_2 \wedge t_1 + t_2 =_A t & \rightarrow & e_1 + e_2 \rrbracket_\rho t & (12)\\
e_1 \rrbracket_\rho t_1 \wedge e_2 \rrbracket_\rho t_2 \wedge t_1 \times t_2 =_A t & \rightarrow & e_1 \times e_2 \rrbracket_\rho t & (13)\\
e_1 \rrbracket_\rho t_1 \wedge e_2 \rrbracket_\rho t_2 \wedge t_2 \neq 0 \wedge t_1/t_2 =_A t & \rightarrow & e_1/e_2 \rrbracket_\rho t & (14)\\
e \rrbracket_\rho t_1 \wedge \rho_1(v_i^1)(t_1) =_A t & \rightarrow & v_i^1(e) \rrbracket_\rho t & (15)
\end{array}
$$

Notice that by omitting (14) we obtain an interpretation relation over rings; omitting also (13) and (11) for $k \neq 0$ we obtain an interpretation relation over groups.

Lemma 2.30 The abbreviated expressions (Definition 2.16) satisfy the following relations.

$$
\begin{array}{rcll}
e \rrbracket_\rho t_1 \wedge -t_1 =_A t & \rightarrow & -e \rrbracket_\rho t & (16)\\
e_1 \rrbracket_\rho t_1 \wedge e_2 \rrbracket_\rho t_2 \wedge t_1 - t_2 =_A t & \rightarrow & e_1 - e_2 \rrbracket_\rho t & (17)\\
e \rrbracket_\rho t_1 \wedge t_1^n =_A t & \rightarrow & e^n \rrbracket_\rho t & (18)
\end{array}
$$

Proof.

(16) Recall that $-e = e \times (-1)$. By $\mathbf{Set_1}$, $-1 =_A -1$; hence $-1 \rrbracket_\rho -1$ by (11). By hypothesis $e \rrbracket_\rho t_1$. Finally, since $-t_1 =_A t$, one has $t_1 \times (-1) =_A t$, whence $e \times (-1) \rrbracket_\rho t$ by (13).

(17) By definition, $e_1 - e_2 = e_1 + (-e_2)$. By hypothesis, $e_1 \rrbracket_\rho t_1$ and $e_2 \rrbracket_\rho t_2$. Since $-t_2 =_A -t_2$ by $\mathbf{Set_1}$, one has that $-e_2 \rrbracket_\rho -t_2$ by (16). By hypothesis $t_1 - t_2 =_A t$, that is (by definition of $-_A$), $t_1 + (-t_2) =_A t$. Hence, by (12) $e_1 + (-e_2) \rrbracket_\rho t$.

(18) By induction on n. If n is 0, then by (8) $e^n = 1$. By hypothesis $t_1^0 =_A t$, or simply $1 =_A t$ since $t_1^0 = 1$ by (4). Hence $1 \rrbracket_\rho t$ by (11).

Consider now $n = m + 1$; then $e^n = e \times e^m$ by (9). By hypothesis $t_1^{m+1} =_A t$, that is to say, $t_1 \times t_1^n =_A t$ according to (5). But $e \rrbracket_\rho t_1$ by hypothesis, and also $e^m \rrbracket_\rho t_1^m$ by induction hypothesis; hence $e \times e^m \rrbracket_\rho t$ by (13).

□

Lemma 2.31 Let $e : E$, $t : A$ and ρ, σ be substitution pairs for A with $\rho \subseteq \sigma$ such that $e \rrbracket_\rho t$; then $e \rrbracket_\sigma t$.

Proof. By induction on the proof of $e \rrbracket_\rho t$.

1. $e = v_i^0$ and $\rho_0(v_i^0) =_A t$: since $\rho \subseteq \sigma$, Proposition 2.28 implies that $\sigma_0(v_i^0) =_A t$, and by (10) also $v_i^0 \rrbracket_\sigma t$.
2. $e = n$ and $\underline{n} =_A t$: then $n \rrbracket_\sigma t$ follows by (11).
3. $e = e_1 + e_2$, $e_1 \rrbracket_\rho t_1$, $e_2 \rrbracket_\rho t_2$ and $t_1 + t_2 =_A t$; by induction hypothesis $e_1 \rrbracket_\sigma t_1$ and $e_2 \rrbracket_\sigma t_2$, whence $e_1 + e_2 \rrbracket_\sigma t$ follows from (12).
4. $e = e_1 \times e_2$: analogous using (13).
5. $e = e_1/e_2$: similar from (14), noticing that the side condition $t_2 \neq 0$ is also given by hypothesis.

6. $e = v_i^1(e')$, $e' \rrbracket_\rho t'$ and $\rho_1(v_i^1)(t') =_A t$: since $\sigma_1(v_i^1) = \rho_1(v_i^1)$ by Proposition 2.28, also $\sigma_1(v_i^1)(t') =_A t$. By induction hypothesis $e' \rrbracket_\sigma t'$, whence $v_i^1(e') \rrbracket_\sigma t$ by (15).

□

Lemma 2.32 Let $e : E$, $t, t' : A$ and ρ be a substitution pair for A such that $e \rrbracket_\rho t$ and $e \rrbracket_\rho t'$. Then the following hold.

(i) $t =_A t'$;

(ii) if $e \rrbracket_\rho t$ and $e \rrbracket_\rho t'$ can be proved without using (14), and no divisions occur in either t or t', then $t =_A t'$ can be proved without using the axiom **F**.

Proof. By induction on $\rrbracket_\rho$ (Coq checked). □

3 Lifting

We now start looking at the actual implementation of rational, focusing on the ML program inside it. This program computes a partial inverse to the interpretation relation described above, that is, given a term $t : A$, with A a field, it returns an expression e and a substitution pair ρ such that $e \rrbracket_\rho t$. In this section we formally describe this program as a function *lift* and prove its correctness.

3.1 Lifting to variables

The first step is to define what to do when we meet a term that is not built from the field operations, e.g. a variable x or an expression like $\sqrt{2}$.

Definition 3.1 Let $t : A$ and ρ be a substitution pair over A. Then $\mathit{lift}_{\mathbb{V}_0}(t, \rho) = \langle v, \sigma \rangle$, $v \in \mathbb{V}_0$, is defined by:

- if there is an i such that $\rho_0(v_i^0) = t$, then $v = v_i^0$ and $\sigma = \rho$;
- else, let k be minimal such that $\rho_0(v_k^0)$ is not defined and take $v = v_k^0$ and $\sigma_0 = \rho_0 \cup [v_k^0 := t]$, $\sigma_1 = \rho_1$.

The behavior of $\mathit{lift}_{\mathbb{V}_0}$ can be described as follows: given a term t and a substitution ρ, it checks whether there is a variable v_i^0 such that $\rho_0(v_i^0) = t$. In the affirmative case, it returns this variable and ρ; else it extends ρ_0 with a fresh variable which is interpreted to t and returns this variable and the resulting substitution. Notice that the result is deterministic, since there is at most one variable i satisfying $\rho_0(v_i^0) = t$.

Lemma 3.2 Let t and ρ be as in Definition 3.1, and suppose that $\mathit{lift}_{\mathbb{V}_0}(t, \rho) = \langle v, \sigma \rangle$. Then $\rho \subseteq \sigma$.

Proof. Immediate: either $\sigma = \rho$, and we invoke reflexivity of $\subseteq$ (Proposition 2.27), or $\langle \sigma_0, \sigma_1 \rangle = \langle \rho_0 \cup [v_k^0 := t], \rho_1 \rangle$ with $v_k^0 \notin \mathrm{dom}\rho_0$, which directly satisfies the definition of $\subseteq$. □

Lemma 3.3 Let t and ρ be as in Definition 3.1, and suppose that $\mathit{lift}_{\mathbb{V}_0}(t, \rho) = \langle v, \sigma \rangle$. Then $v \rrbracket_\sigma t$.

Proof. By definition of $\mathit{lift}_{\mathbb{V}_0}$, there are two cases:

- There is an i such that $\rho_0(v_i^0) = t$, and then also $\rho_0(v_i^0) =_A t$ by $\mathbf{Set_1}$, whence $v_i^0 \rrbracket_\rho t$ by (10). Since in this case $v = v_i^0$ and $\sigma = \rho$, the thesis follows.
- There is no such i; then $v = v_k^0$ where $k \notin \mathrm{dom}\rho_0$, and $\sigma_0 = \rho_0 \cup [v_k^0 := t]$. Then, by definition of $\cup$, $\sigma_0(v_k^0) = t$ and we can conclude as above that $v_k^0 \rrbracket_\sigma t$ using $\mathbf{Set_1}$ and (10).

□

Definition 3.4 Let $f : [A \to A]$ and ρ be a substitution pair over A. Then $\mathit{lift}_{\mathbb{V}_1}(f, \rho) = \langle v, \sigma \rangle$, $v \in \mathbb{V}_1$, is defined by:

- if there is an i such that $\rho_1(v^1_i) = f$, then $v = v^1_i$ and $\sigma = \rho$;
- else, let k be minimal such that $\rho_1(v^1_k)$ is not defined and take $v = v^1_k$ and $\sigma_0 = \rho_0$, $\sigma_1 = \rho_1 \cup [v^1_k := t]$.

Lemma 3.5 Let t and ρ be as in Definition 3.4, and suppose that $\mathit{lift}_{\mathbb{V}_1}(t, \rho) = \langle v, \sigma \rangle$. Then $\rho \subseteq \sigma$.

Proof. Analogous to the proof of Lemma 3.2. □

Lemma 3.6 Let $f : [A \to A]$ and ρ be a substitution pair over A and suppose that $\mathit{lift}_{\mathbb{V}_1}(f, \rho) = \langle v, \sigma \rangle$. Suppose that $t \rrbracket_\rho e$; then $v(t) \rrbracket_\sigma f(e)$.

Proof. By definition of $\mathit{lift}_{\mathbb{V}_1}$, there are again two cases:

- There is an i such that $\rho_1(v^1_i) = f$; then $\rho_1(v^1_i)(t) =_A f(t)$ by $\mathbf{Set_1}$, whence $v^1_i(e) \rrbracket_\rho f(t)$ by (15). Since in this case $v = v^1_i$ and $\sigma = \rho$, the thesis follows.
- There is no such i; then $v = v^1_k$ where $k \notin \mathrm{dom}\rho_1$, and $\sigma_1 = \rho_1 \cup [v^1_k := t]$. Then, by definition of $\cup$, $\sigma_1(v^1_k) = f$ and we can conclude as above that $v^1_k(e) \rrbracket_\sigma f(t)$ using $\mathbf{Set_1}$ and (15).

□

3.2 Lifting expressions

We can now define *lift*.

Definition 3.7 Let $t : A$ and ρ be a substitution pair over A. Then $\mathit{lift}(t, \rho)$ is recursively defined as follows.

$$\begin{array}{rcll}
\mathit{lift}(\underline{n}, \rho) & = & \langle n, \rho \rangle & n : \mathbb{Z} \text{ closed} \\
\mathit{lift}(t_1 \star t_2, \rho) & = & \langle e_1 \star e_2, \sigma \rangle & \text{where } \left\{ \begin{array}{l} \star \in \{+, -, \times, /\} \\ \langle e_1, \theta \rangle = \mathit{lift}(t_1, \rho) \\ \langle e_2, \sigma \rangle = \mathit{lift}(t_2, \theta) \end{array} \right. \\
\mathit{lift}(-t, \rho) & = & \langle -e, \sigma \rangle & \text{where } \langle e, \sigma \rangle = \mathit{lift}(t, \rho) \\
\mathit{lift}(t^n, \rho) & = & \langle e^n, \sigma \rangle & \text{where } \left\{ \begin{array}{l} n : \mathbb{N} \text{ is closed} \\ \langle e, \sigma \rangle = \mathit{lift}(t, \rho) \end{array} \right. \\
\mathit{lift}(f(t), \rho) & = & \langle v^1_i(e), \theta \rangle & \text{where } \left\{ \begin{array}{l} \langle e, \sigma \rangle = \mathit{lift}(t, \rho) \\ \langle v^1_i, \theta \rangle = \mathit{lift}_{\mathbb{V}_1}(f, \sigma) \end{array} \right. \\
\mathit{lift}(t, \rho) & = & \mathit{lift}_{\mathbb{V}_0}(t, \rho) & \text{otherwise}
\end{array}$$

The two last clauses also define $\mathit{lift}(\underline{n}, \rho)$ and $\mathit{lift}(t^n, \rho)$ when n is not a closed term.

Notice that on every recursive call of *lift* the argument decreases w.r.t $\prec_A$; since $\prec_A$ is well founded by Proposition 2.13, this is a valid definition.

Lemma 3.8 Let ρ be a substitution pair for A. For all $t : A$ and $e : E$, if $\langle e, \sigma \rangle = \mathit{lift}(t, \rho)$, then $\rho \subseteq \sigma$.

Proof. By induction on $\prec_A$.

1. t is minimal for $\prec_A$:
   (a) $t = \underline{n}$ with $n : \mathbb{Z}$ closed. Then $\sigma = \rho$.
   (b) otherwise $\langle e, \sigma \rangle = \mathit{lift}_{\mathbb{V}_0}(t, \rho)$. By Lemma 3.2, $\rho \subseteq \sigma$.
2. $t = f(t')$ with $f : [A \to A]$.

(a) f is $-_A$: immediate by induction hypothesis.

(b) f is $\cdot^n$ with n is a closed term: then the result follows by induction hypothesis.

(c) otherwise, $e = v_i^1(e')$ with $\langle e', \theta\rangle = \mathit{lift}(t', \rho)$ and $\langle v_i^1, \sigma\rangle = \mathit{lift}_{\mathbb{V}_1}(f, \theta)$. By induction hypothesis $\rho \subseteq \theta$; by Lemma 3.5 $\theta \subseteq \sigma$; by transitivity $\rho \subseteq \sigma$.

3. $t = t_1 \star t_2$ with $\star \in \{+, -, \times, /\}$: then $e = e_1 \star e_2$ with $\langle e_1, \theta\rangle = \mathit{lift}(t_1, \rho)$ and $\langle e_2, \sigma\rangle = \mathit{lift}(t_1, \theta)$.

By induction hypothesis, $\rho \subseteq \theta$ and $\theta \subseteq \sigma$; since $\subseteq$ is transitive (Proposition 2.27), $\rho \subseteq \sigma$.

□

The following is the main result so far: it expresses the correctness of the ML program inherent to rational. Given a term t and a substitution ρ, the program computes an expression e and a new substitution σ such that $e \rrbracket_\sigma t$.

Theorem 3.9 Let $t : A$ and ρ be a substitution pair over A, and take $\langle e, \sigma\rangle = \mathit{lift}(t, \rho)$. Then $e \rrbracket_\sigma t$.

Proof. By induction on $\prec_A$.

1. t is minimal for $\prec_A$:

(a) $t = \underline{n}$ with $n : \mathbb{Z}$ closed. Then, by definition of *lift*, $e = n$ and $\sigma = \rho$. By $\mathbf{Set_1}$, $\underline{n} =_A \underline{n}$, and by (11) $n \rrbracket_\rho \underline{n}$.

(b) otherwise $\langle e, \sigma\rangle = \mathit{lift}_{\mathbb{V}_0}(t, \rho)$. By Lemma 3.3, it follows that $e \rrbracket_\sigma t$.

2. $t = f(t')$ with $f : [A \to A]$.

(a) f is $-_A$: then $\langle e, \sigma\rangle = \langle -e', \sigma\rangle$ with $\langle e', \sigma\rangle = \mathit{lift}(t', \rho)$. By induction hypothesis, $e' \rrbracket_\sigma t'$; since $-t' = -t'$ by $\mathbf{Set_1}$, $-e' \rrbracket_\sigma -t'$ by (16).

(b) f is $\cdot^n$ with n closed: then $\langle e, \sigma\rangle = \langle (e')^n, \sigma\rangle$ with $\langle e', \sigma\rangle = \mathit{lift}(t', \rho)$. By induction hypothesis, $e' \rrbracket_\sigma t'$; since $(t')^n = (t')^n$ by $\mathbf{Set_1}$, $(e')^n \rrbracket_\sigma (t')^n$ by (18).

(c) otherwise $e = v_i^1(e')$ with $\langle e', \theta\rangle = \mathit{lift}(t', \rho)$ and $\langle v_i^1, \sigma\rangle = \mathit{lift}_{\mathbb{V}_1}(f, \theta)$. By induction hypothesis $e' \rrbracket_\theta t'$; Lemma 3.6 allows us to conclude that $f(e') \rrbracket_\sigma v_i^1(t')$.

3. $t = t_1 \star t_2$ with $\star \in \{+, -, \times, /\}$ (if $\star - /$, then also $t_2 \neq 0$): then $e = e_1 \star e_2$ with $\langle e_1, \theta\rangle = \mathit{lift}(t_1, \rho)$ and $\langle e_2, \sigma\rangle = \mathit{lift}(t_1, \theta)$.

By induction hypothesis, $e_1 \rrbracket_\theta t_1$; by Lemma 3.8, $\theta \subseteq \sigma$, whence by Lemma 2.31 also $e_1 \rrbracket_\sigma t_1$.

Also by induction hypothesis, $e_2 \rrbracket_\theta t_2$. Furthermore, $\mathbf{Set_1}$ implies $t_1 \star t_2 =_A t_1 \star t_2$, hence $e_1 \star e_2 \rrbracket_\theta t_1 \star t_2$ by either (12), (17), (13) or (14), according to whether $\star$ is respectively $+$, $-$, $\times$ or $/$; in the last case, the extra condition $t_2 \neq 0$ also holds.

□

Notice that this result is still valid if A is a group or a ring, as can be seen by removing the corresponding cases in this proof and checking that it remains valid.

3.3 Properties of lifting

The remainder of this section is concerned with other properties of the ML program, and of *lift*, that are needed for the rest of the paper.

First, lifting is idempotent on the second component: if lifting e with ρ returns t and σ, and θ is any substitution extending σ (in particular, σ itself), then $\mathit{lift}(t, \theta) = \langle e, \theta\rangle$.

Lemma 3.10 Let $t : A$, $e : E$ and ρ, σ, θ be substitution pairs over A such that $\langle e, \sigma\rangle = \mathit{lift}(t, \rho)$ and $\sigma \subseteq \theta$. Then $\mathit{lift}(t, \theta) = \langle e, \theta\rangle$.

Proof. By induction on $\prec_A$.

1. t is minimal for $\prec_A$:

   (a) $t = \underline{n}$ with $n : \mathbb{Z}$ closed. Then $\mathit{lift}(\underline{n}, \rho) = \langle n, \rho \rangle$ and $\mathit{lift}(\underline{n}, \theta) = \langle n, \theta \rangle$; hence the thesis holds.

   (b) otherwise $\langle e, \sigma \rangle = \mathit{lift}_{\mathbb{V}_0}(t, \rho)$. Then $e = v_i^0$ for some i, and by Lemma 3.3, $\sigma_0(v_i^0) = t$. Since $\sigma \subseteq \theta$, $\theta_0(v_i^0) = t$ by Lemma 2.31, and, according to the definition of $\mathit{lift}_{\mathbb{V}_0}$, $\mathit{lift}_{\mathbb{V}_0}(t, \theta) = \langle v_i^0, \theta \rangle$.

2. $t = f(t')$ with $f : [A \to A]$.

   (a) f is $-_A$: then $\langle e, \sigma \rangle = \langle -e', \sigma \rangle$ with $\langle e', \sigma \rangle = \mathit{lift}(t', \rho)$. By induction hypothesis, $\mathit{lift}(t', \theta) = \langle e', \theta \rangle$, whence $\mathit{lift}(-t', \theta) = \langle -e', \theta \rangle$.

   (b) f is $\cdot^n$ and n is closed: then $\langle e, \sigma \rangle = \langle (e')^n, \sigma \rangle$ with $\langle e', \sigma \rangle = \mathit{lift}(t', \rho)$. By induction hypothesis, $\mathit{lift}(t', \theta) = \langle e', \theta \rangle$, and it follows that $\mathit{lift}((t')^n, \theta) = \langle (-e')^n, \theta \rangle$.

   (c) otherwise $e = v_i^1(e')$ with $\langle e', \sigma' \rangle = \mathit{lift}(t', \rho)$ and $\langle v_i^1, \sigma \rangle = \mathit{lift}_{\mathbb{V}_1}(f, \sigma')$. By induction hypothesis, $\mathit{lift}(t', \theta) = \langle e', \theta \rangle$; by Lemma 3.6, $\sigma_1(v_i^1) = f$ and hence $\theta_1(v_i^1) = f$ by Lemma 2.31. Therefore, the definition of $\mathit{lift}_{\mathbb{V}_1}$ ensures that $\mathit{lift}_{\mathbb{V}_1}(f, \theta) = \langle v_i^1, \theta \rangle$ and $\mathit{lift}(f(t'), \theta) = \langle v_i^1(e'), \theta \rangle$.

3. $t = t_1 \star t_2$ with $\star \in \{+, -, \times, /\}$: then $e = e_1 \star e_2$ with $\langle e_1, \sigma_1 \rangle = \mathit{lift}(t_1, \rho)$ and $\langle e_2, \sigma \rangle = \mathit{lift}(t_1, \sigma_1)$.

   By Lemma 3.8, $\sigma_1 \subseteq \sigma$, hence $\sigma_1 \subseteq \theta$; then, by induction hypothesis, $\mathit{lift}(t_1, \theta) = \langle e_1, \theta \rangle$. Also by induction hypothesis, $\mathit{lift}(t_2, \theta) = \langle e_2, \theta \rangle$. It follows that $\mathit{lift}(t_1 \star t_2, \theta) = \langle e_1 \star e_2, \theta \rangle$.

□

All variables in the expression output by *lift* can be interpreted by the corresponding substitution.

Lemma 3.11 Let $t : A$ and ρ be a substitution pair over A. If $\mathit{lift}(t, \rho) = \langle e, \sigma \rangle$, then $v_k^i \in \mathrm{dom}(\sigma_k)$ for all variables v_k^i occurring in e.

Proof. By induction on t according to $\prec_A$.

1. t is minimal for $\prec_A$.

   (a) $t = \underline{n}$: then $e = n$ and no variables occur in e, so the result vacuously holds.

   (b) otherwise $\langle e, \sigma \rangle = \mathit{lift}_{\mathbb{V}_0}(t, \rho)$ and the result is immediate by definition of $\mathit{lift}_{\mathbb{V}_0}$.

2. $t = f(t')$ with $f : [A \to A]$.

   (a) f is $-_A$: then $e = e'$ and $\mathit{lift}(t', \rho) = \langle e', \sigma \rangle$. Any variable v_k^i occurring in e must occur in e', and by induction hypothesis $v_k^i \in \mathrm{dom}(\sigma_i)$.

   (b) f is $\cdot^n$ with n closed: analogous.

   (c) otherwise there exist a natural number j, an expression e' and a substitution pair θ such that $\mathit{lift}(t', \rho) = \langle e', \theta \rangle$, $\mathit{lift}_{\mathbb{V}_1}(f, \theta) = \langle v_j^1, \sigma \rangle$ and $e = v_j^1(e')$. If v_k^i is a variable occurring in e, then either $v_k^i = v_j^1$ and the result holds by definition of $\mathit{lift}_{\mathbb{V}_1}$ or v_k^i occurs in e'; in the latter case, by induction hypothesis $v_k^i \in \mathrm{dom}(\theta_i)$, and since $\theta \subseteq \sigma$ also $v_k^i \in \mathrm{dom}(\sigma_i)$.

3. $t = t_1 \star t_2$ with $\star \in \{+, -, \times, /\}$: then $e = e_1 \star e_2$ and there is a substitution pair θ such that $\mathit{lift}(t_1, \rho) = \langle e_1, \theta \rangle$ and $\mathit{lift}(t_2, \theta) = \langle e_2, \sigma \rangle$. Suppose v_k^i occurs in e; then it either occurs in e_1 or in e_2. In the first case, by induction hypothesis $v_k^i \in \mathrm{dom}(\theta_i)$, and since $\theta \subseteq \sigma$ also $v_k^i \in \mathrm{dom}(\sigma_i)$. The second case follows directly from the induction hypothesis.

□

3.4 Permutation of lifting

To prove properties of rational, we need to consider situations when the same terms are lifted in different orders. This section proves some results about the corresponding outputs: under quite general hypotheses, they differ only in the names of the variables.

Definition 3.12 Let ρ, σ be substitution pairs for A. We say that σ is obtained from ρ *by a renaming of variables* if there is a pair $\xi = \langle \xi_0, \xi_1 \rangle$ of permutations of $\mathbb{N}$ such that, for $i = 0, 1$, the following conditions hold:

- $\xi_i(k) \neq k \rightarrow v^i_k \in \mathrm{dom}(\rho_i)$;
- for all k, $\sigma_i\left(v^i_{\xi_i(k)}\right) \simeq \rho_i(v^i_k)$ (that is, either they are both undefined or they are both defined and coincide).

We denote this situation by $\sigma = \rho^\xi$ and say that ξ is a renaming of variables for ρ (or simply ξ is a renaming of variables, if the ρ is not relevant). Also, we will abuse notation and write $\mathrm{dom}(\xi_i) = \{k | \xi_i(k) \neq k\}$ for $i = 0, 1$; it follows that $\xi_i(j) = j$ if $j \notin \mathrm{dom}(\xi_i)$. The first condition then becomes simply $\mathrm{dom}(\xi_i) \subseteq \mathrm{dom}(\rho_i)$.

Notice that the second condition totally defines σ, since each ξ_i is a permutation. For this reason, we will also use the notation $\sigma = \rho^\xi$ as a definition of σ.

Another important consequence is that, if $\sigma = \rho^\xi$, then $\mathrm{dom}(\sigma_i) = \mathrm{dom}(\rho_i)$ for $i = 0, 1$.

Proposition 3.13 The relation $R(\rho, \sigma)$ defined as "σ is obtained from ρ by a renaming of variables" is an equivalence relation.

Proof.

- Reflexivity: just take $\xi = \langle (), () \rangle$.
- Symmetry: suppose $\sigma = \rho^\xi$ for some ξ; then, since each ξ_i is a bijection, trivially $\rho = \sigma^{\langle \xi_0^{-1}, \xi_1^{-1} \rangle}$.
- Transitivity: suppose $\sigma = \rho^\xi$ and $\theta = \sigma^{\xi'}$; then $\theta = \rho^{\xi' \circ \xi}$ where $\xi' \circ \xi$ denotes pointwise composition. In fact, for $i = 0, 1$, and for every k, $\theta_i\left(v^i_{\xi' \circ \xi(k)}\right) \simeq \sigma_i\left(v^i_{\xi(k)}\right) \simeq \rho_i(v^i_k)$.

  Finally, suppose that, for some k, $v^i_k \notin \mathrm{dom}(\rho_i)$; then $\xi_i(k) = k$ and, since $\mathrm{dom}(\sigma_i) = \mathrm{dom}(\rho_i)$, also $v^i_k \notin \mathrm{dom}(\sigma_i)$ and hence $\xi'_i \circ \xi_i(k) = \xi'_i(k) = k$. But then $\xi'_i \circ \xi_i(k) \neq k \rightarrow v^i_k \in \mathrm{dom}(\rho_i)$.

□

Definition 3.14 Let ξ be a renaming of variables and $e, e' : E$. We say that e' is obtained from e by ξ, denoted $(e') = e^\xi$, if e' is obtained from e by replacing each occurrence of v^i_k by $v^i_{\xi_i(k)}$, $i = 0, 1$.

Lemma 3.15 Let ρ be a substitution pair for A and ξ be a renaming of variables for ρ. For every $t : A$, if $\mathit{lift}(t, \rho) = \langle e, \sigma \rangle$ then $\mathit{lift}(t, \rho^\xi) = \langle e^\xi, \sigma^\xi \rangle$.

Proof. By induction on $\prec_A$.

1. t is minimal for $\prec_A$:
   (a) $t = \underline{n}$: then $e = n$, $\sigma = \rho$, $\mathit{lift}(t, \rho^\xi) = \langle n, \rho^\xi \rangle$ and the conclusion trivially holds.

(b) otherwise, $e = \mathit{lift}_{\mathbb{V}_0}(t, \rho)$ and we have to distinguish two cases.

Suppose there is an i such that $\rho_0(v^0_i) = t$. Then $e = v^0_i$ and $\sigma = \rho$; but by Definition 3.12 $\rho^\xi_0\left(v^0_{\xi_0(i)}\right) = \rho_0(v^0_i)$, so $\mathit{lift}(t, \rho^\xi) = \langle v^0_{\xi_0(i)}, \rho^\xi\rangle$, and by definition $v^0_{\xi_0(i)} = (v^0_i)^\xi$.

Otherwise, pick k minimal such that $v^0_k \notin \mathrm{dom}(\rho_0)$. Then $e = v^0_k$ and $\sigma = \langle \rho_0 \cup [v^0_k := t], \rho_1\rangle$. But then $\mathit{lift}(t, \rho^\xi) = \langle v^0_k, \sigma'\rangle$ with $\sigma' = \langle \rho^\xi_0 \cup [v^0_k := t], \rho^\xi_1\rangle$: since $\mathrm{dom}(\rho_0) = \mathrm{dom}(\rho^\xi_0)$ (see remark after Definition 3.12), k is also the minimal natural number satisfying $v^0_k \notin \mathrm{dom}(\rho^\xi_0)$; furthermore, there can be no i such that $\rho^\xi_0(v^0_i) = t$ because $\rho^\xi_0(v^0_i) = \rho_0(v^0_{\xi_0^{-1}(i)})$. But $k \notin \mathrm{dom}(\xi_0)$, so $v^0_k = {v^0_k}^\xi$ and $\sigma' = \sigma^\xi$.

2. $t = f(t')$ with $f : [A \to A]$.

(a) f is $-_A$: then there is an expression e' such that $\mathit{lift}(t', \rho) = \langle e', \sigma\rangle$ and $e = -e'$. By induction hypothesis, $\mathit{lift}(t', \rho^\xi) = \langle (e')^\xi, \sigma^\xi\rangle$ and hence $\mathit{lift}(t, \rho^\xi) = \langle e^\xi, \sigma^\xi\rangle$.

(b) f is $\cdot^n$ with n closed: analogous.

(c) otherwise there exist an expression e', an index i and a substitution pair θ such that $\mathit{lift}(t', \rho) = \langle e', \theta\rangle$, $\mathit{lift}_{\mathbb{V}_1}(f, \theta) = \langle v^1_i, \sigma\rangle$ and $e = v^1_i(e')$. By induction hypothesis, $\mathit{lift}(t', \rho^\xi) = \langle (e')^\xi, \theta^\xi\rangle$.

Suppose there is an k such that $\theta_1(v^1_k) = f$. Then $i = k$ and $\sigma = \theta$; but by Definition 3.12 $\theta^\xi_1\left(v^1_{\xi_1(i)}\right) = \theta_1(v^1_i) = f$, so $\mathit{lift}_{\mathbb{V}_1}(f, \theta^\xi) = \langle v^1_{\xi_1(i)}, \theta^\xi\rangle$. Trivially $v^1_{\xi_1(i)} = (v^1_i)^\xi$; since $\theta = \sigma$, $\mathit{lift}(t, \rho^\xi) = \langle v^1_i(e')^\xi, \sigma^\xi\rangle$, which establishes the result.

Otherwise, i is the minimal k such that $v^1_k \notin \mathrm{dom}(\theta_1)$ and $\sigma = \langle \theta_0, \theta_1 \cup [v^1_i := f]\rangle$. But then $\mathit{lift}_{\mathbb{V}_1}(f, \theta^\xi) = \langle v^1_i, \sigma'\rangle$ with $\sigma' = \langle \theta^\xi_0, \theta^\xi_1 \cup [v^1_i := f]\rangle$: since $\mathrm{dom}(\theta_1) = \mathrm{dom}(\theta^\xi_1)$ (second condition in Definition 3.12), i is also the minimal k satisfying $v^1_k \notin \mathrm{dom}(\theta^\xi_1)$; furthermore, there can be no k such that $\rho^\xi_1(v^1_k) = f$, since $\theta^\xi_1(v^1_k) = \theta_1(v^1_{\xi_1^{-1}(k)})$. But then $\sigma' = \sigma^\xi$; since $i = \xi_1(i)$, we also have in this situation that $\mathit{lift}(t, \rho^\xi) = \langle v^1_i(e')^\xi, \sigma^\xi\rangle$.

3. $t = t_1 \star t_2$ with $\star \in \{+, -, \times, /\}$: then there are expressions e_1, e_2 and a substitution pair θ such that $\mathit{lift}(t_1, \rho) = \langle e_1, \theta\rangle$, $\mathit{lift}(t_2, \theta) = \langle e_2, \sigma\rangle$ and $e = e_1 \star e_2$.

By induction hypothesis $\mathit{lift}(t_1, \rho^\xi) = \langle {e_1}^\xi, \theta^\xi\rangle$. But then the induction hypothesis applies again, and $\mathit{lift}(t_2, \theta^\xi) = \langle {e_2}^\xi, \sigma^\xi\rangle$. Hence, $\mathit{lift}(t_1 \star t_2, \rho^\xi) = \langle ({e_1}^\xi) \star ({e_2}^\xi), \sigma^\xi\rangle$ and trivially $({e_1}^\xi) \star ({e_2}^\xi) = e^\xi$.

□

We now prove some lemmas about the order in which terms are lifted.

Lemma 3.16 Let $t : A$, $f : [A \to A]$ and ρ be a substitution pair for A. Suppose $\mathit{lift}_{\mathbb{V}_0}(t, \rho) = \langle v^0_i, \sigma\rangle$ and $\mathit{lift}_{\mathbb{V}_1}(f, \rho) = \langle v^1_j, \theta\rangle$. Then $\mathit{lift}_{\mathbb{V}_1}(f, \sigma) = \langle v^1_j, \langle \sigma_0, \theta_1\rangle\rangle$ and $\mathit{lift}_{\mathbb{V}_0}(t, \theta) = \langle v^0_i, \langle \sigma_0, \theta_1\rangle\rangle$.

Proof. Let τ be an arbitrary substitution pair. From the definition of $\mathit{lift}_{\mathbb{V}_0}$ (Definition 3.1), one sees that the result of $\mathit{lift}_{\mathbb{V}_0}(u, \tau)$ always has τ_1 as the second component of the substitution pair in the output and the remaining values do not depend on τ_1. Therefore, $\sigma = \langle \sigma_0, \rho_1\rangle$.

Similarly, from the definition of $\mathit{lift}_{\mathbb{V}_1}$ (Definition 3.4), one sees that τ_0 is the first component of the substitution pair in the result of $\mathit{lift}_{\mathbb{V}_1}(g, \tau)$, the other values being independent of τ_0. Therefore, $\theta = \langle \rho_0, \theta_1\rangle$.

But then $\mathit{lift}_{\mathbb{V}_1}(f, \sigma) = \mathit{lift}_{\mathbb{V}_1}(f, \langle \sigma_0, \rho_1\rangle) = \langle v^1_j, \langle \sigma_0, \theta_1\rangle$ and $\mathit{lift}_{\mathbb{V}_0}(t, \theta) = \mathit{lift}_{\mathbb{V}_0}(t, \langle \rho_0, \theta_1\rangle) = \langle v^0_i, \langle \sigma_0, \theta_1\rangle\rangle$. □

Lemma 3.17 Let $t_1, t_2 : A$ and ρ be a substitution pair for A. Suppose that

$$\begin{aligned} \mathit{lift}_{\mathbb{V}_0}(t_1,\rho) &= \langle v^0_i, \sigma\rangle \\ \mathit{lift}_{\mathbb{V}_0}(t_2,\sigma) &= \langle v^0_j, \theta\rangle \\ \mathit{lift}_{\mathbb{V}_0}(t_2,\rho) &= \langle v^0_{j'}, \sigma'\rangle \\ \mathit{lift}_{\mathbb{V}_0}(t_1,\sigma') &= \langle v^0_{i'}, \theta'\rangle \end{aligned}$$

Then there is a renaming of variables ξ for θ such that $\xi_1 = ()$, $\mathrm{dom}(\xi_0) \cap \mathrm{dom}(\rho_0) = \emptyset$, $\theta' = \theta^\xi$, $i' = \xi_0(i)$ and $j' = \xi_0(j)$.

Proof. There are four cases to consider.

If t_1 and t_2 are (syntactically) equal, then $\xi = \langle (), ()\rangle$ trivially establishes the thesis: in this case $j' = i$ and $\sigma' = \sigma$, whence $i' = j$ and $\theta' = \theta$; furthermore, since we are in a special case of Lemma 3.10, also $j = i$ and $i' = j'$.

Let us now assume that t_1 and t_2 are different. Suppose first that there is a variable v^0_k such that $\rho_0(v^0_k) = t_1$; then $i = k$ and again $\sigma = \rho$, from which we can deduce $j' = j$ and $\sigma' = \sigma$. But from Lemma 3.2, $\rho \subseteq \sigma$, hence from Lemma 3.10 also $i' = i$ and $\theta' = \theta$; therefore ξ can again be taken to be $\langle (), ()\rangle$.

A symmetric argument proves the case where there is a variable v^0_k such that $\rho_0(v^0_k) = t_2$.

Finally, suppose that for no k either $\rho_0(v^0_k) = t_1$ or $\rho_0(v^0_k) = t_2$. Then i is the minimal natural number satisfying $v^0_i \notin \mathrm{dom}(\rho_0)$ and $\sigma = \langle \rho_0 \cup [v^0_i := t_1], \rho_1\rangle$. By definition of $\cup$, there is still no k such that $\sigma_0(v^0_k) = t_2$, whence j is the least natural number such that $v^0_j \notin \mathrm{dom}(\sigma_0)$ and $\theta = \langle \sigma_0 \cup [v^0_j := t_2], \sigma_1\rangle$.

On the other hand, j' is also the least natural satisfying $v^0_{j'} \notin \mathrm{dom}(\rho_0)$, so $j' = i$ and $\sigma' = \langle \rho_0 \cup [v^0_i := t_2], \rho_1\rangle$. Then $\mathrm{dom}(\sigma'_0) = \mathrm{dom}(\rho_0) \cup \{i\} = \mathrm{dom}(\sigma_0)$, whence necessarily $i' = j$ and $\theta' = \langle \sigma'_0 \cup [v^0_j := t_2], \sigma'_1\rangle$. It then trivially follows that the renaming of variables $\langle (i\ j), ()\rangle$ satisfies all the desired conditions. □

Lemma 3.18 Let $f_1, f_2 : [A \to A]$ and ρ be a substitution pair for A. Suppose that

$$\begin{aligned} \mathit{lift}_{\mathbb{V}_1}(f_1,\rho) &= \langle v^1_i, \sigma\rangle \\ \mathit{lift}_{\mathbb{V}_1}(f_2,\sigma) &= \langle v^1_j, \theta\rangle \\ \mathit{lift}_{\mathbb{V}_1}(f_2,\rho) &= \langle v^1_{j'}, \sigma'\rangle \\ \mathit{lift}_{\mathbb{V}_1}(f_1,\sigma') &= \langle v^1_{i'}, \theta'\rangle \end{aligned}$$

Then there is a renaming of variables ξ for θ such that $\xi_0 = ()$, $\mathrm{dom}(\xi_1) \cap \mathrm{dom}(\rho_1) = \emptyset$, $\theta' = \theta^\xi$, $i' = \xi_1(i)$ and $j' = \xi_1(j)$.

Proof. The proof is exactly analogous to that of Lemma 3.17, interchanging the indices 0 and 1 of the variables and substitutions. □

Lemma 3.19 Let $t_1, t_2 : A$, $e_1, e'_1, e_2, e'_2 : E$ and $\rho, \sigma, \sigma', \theta, \theta'$ be substitution pairs for A satisfying the following relations.

$$\begin{aligned} \mathit{lift}(t_1,\rho) &= \langle e_1, \sigma\rangle \\ \mathit{lift}_{\mathbb{V}_0}(t_2,\sigma) &= \langle e_2, \theta\rangle \\ \mathit{lift}_{\mathbb{V}_0}(t_2,\rho) &= \langle e'_2, \sigma'\rangle \\ \mathit{lift}(t_1,\sigma') &= \langle e'_1, \theta'\rangle \end{aligned}$$

Then there is a renaming of variables ξ for θ such that:

(i) $\xi_1 = ()$ and $\mathrm{dom}(\xi_0) \cap \mathrm{dom}(\rho_0) = \emptyset$;

(ii) $\theta' = \theta^{\xi}$ and $e'_i = {e_i}^{\xi}$ for $i = 1, 2$.

Proof. By induction on t_1 according to $\prec_A$.

1. t_1 is minimal for $\prec_A$.

   (a) $t_1 = \underline{n}$: then $e_1 = n$, $\sigma = \rho$ whence trivially $e'_2 = e_2$, $\sigma' = \theta$ and also $e'_1 = e_1$ and $\theta' = \theta$; thus $\xi = \langle (), () \rangle$ trivially satisfies (i) and (ii).

   (b) otherwise $\mathit{lift}(t_1, \rho) = \mathit{lift}_{\mathbb{V}_0}(t_1, \rho)$ and Lemma 3.17 establishes the result.

2. $t_1 = f(t)$ with $f : [A \to A]$.

   (a) f is $-_A$: then $e_1 = -e$ where $\langle e, \sigma \rangle = \mathit{lift}(t, \rho)$; similarly $e'_1 = -e'$ where $\langle e', \theta' \rangle = \mathit{lift}(t, \sigma')$. By induction hypothesis there is a renaming of variables ξ for θ such that $\xi_1 = ()$, $\mathrm{dom}(\xi_0) \cap \mathrm{dom}(\rho_0) = \emptyset$, $\theta' = \theta^{\xi}$, $e' = e^{\xi}$ and $e'_2 = {e_2}^{\xi}$. The only thing left to show is that $e'_1 = {e_1}^{\xi}$; but this is trivial, since $e_1 = e$ and $e'_1 = -e'$. Therefore ξ is the desired renaming of variables.

   (b) f is $\cdot^n$ with n is closed: analogous.

   (c) otherwise $e_1 = v_i^1(e)$ with $\mathit{lift}(t, \rho) = \langle e, \tau \rangle$ and $\mathit{lift}_{\mathbb{V}_1}(f, \tau) = \langle v_i^1, \sigma \rangle$; also $e'_1 = v_j^1(e')$ with $\mathit{lift}(t, \sigma') = \langle e', \tau' \rangle$ and $\mathit{lift}_{\mathbb{V}_1}(f, \tau') = \langle v_j^1, \theta' \rangle$.

   By Lemma 3.16, $\theta = \langle \theta_0, \sigma_1 \rangle$ and $\mathit{lift}_{\mathbb{V}_0}(t_2, \tau) = \langle e_2, \langle \theta_0, \tau_1 \rangle \rangle$. By induction hypothesis, there is a renaming of variables ξ for $\langle \theta_0, \tau_1 \rangle$ such that $\xi_1 = ()$, $\mathrm{dom}(\xi_0) \cap \mathrm{dom}(\rho_0) = \emptyset$, $\tau' = \langle \theta_0, \tau_1 \rangle^{\xi}$, $e' = e^{\xi}$ and $e'_2 = {e_2}^{\xi}$.

   It remains to show that $e'_1 = {e_1}^{\xi}$; but $\tau' = \langle \theta_0, \tau_1 \rangle^{\xi}$ and $\xi_1 = ()$ imply $\tau'_1 = \tau_1$. Similar considerations as made in the proof of Lemma 3.16 make it clear that $\theta'_1 = \tau'_1$ and $j = i$. Hence the thesis follows.

3. $t_1 = u \star v$ with $\star \in \{+, -, \times, /\}$: then there are expressions e_u and e_v and a substitution pair τ such that $\mathit{lift}(u, \rho) = \langle e_u, \tau \rangle$, $\mathit{lift}(v, \tau) = \langle e_v, \sigma \rangle$ and $e = e_u \star e_v$. Also, there are expressions e'_u and e'_v and a substitution pair τ' such that $\mathit{lift}(u, \sigma') = \langle e'_u, \tau' \rangle$, $\mathit{lift}(v, \tau') = \langle e'_v, \theta' \rangle$ and $e' = e'_u \star e'_v$.

   Consider now $\mathit{lift}_{\mathbb{V}_0}(t_2, \tau) = \langle e_2^*, \tau^* \rangle$. By induction hypothesis, there is a renaming of variables ξ for τ^* satisfying (i) such that $e'_2 = {e_2^*}^{\xi}$, $e'_u = {e_u}^{\xi}$ and $\tau' = {\tau^*}^{\xi}$.

   Let now $\mathit{lift}(v, \tau^*) = \langle e_v^*, \theta^* \rangle$. Induction hypothesis now implies that there is a renaming of variables ξ' for θ such that $\xi'_1 = ()$, $\mathrm{dom}(\xi'_0) \cap \mathrm{dom}(\tau_0) = \emptyset$, $e_2^* = {e_2}^{\xi'}$, $e_v^* = {e_v}^{\xi'}$ and $\theta^* = \theta^{\xi'}$ (see Figure 1).

$$\begin{tikzcd}
 & \rho \arrow[dl, "u"'] \arrow[dr, "t_2"] & \\
\tau \arrow[d, "v"'] \arrow[dr, "t_2"] & & \sigma' \arrow[d, "u"'] \\
\sigma \arrow[d, "t_2"'] & \tau^* \arrow[r, dotted, "\xi"] \arrow[d, "v"'] & \tau' \arrow[d, "v"'] \\
\theta \arrow[r, dotted, "\xi'"] & \theta^* \arrow[r, dotted, "\xi"] & \theta'
\end{tikzcd}$$

Figure 1: Induction step on the proof of Lemma 3.19. An arrow from ρ to ρ' with label t means that ρ' is obtained by $\mathit{lift}(t, \rho)$.

We now prove that $\xi \circ \xi'$ is the desired renaming of variables.

- Trivially, $\xi_1 \circ \xi'_1 = ()$; since $\rho \subseteq \tau$, if $v^0_k \in \mathrm{dom}(\rho_0)$ then $\xi_0(k) = k$ and $\xi'_0(k) = k$, hence $\mathrm{dom}(\xi_0 \circ \xi'_0) \cap \mathrm{dom}(\rho_0) = \emptyset$.
- By hypothesis, $e'_2 = {e^*_2}^\xi$ and $e^*_2 = {e_2}^{\xi'}$, whence $e'_2 = {e_2}^{\xi \circ \xi'}$.
- By Lemma 3.15, $\mathit{lift}(v, \tau') = \mathit{lift}(v, (\tau^*)^\xi) = \langle (e^*_v)^\xi, (\theta^*)^\xi \rangle$, which is $\langle ({e_v}^{\xi'})^\xi, (\theta^{\xi'})^\xi \rangle$. In other words, $\mathit{lift}(v, \tau') = \langle {e_v}^{\xi \circ \xi'}, \theta^{\xi \circ \xi'} \rangle$.

  Also, $\mathrm{dom}(\xi'_0) \cap \mathrm{dom}(\tau_0) = \emptyset$, hence no variable occurring in e_u is in the domain of ξ_0 by Lemma 3.11. Therefore, $e'_u = {e_u}^\xi = ({e_u}^{\xi'})^\xi = {e_u}^{\xi \circ \xi'}$, whence $e' = e^{\xi \circ \xi'}$.

Thus $\xi \circ \xi'$ is the desired renaming of variables.

□

Lemma 3.20 Let $t : A$, $f : [A \to A]$, $e, e' : E$, $i, i' : \mathbb{N}$ and $\rho, \sigma, \sigma', \theta, \theta'$ be substitution pairs for A satisfying the following relations.

$$\begin{aligned} \mathit{lift}(t, \rho) &= \langle e, \sigma \rangle \\ \mathit{lift}_{\mathbb{V}_1}(f, \sigma) &= \langle v^1_i, \theta \rangle \\ \mathit{lift}_{\mathbb{V}_1}(f, \rho) &= \langle v^1_{i'}, \sigma' \rangle \\ \mathit{lift}(t, \sigma') &= \langle e', \theta' \rangle \end{aligned}$$

Then there is a renaming of variables ξ for θ such that:

(i) $\xi_0 = ()$ and $\mathrm{dom}(\xi_1) \cap \mathrm{dom}(\rho_1) = \emptyset$;

(ii) $\theta' = \theta^\xi$, $e' = e^\xi$ and $i' = \xi_1(i)$.

Proof. By induction on t according to $\prec_A$.

1. t is minimal for $\prec_A$.

   (a) $t = \underline{n}$: then $e = n$, $\sigma = \rho$ whence trivially $i' = i$, $\sigma' = \theta$ and also $e' = e$ and $\theta' = \theta$; thus $\xi = \langle (), () \rangle$ trivially satisfies (i) and (ii).

   (b) otherwise $\mathit{lift}(t, \rho) = \mathit{lift}_{\mathbb{V}_0}(t, \rho)$. By Lemma 3.16, $\langle (), () \rangle$ also satisfies both (i) and (ii).

2. $t = g(t_0)$ with $g : [A \to A]$.

   (a) g is $-_A$: again analogous to the corresponding case in the proof of Lemma 3.19.

   (b) g is $\cdot^n$ with n is closed: analogous.

   (c) otherwise $e = v^1_j(e_0)$ with $\mathit{lift}(t_0, \rho) = \langle e_0, \tau \rangle$ and $\mathit{lift}_{\mathbb{V}_1}(g, \tau) = \langle v^1_j, \sigma \rangle$; also $e' = v^1_{j'}(e'_0)$ with $\mathit{lift}(t, \sigma') = \langle e'_0, \tau' \rangle$ and $\mathit{lift}_{\mathbb{V}_1}(g, \tau') = \langle v^1_{j'}, \theta' \rangle$.

3. $t_1 = u \star v$ with $\star \in \{+, -, \times, /\}$: then there are expressions e_u and e_v and a substitution pair τ such that $\mathit{lift}(u, \rho) = \langle e_u, \tau \rangle$, $\mathit{lift}(v, \tau) = \langle e_v, \sigma \rangle$ and $e = e_u \star e_v$. Also, there are expressions e'_u and e'_v and a substitution pair τ' such that $\mathit{lift}(u, \sigma') = \langle e'_u, \tau' \rangle$, $\mathit{lift}(v, \tau') = \langle e'_v, \theta' \rangle$ and $e' = e'_u \star e'_v$.

   If we define $\mathit{lift}_{\mathbb{V}_1}(f, \tau) = \langle v^1_{i^*}, \tau^* \rangle$ and $\mathit{lift}_{\mathbb{V}_1}(g, \tau^*) = \langle v^1_{j^*}, \theta^* \rangle$, we can draw the picture on Figure 2. Again, by induction hypothesis, there is a renaming of variables ξ for τ^* satisfying (i) such that $i' = \xi_1(i^*)$, $e'_0 = {e_0}^\xi$ and $\tau' = {\tau^*}^\xi$. By Lemma 3.18, there is a renaming of variables ξ' for θ such that $\xi'_0 = ()$, $\mathrm{dom}(\xi'_1) \cap \mathrm{dom}(\tau_1) = \emptyset$, $i^* = \xi'_1(i)$, $j^* = \xi'_1(j)$ and $\theta^* = \theta^{\xi'}$.

   Once again, $\xi \circ \xi'$ is the desired renaming of variables.

   - Trivially, $\xi_0 \circ \xi'_0 = ()$; since $\rho \subseteq \tau$, if $v^1_k \in \mathrm{dom}(\rho_1)$ then $\xi_1(k) = k$ and $\xi'_1(k) = k$, hence $\mathrm{dom}(\xi_1 \circ \xi'_1) \cap \mathrm{dom}(\rho_1) = \emptyset$.

$$\begin{tikzcd}
& \rho \arrow[dl, "t_0"'] \arrow[dr, "f"] & \\
\tau \arrow[d, "g"'] \arrow[dr, "f"] & & \sigma' \arrow[d, "t_0"] \\
\sigma \arrow[d, "f"'] & \tau^* \arrow[r, dotted, "\xi"] \arrow[d, "g"'] & \tau' \arrow[d, "g"'] \\
\theta \arrow[r, dotted, "\xi'"] & \theta^* \arrow[r, dotted, "\xi"] & \theta'
\end{tikzcd}$$

Figure 2: Last case of the proof of Lemma 3.20. An arrow from ρ to ρ' with label t means that ρ' is obtained by either $\mathit{lift}(t, \rho)$ or $\mathit{lift}_{\mathbb{V}_1}(t, \rho)$.

- By hypothesis, $i' = \xi_1(i^*)$ and $i^* = \xi'(i)$, whence $i' = \xi \circ \xi'(i)$.
- $\mathit{lift}(g(t_0), \tau^*) = \langle v^1_{j^*}(e_0), \theta^* \rangle$: since $\tau \subseteq \tau^*$ by Lemma 3.5, $\mathit{lift}(t_0, \tau^*) = \langle e_0, \tau^* \rangle$ due to Lemma 3.10; the rest follows by definition of $\mathit{lift}_{\mathbb{V}_1}(g, \tau^*)$. Similar considerations show that $\mathit{lift}(g(t_0), \tau') = \langle v^1_{j'}(e'_0), \theta' \rangle$.

  By Lemma 3.15, $\mathit{lift}(g(t_0), \tau') = \mathit{lift}(g(e_0), \tau^{*\xi}) = \langle v^1_{j^*}(e_0)^{\xi}, \theta^{*\xi} \rangle$; hence $\theta' = \theta^{*\xi}$ and $v^1_{j'}(e'_0) = v^1_{j^*}(e_0)^{\xi}$.

  From $\theta' = \theta^{*\xi}$ and $\theta^* = \theta^{\xi'}$ we can deduce that $\theta' = \theta^{\xi \circ \xi'}$.

  Finally we show that $v^1_{j'}(e'_0) = v^1_j(e_0)^{\xi\circ\xi'}$. Obviously, $v^1_j(e_0)^{\xi\circ\xi'} = v^1_{\xi\circ\xi'(j)}({e_0}^{\xi\circ\xi'})$. From $v^1_{j'}(e'_0) = v^1_{j^*}(e_0)^{\xi}$ we get first that $j' = \xi_1(j^*)$, and since $j^* = \xi'_1(j)$ we conclude that $\xi_1 \circ \xi'_1(j) = j'$. Also $e'_0 = {e_0}^{\xi}$; since $\mathrm{dom}(\xi'_0) \cap \mathrm{dom}(\tau_0) = \emptyset$, no variable occurring in e_0 is in the domain of ξ'_0 by Lemma 3.11. Therefore, $e'_0 = {e_0}^{\xi} = ({e_0}^{\xi'})^{\xi} = {e_0}^{\xi\circ\xi'}$.

Thus $\xi \circ \xi'$ is the desired renaming of variables.

□

Lemma 3.21 Let $t_1, t_2 : A$, $e_1, e'_1, e_2, e'_2 : E$ and $\rho, \sigma, \sigma', \theta, \theta'$ be substitution pairs for A satisfying the following relations.

$$\begin{aligned}
\mathit{lift}(t_1, \rho) &= \langle e_1, \sigma \rangle \\
\mathit{lift}(t_2, \sigma) &= \langle e_2, \theta \rangle \\
\mathit{lift}(t_2, \rho) &= \langle e'_2, \sigma' \rangle \\
\mathit{lift}(t_1, \sigma') &= \langle e'_1, \theta' \rangle
\end{aligned}$$

Then there is a renaming of variables ξ for θ such that:

(i) $\mathrm{dom}(\xi_i) \cap \mathrm{dom}(\rho_i) = \emptyset$ for $i = 1, 2$;

(ii) $\theta' = \theta^{\xi}$ and $e'_i = {e_i}^{\xi}$ for $i = 1, 2$.

Proof. By induction on t_1 with respect to $\prec_A$; most cases can be dealt with as in the proof of Lemma 3.19. First, notice that the only steps where use was made of the fact that e_2 was obtained from t_2 by $\mathit{lift}_{\mathbb{V}_0}$ were the cases where t_1 was minimal for $\prec_A$ and not of the form $\underline{n}$ or $t_1 = f(t)$. In all other cases, proving that $\mathrm{dom}(\xi_0) \cap \mathrm{dom}(\rho_0) = \emptyset$ made use only of the induction hypothesis, so that replacing 0 by 1 in that subproof yields a valid proof of $\mathrm{dom}(\xi_1) \cap \mathrm{dom}(\rho_1) = \emptyset$ from the induction hypothesis. Therefore, we only need to consider those two cases.

If t_1 is minimal for $\prec_A$ and not of the form $\underline{n}$, then $\mathit{lift}(t_1,\rho) = \mathit{lift}_{\mathbb{V}_0}(t_1,\rho)$ and $\mathit{lift}(t_1,\sigma') = \mathit{lift}_{\mathbb{V}_0}(t_1,\sigma')$. Lemma 3.19 then allows us to conclude that there is a renaming of variables ξ for θ' such that $\xi_1 = ()$, $\mathrm{dom}(\xi_0) \cap \mathrm{dom}(\rho_0) = \emptyset$ and $\theta = \theta'^{\xi}$ and $e_i = e_i'^{\xi}$ for $i = 1, 2$. Then ξ^{-1} satisfies our requirements: since ξ_0 is a permutation, $\mathrm{dom}(\xi_0^{-1}) = \mathrm{dom}(\xi_0)$ and therefore $\mathrm{dom}(\xi_0^{-1}) \cap \mathrm{dom}(\rho_0) = \emptyset$; $\mathrm{dom}(()) = \emptyset$, hence $\mathrm{dom}(\xi_0^{-1}) \cap \mathrm{dom}(\rho_0) = \emptyset$; $\theta' = \theta^{\xi^{-1}}$ follows from the second case in the proof of Lemma 3.13; and $e_i' = {e_i}^{\xi^{-1}}$ follows from the definition of inverse.

If $t_1 = f(t)$, then there are expressions e, e', natural numbers i, i' and substitution pairs τ, τ' such that $\mathit{lift}(t,\rho) = \langle e, \tau\rangle$, $\mathit{lift}_{\mathbb{V}_1}(f,\tau) = \langle v_i^1, \sigma\rangle$, $e_1 = v_i^1(e)$, $\mathit{lift}(t,\sigma') = \langle e', \tau'\rangle$, $\mathit{lift}_{\mathbb{V}_1}(f,\tau') = \langle v_{i'}^1, \theta\rangle$ and $e_1' = v_{i'}^1(e')$.

We once again let $\mathit{lift}(t_2,\tau) = \langle e_2^*, \tau^*\rangle$ and $\mathit{lift}_{\mathbb{V}_1}(f,\tau^*) = \langle v_{i^*}^1, \theta^*\rangle$ (see Figure 3). By induction hypothesis there is a renaming of variables ξ for τ^* such that (i) holds, $\tau' = \tau^{*\xi}$, $e' = e^{\xi}$ and $e_2' = {e_2}^{\xi}$. By Lemma 3.20 there is a renaming of variables ξ' for θ such that $\xi_0' = ()$, $\mathrm{dom}(\xi_1') \cap \mathrm{dom}(\tau_1) = \emptyset$, $\theta^* = \theta^{\xi'}$, $e_2^* = {e_2}^{\xi'}$ and $i^* = \xi_1'(i)$.

$$\begin{tikzcd}
 & \rho \arrow[dl, "t"'] \arrow[dr, "t_2"] & \\
\tau \arrow[d, "f"'] \arrow[dr, "t_2"] & & \sigma' \arrow[d, "t"] \\
\sigma \arrow[d, "t_2"'] & \tau^* \arrow[r, dotted, "\xi"] \arrow[d, "f"'] & \tau' \arrow[d, "f"'] \\
\theta \arrow[r, dotted, "\xi'"] & \theta^* \arrow[r, dotted, "\xi"] & \theta'
\end{tikzcd}$$

Figure 3: Last case of the proof of Lemma 3.21. An arrow from ρ to ρ' with label t means that ρ' is obtained by either $\mathit{lift}(t,\rho)$ or $\mathit{lift}_{\mathbb{V}_1}(t,\rho)$.

In a similar way to the proof of the last case of Lemma 3.20, we can conclude that $\theta' = \theta^{\xi\circ\xi'}$, $i' = \xi_1(i^*)$ and $e' = e^{\xi\circ\xi'}$. Then trivially $v_{i'}^1(e') = v_i^1(e)^{\xi\circ\xi'}$. Finally, if $v_k^i \in \mathrm{dom}(\rho_i)$, then $v_k^i \in \mathrm{dom}(\tau_i)$, hence $\xi_i'(k) = k$, $\xi_i \circ \xi_i'(k) = \xi(k) = k$ and $\mathrm{dom}(\xi_i) \cap \mathrm{dom}(\rho_i) = \emptyset$. □

Lemma 3.22 Let $t_1, t_2, t_3 : A$, $e_1, e_2, e_2', e_3, e_3' : E$ and $\rho, \sigma, \sigma', \theta, \theta'$ be substitution pairs for A satisfying the following relations.

$$\begin{array}{rcl}
\mathit{lift}(t_2,\emptyset) & = & \langle e_2, \sigma\rangle \\
\mathit{lift}(t_3,\sigma) & = & \langle e_3, \theta\rangle \\
\mathit{lift}(t_1,\emptyset) & = & \langle e_1, \rho\rangle \\
\mathit{lift}(t_2,\rho) & = & \langle e_2', \sigma'\rangle \\
\mathit{lift}(t_3,\sigma') & = & \langle e_3', \theta'\rangle
\end{array}$$

Then there exist a substitution pair τ and a renaming of variables ξ for τ such that:

(i) $\theta \subseteq \tau$;

(ii) $\theta' = \tau^{\xi}$ and $e_i' = {e_i}^{\xi}$ for $i = 2, 3$.

Proof. Define $\mathit{lift}(t_1,\sigma) = \langle e_1^*, \rho^*\rangle$. By Lemma 3.21, there is a renaming of variables ξ for τ^* such that $\sigma' = \rho^{*\xi}$, $e_1 = e_1^{*\xi}$ and $e_2' = {e_2}^{\xi}$.

Define $\mathit{lift}(t_3,\rho^*) = \langle e_3^*, \theta^*\rangle$. Then, by Lemma 3.15, $e_3' = e_3^{*\xi}$ and $\theta' = \theta^{*\xi}$.

Now take $\mathit{lift}(t_1,\theta) = \langle e_1', \tau\rangle$. By Lemma 3.21 there is a renaming of variables ξ' for τ such that also $e_3^* = {e_3}^{\xi'}$ and $\theta^* = \tau^{\xi'}$.

It then follows that $\xi \circ \xi'$ is the desired renaming of variables.

The situation is graphically depicted in Figure 4. □

$$\begin{tikzcd}
 & \emptyset \arrow[dl, "t_2"'] \arrow[dr, "t_1"] & \\
\sigma \arrow[d, "t_3"'] \arrow[dr, "t_1"] & & \rho \arrow[d, "t_2"'] \\
\theta \arrow[d, "t_1"'] & \rho^* \arrow[r, dotted, "\xi"] \arrow[d, "t_3"'] & \sigma' \arrow[d, "t_3"'] \\
\tau \arrow[r, dotted, "\xi'"] & \theta^* \arrow[r, dotted, "\xi"] & \theta'
\end{tikzcd}$$

Figure 4: Proof of Lemma 3.22. An arrow from ρ to ρ' with label t means that ρ' is obtained by $\mathit{lift}(t, \rho)$.

4 Completeness of rational: rings

We now move to the Coq portion of the tactic. We identify a subset of the set of expressions which we call *normal forms*. Then we define a normalization function N that assigns to any expression e an expression $\mathcal{N}(e)$ in normal form. In this section we prove the fundamental properties of this function.

In this first stage we will forget about division and work only with the subset of expressions interpretable in a ring. Section 6 discusses how these definitions can be generalized for fields and how the results we show here can be transposed to the general case.

4.1 Normal forms

The intuition for the normal forms is as follows. A normal form is a polynomial where all terms have been multiplied, so that it is written as a sum of products of atomic terms (integers, variables of arity 0 or variables of arity 1 applied to a normal form). To guarantee uniqueness of the normal form we further require that these terms be ordered.

We begin by defining monomials and polynomials. These can be seen in a precise way as lists of expressions; hence we can identify the subset of monomials and polynomials whose lists are ordered. These will be our normal forms.

Definition 4.1 The sets of *monomials* and *polynomials* are inductively defined by the following grammar:

$$\begin{array}{rcl} M' & ::= & \mathbb{Z} \mid \mathbb{V}_0 \times M' \mid \mathbb{V}_1(P') \times M' \\ P' & ::= & \mathbb{Z} \mid M' + P' \end{array}$$

Notice that $M' \subseteq E$ and $P' \subseteq E$.

Definition 4.2 For every $m : M'$ we define:

1. the *list of variables* of m, $|m|$;
2. the *coefficient* of m, $\|m\|$.

$$\begin{array}{rcl} |\cdot| : M' & \to & \mathrm{list}(E) \\ i & \mapsto & [] \\ v_i^0 \times m & \mapsto & v_i^0 :: m \\ v_i^1(p') \times m & \mapsto & v_i^1(p') :: m \end{array} \qquad \begin{array}{rcl} \|\cdot\| : M' & \to & \mathbb{Z} \\ i & \mapsto & i \\ v_i^0 \times m & \mapsto & \|m\| \\ v_i^1(p') \times m & \mapsto & \|m\| \end{array}$$

Definition 4.3 For every $p : P'$ we define the *list of monomials* of p as follows:

$$\begin{array}{rcl} |\cdot| : P' & \to & \mathrm{list}(\mathrm{list}(E)) \\ i & \mapsto & [] \\ m + p & \mapsto & |m| :: |p| \end{array}$$

Definition 4.4 We define the following mutually recursive predicates over M' and P'.

(i) $\mathrm{ord}_{M'}(m)$ holds if $|m|$ is an ordered list (with the ordering from Definition 2.17).

(ii) $\mathrm{ord}_{P'}(p)$ holds if $|p|$ is ordered (using the lexicographic ordering for each element of $|p|$) and $|p|$ does not contain repetitions.

(iii) $\mathrm{wf}_{M'}$ is defined recursively as follows:

- $\mathrm{wf}_{M'}(i)$ holds for $i \neq 0$;
- $\mathrm{wf}_{M'}(v_i^0 \times m) \iff \mathrm{wf}_{M'}(m)$;
- $\mathrm{wf}_{M'}(v_i^1(p) \times m) \iff (\mathrm{wf}_{M'}(m) \wedge \mathrm{nf}_{P'}(p))$.

(iv) $\mathrm{nf}_{M'}(m)$ holds if either $m = 0$ or $\mathrm{wf}_{M'}(m) \wedge \mathrm{ord}_{M'}(m)$ holds.

(v) $\mathrm{wf}_{P'}$ is defined recursively as follows:

- $\mathrm{wf}_{P'}(i)$ holds for $i \in \mathbb{Z}$;
- $\mathrm{wf}_{P'}(m + p) \iff (\mathrm{wf}_{P'}(p) \wedge \mathrm{nf}_{M'}(m))$.

(vi) $\mathrm{nf}_{P'}(p)$ holds iff $\mathrm{wf}_{P'}(p) \wedge \mathrm{ord}_{P'}(p)$ holds.

Definition 4.5 The set M of monomials *in normal form* is defined as

$$M = \{m : M' \mid \mathrm{nf}_{M'}(m)\}.$$

The set P of polynomials *in normal form*, or simply of normal forms, is defined as

$$P = \{p : P' \mid \mathrm{nf}_{P'}(p)\}.$$

We will use the definitions of $\|m\|$, $|m|$ and $|p|$ above also for monomials and polynomials in normal form.

Definition 4.6 Let $m : M$ and $p : P$. The *coefficient* of m in p, denoted by $\|p\|_m$, is recursively defined as follows.

$$\begin{array}{rcl} \|\cdot\|_{\_} : P \times M & \to & \mathbb{Z} \\ i, j & \mapsto & i \\ i, m & \mapsto & 0 \\ m' + p, m & \mapsto & \left\{ \begin{array}{ll} \|m'\| & \text{if } |m'| = |m| \\ \|p\|_m & \text{else} \end{array} \right. \end{array}$$

The first clause in this definition may look somewhat strange; the idea is that we only look at $|m|$ to define $\|p\|_m$, and thus any integer should correspond to the independent term of p.

The reason for introducing the operations $|\cdot|$ and $\|\cdot\|$ is that they totally characterize normal forms.

Lemma 4.7 Let $m, m' : M$. Then $m = m' \iff \|m\| = \|m'\| \wedge |m| = |m'|$.

Proof. Straightforward. The direct implication is immediate, since both $|\cdot|$ and $\|\cdot\|$ are functions. For the converse, assume that $|m| = |m'|$. Then m and m' share the same variables (counting repetitions); since they are ordered, these must appear in exactly the same order. If we also assume that $\|m\| = \|m'\|$, then their integer coefficient is also the same, whence $m = m'$. □

Lemma 4.8 Let $p, q : P$. Then $p = q \iff \forall m : M. \|m\|_p = \|m\|_q$.

Proof. The direct implication is again immediate, since $\|\cdot\|_{\_}$ is a function. For the converse, assume that $\|m\|_p = \|m\|_q$ for all m; then every monomial occurring in p also occurs in q with the same coefficient, and reciprocally. But $|p|$ and $|q|$ are both ordered, hence $p = q$. □

4.2 The normalization function

The normalization function is not defined directly, but by means of a number of auxiliary functions. This makes it easier to state and prove results about it.

Definition 4.9 $\cdot_{\mathrm{M}\mathbb{Z}}$ is defined by:

$$\begin{array}{rcl} \cdot_{\mathrm{M}\mathbb{Z}} : M \times \mathbb{Z} & \to & M \\ m, 0 & \mapsto & 0 \\ i, j & \mapsto & i \times j \\ x \times m, j & \mapsto & x \times (m \cdot_{\mathrm{M}\mathbb{Z}} j) \end{array}$$

Proposition 4.10 $\cdot_{\mathrm{M}\mathbb{Z}}$ satisfies the following properties:

(i) $\|m \cdot_{\mathrm{M}\mathbb{Z}} i\| = \|m\| \times i$;

(ii) $|m \cdot_{\mathrm{M}\mathbb{Z}} 0| = []$;

(iii) $|m \cdot_{\mathrm{M}\mathbb{Z}} i| = |m|$ for $i \neq 0$;

(iv) $\cdot_{\mathrm{M}\mathbb{Z}}$ is well defined, i.e. its output is in M;

(v) if $m \rrbracket_\rho t$, then $m \cdot_{\mathrm{M}\mathbb{Z}} i \rrbracket_\rho t \times i$.

Proof. The first two properties follow directly from the definition; for the third, just notice that, if $i \neq 0$, then $\times_{M\mathbb{Z}}$ translates to the identity on the list of variables of m. From these three properties, the fourth then follows: if $i = 0$, then this is a consequence of $0 : M$; else only the coefficient of m changes, hence $\mathrm{nf}_{M'}(m \cdot_{\mathrm{M}\mathbb{Z}} i)$ still holds. The last property is proved by straightforward induction (Coq checked). □

Definition 4.11 $\cdot_{\mathrm{M}\mathbb{V}}$ is defined by:

$$\begin{array}{rcl} \cdot_{\mathrm{M}\mathbb{V}} : M \times (\mathbb{V}_0 \cup \mathbb{V}_1(P)) & \to & M \\ i, y & \mapsto & (y \times 1) \cdot_{\mathrm{M}\mathbb{Z}} i \\ x \times m, y & \mapsto & \left\{ \begin{array}{ll} x \times (m \cdot_{\mathrm{M}\mathbb{V}} y) & x <_E y \\ y \times x \times m & \text{otherwise} \end{array} \right. \end{array}$$

Proposition 4.12 $\cdot_{\mathrm{M}\mathbb{V}}$ satisfies the following properties:

(i) $\|m \cdot_{\mathrm{M}\mathbb{V}} x\| = \|m\|$;

(ii) if $m \neq 0$, then $|m \cdot_{\mathrm{M}\mathbb{V}} x|$ is the sorted list obtained from m and x;

(iii) $\cdot_{\mathrm{M}\mathbb{V}}$ is well defined;

(iv) if $m \rrbracket_\rho t$ and $x \rrbracket_\rho t'$, then $m \cdot_{\mathrm{M}\mathbb{V}} x \rrbracket_\rho t \times t'$.

Proof. If $m = 0$ these properties follow from Proposition 4.10, so assume $m \neq 0$. The first property follows directly from the definition; for the second, just notice that $\cdot_{\mathrm{M}\mathbb{V}}$ translates to the algorithm of straight insertion on lists. From these two properties, the third then follows: the elements of $|m|$ are not changed by $\cdot_{\mathrm{M}\mathbb{V}}$ and x is either v_i^0 or $v_i^1(p)$ with $p : P$, hence $m \cdot_{\mathrm{M}\mathbb{V}} x$ satisfies $\mathrm{wf}_{M'}$. Also the correctness of straight insertion guarantees that $|m \cdot_{\mathrm{M}\mathbb{V}} x|$ is sorted if m is. The last property is again proved by straightforward induction using Proposition 4.10 (Coq checked). □

Definition 4.13 $\cdot_{\mathrm{MM}}$ is defined by:

$$\begin{array}{rcl} \cdot_{\mathrm{MM}} : M \times M & \to & M \\ i, m & \mapsto & m \cdot_{\mathrm{M}\mathbb{Z}} i \\ x \times m, m' & \mapsto & (m \cdot_{\mathrm{MM}} m') \cdot_{\mathrm{M}\mathbb{V}} x \end{array}$$

Proposition 4.14 $\cdot_{\mathrm{MM}}$ satisfies the following properties:

(i) $\|m \cdot_{\mathrm{MM}} m'\| = \|m\| \times \|m'\|$;

(ii) if $m, m' \neq 0$, then $|m \cdot_{\mathrm{MM}} m'|$ is the sorted list obtained by merging $|m|$ with $|m'|$;

(iii) $\cdot_{\mathrm{MM}}$ is well defined;

(iv) if $m \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$, then $m \cdot_{\mathrm{MM}} m' \rrbracket_\rho t \times t'$.

Proof. The first property again follows directly from the definition of $\cdot_{\mathrm{MM}}$ and Propositions 4.10 and 4.12. The second holds because $\cdot_{\mathrm{MM}}$ simply implements straight insertion sort on the list obtained by appending $|m|$ to $|m'|$. From these two the third property follows, and the last one is again proved by straightforward induction using Propositions 4.10 and 4.12 (Coq checked). □

The next function is of a different nature: it takes two monomials m and m' that coincide as lists (that is, $|m| = |m'|$) and returns the monomial obtained by adding them. Obviously this is only well defined under the assumption that $|m| = |m'|$.

Definition 4.15 Let Δ_M denote the subset of $M \times M$ defined by

$$\Delta_M = \{\langle m, m' \rangle \in M \times M \mid |m| = |m'|\}.$$

$+_{\mathrm{MM}}$ is defined as follows.

$$\begin{array}{rcl} +_{\mathrm{MM}} : \Delta_M & \to & M \\ i, j & \mapsto & i + j \\ x \times m, x \times m' & \mapsto & (m +_{\mathrm{MM}} m') \cdot_{\mathrm{M}\mathbb{V}} x \end{array}$$

Notice that this definition covers all cases because of the structure of Δ_M.

Proposition 4.16 $+_{\mathrm{MM}}$ satisfies the following properties:

(i) $\|m +_{\mathrm{MM}} m'\| = \|m\| + \|m'\|$;

(ii) $m +_{\mathrm{MM}} m' = 0$ if $\|m\| + \|m'\| = 0$;

(iii) $|m +_{\mathrm{MM}} m'| = |m| = |m'|$ otherwise;

(iv) $+_{\mathrm{MM}}$ is well defined;

(v) if $m \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$, then $m +_{\mathrm{MM}} m' \rrbracket_\rho t + t'$.

Proof. The first condition is straightforward from the definition of $+_{\mathrm{MM}}$. The second and third follow from this definition and Proposition 4.12; and from these the fourth is a direct consequence. Finally the last point is again proved by induction using Proposition 4.12 (Coq checked). □

In the sequence we will need the following notations. We will denote by $<_M$ the lexicographic ordering on list(E) obtained from $<_E$. Given two lists l, w of expressions, we write $l \subseteq w$ to mean that l is a sublist of w, i.e. all elements of l occur in w and in the same order.

Definition 4.17 $+_{\mathrm{PM}}$ is defined as follows.

$$\begin{array}{rcl}
+_{\mathrm{PM}} : P \times M & \to & P \\
i, j & \mapsto & i + j \\
i, m & \mapsto & m + i \\
m + p, j & \mapsto & m + (p +_{\mathrm{PM}} j) \\
m + p, m' & \mapsto & \left\{ \begin{array}{ll} m + (p +_{\mathrm{PM}} m') & |m| <_M |m'| \\ p +_{\mathrm{PM}} (m +_{\mathrm{MM}} m') & |m| = |m'| \\ m' + m + p & \text{else} \end{array} \right.
\end{array}$$

Proposition 4.18 $+_{\mathrm{PM}}$ satisfies the following properties:

(i) if $|m| = |m'|$, then $\|p +_{\mathrm{PM}} m\|_{m'} = \|p\|_{m'} + \|m\|$;

(ii) if $|m| \neq |m'|$, then $\|p +_{\mathrm{PM}} m\|_{m'} = \|p\|_{m'}$;

(iii) $|p +_{\mathrm{PM}} m| \subseteq l$, where l is the list obtained by appending $|m|$ to $|p|$ and sorting the result;

(iv) $+_{\mathrm{PM}}$ is well defined;

(v) if $p \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$, then $p +_{\mathrm{PM}} m' \rrbracket_\rho t + t'$.

Proof. The two first properties follow from the definition of $+_{\mathrm{PM}}$ (in the first case also appealing to Proposition 4.16).

The third property is proved by induction. The basis is trivial; for the induction step we need to consider two cases. Let $p = m' + p'$; if $|m| \neq |m'|$, then the algorithm reduces again to straight insertion of an element in a list (since the only difference is in the case $|m| = |m'|$). If $|m| = |m'|$, then $|m' +_{\mathrm{MM}} m| = |m|$ by Proposition 4.16, so we can use the induction hypothesis to conclude that this call returns a q such that $|q|$ is the straight insertion of $|m'|$ in $|p'|$, which is $|m'| :: |p'|$ (since $m' + p : P$), and this is a sublist of $|m| :: |m| :: |p'|$, which would be the outcome of the straight insertion of $|m|$ in $|m'| :: |p'|$ (since $|m| = |m'|$). Hence also in this case the thesis holds.

The fourth property is a consequence of the previous ones, since a sublist of an ordered list is ordered. The last property is proved by induction (Coq checked). □

Definition 4.19 $+_{\mathrm{PP}}$ is defined as follows.

$$\begin{array}{rcl}
+_{\mathrm{PP}} : P \times P & \to & P \\
i, q & \mapsto & q +_{\mathrm{PM}} i \\
m + p, q & \mapsto & (p +_{\mathrm{PP}} q) +_{\mathrm{PM}} m
\end{array}$$

Proposition 4.20 $+_{\mathrm{PP}}$ satisfies the following properties:

(i) for all m, $\|p +_{\mathrm{PP}} q\|_m = \|p\|_m + \|q\|_m$;

(ii) $|p +_{\mathrm{PP}} q| \subseteq l$, where l is the list obtained by appending $|q|$ to $|p|$ and sorting the result;

(iii) $+_{\mathrm{PP}}$ is well defined;

(iv) if $p \rrbracket_\rho t$ and $q \rrbracket_\rho t'$, then $p +_{\mathrm{PP}} q \rrbracket_\rho t + t'$.

Proof. The first property is proved by induction on p. If $p = i$, then either $m = j$ for some $j \in \mathbb{Z}$ and the thesis holds by the first part of Proposition 4.18 or else $|m| \neq |i|$ and the thesis holds by the second part of Proposition 4.18. If $p = m' + p'$, then by induction hypothesis $\|p' +_{\mathrm{PP}} q\|_m = \|p'\|_m + \|q\|_m$ and there are two cases. If $|m'| = |m|$, then $\|p\|_m = \|m'\|$ and $\|p'\|_m = 0$ (since $|p|$ does not have repetitions), and by the first part of Proposition 4.18 $\|(p' +_{\mathrm{PP}} q) +_{\mathrm{PM}} m'\|_m = \|p' +_{\mathrm{PP}} q\|_m + \|m'\| = \|p'\|_m + \|q\|_m + \|m'\| = \|q\|_m + \|m'\| = \|q\|_m + \|p\|_m$. If $|m'| \neq |m|$ then $\|p\|_m = \|p'\|_m$ and by the second part of Proposition 4.18 $\|(p' +_{\mathrm{PP}} q) +_{\mathrm{PM}} m'\|_m = \|p'\|_m + \|q\|_m = \|p\|_m + \|q\|_m$.

The second and third properties are proved from Proposition 4.18 by straightforward induction. The last property is similar (Coq checked). □

The last operations have no analogue in sorting algorithms. We will use juxtaposition to denote the sorted merge of two lists.

Definition 4.21 $\cdot_{\mathrm{PM}}$ is defined as follows.

$$\begin{array}{rcl} \cdot_{\mathrm{PM}} : P \times M & \to & P \\ i, m' & \mapsto & 0 +_{\mathrm{PM}} (m' \cdot_{\mathrm{M}\mathbb{Z}} i) \\ m + p, m' & \mapsto & (p \cdot_{\mathrm{PM}} m') +_{\mathrm{PM}} (m \cdot_{\mathrm{MM}} m') \end{array}$$

Proposition 4.22 $\cdot_{\mathrm{PM}}$ satisfies the following properties:

(i) for all m, $\|p \cdot_{\mathrm{PM}} m'\|_m = \|p\|_{m^*} \times \|m'\|$ if there is[1] an m^* such that $|m| = |m^*||m'|$ and 0 otherwise;

(ii) $p \cdot_{\mathrm{PM}} 0 = 0$;

(iii) if $m' \neq 0$, then $|p \cdot_{\mathrm{PM}} m'|$ is the sorted list whose elements are obtained by appending $|m'|$ to each element of p and sorting the result;

(iv) $\cdot_{\mathrm{PM}}$ is well defined;

(v) if $p \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$, then $p \cdot_{\mathrm{PM}} m' \rrbracket_\rho t \times t'$.

Proof. The first property is a straightforward induction on p using Propositions 4.18 and 4.14 (notice that $\cdot_{\mathrm{M}\mathbb{Z}}$ is a special case of $\cdot_{\mathrm{MM}}$). The second property can be proved directly by induction, since $0 \cdot_{\mathrm{MM}} 0 = 0$ and $0 +_{\mathrm{PM}} 0$.

The third property is also proved by induction on p. If $p = i$ then the result follows from Propositions 4.10 and 4.18. If $p = m + p'$, then $(m+p') \cdot_{\mathrm{PM}} m' = (p \cdot_{\mathrm{PM}} m') +_{\mathrm{PM}} (m \cdot_{\mathrm{MM}} m')$. Since $|p'|$ does not have any repeated elements, by induction hypothesis neither does $|p \cdot_{\mathrm{PM}} m'|$ (since its elements are the image of the elements of $|p|$ via an injective function). By Proposition 4.14, $|m \cdot_{\mathrm{MM}} m'|$ is the sorted list whose elements are either in $|m|$ or in $|m'|$, and this does not occur in $|p \cdot_{\mathrm{PM}} m'|$. Hence the thesis follows from Proposition 4.18.

The fourth property is straightforward since $\cdot_{\mathrm{MM}}$ and $+_{\mathrm{PM}}$ are both well defined. The last one is again proved by induction on p (Coq checked). □

Definition 4.23 $\cdot_{\mathrm{PP}}$ is defined as follows.

$$\begin{array}{rcl} \cdot_{\mathrm{PP}} : P \times P & \to & P \\ i, q & \mapsto & q \cdot_{\mathrm{PM}} i \\ m + p, q & \mapsto & (q \cdot_{\mathrm{PM}} m) +_{\mathrm{PP}} (p \cdot_{\mathrm{PP}} q) \end{array}$$

[1] Notice that there may exist at most one such m^*.

PROPOSITION 4.24 $\cdot_{\mathrm{PP}}$ satisfies the following properties:

(i) for all $m \in M$, $\|p \cdot_{\mathrm{PP}} q\|_m = \sum \|p\|_{m_1} \|q\|_{m_2}$, where the sum ranges over all $m_1 \in |p| \cup \{1\}$ and $m_2 \in |q| \cup \{1\}$ for which $|m| = |m_1||m_2|$;

(ii) $\cdot_{\mathrm{PP}}$ is well defined;

(iii) if $p \rrbracket_\rho t$ and $q \rrbracket_\rho t'$, then $p \cdot_{\mathrm{PP}} q \rrbracket_\rho t \times t'$.

PROOF. We prove the first property by induction. If $p = i$ then the result follows from Proposition 4.22, since then m_1 can only be 1 ($|p|$ is the empty list). If $p = m' + p'$, then by Proposition 4.20 $\|(q \cdot_{\mathrm{PM}} m') +_{\mathrm{PP}} (p' \cdot_{\mathrm{PP}} q)\|_m = \|q \cdot_{\mathrm{PM}} m'\|_m + \|p' \cdot_{\mathrm{PP}} q\|_m$; the result now follows from induction hypothesis and Proposition 4.22.

The second property is trivial; the last is proved by induction (Coq checked). □

DEFINITION 4.25 The normalization function $\mathcal{N}$ is defined as follows, where E^* denotes the type of expressions that do not use division.

$$\begin{array}{rcl}
\mathcal{N} : E^* & \to & P \\
i & \mapsto & i \\
v_i^0 & \mapsto & v_i^0 \times 1 + 0 \\
e + f & \mapsto & \mathcal{N}(e) +_{\mathrm{PP}} \mathcal{N}(f) \\
e \times f & \mapsto & \mathcal{N}(e) \cdot_{\mathrm{PP}} \mathcal{N}(f) \\
v_i^1(e) & \mapsto & v_i^1(\mathcal{N}(e)) \times 1 + 0
\end{array}$$

PROPOSITION 4.26 N satisfies the following properties:

(i) N is well defined;

(ii) if $e \rrbracket_\rho t$ then $\mathcal{N}(e) \rrbracket_\rho t$.

PROOF. The first part is a straightforward induction. $\mathcal{N}(i)$ and $\mathcal{N}(v_i^0)$ are in normal form by definition of P; $\mathcal{N}(e + f)$ and $\mathcal{N}(e \times f)$ are in normal form by induction hypothesis and Propositions 4.20 and 4.24; and $\mathcal{N}(v_i^1(e))$ is in normal form by definition of P and induction hypothesis.

The second property is a straightforward induction (Coq checked). □

COROLLARY 4.27 Let $t, t' : A$ and define $\langle e, \rho \rangle = \mathit{lift}(t, \emptyset)$ and $\langle e', \sigma \rangle = \mathit{lift}(t', \rho)$. If $\mathcal{N}(e) = \mathcal{N}(e')$, then $t =_A t'$ can be proved from the ring axioms and unfolding of the definitions of $-$, zring and nexp.

PROOF. Let e and e' be as defined above and suppose that $\mathcal{N}(e) = \mathcal{N}(e')$. By Lemma 3.9, both $e \rrbracket_\rho t$ and $e' \rrbracket_\rho t'$. By Proposition 4.26 also $\mathcal{N}(e) \rrbracket_\rho t$ and $\mathcal{N}(e') \rrbracket_\rho t'$. Since $\mathcal{N}(e) = \mathcal{N}(e')$, we have that $\mathcal{N}(e) \rrbracket_\rho t$ and $\mathcal{N}(e) \rrbracket_\rho t'$, whence $t =_A t'$ by Lemma 2.32. □

4.3 Properties of P and $\mathcal{N}$

We now show that $\langle P, +_{\mathrm{PP}}, 0, \cdot_{\mathrm{PP}}, 1 \rangle$ is a ring (w.r.t. syntactic equality). This will be essential later on, where we will use the properties of these operations without comment.

LEMMA 4.28 For all $m, m' : M$, $m \cdot_{\mathrm{MM}} m' = m' \cdot_{\mathrm{MM}} m$.

PROOF. By Lemma 4.7, it is sufficient to show that $\|m \cdot_{\mathrm{MM}} m'\| = \|m' \cdot_{\mathrm{MM}} m\|$ and $|m \cdot_{\mathrm{MM}} m'| = |m' \cdot_{\mathrm{MM}} m|$. But both of these are consequences of Proposition 4.14, commutativity of addition and uniqueness of sort. □

Lemma 4.29 Let $p, q, r : P$. Then the following hold:

(i) $p +_{\mathrm{PP}} 0 = p$

(ii) $p +_{\mathrm{PP}} (q +_{\mathrm{PP}} r) = (p +_{\mathrm{PP}} q) +_{\mathrm{PP}} r$

(iii) $p +_{\mathrm{PP}} q = q +_{\mathrm{PP}} p$

(iv) $p +_{\mathrm{PP}} (p \cdot_{\mathrm{PP}} (-1)) = 0$

Proof. Remember that $p = q \iff \forall m : M. \|m\|_p = \|m\|_q$ (Proposition 4.8). Let $m : M$ be arbitrary; then, by Proposition 4.20, the following are immediate:

(i) $\|p +_{\mathrm{PP}} 0\|_m = \|p\|_m + \|0\|_m = \|p\|_m$

(ii) $\|p +_{\mathrm{PP}} (q +_{\mathrm{PP}} r)\|_m = \|p\|_m + \|q +_{\mathrm{PP}} r\|_m = \|p\|_m + \|q\|_m + \|r\|_m = \|p +_{\mathrm{PP}} q\|_m + \|r\|_m = \|(p +_{\mathrm{PP}} q) +_{\mathrm{PP}} r\|_m$.

(iii) $\|p +_{\mathrm{PP}} q\|_m = \|p\|_m + \|q\|_m = \|q\|_m + \|p\|_m = \|q +_{\mathrm{PP}} p\|_m$.

(iv) Given $m : M$, $\|p +_{\mathrm{PP}} (p \cdot_{\mathrm{PP}} (-1))\|_m = \|p\|_m + \|p \cdot_{\mathrm{PP}} (-1)\|_m$, so it suffices to show that $\|p \cdot_{\mathrm{PP}} (-1)\|_m = -\|p\|_m$. By Proposition 4.24, $\|p \cdot_{\mathrm{PP}} (-1)\|_m = \sum \|p\|_{m_1} \| - 1\|_{m_2}$. Now in this sum m_2 can only assume value 1, whence $m_1 = m$ and the previous expression reduces to $\|p\|_m(-1) = -\|p\|_m$.

□

Lemma 4.30 Let $p, q, r : P$. Then the following hold:

(i) $p \cdot_{\mathrm{PP}} 0 = 0$

(ii) $p \cdot_{\mathrm{PP}} 1 = p$

(iii) $p \cdot_{\mathrm{PP}} (q \cdot_{\mathrm{PP}} r) = (p \cdot_{\mathrm{PP}} q) \cdot_{\mathrm{PP}} r$

(iv) $p \cdot_{\mathrm{PP}} q = q \cdot_{\mathrm{PP}} p$

Proof. Again we appeal to Proposition 4.8.

We begin by proving commutativity. For any $m : M$, $\|p \cdot_{\mathrm{PP}} q\|_m = \sum \|p\|_{m_1} \|q\|_{m_2} = \sum \|q\|_{m_2} \|p\|_{m_1} = \|q \cdot_{\mathrm{PP}} p\|_m$ where the sums range over all $m_1 \in |p| \cup \{1\}$ and $m_2 \in |q| \cup \{1\}$ for which $|m| = |m_1||m_2|$; the equalities hold by Proposition 4.24.

$p \cdot_{\mathrm{PP}} 0 = 0$ is proved straightforwardly by induction, using Proposition 4.22.

Next, $p \cdot_{\mathrm{PP}} 1 = 1 \cdot_{\mathrm{PP}} p = p \cdot_{\mathrm{PM}} 1$. For any $m : M$, $|m| = |m||1|$, hence by Proposition 4.22 $\|p \cdot_{\mathrm{PM}} 1\|_m = \|p\|_m \times \|1\| = \|p\|_m$, hence $p \cdot_{\mathrm{PP}} 1 = p$.

Finally, for associativity, we again obtain from Proposition 4.24 that, for $m : M$, $\|p \cdot_{\mathrm{PP}} (q \cdot_{\mathrm{PP}} r)\|_m = \sum \|p\|_{m_1} \|q \cdot_{\mathrm{PP}} r\|_{m_2} = \sum \|p\|_{m_1} \left(\sum \|q\|_{m_2^1} \|r\|_{m_2^2} \right) = \sum \|p\|_{m_1} \|q\|_{m_2^1} \|r\|_{m_2^2}$

The last expression is completely symmetric on p, q and r, since the last sum in fact ranges over all m_1, m_2^1 and m_2^2 such that $|m| = |m_1||m_2^1||m_2^2|$ with $m_1 \in |p| \cup \{1\}$, $m_2^1 \in |q| \cup \{1\}$ and $m_2^2 \in |r| \cup \{1\}$. Therefore, from associativity and commutativity of sums and products of integers, we immediately get that $\|p \cdot_{\mathrm{PP}} (q \cdot_{\mathrm{PP}} r)\|_m = \|r \cdot_{\mathrm{PP}} (p \cdot_{\mathrm{PP}} q)\|_m$, and applying commutativity of $\cdot_{\mathrm{PP}}$ twice we get the desired result. □

Lemma 4.31 Let $p, q, r : P$. Then $p \cdot_{\mathrm{PP}} (q +_{\mathrm{PP}} r) = (p \cdot_{\mathrm{PP}} q) +_{\mathrm{PP}} (p \cdot_{\mathrm{PP}} r)$.

Proof. Once again, if $m : M$ then $\|p \cdot_{\mathrm{PP}} (q +_{\mathrm{PP}} r)\|_m = \sum \|p\|_{m_1} \|q +_{\mathrm{PP}} r\|_{m_2} = \sum \|p\|_{m_1} (\|q\|_{m_2} + \|r\|_{m_2}) = \sum \|p\|_{m_1} \|q\|_{m_2} + \sum \|p\|_{m_1} \|r\|_{m_2} = \|(p \cdot_{\mathrm{PP}} q) +_{\mathrm{PP}} (p \cdot_{\mathrm{PP}} r)\|_m$ □

Lemma 4.32 Let $m : M \setminus \mathbb{Z}$ and $p : P$. Then $\mathcal{N}(m) = m + 0$ and $\mathcal{N}(p) = p$.

Proof. We prove both results by simultaneous induction on m and p.

If $m = v_i^0 \times i$ then $\mathcal{N}(m) = \mathcal{N}(v_i^0) \cdot_{\mathrm{PP}} \mathcal{N}(i) = (v_i^0 \times 1 + 0) \cdot_{\mathrm{PP}} i = v_i^0 \times i + 0 = m + 0$, where the last-but-one equality is simply computation of $\cdot_{\mathrm{PP}}$. If $m = v_i^1(p) \times i$ then $\mathcal{N}(m) = \mathcal{N}(v_i^1(p)) \cdot_{\mathrm{PP}} \mathcal{N}(i) = (v_i^1(\mathcal{N}(p)) \times 1 + 0) \cdot_{\mathrm{PP}} i = v_i^1(p) \times i + 0 = m + 0$, where the last-but-one equality follows from computation and induction hypothesis for p.

If $m = v_i^0 \times m'$, then notice first that $m' \cdot_{\mathrm{MM}} (v_i^0 \times 1) = m$: $\|m' \cdot_{\mathrm{MM}} (v_i^0 \times 1)\| = \|m'\| \times 1 = \|m'\|$ by Proposition 4.14 and $|m' \cdot_{\mathrm{MM}} (v_i^0 \times 1)|$ is the list obtained by inserting v_i^0 at the right position in $|m'|$, which is by definition $|m|$ (since this list is sorted), hence by Lemma 4.7 the result holds. Using this fact, the induction hypothesis and Lemmas 4.30 and 4.29, we see that the thesis holds.

$$\begin{aligned}
\mathcal{N}(m) &= \mathcal{N}(v_i^0) \cdot_{\mathrm{PP}} \mathcal{N}(m') \\
&= (v_i^0 \times 1 + 0) \cdot_{\mathrm{PP}} (m' + 0) \\
&= (m' + 0) \cdot_{\mathrm{PM}} (v_i^0 \times 1) +_{\mathrm{PP}} (0 \cdot_{\mathrm{PP}} (e' + 0)) \\
&= (m' + 0) \cdot_{\mathrm{PM}} (v_i^0 \times 1) +_{\mathrm{PP}} 0 \\
&= (m' + 0) \cdot_{\mathrm{PM}} (v_i^0 \times 1) \\
&= 0 \cdot_{\mathrm{PM}} (v_i^0 \times 1) +_{\mathrm{PM}} m' \cdot_{\mathrm{MM}} (v_i^0 \times 1) \\
&= (0 +_{\mathrm{PM}} (v_i^0 \times 1) \cdot_{\mathrm{M}\mathbb{Z}} 0) +_{\mathrm{PM}} m' \cdot_{\mathrm{MM}} (v_i^0 \times 1) \\
&= (0 +_{\mathrm{PM}} 0) +_{\mathrm{PM}} (m' \cdot_{\mathrm{MM}} (v \times 1)) \\
&= 0 +_{\mathrm{PM}} m \\
&= m + 0.
\end{aligned}$$

If $m = v_i^1(p) \times m'$, then by induction hypothesis $\mathcal{N}(v_i^1(p)) = v_i^1(\mathcal{N}(p)) \times 1 + 0 = v_i^1(p) + 0$ and the previous chain of equalities holds replacing $v_i^1(p) + 0$ for v_i^0 everywhere.

Now suppose that p is an integer; then $\mathcal{N}(p) = p$ by definition. Else take $p = m + q$; by induction hypothesis $\mathcal{N}(q) = q$ and $\mathcal{N}(m) = m + 0$, hence

$$\begin{aligned}
\mathcal{N}(m + q) &= \mathcal{N}(m) +_{\mathrm{PP}} \mathcal{N}(q) \\
&= (m + 0) +_{\mathrm{PP}} q \\
&= (0 +_{\mathrm{PP}} q) +_{\mathrm{PM}} m \\
&= q +_{\mathrm{PM}} m
\end{aligned}$$

by Lemma 4.29; but by definition of P, $|m|$ cannot occur in $|q|$ and must be smaller (w.r.t. $<_M$), hence the last expression reduces to $m + q$, or p. □

Corollary 4.33 $\mathcal{N}$ is idempotent, i.e., for every $e : E^*$, $\mathcal{N}(\mathcal{N}(e)) = \mathcal{N}(e)$.

Proof. Since $\mathcal{N}(e) : P$, the previous lemma is applicable, yielding the result. □

4.4 The substitution lemma

In this subsection, we show that the following "substitution lemma" holds: if, in two expressions that normalize to the same, some variables get uniformly renamed, then the resulting expressions also normalize to the same term.

This is proven in two steps.

Lemma 4.34 Let $e : E$ and ξ be a renaming of variables. Then $\mathcal{N}(e^\xi) = \mathcal{N}(\mathcal{N}(e)^\xi)$.

Proof. By induction on e.

Suppose $e = i$; then $\mathcal{N}(\mathcal{N}(i)^\xi) = \mathcal{N}(i^\xi) = \mathcal{N}(i) = \mathcal{N}(i^\xi)$.

Now let $e = v_i^0$. Then $\mathcal{N}(\mathcal{N}(e)^\xi) = \mathcal{N}((v_i^0 \times 1 + 0)^\xi) = \mathcal{N}(v_{\xi_0(i)}^0 \times 1 + 0) = \mathcal{N}(v_{\xi_0(i)}^0) \cdot_{\mathrm{PP}} 1 +_{\mathrm{PP}} 0 = \mathcal{N}(v_{\xi_0(i)}^0)) = \mathcal{N}((v_i^0)^\xi)$ by virtue of Propositions 4.29 and 4.30.

If $e = v_i^1(e')$, then we use the induction hypothesis to show that

$$\begin{array}{rcl}
\mathcal{N}(\mathcal{N}(v_i^1(e'))^\xi) & = & \mathcal{N}((v_i^1(\mathcal{N}(e')) \times 1 + 0)^\xi) \\
& = & \mathcal{N}(v_{\xi_1(i)}^1(\mathcal{N}(e')^\xi) \times 1 + 0) \\
& = & \mathcal{N}(v_{\xi_1(i)}^1(\mathcal{N}(e')^\xi)) \cdot_{\mathrm{PP}} 1 +_{\mathrm{PP}} 0 \\
& = & \mathcal{N}(v_{\xi_1(i)}^1(\mathcal{N}(e')^\xi)) \\
& = & v_{\xi_1(i)}^1(\mathcal{N}(\mathcal{N}(e')^\xi)) \times 1 + 0 \\
& \overset{IH}{=} & v_{\xi_1(i)}^1(\mathcal{N}(e'^\xi)) \times 1 + 0 \\
& = & \mathcal{N}(v_{\xi_1(i)}^1(e'^\xi)) \\
& = & \mathcal{N}((v_i^1(e'))^\xi)
\end{array}$$

For the case $e = e_1 \star e_2$, with $\star = +, \times$, we need besides the induction hypothesis the equality

$$\mathcal{N}((p \star q)^\xi) = \mathcal{N}((p \star_{\mathrm{PP}} q)^\xi) \tag{19}$$

for all $p, q : P$. The proof of this is included in the Appendix; its use is marked here by $*$.

$$\begin{array}{rcl}
\mathcal{N}(\mathcal{N}(e_1 \star e_2)^\xi) & = & \mathcal{N}((\mathcal{N}(e_1) \star_{\mathrm{PP}} \mathcal{N}(e_2))^\xi) \\
& \overset{*}{=} & \mathcal{N}((\mathcal{N}(e_1) \star \mathcal{N}(e_2))^\xi) \\
& = & \mathcal{N}(\mathcal{N}(e_1)^\xi \star \mathcal{N}(e_2)^\xi) \\
& = & \mathcal{N}(\mathcal{N}(e_1)^\xi) \star_{\mathrm{PP}} \mathcal{N}(\mathcal{N}(e_2)^\xi) \\
& \overset{IH}{=} & \mathcal{N}({e_1}^\xi) \star_{\mathrm{PP}} \mathcal{N}({e_2}^\xi) \\
& = & \mathcal{N}({e_1}^\xi \star {e_2}^\xi) \\
& = & \mathcal{N}((e_1 \star e_2)^\xi)
\end{array}$$

□

With this we can prove the main result of this section:

THEOREM 4.35 Let $e, e' : E$ be expressions such that $\mathcal{N}(e) = \mathcal{N}(e')$ and let ξ be a renaming of variables. Then $\mathcal{N}(e^\xi) = \mathcal{N}(e'^\xi)$.

PROOF. According to the previous lemma, $\mathcal{N}(e^\xi) = \mathcal{N}(N(e)^\xi) = \mathcal{N}(N(e')^\xi) = \mathcal{N}(e'^\xi)$. □

4.5 Completeness

We are now ready to state our main result.

THEOREM 4.36 Let $t, t' : A$ be such that the equality $t =_A t'$ can be proved (in the sense of Definition 2.11) only from the ring axioms and unfolding of the definitions of $-$, zring and nexp in t and t'. Define $\langle e, \rho \rangle = \mathit{lift}(t, \emptyset)$ and $\langle e', \sigma \rangle = \mathit{lift}(t', \rho)$. Then $\mathcal{N}(e) = \mathcal{N}(e')$.

The proof of this is split in several stages.

LEMMA 4.37 Let $t, t' : A$ be terms such that t' is obtained from t by unfolding the definitions of $-$, zring and $\cdot^n$ (n closed) in t. Let $\mathit{lift}(t, \rho) = \langle e, \sigma \rangle$ and $\mathit{lift}(t', \rho) = \langle e', \sigma' \rangle$. Then $\sigma = \sigma'$ and $\mathcal{N}(e) = \mathcal{N}(e')$.

Proof. For $-$ and $\cdot^n$ this is immediate, since terms using these constructors are lifted to expressions using the corresponding abbreviations whose definition coincides with those of $-$ and $\cdot^n$.

For zring the proof is by induction[2]: $\underline{0}$ unfolds to 0, both of which are lifted to 0; $\underline{n+1}$ is lifted to $n+_{\mathbb{Z}}1$, which is in normal form, whereas $\underline{n}+1$ is lifted to $n+1$ which normalizes to $\mathcal{N}(n)+_{\mathrm{PP}}1 = n+_{\mathbb{Z}}1$; finally, $\underline{n-1}$ is lifted to $n+1\times(-1)$, which normalizes to $\mathcal{N}(n)+_{\mathrm{PP}}1\cdot_{\mathrm{PP}}(-1) = n-_{\mathbb{Z}}1$. □

Lemma 4.38 Let $t, t' : A$ be such that $t =_A t'$ is an instance of one of the axioms $\mathbf{Set_1}$, $\mathbf{SG}$, $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{G_1}$, $\mathbf{G_2}$, $\mathbf{AG}$ or $\mathbf{R_i}$ with $1 \le i \le 5$. Define $\langle e,\tau\rangle = \mathit{lift}(t,\emptyset)$ and $\langle e',\tau'\rangle = \mathit{lift}(t',\tau)$. Then $\mathcal{N}(e) = \mathcal{N}(e')$.

Proof. All these proofs are very similar, being a consequence of Lemmas 4.29 and 4.30. We detail a few:

$\mathbf{Set_1}$ Then $t = t'$; by Lemma 3.10 $e' = e$, and obviously $\mathcal{N}(e) = \mathcal{N}(e)$.

$\mathbf{SG}$ Then $t = (t_1+t_2)+t_3$ and $t' = t_1+(t_2+t_3)$. Let $\mathit{lift}(t_1,\emptyset) = \langle e_1,\rho\rangle$, $\mathit{lift}(t_2,\rho) = \langle e_2,\sigma\rangle$ and $\mathit{lift}(t_3,\sigma) = \langle e_3,\theta\rangle$. Then $\mathit{lift}(t_1+t_2,\emptyset) = \langle e_1+e_2,\sigma\rangle$ and $\mathit{lift}((t_1+t_2)+t_3,\emptyset) = \langle (e_1+e_2)+e_3,\theta\rangle$.

Furthermore, since $\rho \subseteq \sigma \subseteq \theta$ by Lemma 3.8, Lemma 3.10 yields $\mathit{lift}(t_1,\theta) = \langle e_1,\theta\rangle$, $\mathit{lift}(t_2,\theta) = \langle e_2,\theta\rangle$ and $\mathit{lift}(t_3,\sigma) = \langle e_3,\theta\rangle$, whence $\mathit{lift}(t_2+t_3,\theta) = \langle e_2+e_3,\theta\rangle$ and $\mathit{lift}(t_1+(t_2+t_3),\theta) = \langle e_1+(e_2+e_3),\theta\rangle$.

Then $\mathcal{N}((e_1+e_2)+e_3) = \mathcal{N}(e_1+e_2)+_{\mathrm{PP}}\mathcal{N}(e_3) = (\mathcal{N}(e_1)+_{\mathrm{PP}}\mathcal{N}(e_2))+_{\mathrm{PP}}\mathcal{N}(e_3) = \mathcal{N}(e_1)+_{\mathrm{PP}}(\mathcal{N}(e_2)+_{\mathrm{PP}}\mathcal{N}(e_3)) = \mathcal{N}(e_1)+_{\mathrm{PP}}\mathcal{N}(e_2+e_3) = \mathcal{N}(e_1+(e_2+e_3))$.

$\mathbf{G_1}$ Then $t = t_1+(-t_1)$ and $t' = 0$. Let $\mathit{lift}(t_1,\emptyset) = \langle e_1,\rho\rangle$; then by Lemma 3.10 also $\mathit{lift}(t_1,\rho) = \langle e_1,\rho\rangle$, hence $e = e_1+(e_1\times(-1))$; by definition $\mathit{lift}(0,\rho) = \langle 0,\rho\rangle$, so $e' = 0$.

Now $\mathcal{N}(e_1+(e_1\times(-1))) = \mathcal{N}(e_1)+_{\mathrm{PP}}(\mathcal{N}(e_1)\cdot_{\mathrm{PP}}(-1)) = 0 = \mathcal{N}(0)$, according to Lemma 4.29.

$\mathbf{R_5}$ In this case $t = t_1\times(t_2+t_3)$ and $t' = (t_1\times t_2)+(t_1\times t_3)$. Reasoning in an analogous way to the case of $\mathbf{SG}$ above, we conclude that $e = e_1\times(e_2+e_3)$ and $e' = (e_1\times e_2)+(e_1\times e_3)$. By Lemma 4.30, $\mathcal{N}(e_1\times(e_2+e_3)) = \mathcal{N}(e_1)\cdot_{\mathrm{PP}}(\mathcal{N}(e_2)+_{\mathrm{PP}}\mathcal{N}(e_3)) = \mathcal{N}(e_1)\cdot_{\mathrm{PP}}\mathcal{N}(e_2)+_{\mathrm{PP}}\mathcal{N}(e_1)\cdot_{\mathrm{PP}}\mathcal{N}(e_3) = \mathcal{N}((e_1\times e_2)+(e_1\times e_3))$.

□

Lemma 4.39 Let $t_1, t_2 : A$ be such that, if $\langle e_1,\rho\rangle = \mathit{lift}(t_1,\emptyset)$ and $\langle e_2,\sigma\rangle = \mathit{lift}(t_2,\rho)$, then $\mathcal{N}(e_1) = \mathcal{N}(e_2)$. Define $\langle e_2',\sigma'\rangle = \mathit{lift}(t_2,\emptyset)$ and $\langle e_1',\rho'\rangle = \mathit{lift}(t_1,\sigma')$. Then $\mathcal{N}(e_1') = \mathcal{N}(e_2')$.

Proof. Let e_1, e_1', e_2 and e_2' be as given. By Lemma 3.21 there is a renaming of variables ξ such that $e_i' = {e_i}^{\xi}$ for $i = 1,2$; but then

$$\mathcal{N}(e_1') = \mathcal{N}\left({e_1}^{\xi}\right) = \mathcal{N}\left({e_2}^{\xi}\right) = \mathcal{N}(e_2')$$

using the hypothesis $\mathcal{N}(e_1) = \mathcal{N}(e_2)$ and Theorem 4.35. □

Lemma 4.40 Let $t_1, t_2, t_3 : A$ and define

$$\begin{array}{ll} \langle e_1,\rho\rangle = \mathit{lift}(t_1,\emptyset) & \langle e_2',\sigma'\rangle = \mathit{lift}(t_2,\emptyset) \\ \langle e_2,\sigma\rangle = \mathit{lift}(t_2,\rho) & \langle e_3',\theta'\rangle = \mathit{lift}(t_3,\sigma') \end{array}$$

Assume that $\mathcal{N}(e_1) = \mathcal{N}(e_2)$ and $\mathcal{N}(e_2') = \mathcal{N}(e_3')$. Define $\langle e_3,\theta\rangle = \mathit{lift}(t_3,\rho)$. Then $\mathcal{N}(e_1) = \mathcal{N}(e_3)$.

[2] In this paragraph we write $+_{\mathbb{Z}}$ to emphasize the distinction between addition of integers and addition of expressions.

Proof. Let e_1, e_2, e_2', e_3 and e_3' be as given and define $\langle e_3'', \theta'' \rangle = \mathit{lift}(t_3, \sigma)$. By Lemma 3.22, there exists a renaming of variables ξ such that $e_3'' = {e_3'}^{\xi}$ and $e_2 = {e_2'}^{\xi}$. By Lemma 3.21 there is another renaming of variables ξ' such that $e_3 = {e_3''}^{\xi'}$ and $\mathrm{dom}(\xi_i') \cap \mathrm{dom}(\rho_i) = \emptyset$ (see Figure 5). Then,

$$\begin{tikzcd}
 & \emptyset \arrow[dl, "t_2"'] \arrow[dr, "t_1"] & \\
\sigma' \arrow[d, "t_3"'] \arrow[dr, dotted, "\xi"] & & \rho \arrow[dl, "t_2"'] \arrow[d, "t_3"] \\
\theta' \arrow[dr, dotted, "\xi"] & \sigma \arrow[d, "t_3"] & \theta \\
 & \theta'' \arrow[ur, dotted, "\xi'"] &
\end{tikzcd}$$

Figure 5: Proof of Lemma 4.40

$$\mathcal{N}(e_3) = \mathcal{N}\left({e_3''}^{\xi'}\right) = \mathcal{N}\left({e_3'}^{\xi' \circ \xi}\right) = \mathcal{N}\left({e_2'}^{\xi' \circ \xi}\right) = \mathcal{N}\left({e_2}^{\xi'}\right) = \mathcal{N}\left({e_1}^{\xi'}\right) = \mathcal{N}(e_1)$$

using the hypotheses $\mathcal{N}(e_1) = \mathcal{N}(e_2)$ and $\mathcal{N}(e_2') = \mathcal{N}(e_3')$ together with Theorem 4.35 and the equalities above stated. The last equality follows from the fact that $\mathrm{dom}(\xi_i') \cap \mathrm{dom}(\rho_i) = \emptyset$: by Lemma 3.11 every variable v_k^i occurring in e_1 is in $\mathrm{dom}(\rho_i)$, so $e_1 = {e_1}^{\xi'}$. □

Lemma 4.41 Let $t_1, t_2 : A$ be such that, if $\langle e_1, \rho \rangle = \mathit{lift}(t_1, \emptyset)$ and $\langle e_2, \sigma \rangle = \mathit{lift}(t_2, \rho)$, then $\mathcal{N}(e_1) = \mathcal{N}(e_2)$. Let $f : [A \to A]$ be other than $\cdot^n$ with n closed and define $\langle e_1', \rho' \rangle = \mathit{lift}(f(t_1), \emptyset)$ and $\langle e_2', \sigma' \rangle = \mathit{lift}(f(t_2), \emptyset)$. Then $\mathcal{N}(e_1') = \mathcal{N}(e_2')$.

Proof. We have to consider two cases. If f is the unary inverse $(-)$, then immediately $e_1' = -e_1$, $\rho' = \rho$ and hence $e_2' = -e_2$; in this case, $\mathcal{N}(e_1') = \mathcal{N}(-e_1) = \mathcal{N}(e_1 \times (-1)) = \mathcal{N}(e_1) \cdot_{\mathrm{PP}} (-1) = \mathcal{N}(e_2) \cdot_{\mathrm{PP}} (-1) = \mathcal{N}(e_2 \times (-1)) = \mathcal{N}(-e_2) = \mathcal{N}(e_2')$.

Else, $e_1' = v_i^1(e_1)$ with $\mathit{lift}_{\mathbb{V}_1}(f, \rho) = \langle v_i^1, \rho' \rangle$ and $e_2' = v_i^1(e_2'')$, with $\mathit{lift}(t_2, \rho') = \langle e_2'', \sigma' \rangle$ (since by Lemma 3.8 $\rho' \subseteq \sigma'$, $\sigma_1'(v_i^1) = f$ and thus $\mathit{lift}_{\mathbb{V}_1}(f, \sigma') = \langle v_i^1, \sigma \rangle$).

By Lemma 3.20 there is a renaming of variables ξ such that $e_2'' = {e_2}^{\xi}$ and $\mathrm{dom}(\xi_i) \cap \mathrm{dom}(\rho_i) = \emptyset$. Hence $\mathcal{N}(e_2') = \mathcal{N}(v_i^1(e_2'')) = v_i^1(\mathcal{N}(e_2'')) \times 1 + 0 = v_i^1(\mathcal{N}({e_2}^{\xi})) \times 1 + 0 = v_i^1(\mathcal{N}({e_1}^{\xi})) \times 1 + 0 = v_i^1(\mathcal{N}(e_1)) \times 1 + 0 = \mathcal{N}(v_i^1(e_1)) = \mathcal{N}(e_1')$, using Theorem 4.35 together with the assumption $\mathcal{N}(e_1) = \mathcal{N}(e_2)$ and the fact that $e_1 = {e_1}^{\xi}$ by virtue of Lemma 3.11 and $\mathrm{dom}(\xi_i) \cap \mathrm{dom}(\rho_i) = \emptyset$. □

Lemma 4.42 Let $t_1, t_2, t_3, t_4 : A$ and define

$$\begin{array}{ll}
\langle e_1, \rho \rangle = \mathit{lift}(t_1, \emptyset) & \quad \langle e_3, \theta \rangle = \mathit{lift}(t_3, \emptyset) \\
\langle e_2, \sigma \rangle = \mathit{lift}(t_2, \rho) & \quad \langle e_4, \tau \rangle = \mathit{lift}(t_4, \theta)
\end{array}$$

Assume that $\mathcal{N}(e_1) = \mathcal{N}(e_2)$ and $\mathcal{N}(e_3) = \mathcal{N}(e_4)$ and let

$$\langle e, \gamma \rangle = \mathit{lift}(t_1 \star t_3) \qquad \langle e', \gamma' \rangle = \mathit{lift}(t_2 \star t_4)$$

where $\star$ is $+$ or $\times$. Then $\mathcal{N}(e) = \mathcal{N}(e')$.

Proof. By definition of lift, $e = e_1 \star e_3'$ with $\langle e_3', \gamma \rangle = \mathit{lift}(t_3, \rho)$. Also, $e' = e_2' \star e_4'$, with $\langle e_2', \gamma'' \rangle = \mathit{lift}(t_2, \gamma)$ and $\langle e_4', \gamma' \rangle = \mathit{lift}(t_4, \gamma'')$.

$$\begin{tikzcd}
 & & \emptyset \arrow[dl, "t_1"'] \arrow[dr, "t_3"] & & \\
 & \rho \arrow[dl, "t_2"'] \arrow[dr, "t_3"] & & \theta \arrow[dl, dotted, "\xi"'] \arrow[dr, "t_4"] & \\
\sigma \arrow[dr, dotted, "\xi'"] & & \gamma \arrow[dl, "t_2"'] \arrow[dr, "t_4"] & & \tau \arrow[dl, dotted, "\xi"'] \\
 & \gamma'' \arrow[dr, "t^4"] & & \gamma''' \arrow[dl, dotted, "\xi''"'] & \\
 & & \gamma' & &
\end{tikzcd}$$

Figure 6: Proof of Lemma 4.42

Take $\mathit{lift}(t_4, \gamma) = \langle e_4'', \gamma''' \rangle$.

According to Lemma 3.22, there exists a renaming of variables ξ such that $e_3' = {e_3}^{\xi}$ and $e_4'' = {e_4}^{\xi}$. By Lemma 3.21, there is a renaming of variables ξ' such that $e_2' = {e_2}^{\xi'}$ and $\mathrm{dom}(\xi_i') \cap \mathrm{dom}(\rho_i) = \emptyset$ (and hence $e_1 = {e_1}^{\xi'}$ due to Lemma 3.11). Again by Lemma 3.21, there exists a renaming of variables ξ'' such that $e_4' = {e_4''}^{\xi''}$ and $\mathrm{dom}(\xi_i'') \cap \mathrm{dom}(\gamma_i) = \emptyset$ (so that $e_3' = {e_3'}^{\xi''}$) (see Figure 6).

Then, $\mathcal{N}(e') = \mathcal{N}(e_2' \star e_4') = \mathcal{N}(e_2') \star_{\mathrm{PP}} \mathcal{N}(e_4') = \mathcal{N}({e_2}^{\xi'}) \star_{\mathrm{PP}} \mathcal{N}({e_4''}^{\xi''}) = \mathcal{N}({e_2}^{\xi'}) \star_{\mathrm{PP}} \mathcal{N}({e_4}^{\xi'' \circ \xi}) = \mathcal{N}({e_1}^{\xi'}) \star_{\mathrm{PP}} \mathcal{N}({e_3}^{\xi'' \circ \xi}) = \mathcal{N}(e_1) \star_{\mathrm{PP}} \mathcal{N}({e_3'}^{\xi''}) = \mathcal{N}(e_1) \star_{\mathrm{PP}} \mathcal{N}(e_3') = \mathcal{N}(e_1 \star e_3') = \mathcal{N}(e)$ using the hypotheses and Theorem 4.35. □

Definition 4.43 A *normal proof* of $t =_A t'$ is a proof of $t =_A t'$ where $\mathbf{Set_4}$ is never applied with $\cdot^n$ (n closed) and $\mathbf{Set_5}$ is never applied with $-$.

Lemma 4.44 Suppose that $t =_A t'$ can be proved only from the ring axioms and unfolding of the definitions of $-$, zring and nexp in t and t'. Then there exists a normal proof of $t =_A t'$.

Proof. By induction on the length of the proof of $t =_A t'$. The only non-trivial cases are those when the last axiom to be applied is $\mathbf{Set_4}$ with $\cdot^n$ (n closed) or $\mathbf{Set_5}$ with $-$.

Suppose we prove $t_1^n =_A t_2^n$ from $t_1 =_A t_2$ using $\mathbf{Set_4}$. We proceed by induction. If $n = 0$, then we can replace the whole proof by ($\mathbf{Set_1}$ 1), and folding produces $t_1^0 =_A t_2^0$. If $n = k + 1$, we first find a normal proof of $t_1^k =_A t_2^k$ using the induction hypothesis (for n) and a normal proof of $t_1 =_A t_2$ using the induction hypothesis for the lemma. Then we apply $\mathbf{Set_5}$ to get $t_1 \times t_1^k =_A t_2 \times t_2^k$; folding $\cdot^{k+1}$ on the last equality produces the desired proof.

Finally, if we prove $t_1 - t_3 =_A t_2 - t_4$ from $t_1 =_A t_2$ and $t_3 =_A t_4$ using $\mathbf{Set_5}$, we first find normal proofs of $t_1 =_A t_2$ and $t_3 =_A t_4$ (induction hypothesis), apply $\mathbf{Set_4}$ to the latter to get $-t_3 =_A -t_4$ and apply $\mathbf{Set_5}$ to get $t_1 + (-t_3) =_A t_2 + (-t_4)$, which is the desired equality with the definition of $-$ unfolded. □

Theorem 4.45 Let $t, t' : A$ and $e, e' : E$ be as in Theorem 4.36 and assume furthermore that there is a normal proof of the equality $t =_A t'$. Then $\mathcal{N}(e) = \mathcal{N}(e')$.

Proof. By induction on the length of the normal proof of $t =_A t'$.

If $t =_A t'$ is an instance of one of the axioms $\mathbf{Set_1}$, $\mathbf{SG}$, $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{G_1}$, $\mathbf{G_2}$, $\mathbf{AG}$ or $\mathbf{R_i}$ with $1 \leq i \leq 5$, then by Lemma 4.38 $\mathcal{N}(e) = \mathcal{N}(e')$.

Suppose $t =_A t'$ is proved by $\mathbf{Set_2}$ from $t' =_A t$. Then we can apply Lemma 4.39 and the induction hypothesis to conclude that the thesis holds.

Suppose $t =_A t'$ is proved by $\mathbf{Set_3}$ from $t =_A t_1$ and $t_1 =_A t'$. Then we can apply Lemma 4.40 and the induction hypothesis to conclude that the thesis holds.

Suppose $t =_A t'$ is proved from $t_1 =_A t_2$ by $\mathbf{Set_4}$ and f is not $\cdot^n$ with n closed. Then by Lemma 4.41 and the induction hypothesis the thesis holds.

Suppose $t =_A t'$ is proved from $t_1 =_A t_2$ and $t_3 =_A t_4$ by $\mathbf{Set_5}$ and f is not $-$. Then by Lemma 4.42 and the induction hypothesis the thesis holds.

If t_1 and t_2 can be obtained from t and t' by unfolding the definitions of $-$, $\cdot^n$ and zring, then by Lemma 4.37 $\mathit{lift}(t_1, \emptyset) = \mathit{lift}(t, \emptyset) = \langle e, \rho\rangle$ and $\mathit{lift}(t_2, \rho) = \mathit{lift}(t', \rho) = \langle e', \sigma\rangle$, hence the induction hypothesis immediately asserts the thesis. □

We are now ready to prove Theorem 4.36.

Proof.*(Completeness Theorem 4.36)* Assume there is a proof of $t =_A t'$. By Lemma 4.44 there is also a normal proof of $t =_A t'$, so by Theorem 4.45 $\mathcal{N}(e) = \mathcal{N}(e')$. □

5 Completeness of rational: groups

We now show how we can get a completeness theorem for groups similar to Theorem 4.36. We begin by observing that the theory developed above is not enough as is: if G is a group, $a : G$ and $v_0^0 \,]\!]_\rho\, a$, then $v_0^0 + v_0^0 \,]\!]_\rho\, a + a$, but $\mathcal{N}(v_0^0 + v_0^0) = v_0^0 \times 2 + 0$ which cannot be interpreted in G, so part (ii) of Lemma 4.26 fails to hold. Therefore we begin by extending the interpretation relation in a conservative way.

Definition 5.1 Let G be a group, $n : \mathbb{Z}$ and $a : G$. Then $n \cdot a$ is inductively defined as follows.

$$\begin{aligned} 0 \cdot a &:= 0 && (20)\\ (n+1)\cdot a &:= n\cdot a + a, \text{ for } n \geq 0 && (21)\\ (n-1)\cdot a &:= n \cdot a - a, \text{ for } n \leq 0 && (22)\end{aligned}$$

Proposition 5.2 Let R be a ring. Then, for all $n : \mathbb{Z}$ and $a : R$, $n \cdot a =_R \underline{n} \times a$ is provable.

Proof. Straightforward induction. If $n = 0$ then $n \cdot a = 0$ and $\underline{0} = 0$, so the equality reduces to $0 \times a =_R 0$, which is provable. Assume that $n \cdot a =_R \underline{n} \times a$ for $n \geq 0$; then $(n+1)\cdot a = n \cdot a + a =_R \underline{n} \times a + a =_R (\underline{n}+1) \times a = \underline{n+1} \times a$. Similarly, if $n \leq 0$ then $(n-1)\cdot a = n\cdot a - a =_R \underline{n} \times a - a =_R (\underline{n} - 1) \times a = \underline{n-1} \times a$. □

Lemma 5.3 Let ρ be a substitution pair for a ring A. The interpretation relation satisfies the following rule:

$$e \,]\!]_\rho\, t_1 \wedge n \cdot t_1 =_A t \quad\rightarrow\quad e \times n \,]\!]_\rho\, t$$

where $n : \mathbb{Z}$.

Proof. By the previous proposition $n \cdot t_1 =_A \underline{n} \times t_1$ is provable, whence $\underline{n} \times t_1 =_A t$ is provable by hypothesis, $\mathbf{Set_2}$ and $\mathbf{Set_3}$. Furthermore, $\underline{n} \,]\!]_\rho\, n$ by $\mathbf{Set_1}$ and (11). By hypothesis $e \,]\!]_\rho\, t_1$. Therefore, by (13), $e \times n \,]\!]_\rho\, t$. □

Hence, this clause can be added to the inductive definition of the interpretation relation without changing it when defined over a ring or field but extending it in the case of groups. We also need the case $k = 0$ of (11). That is, we consider the interpretation relation as defined in Definition 2.29 extended with the two following clauses.

$$\begin{aligned} 0 =_G t \quad&\rightarrow\quad 0 \,]\!]_\rho\, t && (23)\\ e \,]\!]_\rho\, t_1 \wedge n \cdot t_1 =_G t \quad&\rightarrow\quad e \times n \,]\!]_\rho\, t && (24)\end{aligned}$$

Notice that conditions (16) and (17) in Lemma (2.30) can be proved from these clauses, so that they also hold for groups with this extended interpretation relation. This allows us to prove the following version of Lemma 2.32.

Lemma 5.4 Let $e : E$, $t, t' : G$ and ρ be a substitution pair for G such that $e \rrbracket_\rho t$ and $e \rrbracket_\rho t'$. Then $t =_G t'$.

Proof. By induction on $\rrbracket_\rho$ (Coq checked). □

We can now prove the following results, which are group analogues of those proved in Subsection 4.2.

Lemma 5.5 Let G be a group and ρ be a substitution pair for G. The auxiliary normalization functions satisfy the following properties.

(i) if $m \rrbracket_\rho t$ then $m \cdot_{\mathrm{M}\mathbb{Z}} i \rrbracket_\rho i \cdot t$;

(ii) if $x \times m \rrbracket_\rho t$ then $m \cdot_{\mathrm{M}\mathbb{V}} x \rrbracket_\rho t$;

(iii) if $m \times m' \rrbracket_\rho t$ or $m' \times m \rrbracket_\rho t$ then $m \cdot_{\mathrm{MM}} m' \rrbracket_\rho t$;

(iv) if $m \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$ then $m +_{\mathrm{MM}} m' \rrbracket_\rho t + t'$;

(v) if $p \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$ then $p +_{\mathrm{PM}} m' \rrbracket_\rho t + t'$;

(vi) if $p \rrbracket_\rho t$ and $p' \rrbracket_\rho t'$ then $p +_{\mathrm{PP}} p' \rrbracket_\rho t + t'$;

(vii) if $p \times m' \rrbracket_\rho t$ or $m' \times p \rrbracket_\rho t$ then $p \cdot_{\mathrm{PM}} m' \rrbracket_\rho t$;

(viii) if $p \times p' \rrbracket_\rho t$ then $p \cdot_{\mathrm{PP}} p' \rrbracket_\rho t$.

Proof. By induction (Coq checked). □

Some of the hypotheses in the previous lemma may seem a bit strange. The problem is, we cannot say as before that "if $m \rrbracket_\rho t$ and $m' \rrbracket_\rho t'$ then $m \cdot_{\mathrm{MM}} m' \rrbracket_\rho t \times t'$" because in G there is no multiplication. Hence, we replace this by the equivalent (in a ring) form "if $m \times m' \rrbracket_\rho t$ then $m \cdot_{\mathrm{MM}} m' \rrbracket_\rho t$". However, this is still not enough, since $\cdot_{\mathrm{MM}}$ may switch the order of its arguments; hence the disjunction in the actual lemma, which in fact says that one of the arguments to $\cdot_{\mathrm{MM}}$ is an integer.

Similar remarks hold for $\cdot_{\mathrm{PM}}$. In the case of $\cdot_{\mathrm{M}\mathbb{V}}$ we already know that the second argument is a variable, so one of the clauses of the disjunction never holds and we can erase it. As for $\cdot_{\mathrm{PP}}$, it will only be called by $\mathcal{N}$ when a product appears in the original expression, which is clearly impossible if this is the result of lifting a term in G; it is however needed in the proof of the following lemma.

Lemma 5.6 Let $e : E$ and $t : G$. If $e \rrbracket_\rho t$ then $\mathcal{N}(e) \rrbracket_\rho t$.

Proof. By induction (Coq checked). Since products in expressions can now only be interpreted by means of (24), the stronger hypotheses in Lemma 5.5 are seen to be satisfied by analyzing the proof of $e \rrbracket_\rho t$. □

Corollary 5.7 Let $t, t' : G$ and define $\langle e, \rho\rangle = \mathit{lift}(t, \emptyset)$ and $\langle e', \sigma\rangle = \mathit{lift}(t', \rho)$. If $\mathcal{N}(e) = \mathcal{N}(e')$, then $t =_G t'$ can be proved from the group axioms and unfolding of the definition of $-$.

Proof. Let e and e' be as defined above and suppose that $\mathcal{N}(e) = \mathcal{N}(e')$. By Lemma 3.9, both $e \rrbracket_\rho t$ and $e' \rrbracket_\rho t'$. By Proposition 5.6 also $\mathcal{N}(e) \rrbracket_\rho t$ and $\mathcal{N}(e') \rrbracket_\rho t'$. Since $\mathcal{N}(e) = \mathcal{N}(e')$, we have that $\mathcal{N}(e) \rrbracket_\rho t$ and $\mathcal{N}(e) \rrbracket_\rho t'$, whence $t =_G t'$ by Lemma 5.4. □

THEOREM 5.8 Let $t, t' : G$ be such that the equality $t =_G t'$ can be proved only from the group axioms and unfolding of the definition of $-$. Define $\langle e, \rho\rangle = \mathit{lift}(t, \emptyset)$ and $\langle e', \sigma\rangle = \mathit{lift}(t', \rho)$. Then $\mathcal{N}(e) = \mathcal{N}(e')$.

PROOF. Immediate from Theorem 4.36, since the group axioms are a proper subset of the ring axioms. □

6 Partial completeness of **rational**: fields

We now try to extend the results in the previous sections to an arbitrary field structure A.

We begin by extending the type of normal forms and the normalization function.

DEFINITION 6.1 The set F of field expressions in normal form is the set $\{p/q|p, q \in P\}$.

DEFINITION 6.2 $+_{\mathrm{FF}}$ is defined as follows.

$$\begin{array}{rcl} +_{\mathrm{FF}} : F \times F & \to & F \\ e_1/e_2, f_1/f_2 & \mapsto & ((e_1 \cdot_{\mathrm{PP}} f_2) +_{\mathrm{PP}} (e_2 \cdot_{\mathrm{PP}} f_1))/(e_2 \cdot_{\mathrm{PP}} f_2) \end{array}$$

PROPOSITION 6.3 $+_{\mathrm{FF}}$ satisfies the following properties:

(i) $+_{\mathrm{FF}}$ is well defined;

(ii) if $p \,\rrbracket_\rho\, t$ and $q \,\rrbracket_\rho\, t'$, then $p +_{\mathrm{FF}} q \,\rrbracket_\rho\, t + t'$.

PROOF. Direct consequence of the definition of F and Propositions 4.20 and 4.24 (the second is Coq checked). □

DEFINITION 6.4 $\cdot_{\mathrm{FF}}$ is defined as follows.

$$\begin{array}{rcl} +_{\mathrm{FF}} : F \times F & \to & F \\ e_1/e_2, f_1/f_2 & \mapsto & (e_1 \cdot_{\mathrm{PP}} f_1)/(e_2 \cdot_{\mathrm{PP}} f_2) \end{array}$$

PROPOSITION 6.5 $\cdot_{\mathrm{FF}}$ satisfies the following properties:

(i) $\cdot_{\mathrm{FF}}$ is well defined;

(ii) if $p \,\rrbracket_\rho\, t$ and $q \,\rrbracket_\rho\, t'$, then $p \cdot_{\mathrm{FF}} q \,\rrbracket_\rho\, t \times t'$.

PROOF. Direct consequence of the definition of F and Proposition 4.24 (the second is Coq checked). □

DEFINITION 6.6 $/_{\mathrm{FF}}$ is defined as follows.

$$\begin{array}{rcl} /_{\mathrm{FF}} : F \times F & \to & F \\ e_1/e_2, f_1/f_2 & \mapsto & (e_1 \cdot_{\mathrm{PP}} f_2)/(e_2 \cdot_{\mathrm{PP}} f_1) \end{array}$$

PROPOSITION 6.7 $/_{\mathrm{FF}}$ satisfies the following properties:

(i) $/_{\mathrm{FF}}$ is well defined;

(ii) if $p \,\rrbracket_\rho\, t$ and $q \,\rrbracket_\rho\, t' \neq 0$, then $p/_{\mathrm{FF}}q \,\rrbracket_\rho\, t/t'$.

PROOF. Direct consequence of the definition of F and Propositions 4.20 and 4.24 (the second is Coq checked). □

Definition 6.8 The normalization function $\mathcal{N}_F$ is defined as follows.

$$\begin{array}{rcl}
\mathcal{N}_F : E & \to & P \\
i & \mapsto & i \\
v_i^0 & \mapsto & \left(v_i^0 \times 1 + 0\right)/1 \\
e + f & \mapsto & \mathcal{N}_F(e) +_{\mathrm{FF}} \mathcal{N}_F(f) \\
e \times f & \mapsto & \mathcal{N}_F(e) \cdot_{\mathrm{FF}} \mathcal{N}_F(f) \\
e/f & \mapsto & \mathcal{N}_F(e) /_{\mathrm{FF}} \mathcal{N}_F(f) \\
v_i^1(e) & \mapsto & \left(v_i^1(\mathcal{N}_F(e)) \times 1 + 0\right)/1
\end{array}$$

Proposition 6.9 $\mathcal{N}_F$ satisfies the following properties:

(i) $\mathcal{N}_F$ is well defined;

(ii) if $e \,]\!]_\rho\, t$ then $\mathcal{N}_F(e) \,]\!]_\rho\, t$.

Proof. As before, the first part is a straightforward induction, similar to the proof of Proposition 4.26.

The second property is proved by induction (Coq checked); notice that the hypothesis $e \,]\!]_\rho\, t$ is essential to guarantee that $\mathcal{N}_F$ will not introduce divisions by zero (compare with the situation for groups). □

6.1 Correctness and completeness

Unfortunately, rational as described above does not work so well with this normalization function as before, as the following (simple) example shows.

Example 6.10 Let $x : A$ be a variable such that $x \neq 0$. Then $x \times 1/x =_A 1$ is a special case of axiom **F**.

A simple calculation shows that

$$\begin{array}{rcl}
\mathit{lift}(x \times 1/x, \emptyset) & = & \langle v_0^0 \times 1/v_0^0, [v_0^0 := x]\rangle \\
\mathit{lift}(1, [v_0^0 := x]) & = & \langle 1, [v_0^0 := x]\rangle
\end{array}$$

but $\mathcal{N}_F(v_0^0 \times 1/v_0^0) = (v^0 \times 1 + 0)/(v^0 \times 1 + 0)$, while $\mathcal{N}_F(1) = 1$.

The problem lies in the algebraic structure of F with the operations above defined, and in trying to generalize the properties in Section 4.3. Although $\langle F, +_{\mathrm{FF}}, 0/1, \cdot_{\mathrm{FF}}, 1/1\rangle$ is a ring, it is not an integral domain: *any* expression of the form $0/e$ is an additive unit, and therefore F does not become a field when we add $/_{\mathrm{FF}}$ as a division operator.

The crux of the matter is that terms in F are not restricted to irreducible fractions (with the intuitive meaning of what "irreducible" should mean). Adding this restriction is also far from trivial: rewriting quotients of polynomials to irreducible fractions is known to be an extremely difficult problem, and implementing such an algorithm in $\mathcal{N}_F$ would make rational extremely slow.

Therefore, we will use a different approach. Going back to the example, it is easy to check that $\mathcal{N}_F(v_0^0 \times 1/v_0^0 - 1) = 0/(v_0^0 \times 1 + 0)$. Therefore, we will use the following modified version of rational for fields: instead of comparing the normal form of the two expressions e and f, we compute the normal form of $e - f$ and check that it has the form $0/e'$. This is correct.

Corollary 6.11 Let $t, t' : A$ and define $\langle e, \rho\rangle = \mathit{lift}(t, \emptyset)$ and $\langle e', \sigma\rangle = \mathit{lift}(t', \rho)$. If $\mathcal{N}_F(e - e') = 0/e''$, where e'' is an arbitrary expression, then $t =_A t'$ can be proved from the field axioms and unfolding of the definitions of $-$, zring and nexp.

Proof. Let e and e' be as defined above and suppose that $\mathcal{N}(e - e') = 0/e''$ for some e''. By Lemma 3.9, both $e \rrbracket_\rho t$ and $e' \rrbracket_\rho t'$. By Proposition 4.26 also $\mathcal{N}(e) \rrbracket_\rho t$ and $\mathcal{N}(e') \rrbracket_\rho t'$. Since $\mathcal{N}(e - e') = \mathcal{N}(e) +_{\mathrm{FF}} \mathcal{N}(e') \cdot_{\mathrm{FF}} (-1)$, Lemmas 6.3 and 6.5 together with (11) imply that $\mathcal{N}(e - e') \rrbracket_\rho t + t' \times -1$; but $\mathcal{N}(e - e') = 0/e''$, hence $0/e''$ can be interpreted, and therefore $0/e'' \rrbracket_\rho 0$ by (14) and (11). By Lemma 2.32 it then follows that $t + t' \times -1 =_A 0$, from which the thesis follows. □

The only drawback of this approach is that the completeness proof does not go through. A proof analogous to that of Theorem 4.36, obtained by replacing "$\mathcal{N}(e) = \mathcal{N}(e')$" with "$\mathcal{N}(e-e') = 0/e''$" everywhere, fails on the induction step for $\mathbf{Set_4}$, since the induction hypothesis will not be strong enough to prove an equivalent of Lemma 4.41. All other proofs can be adapted, though, thus yielding the following (partial) completeness result.

Theorem 6.12 Let $t, t' : A$ be such that the equality $t =_A t'$ can be proved only from the field axioms and unfolding of the definitions of $-$, zring and nexp in t and t', without using $\mathbf{Set_4}$ except for $-$ and $\cdot^n$ (n closed). Define $\langle e, \rho\rangle = \mathit{lift}(t, \emptyset)$ and $\langle e', \sigma\rangle = \mathit{lift}(t', \rho)$. Then $\mathcal{N}(e - e')$ has the form $0/e''$ for some expression e''.

Proof. Similar to the proof of Theorem 4.36. □

To see that the extra hypothesis is really needed, consider $f(x) =_A f(x/2 + x/2)$, which is clearly provable. Then

$$\begin{aligned}
\mathit{lift}(f(x), \emptyset) &= \langle v_0^1(v_0^0), \langle [v_0^0 := x], [v_0^1 := f]\rangle\rangle \\
\mathit{lift}(f(x/2 + x/2), \langle [v_0^0 := x], [v_0^1 := f]\rangle) &= \langle v_0^1(v_0^0/2 + v_0^0/2), \langle [v_0^0 := x], [v_0^1 := f]\rangle\rangle
\end{aligned}$$

and $\mathcal{N}_F(v_0^1(v_0^0) - v_0^1(v_0^0/2 + v_0^0/2)) = (v_0^1((v_0^0 \times 1 + 0)/1) \times 1 + v_0^1((v_0^0 \times 4 + 0)/4) \times (-1) + 0)/1 \neq 0$.

In practice, though, the difference in strength between Theorem 4.36 and Theorem 6.12 is not very serious. In most situations axiom $\mathbf{Set_4}$ is not needed, and in several where it is used rational still works (this will be the case whenever the hypothesis of this axiom can be proved just from the ring axioms). In particular, rational still works on goals like $f(x+x)/4 + f(2x)/4 = f(x+x+0)/2$, and this is usually enough. Throughout C-CoRN, less than five situations were found where this limitation of rational made an alternative proof necessary.

7 Remarks on the implementation

As mentioned in the Introduction, the theoretical treatment of rational we made considered a simplified version of the tactic. The actual implementation covers all the expressions considered in the type of setoids in C-CoRN, in particular binary functions and partial unary functions, the latter being implemented as functions of a setoid element and a proof term.

These extra cases pose no new difficulties. There is one new axiom $\mathbf{Set_4'}$, stating a similar version of $\mathbf{Set_4}$ for partial functions. The type of expressions needs to be extended with two new constructors for variables representing these functions, and the interpretation and lift must be adapted accordingly. As a consequence several new cases need to be considered when proving results about the order in which terms are lifted, but these can be treated in a similar way to the like cases for variables in $\mathbb{V}_1$ (unlike variables in $\mathbb{V}_0$, which behave differently). The completeness results for groups and rings still hold; as for fields, as would be expected, the hypothesis of Theorem 6.12 has to be strengthened since $\mathbf{Set_4'}$ and $\mathbf{Set_5}$ cannot be used either in the proof of $t = t'$.

8 Conclusions

In this paper we formally described rational and undertook a study of its behavior as a decision procedure. It was shown to be correct and complete for groups and rings, which is very useful information in interactive proof development, and correct and partially complete for fields, which is also very useful, as explained in Section 6.

Furthermore, we hope to use the completeness of rational to take the tactic a step further. By the completeness of the theory of fields we also know that for every equality $t = t'$ that cannot be proved from the axioms there is a field where $t \neq t'$ holds. We hope to use the information provided by rational upon failure (namely, an expression in normal form that does not equal zero) to construct such a model *within* Coq, thus reflecting completeness within the system.

Although rational is designed for Coq, we conducted this study at a level of abstraction that should make it easy to develop similar (partially) complete tactics for other proof assistants based on type theory. It is also possible that rational can be adapted to other systems.

Acknowledgments

The authors wish to thank Henk Barendregt and Herman Geuvers for their helpful suggestions and support.

This work was partially supported by the European Project IST-2001-33562 MoWGLI and by FCT and FEDER under POCTI, namely through CLC project FibLog FEDER POCTI / 2001 / MAT / 37239.

References

[1] Stuart F. Allen, Robert L. Constable, Douglas J. Howe, and William Aitken. The Semantics of Reflected Proof. In *Proceedings of the 5th Symposium on Logic in Computer Science*, pages 95–197, Philadelphia, Pennsylvania, June 1990. IEEE, IEEE Computer Society Press.

[2] C. C. Chang and H. Jerome Keisler. *Model Theory.* North-Holland, 1990.

[3] The Coq Development Team. *The Coq Proof Assistant Reference Manual*, April 2004. Version 8.0.

[4] L. Cruz-Filipe, H. Geuvers, and F. Wiedijk. C-CoRN: the Constructive Coq Repository at Nijmegen. In *MKM 2004*, LNCS. Springer Verlag, 2004. To appear.

[5] L. Cruz-Filipe and F. Wiedijk. Hierarchical Reflection. In *Theorem Proving in Higher Order Logics, 17th International Conference, TPHOLs 2004*, LNCS. Springer Verlag, 2004. To appear.

[6] H. Geuvers, R. Pollack, F. Wiedijk, and J. Zwanenburg. The Algebraic Hierarchy of the FTA Project. *Journal of Symbolic Computation, Special Issue on the Integration of Automated Reasoning and Computer Algebra Systems*, pages 271–286, 2002.

[7] H. Geuvers, F. Wiedijk, and J. Zwanenburg. Equational Reasoning via Partial Reflection. In M. Aagaard and J. Harrison, editors, *Theorem Proving in Higher Order Logics, 13th International Conference, TPHOLs 2000*, volume 1869 of *LNCS*, pages 162–178, Berlin, Heidelberg, New York, 2000. Springer Verlag.

A Proof of Equality (19)

Throughout this section, ξ is a (fixed) renaming of variables. We prove the following equality, valid for all $p, q : P$:

$$\mathcal{N}((p \star q)^{\xi}) = \mathcal{N}((p \star_{\mathrm{PP}} q)^{\xi}).$$

We will only deal with the case $\star = +$, since the case $\star = \times$ is similar. We prove this in a series of steps.

Lemma A.1 Let $m : M$ and $v_i^0 : \mathbb{V}_0$. Then $\mathcal{N}((m \cdot_{\mathrm{M}\mathbb{V}} v_i^0)^\xi) = \mathcal{N}(m^\xi) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi})$.

Proof. By induction on m. If $m \in \mathbb{Z}$, then trivially

$$\begin{aligned}
\mathcal{N}((m \cdot_{\mathrm{M}\mathbb{V}} v_i^0)^\xi) &= \mathcal{N}((v_i^0 \times m)^\xi) \\
&= \mathcal{N}(v_i^{0^\xi} \times m) \\
&= \mathcal{N}(v_i^{0^\xi}) \cdot_{\mathrm{PP}} \mathcal{N}(m) \\
&= \mathcal{N}(m) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi}) \\
&= \mathcal{N}(m \times v_i^{0^\xi}) \\
&= \mathcal{N}((m \times v_i^0)^\xi)
\end{aligned}$$

Suppose now that $m = v_j^0 \times e$. If $i \leq j$, the previous proof still holds replacing m with m^ξ in the third through sixth expression; else the following shows the equality.

$$\begin{aligned}
\mathcal{N}(((v_j^0 \times e) \cdot_{\mathrm{M}\mathbb{V}} v_i^0)^\xi) &= \mathcal{N}((v_j^0 \times (e \cdot_{\mathrm{M}\mathbb{V}} v_i^0))^\xi) \\
&= \mathcal{N}(v_j^{0^\xi}) \cdot_{\mathrm{PP}} \mathcal{N}((e \cdot_{\mathrm{M}\mathbb{V}} v_i^0)^\xi) \\
&\overset{IH}{=} \mathcal{N}(v_j^{0^\xi}) \cdot_{\mathrm{PP}} \left(\mathcal{N}(e^\xi) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi})\right) \\
&= \left(\mathcal{N}(v_j^{0^\xi}) \cdot_{\mathrm{PP}} \mathcal{N}(e^\xi)\right) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi}) \\
&= \mathcal{N}((v_j^0 \times e)^\xi) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi})
\end{aligned}$$

Finally, if $m = v_j^1(p) \times e$ then again the first argument holds. □

Lemma A.2 Let $m : M$, $v_i^1 : \mathbb{V}_1$ and $p : P$. Then $\mathcal{N}((m \cdot_{\mathrm{M}\mathbb{V}} v_i^1(p))^\xi) = \mathcal{N}(m^\xi) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^1(p)^\xi)$.

Proof. Analogous to the previous. □

Lemma A.3 Let $m_1, m_2 : M$ be such that $|m_1| = |m_2|$. Then $\mathcal{N}((m_1 +_{\mathrm{MM}} m_2)^\xi) = \mathcal{N}({m_1}^\xi) +_{\mathrm{PP}} \mathcal{N}({m_2}^\xi)$.

Proof. By induction on m_1.

If $m_1 = i \in \mathbb{Z}$, then also $m_2 = j \in \mathbb{Z}$ because $|m_1| = |m_2|$. Then both sides of the equality reduce to $i + j$.

If $m_1 = v_i^0 \times e$, then also $m_2 = v_i^0 \times e'$, whence

$$\begin{aligned}
\mathcal{N}((v_i^0 \times e +_{\mathrm{MM}} v_i^0 \times e')^\xi) &= \mathcal{N}(((e +_{\mathrm{MM}} e') \cdot_{\mathrm{M}\mathbb{V}} v_i^0)^\xi) \\
&\overset{\star}{=} \mathcal{N}((e +_{\mathrm{MM}} e')^\xi) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi}) \\
&\overset{IH}{=} \left(\mathcal{N}(e^\xi) +_{\mathrm{PP}} \mathcal{N}(e'^\xi)\right) \cdot_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi}) \\
&= \mathcal{N}(v_i^{0^\xi}) \cdot_{\mathrm{PP}} \mathcal{N}(e^\xi) +_{\mathrm{PP}} \mathcal{N}(v_i^{0^\xi}) \cdot_{\mathrm{PP}} \mathcal{N}(e'^\xi) \\
&= \mathcal{N}((v_i^0 \times e)^\xi) +_{\mathrm{PP}} \mathcal{N}((v_i^0 \times e')^\xi)
\end{aligned}$$

where $\star$ denotes application of Lemma A.1.

The case $m_1 = v_i^1(p) \times e$ is analogous resorting to Lemma A.2. □

Lemma A.4 Let $p : P$ and $m : M$. Then $\mathcal{N}((p +_{\mathrm{PM}} m)^\xi) = \mathcal{N}(p^\xi) +_{\mathrm{PP}} \mathcal{N}(m^\xi)$.

Proof. By induction on p and m.

Suppose $p = i \in \mathbb{Z}$. If $m = j \in \mathbb{Z}$, then both expressions reduce to $i + j$; else $\mathcal{N}((i +_{\mathrm{PM}} m)^\xi) = \mathcal{N}((m + i)^\xi) = \mathcal{N}(m^\xi) +_{\mathrm{PP}} \mathcal{N}(i^\xi) = \mathcal{N}(i^\xi) +_{\mathrm{PP}} \mathcal{N}(m^\xi)$.

Suppose now that $p = e_1 + e_2$. There are several cases to consider.

- if $m = i \in \mathbb{Z}$ or $|e_1| <_M |m|$, then

$$\begin{array}{rcl}
\mathcal{N}(((e_1 + e_2) +_{\mathrm{PM}} m)^{\xi}) & = & \mathcal{N}((e_1 + (e_2 +_{\mathrm{PM}} m))^{\xi}) \\
& = & \mathcal{N}({e_1}^{\xi}) +_{\mathrm{PP}} \mathcal{N}((e_2 +_{\mathrm{PM}} m)^{\xi}) \\
& \overset{IH}{=} & \mathcal{N}({e_1}^{\xi}) +_{\mathrm{PP}} \big(\mathcal{N}({e_2}^{\xi}) +_{\mathrm{PP}} \mathcal{N}(m^{\xi})\big) \\
& = & \big(\mathcal{N}({e_1}^{\xi}) +_{\mathrm{PP}} \mathcal{N}({e_2}^{\xi})\big) +_{\mathrm{PP}} \mathcal{N}(m^{\xi}) \\
& = & \mathcal{N}((e_1 + e_2)^{\xi}) +_{\mathrm{PP}} \mathcal{N}(m^{\xi})
\end{array}$$

- if $|e_1| = |m|$, then

$$\begin{array}{rcl}
\mathcal{N}(((e_1 + e_2) +_{\mathrm{PM}} m)^{\xi}) & = & \mathcal{N}((e_2 +_{\mathrm{PM}} (e_1 +_{\mathrm{MM}} m))^{\xi}) \\
& \overset{IH}{=} & \mathcal{N}({e_2}^{\xi}) +_{\mathrm{PP}} \mathcal{N}((e_1 +_{\mathrm{MM}} m)^{\xi}) \\
& \overset{\star}{=} & \mathcal{N}({e_2}^{\xi}) +_{\mathrm{PP}} \big(\mathcal{N}({e_1}^{\xi}) +_{\mathrm{PP}} \mathcal{N}(m^{\xi})\big) \\
& = & \big(\mathcal{N}({e_1}^{\xi}) +_{\mathrm{PP}} \mathcal{N}({e_2}^{\xi})\big) +_{\mathrm{PP}} \mathcal{N}(m^{\xi}) \\
& = & \mathcal{N}((e_1 + e_2)^{\xi}) +_{\mathrm{PP}} \mathcal{N}(m^{\xi})
\end{array}$$

  where $\star$ denotes application of Lemma A.3.

- if $|e_1| \geq_M |m|$, then

$$\begin{array}{rcl}
\mathcal{N}((p +_{\mathrm{PM}} m)^{\xi}) & = & \mathcal{N}((m + p)^{\xi}) \\
& = & \mathcal{N}(m^{\xi}) +_{\mathrm{PP}} \mathcal{N}(p^{\xi}) \\
& = & \mathcal{N}(p^{\xi}) +_{\mathrm{PP}} \mathcal{N}(m^{\xi})
\end{array}$$

□

Lemma A.5 Let $p, q : P$. Then $\mathcal{N}((p +_{\mathrm{PP}} q)^{\xi}) = \mathcal{N}(p^{\xi}) +_{\mathrm{PP}} \mathcal{N}(q^{\xi})$.

Proof. By induction on p. If $p = i \in \mathbb{Z}$ then $\mathcal{N}((i +_{\mathrm{PP}} q)^{\xi}) = \mathcal{N}((q +_{\mathrm{PM}} i)^{\xi}) = \mathcal{N}(q^{\xi}) +_{\mathrm{PP}} \mathcal{N}(i^{\xi}) = \mathcal{N}(i^{\xi}) +_{\mathrm{PP}} \mathcal{N}(q^{\xi})$ by Lemma A.4.

Finally, if $p = e_1 + e_2$ then the following reasoning proves the desired equality.

$$\begin{array}{rcl}
\mathcal{N}(((e_1 + e_2) +_{\mathrm{PP}} q)^{\xi}) & = & \mathcal{N}(((e_2 +_{\mathrm{PP}} q) +_{\mathrm{PM}} e_1)^{\xi}) \\
& \overset{\star}{=} & \mathcal{N}((e_2 +_{\mathrm{PP}} q)^{\xi}) +_{\mathrm{PP}} \mathcal{N}({e_1}^{\xi}) \\
& \overset{IH}{=} & \big(\mathcal{N}({e_2}^{\xi}) +_{\mathrm{PP}} \mathcal{N}(q^{\xi})\big) +_{\mathrm{PP}} \mathcal{N}({e_1}^{\xi}) \\
& = & \big(\mathcal{N}({e_1}^{\xi}) +_{\mathrm{PP}} \mathcal{N}({e_2}^{\xi})\big) +_{\mathrm{PP}} \mathcal{N}(q^{\xi}) \\
& = & \mathcal{N}((e_1 + e_2)^{\xi}) +_{\mathrm{PP}} \mathcal{N}(q^{\xi})
\end{array}$$

□

Corollary A.6 Let $p, q : P$. Then $\mathcal{N}((p +_{\mathrm{PP}} q)^{\xi}) = \mathcal{N}((p + q)^{\xi})$.

Proof. $\mathcal{N}((p + q)^{\xi}) = \mathcal{N}(p^{\xi}) +_{\mathrm{PP}} \mathcal{N}(q^{\xi})$, and by Lemma A.5 we are done. □