The initial meadows

Bethke, I.; Rodenburg, P.

Publication date
2008
Document Version
Final published version

The initial meadows

Inge Bethke and Piet Rodenburg

University of Amsterdam, Faculty of Science,

Section Theoretical Software Engineering (former Programming Research Group)

Abstract: A *meadow* is a commutative ring with an inverse operator satisfying $0^{-1} = 0$. We determine the initial algebra of the meadows of characteristic 0 and show that its word problem is decidable.

Keywords: data structures, specification languages, initial algebra semantics, word problem, decidability.

1. Introduction

A *field* is a fundamental algebraic structure with total operations of addition, subtraction and multiplication. Division, as the inverse of multiplication, is subjected to the restriction that every element has a multiplicative inverse—except 0. In a field, the rules hold which are familiar from the arithmetic of ordinary numbers. That is, fields can be specified by the axioms for commutative rings with identity element (CR, see Table 1), and the negative conditional formula

$$x \neq 0 \to x \cdot x^{-1} = 1.$$

The prototypical example is the field of rational numbers.

In Bergstra and Tucker (2007) the name *meadow* was proposed for commutative rings

$(x + y) + z$	$=$	$x + (y + z)$
$x + y$	$=$	$y + x$
$x + 0$	$=$	x
$x + (-x)$	$=$	0
$(x \cdot y) \cdot z$	$=$	$x \cdot (y \cdot z)$
$x \cdot y$	$=$	$y \cdot x$
$x \cdot 1$	$=$	x
$x \cdot (y + z)$	$=$	$x \cdot y + x \cdot z$

Table 1. Specification CR of commutative rings with multiplicative identity

(*Ref*)	$(x^{-1})^{-1}$	$=$	x
(*Ril*)	$x \cdot (x \cdot x^{-1})$	$=$	x

Table 2. Reflection and restricted inverses law

with a multiplicative identity element and a total operation $^{-1}$—inversion—governed by *reflection* and the *restricted inverse law*. We write Md for the set of axioms in Table 1 augmented by the additional equations in Table 2. In fact, Bergstra and Tucker (2007) requires in addition that $(-x)^{-1} = -x^{-1}$ and $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$. Those equations have been shown derivable from Md.

From the axioms in Md the following identities are derivable (cf. Bergstra et al. (2007), Bergstra et al. (2008)).

$$\begin{aligned} 0^{-1} &= 0 \\ (-x)^{-1} &= -(x^{-1}) \\ (x \cdot y)^{-1} &= x^{-1} \cdot y^{-1} \\ x \cdot 0 &= 0 \\ x \cdot -y &= -(x \cdot y) \\ -(-x) &= x \end{aligned}$$

One can also e.g. show that a meadow has no nonzero nilpotent elements: Suppose $x \cdot x = 0$. Then

$$x = x \cdot (x \cdot x^{-1}) = (x \cdot x) \cdot x^{-1} = 0 \cdot x^{-1} = x^{-1} \cdot 0 = 0.$$

Fields are meadows if we complete the inversion operation by $0^{-1} = 0$. The result is called a *zero-totalized field*.

When abstract data types are specified algebraically, the *initial algebra* is often taken as the meaning of the specification. The initial algebra always exists, is unique up to isomorphism, and can be constructed from the closed term algebra by dividing out over provable equality. Some references to universal algebra and initial algebra semantics are e.g. Goguen et al. (1977), Grätzer (1977), McKenzie et al. (1987) and Wechler (1992).

The initial meadows of finite characteristic $k > 0$ have been described already: in Bergstra et al. (2007) it is proved that k must be squarefree and that the initial meadow of charateristic k has $p_1 \cdots p_n$ elements, where $p_1, \ldots, p_n$ are the distinct prime factors of k. It then follows from Corollary 2.9 in Bethke and Rodenburg (2007) that the initial meadow is isomorphic with $\mathbb{G}_{p_1} \times \cdots \times \mathbb{G}_{p_n}$ where $\mathbb{G}_{p_i}$ is the prime field of order p_i.

In this paper we represent the initial meadow of characteristic 0 as the minimal subalgebra of the direct product of all finite prime fields and show that its word problem is decidable. Theorem 2.3 stems from a suggestion made by Yoram Hirshfeld, Tel Aviv University, in a private communication. The decidability result is a rigorous elaboration of a remark made in Bergstra and Tucker (2007)—in the proof of Corollary 5.11—and can be read between the lines in their Section 5.

2. The initial meadow of characteristic 0

In this section we shall show that the initial meadow is a proper subdirect product of all prime fields.

Definition 2.1 1 A *subdirect embedding* of a meadow M in a family $(M_j)_{j\in J}$ of meadows is a family $(\phi_j : M \twoheadrightarrow M_j)_{j\in J}$ of surjective homomorphisms such that for any distinct $x, y \in M$ there exists $j \in J$ such that $\phi_j(x) \neq \phi_j(y)$.

2 We say M is a *subdirect product* of $(M_j)_{j\in J}$ if $M \subseteq \Pi_{j\in J} M_j$ and the restricted projections $M \to M_j$ form a subdirect embedding of M.

3 A meadow M is called *subdirectly irreducible* when every subdirect embedding of M contains an isomorphism.

Loosely speaking, this means that a meadow is subdirectly irreducible when it cannot be represented as a subdirect product of "smaller" meadows, i.e. proper epimorphic images. An instance of Birkhoff's Subdirect Decomposition Theorem (see Birkhoff (1944) and Birkhoff (1991)) states

1 *Every meadow is isomorphic with a subdirect product of subdirectly irreducible meadows.*

If we forget the multiplicative identity element and the inversion operation in a given meadow, what remains is a commutative ring satisfying

$\exists x \forall y$	$x \cdot y$	$=$	y,
$\forall x \exists y$	$x \cdot x \cdot y$	$=$	x,

a commutative *regular ring* in the sense of Von Neumann (see Goodearl (1979)). It is not hard to see that the x in the first formula is unique, and it is shown in Bergstra et al. (2007) and Bergstra et al. (2008) that for any x, there is a unique y such that both $x \cdot x \cdot y = x$ and $y \cdot y \cdot x = y$. So a commutative regular ring determines a unique meadow, and vice versa. Since $x^{-1} = x^{-1} \cdot x^{-1} \cdot x$, the ideals of a meadow are closed under inversion, so that in meadows, as in rings, ideals correspond completely to congruence relations. As a consequence, the lattice of congruence relations of the ring reduct of a meadow coincides with the lattice of congruence relations of the meadow. We may therefore restate Lemma 2 of Birkhoff (1944) as follows:

2 *A subdirectly irreducible meadow is a zero-totalized field.*

Combining (1) and (2), we have that the initial meadow lies subdirectly embedded in a product of subdirectly irreducible zero-totalized fields. We may assume that every factor occurs only once—we still have a representation if we remove doubles. All factors are minimal, since they are homomorphic images of a minimal algebra. The minimal zero-totalized fields are the prime fields $\mathbb{G}_p$, p a prime number, and $\mathbb{Q}$, the rational numbers.

Lemma 2.2
Let A be the minimal subalgebra of the direct product $\mathbb{G} := \prod_{p \text{ prime}} \mathbb{G}_p$. Let Z_p be the element of $\mathbb{G}$ that is 0 in all coordinates except p, where it is 1. Then

1 *$Z_p \in A$,*
2 *the direct sum $\sum_{p \text{ prime}} \mathbb{G}_p$ lies embedded as an ideal in A, and*
3 *if we identify $\sum_{p \text{ prime}} \mathbb{G}_p$ with its image in A, $A/\sum_{p \text{ prime}} \mathbb{G}_p \cong \mathbb{Q}$.*

Proof. (1) Z_p is the denotation of the ground term $1 - \underline{p} \cdot \underline{p}^{-1}$, where $\underline{p}$ stands for the ground term $1 + \cdots + 1$, with p occurrences of 1.
(2) Modulo isomorphism, $\sum_{p \text{ prime}} \mathbb{G}_p$ is the ideal of A generated by the Z_p's. If we multiply an element of this ideal with any element of $\mathbb{G}$, the result is almost everywhere zero, and therefore belongs to the ideal.
(3) $A/\sum_{p \text{ prime}} \mathbb{G}_p$ is a minimal meadow of characteristic 0 that satisfies the equations $\underline{n} \cdot \underline{n}^{-1} = 1$, for all positive integers n. So by Theorem 3.1 of Bergstra and Tucker (2007), $A/\sum_{p \text{ prime}} \mathbb{G}_p$ is a homomorphic image of $\mathbb{Q}$; since $\mathbb{Q}$ has no proper ideals, the homomorphism must be injective. □

Theorem 2.3
The minimal subalgebra of $\prod_{p \text{ prime}} \mathbb{G}_p$ is an initial object in the category of meadows.

Proof. From the observations above, it appears that the initial meadow is the minimal subalgebra of the direct product of a set $\mathcal{G}$ of zero-totalized minimal fields. It is easily seen that every prime field $\mathbb{G}_p$ must be in $\mathcal{G}$, otherwise there is no nontrivial homomorphism from a subalgebra of $\prod \mathcal{G}$ into $\mathbb{G}_p$. So if $\mathbb{Q} \notin \mathcal{G}$, the initial meadow is the algebra A of the previous lemma. On the other hand, if $\mathbb{Q} \in \mathcal{G}$, by (3) of the lemma we have a surjective homomorphism $h : A \to \mathbb{Q}$. Then $(1, h) : A \to A \times \mathbb{Q}$ shows that A must be isomorphic to the minimal subalgebra of $\prod \mathcal{G}$. □

The initial meadow is countable, whereas the product of all finite prime fields is uncountable. This cardinality consideration shows that the initial algebra is properly contained in the product, and is—in contrast to the finite initial meadows—not a product of fields.

3. Decidability of the closed word problem

The main result of this section is a rigorous description of normal forms for closed meadow terms. To be precise, we shall prove that every closed meadow term t is provably equal to a term of the form

$$\Sigma_{i=0}^{\psi(t)-1} Z_i \cdot \phi_i(t) + G_{\psi(t)} \cdot \phi(t)$$

where ϕ_i interprets t in the Galois field with order p_i (the i-th prime), ϕ is its interpretation in the rational numbers, Z_i and G_i select significant models, and $\psi(t)$ is an effective upper bound. This is Proposition 3.14. From this it follows immediately , that the closed word problem for meadows is decidable.

We denote by $\mathbb{N}$ the set of natural numbers; Ter_{Md} denotes the set of closed meadow terms.

Definition 3.1 1 We define the set of *numerals* $\mathbb{N}_{Md} \subseteq Ter_{Md}$ by

$$\mathbb{N}_{Md} = \{\underline{n} \mid n \in \mathbb{N}\}$$

where for $n \in \mathbb{N}$, $\underline{n}$ is defined inductively as follows:

(a)$\underline{0} = 0$,

(b)$\underline{n+1} = \underline{n} + 1$.

2 We define the set of *normal rational terms* $\mathbb{Q}_{Md} \subseteq Ter_{Md}$ by

$$\mathbb{Q}_{Md} = \{0\} \cup \{\underline{n} \cdot \underline{m}^{-1}, -(\underline{n} \cdot \underline{m}^{-1}) \mid n, m \in \mathbb{N} \;\&\; n, m > 0 \;\&\; gcd(n, m) = 1\}$$

For $t \in \mathbb{Q}_{Md}$, we denote by $|t|$ the corresponding irreducible fraction in $\mathbb{Q}$.

Observe that $\underline{\ }$ respects addition, multiplication and subtraction, i.e., $Md \vdash \underline{n} + \underline{m} = \underline{n+m}$, $Md \vdash \underline{n} \cdot \underline{m} = \underline{nm}$ and if $m < n$, then $Md \vdash \underline{n} - \underline{m} = \underline{n-m}$.

We now assign to every closed term a normal rational term.

Definition 3.2 We define $\phi : Ter_{Md} \to \mathbb{Q}_{Md}$ inductively as follows.

1 $\phi(0) = 0$, $\phi(1) = \underline{1} \cdot \underline{1}^{-1}$,

2
$$\phi(-t) = \begin{cases} 0 & \text{if } \phi(t) = 0, \\ -(\underline{n} \cdot \underline{m}^{-1}) & \text{if } \phi(t) = \underline{n} \cdot \underline{m}^{-1}, \\ \underline{n} \cdot \underline{m}^{-1} & \text{if } \phi(t) = -(\underline{n} \cdot \underline{m}^{-1}). \end{cases}$$

3
$$\phi(t^{-1}) = \begin{cases} 0 & \text{if } \phi(t) = 0, \\ \underline{n} \cdot \underline{m}^{-1} & \text{if } \phi(t) = \underline{m} \cdot \underline{n}^{-1}, \\ -(\underline{n} \cdot \underline{m}^{-1}) & \text{if } \phi(t) = -(\underline{m} \cdot \underline{n}^{-1}). \end{cases}$$

4
$$\phi(t + t') = \begin{cases} 0 & \text{if } |\phi(t)| + |\phi(t')| = 0, \\ \underline{n} \cdot \underline{m}^{-1} & \text{if } 0 < |\phi(t)| + |\phi(t')| = \frac{n}{m},\ n, m > 0 \text{ and } gcd(n, m) = 1, \\ -(\underline{n} \cdot \underline{m}^{-1}) & \text{if } 0 > |\phi(t)| + |\phi(t')| = -\frac{n}{m},\ n, m > 0 \text{ and } gcd(n, m) = 1. \end{cases}$$

5
$$\phi(t \cdot t') = \begin{cases} 0 & \text{if } |\phi(t)||\phi(t')| = 0, \\ \underline{n} \cdot \underline{m}^{-1} & \text{if } 0 < |\phi(t)||\phi(t')| = \frac{n}{m},\ n, m > 0 \text{ and } gcd(n, m) = 1, \\ -(\underline{n} \cdot \underline{m}^{-1}) & \text{if } 0 > |\phi(t)||\phi(t')| = -\frac{n}{m},\ n, m > 0 \text{ and } gcd(n, m) = 1. \end{cases}$$

Observe that ϕ assigns to provably equal terms syntactically identical normal rational terms.

Proposition 3.3
For $s, t \in Ter_{Md}$,

$$Md \vdash s = t \Rightarrow \phi(s) = \phi(t).$$

Proof. Clearly, $|\phi(s)|$ is the interpretation of any closed term s in $\mathbb{Q}$. Thus, if $s = t$ is derivable, then $|\phi(s)| = |\phi(t)|$, and hence $\phi(s) = \phi(t)$. □

We can also evaluate closed meadow terms in a finite prime field $\mathbb{G}$. We may think of such a field as the ring with the elements $0, 1, 2, \ldots, p-1$, where arithmetic is performed modulo p. We let $(p_n)_{n\in\mathbb{N}}$ be an enumeration of the primes in increasing order, starting with $p_0 = 2$, and denote by $\mathbb{G}_n$ the prime field of order p_n.

Definition 3.4 1 For $n \in \mathbb{N}$, define $\mathbb{G}_{n,Md} \subseteq \mathbb{N}_{Md}$ by

$$\mathbb{G}_{n,Md} = \{\underline{i} \mid i < p_n\}.$$

2 For $n \in \mathbb{N}$, define the evaluation $\phi_n : Ter_{Md} \to \mathbb{G}_{n,Md}$ inductively by

(a)$\phi_n(0) = 0$, $\phi_n(1) = \underline{1}$,
(b)$\phi_n(-t) = \underline{-|\phi_n(t)| \ mod \ p_n}$,
(c)

$$\phi_n(t^{-1}) = \begin{cases} 0 & \text{if } |\phi_n(t)| = 0 \ mod \ p_n \\ \underline{l} & \text{otherwise, where } 0 < l < p_n \text{ and } l|\phi_n(t)| = 1 \ mod \ p_n, \end{cases}$$

(d)for $\diamond \in \{+, \cdot\}$, $\phi_n(t \diamond t') = \underline{(|\phi_n(t)| \diamond |\phi_n(t')|) \ mod \ p_n}$.

Here we denote by $|\phi_n(t)|$ the corresponding natural number.

Proposition 3.5
For $s, t \in Ter_{Md}$ and $n \in \mathbb{N}$,

$$Md \vdash s = t \Rightarrow \phi_n(s) = \phi_n(t).$$

Proof. Similar to Proposition 3.3. □

We now define terms Z_n which equal 0 in any Galois field $\mathbb{G}_m$ with $m \neq n$, and equal 1 in $\mathbb{G}_n$.

Definition 3.6 For $n \in \mathbb{N}$, define $Z_n = 1 - \underline{p_n} \cdot \underline{p_n}^{-1}$.

Lemma 3.7
For all $n, m \in \mathbb{N}$,

1 $Md \vdash Z_n \cdot Z_n = Z_n$,
2 $Md \vdash Z_n^{-1} = Z_n$, *and*
3 *if $n \neq m$, then $Md \vdash Z_n \cdot Z_m = 0$.*

Proof. Cf. Bergstra and Tucker (2007). □

Lemma 3.8
For all $n, m \in \mathbb{N}$,

1 $Md \vdash Z_n \cdot \underline{m} = Z_n \cdot \underline{m \ mod \ p_n}$,
2 $Md \vdash Z_n \cdot -\underline{m} = Z_n \cdot \underline{-m \mod p_n}$, *and*
3 $Md \vdash Z_n \cdot \underline{m}^{-1} = Z_n \cdot \underline{l}$ *where $l = 0$ if $m = 0$, or $0 < l < p_n$ and $lm = 1 \ mod \ p_n$ otherwise.*

Proof. Suppose $m = kp_n + l$ with $0 \leq l < p_n$. Then

$$\begin{aligned} Z_n \cdot \underline{m} &= Z_n \cdot \underline{kp_n + l} \\ &= Z_n \cdot (\underline{kp_n} + \underline{l}) \\ &= \underline{kp_n} - \underline{p_n} \cdot \underline{p_n}^{-1} \cdot \underline{kp_n} + Z_n \cdot \underline{m \ mod \ p_n} \\ &= \underline{kp_n} - \underline{p_n} \cdot \underline{p_n} \cdot \underline{p_n}^{-1} \cdot \underline{k} + Z_n \cdot \underline{m \ mod \ p_n} \\ &= \underline{kp_n} - \underline{kp_n} + Z_n \cdot \underline{m \ mod \ p_n} \\ &= Z_n \cdot \underline{m \ mod \ p_n} \end{aligned}$$

This proves (1). For (2) observe that

$$\begin{aligned} Z_n \cdot \underline{-m \mod p_n} &= Z_n \cdot \underline{p_n - (m \ mod \ p_n)} \\ &= Z_n \cdot \underline{p_n} - Z_n \cdot \underline{m \ mod \ p_n} \\ &= -Z_n \cdot \underline{m} \qquad \text{by (1)} \\ &= Z_n \cdot -\underline{m} \end{aligned}$$

In order to prove (3) we apply Lemma 2.3 of Bergstra and Tucker (2007), i.e.

$$Md \vdash u \cdot x \cdot y = u \Rightarrow Md \vdash u \cdot x \cdot x^{-1} = u.$$

Assume that $ml = 1 \ mod \ p_n$. Then

$$\begin{aligned} Z_n \cdot \underline{l} &= Z_n \cdot \underline{1} \cdot \underline{l} \\ &= Z_n \cdot \underline{lm} \cdot \underline{l} && \text{by the assumption and (1)} \\ &= (Z_n \cdot \underline{l}) \cdot (Z_n \cdot \underline{l}) \cdot (Z_n \cdot \underline{m}) && \text{by 3.7.1.} \end{aligned}$$

Thus

$$\begin{aligned} Z_n \cdot \underline{l} &= (Z_n \cdot \underline{l}) \cdot (Z_n \cdot \underline{m}) \cdot (Z_n \cdot \underline{m})^{-1} && \text{by the lemma} \\ &= Z_n \cdot \underline{lm} \cdot (Z_n \cdot \underline{m})^{-1} \\ &= Z_n \cdot \underline{m}^{-1} \end{aligned}$$

□

Proposition 3.9
For all $n \in \mathbb{N}$ and $t \in Ter_{Md}$,

$$Md \vdash Z_n \cdot t = Z_n \cdot \phi_n(t).$$

Proof. This follows by structural induction from the previous lemma. □

In addition to the terms Z_n, we can define terms G_n such that for all n, G_{n+1} equals 0 in any Galois field with characteristic p_n or less; in any field of characteristic 0, however, and in particular, in the zero-totalized field of the rational numbers, every G_n equals 1.

Definition 3.10 For $n \in \mathbb{N}$, define $G_n \in Ter_{Md}$ inductively as follows:

1 $G_0 = 1$,
2 $G_{n+1} = G_n \cdot (1 - Z_n)$.

Observe that

$$Md \vdash G_{n+1} = G_n \cdot \underline{p_n} \cdot \underline{p_n}^{-1}.$$

Lemma 3.11
For all $n, m \in \mathbb{N}$ we have

1 $Md \vdash G_n = 1 - Z_0 - \cdots - Z_{n-1}$,
2 $Md \vdash G_n \cdot Z_n = Z_n$,
3 $Md \vdash G_n = G_n^{-1}$,
4 $n \leq m \Rightarrow Md \vdash G_m = G_m \cdot G_n$, *and*
5 *if* $0 < k < p_n$, *then* $Md \vdash G_n \cdot \underline{k} \cdot \underline{k}^{-1} = G_n$.

Proof. Exercise. For (5) observe that if $0 < k < p_n$, then every prime factor of k is a factor of G_n. □

Clearly, we do not have in general

$$Md \vdash G_n \cdot t = G_n \cdot \phi(t).$$

However, we can determine a lower bound in terms of t such that this equation is provable in Md for every n exceeding this bound.

Definition 3.12 We define $\psi : Ter_{Md} \to \mathbb{N}$ inductively as follows.

1 $\psi(0) = 0 = \psi(1)$,
2 $\psi(-t) = \psi(t)$,
3 $\psi(t^{-1}) = \psi(t)$,
4
$$\psi(t + t') = \begin{cases} max\{\psi(t), \psi(t')\} & \text{if } \phi(t) = 0 \text{ or } \phi(t') = 0, \\ i & \text{if } |\phi(t)| = \pm\frac{n}{m} \text{ and } |\phi(t')| = \pm\frac{k}{l} \end{cases}$$
where i is the least natural number such that $p_i > m, l$,
5 $\psi(t \cdot t') = max\{\psi(t), \psi(t')\}$

Proposition 3.13
For each $t \in Ter_{Md}$ and $\psi(t) \leq n \in \mathbb{N}$

$$Md \vdash G_n \cdot t = G_n \cdot \phi(t).$$

Proof. It suffices to prove

$$Md \vdash G_{\psi(t)} \cdot t = G_{\psi(t)} \cdot \phi(t)$$

by Lemma 3.11.4. We employ structural induction. The base cases are trivial. In the induction step the cases for inversion and multiplication follow from Lemma 3.11.3 - 4, and the case for $-t$ from the fact that $Md \vdash \phi(-t) = -\phi(t)$ and $\psi(-t) = \psi(t)$. For addition, let $t = r + s$ and assume that

$$Md \vdash G_{\psi(r)} \cdot r = G_{\psi(r)} \cdot \phi(r) \text{ and } Md \vdash G_{\psi(s)} \cdot s = G_{\psi(s)} \cdot \phi(s)$$

Now we distinguish 2 cases.

1 $\phi(r) = 0$ or $\phi(s) = 0$: Then $Md \vdash \phi(r+s) = \phi(r)+\phi(s)$ and $\psi(r+s) = max\{\psi(r), \psi(s)\}$.

Thus

$$\begin{array}{lcll} Md \vdash G_{\psi(r+s)} \cdot (r+s) & = & G_{\psi(r+s)} \cdot r + G_{\psi(r+s)} \cdot s & \\ & = & G_{\psi(r+s)} \cdot G_{\psi(r)} \cdot r + G_{\psi(r+s)} \cdot G_{\psi(s)} \cdot s & \text{by 3.11.4} \\ & = & G_{\psi(r+s)} \cdot G_{\psi(r)} \cdot \phi(r) + G_{\psi(r+s)} \cdot G_{\psi(s)} \cdot \phi(s) & \\ & = & G_{\psi(r+s)} \cdot \phi(r) + G_{\psi(r+s)} \cdot \phi(s) & \\ & = & G_{\psi(r+s)} \cdot (\phi(r) + \phi(s)) & \\ & = & G_{\psi(r+s)} \cdot \phi(r+s) & \end{array}$$

2 $|\phi(r)| = \pm\frac{n}{m}$ and $|\phi(s)| = \pm\frac{k}{l}$: We consider the case that $\phi(r) = \underline{n} \cdot \underline{m}^{-1}$ and $\phi(s) = \underline{k} \cdot \underline{l}^{-1}$. First observe that since $p_{\psi(r+s)} > m, l$, $p_{\psi(r+s)}$ exceeds every common prime factor of ml and $nl + km$. Thus

$$\begin{array}{lcll} Md \vdash G_{\psi(r+s)} \cdot (r+s) & = & G_{\psi(r+s)} \cdot r + G_{\psi(r+s)} \cdot s & \\ & = & G_{\psi(r+s)} \cdot \underline{n} \cdot \underline{m}^{-1} + G_{\psi(r+s)} \cdot \underline{k} \cdot \underline{l}^{-1} & \\ & = & G_{\psi(r+s)} \cdot \underline{l} \cdot \underline{l}^{-1} \cdot \underline{n} \cdot \underline{m}^{-1} + G_{\psi(r+s)} \cdot \underline{m} \cdot \underline{m}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1} & \text{by 3.11.5} \\ & = & G_{\psi(r+s)} \cdot (\underline{l} \cdot \underline{n} + \underline{m} \cdot \underline{k}) \cdot (\underline{m} \cdot \underline{l})^{-1} & \\ & = & G_{\psi(r+s)} \cdot \underline{ln + mk} \cdot \underline{ml}^{-1} & \\ & = & G_{\psi(r+s)} \cdot \phi(r+s) & \end{array}$$

by repeated removal of shared prime factors using again 3.11.5. The remaining 3 cases follow by a similar argument taking in addition the sign into account. □

We are now able to determine for every closed meadow term the normal form mentioned in the beginning of this section.

Proposition 3.14
For each $t \in Ter_{Md}$,

$$Md \vdash t = \Sigma_{i=0}^{\psi(t)-1} Z_i \cdot \phi_i(t) + G_{\psi(t)} \cdot \phi(t).$$

Proof. First observe that $(*)$

$$\begin{array}{lcll} G_n \cdot t & = & (Z_n + (1 - Z_n)) \cdot G_n \cdot t & \\ & = & Z_n \cdot G_n \cdot t + (1 - Z_n) \cdot G_n \cdot t & \\ & = & Z_n \cdot G_n \cdot t + G_{n+1} \cdot t & \\ & = & G_n \cdot Z_n \cdot \phi_n(t) + G_{n+1} \cdot t & \text{by Proposition 3.9} \\ & = & Z_n \cdot \phi_n(t) + G_{n+1} \cdot t & \text{by Lemma 3.11.2.} \end{array}$$

We therefore can expand t as follows:

$$\begin{array}{lcll} t & = & G_0 \cdot t & \\ & = & Z_0 \cdot \phi_0(t) + G_1 \cdot t & \\ & \vdots & & \\ & = & Z_0 \cdot \phi_0(t) + \cdots + Z_{\psi(t)-1} \cdot \phi_{\psi(t)-1}(t) + G_{\psi(t)} \cdot t & \text{by repeated use of } (*) \\ & = & Z_0 \cdot \phi_0(t) + \cdots + Z_{\psi(t)-1} \cdot \phi_{\psi(t)-1}(t) + G_{\psi(t)} \cdot \phi(t) & \text{by the previous proposition.} \end{array}$$

□

Proposition 3.15
For each $t \in Ter_{Md}$ *and* $\psi(t) \leq n \in \mathbb{N}$,

$$Md \vdash t = \Sigma_{i=0}^{n-1} Z_i \cdot \phi_i(t) + G_n \cdot \phi(t).$$

Proof. By expanding t as far as necessary and Proposition 3.13 . □

Theorem 3.16
For all $s, t \in Ter_{Md}$,

$$Md \vdash s = t \Leftrightarrow \text{ for all } i \leq max\{\psi(s), \psi(t)\} - 1 \;\; \phi_i(s) = \phi_i(t) \;\&\; \phi(s) = \phi(t)$$

Proof. Left to right follows from Propositions 3.3 and 3.5. For the reverse direction apply the previous proposition. □

Corollary 3.17
The closed word problem for meadows is decidable.

In Bergstra and Tucker (2007) it is proved that the closed equational theories of zero-totalized fields and of meadows coincide. Thus decidability of the closed word problem for meadows carries over to zero-totalized fields.

Corollary 3.18
The closed word problem for zero-totalized fields is decidable.

4. Conclusion

We have represented the initial meadows as follows:

1 the initial meadow of characteristic 0 is the minimal submeadow of the direct product of all finite prime fields—it is a proper submeadow and not a product of fields—and
2 the initial meadow of characteristic $k > 0$ is $\prod_{p \text{ with } p|k} \mathbb{G}_p$.

This gives a clear picture of the finite and infinite initial objects in the categories of meadows.

The finite initial meadows are decidable and so is the infinite one. The open word problem, however, remains open. In particular, it is not known whether there exists a finite Knuth-Bendix completion of the specification of meadows.

Acknowledgement

This work was partly supported by The Netherlands Organisation for Scientific Research (NWO) under grant 638.003.611.

References

Bergstra, J.A., Hirshfeld,Y. and Tucker, J.V. (2007). *Meadows*, report PRG0705, (available from `www.science.uva.nl/research/prog/publications.html`).

Bergstra, J.A., Hirshfeld,Y. and Tucker, J.V. (2008). Fields, meadows and abstract data types. In *Pillars of Computer Science, Essays Dedicated to Boris (Boaz) Trakhtenbrot on the Occasion of His 85th Birthday*, A. Avron et al (eds.), Lecture Notes in Computer Science 4800, Springer-Verlag, New York, 166–178.

Bergstra, J.A. and Tucker, J.V. (2007). The Rational Numbers as an Abstract Data Type. *Journal of the ACM*, 54(2).

Bethke, I. and Rodenburg, P. (2007). *Some properties of finite meadows*, CoRR abs/0712.0917.

Birkhoff, G. (1944). Subdirect unions in universal algebra. *Bull. Amer. Math. Soc.*, 50(10):764–768.

Birkhoff, G. (1991). *Lattice Theory*, American Mathematical Society Colloquium Publications, Volume 25.

Goguen, J.A., Thatcher, J.W., Wagner,E.G. and Wright, J.B. (1977) Initial algebra semantics and continuous algebras. *Journal of the ACM*, 24(1):68–95.

Goodearl, K.R. (1979). *Von Neumann Regular Rings*, Pitman, London, San-Francisco, Melbourne.

Grätzer, G. (1979). *Universal Algebra* (2nd ed.), Springer-Verlag.

McKenzie, R.N., Mc Nulty, G.F. and Taylor, W.F. (1987). *Algebras, lattices, varieties*, Wadsworth & Brooks, Monterey, California.

Wechler, W. (1992). *Universal Algebra for Computer Scientists*. EATCS Monographs in Computer Science. Springer-Verlag.