The Initial meadows

Bethke, I.; Rodenburg, P.

Published in:
Journal of Symbolic Logic

DOI:
10.2178/jsl/1278682205

Citation for published version (APA):
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 prove a normal form theorem for it. As an immediate consequence we obtain the decidability of the closed term problem for meadows and the computability of their initial object.

§1. Introduction. Equations are much more easily handled by computers than their Boolean combinations. That is why there are successful theorem provers such as e.g., Waldmeister and Prover9, that can materially contribute to the understanding of equational theories. We suppose that there is some relation with the theoretical fact that all models of a given equational theory are homomorphic images of a suitable free algebra, and in particular that the minimal algebras are images of the initial algebra. A theory that is obviously liable to improvement in this respect, is the theory of fields.

A field is a fundamental algebraic structure with total operations of addition, subtraction and multiplication in which every element except 0 has a multiplicative inverse. 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

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

The prototypical example is the field of rational numbers.

In Bergstra and Tucker [3] the name meadow was proposed for commutative rings with a multiplicative identity element and a total inversion operation 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 [3] require in addition that $(−x)^{-1} = −x^{-1}$ and $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$. These equations have been shown derivable from $Md$.

From the axioms in $Md$ the following identities are derivable (cf. Bergstra et al. [1, 2]):

$$0^{-1} = 0,$$

$$−(x)^{-1} = −(x^{-1}),$$

$$(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}.$$
Table 1. Specification CR of commutative rings with multiplicative identity.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x + y) + z$</td>
<td>$= x + (y + z)$</td>
</tr>
<tr>
<td>$x + y$</td>
<td>$= y + x$</td>
</tr>
<tr>
<td>$x + 0$</td>
<td>$= x$</td>
</tr>
<tr>
<td>$x + (-x)$</td>
<td>$= 0$</td>
</tr>
<tr>
<td>$(x \cdot y) \cdot z$</td>
<td>$= x \cdot (y \cdot z)$</td>
</tr>
<tr>
<td>$x \cdot y$</td>
<td>$= y \cdot x$</td>
</tr>
<tr>
<td>$x \cdot 1$</td>
<td>$= x$</td>
</tr>
<tr>
<td>$x \cdot (y + z)$</td>
<td>$= x \cdot y + x \cdot z$</td>
</tr>
</tbody>
</table>

Table 2. Reflection and restricted inverse law.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Ref)</td>
<td>$(x^{-1})^{-1} = x$</td>
</tr>
<tr>
<td>(Ril)</td>
<td>$x \cdot (x \cdot x^{-1}) = x$</td>
</tr>
</tbody>
</table>

One can also 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. [7], Grätzer [9], McKenzie et al. [10] and Wechler [12].

The initial meadows of finite characteristic $k > 0$ have been described already: in Bergstra et al. [2] it is proved that $k$ must be squarefree and that the initial meadow of characteristic $k$ has $k$ elements. It then follows from Corollary 2.9 in Bethke and Rodenburg [4] that the initial meadow is isomorphic with a direct product of prime fields.

In this note we represent the initial meadow of characteristic 0 as the minimal subalgebra of the direct product of all finite prime fields. This is Theorem 2.5 and stems from a suggestion made by Yoram Hirshfeld, Tel Aviv University, in a private communication. The Normal Form Theorem—Theorem 3.10—is a rigorous elaboration of a remark made in Bergstra and Tucker [3]—in the proof of Corollary 5.11—and can be read between the lines in their Section 5.
§2. Meadows and their initial algebra. Since meadows make rings with a sound division operator into a variety we can apply general results about varieties. In this section we instantiate a few of these results and characterize the initial meadow.

**Definition 2.1.**

1. A subdirect embedding of a meadow $M$ in a family $(M_j)_{j \in J}$ of meadows is a family $(\phi_j : M \rightarrow M_j)_{j \in J}$ 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 $M \subseteq \prod_{j \in J} M_j$ and the restricted projections $M \rightarrow M_j$ 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 [5, 6]) states

**Theorem 2.2.** 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

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

a commutative regular ring in the sense of Von Neumann (see Goodearl [8]). It is not hard to see that the $x$ in the first formula is unique, and it is shown in Bergstra et al. [1, 2] 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 [5] as follows.

**Theorem 2.3.** A subdirectly irreducible meadow is a zero-totalized field.

Combining Theorems 2.2 and 2.3, 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 $\mathbb{F}_p$, $p$ a prime number, and $\mathbb{Q}$, the rational numbers.

**Lemma 2.4.** Let $A$ be the minimal subalgebra of the direct product

$$\mathbb{G} := \prod_{p \text{ prime}} \mathbb{F}_p,$$

Let $Z_p$ be the element of $\mathbb{G}$ that is 0 in all coordinates except $p$, where it is 1. Then
THE INITIAL MEADOWS

1. $Z_p \in A$.
2. The direct sum $\sum_{p \prime \text{prime}} G_p$ lies embedded as an ideal in $A$, and
3. If we identify $\sum_{p \prime \text{prime}} G_p$ with its image in $A$, $A/\sum_{p \prime \text{prime}} G_p \cong Q$.

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

Theorem 2.5. The minimal subalgebra of $\prod_{p \prime \text{prime}} G_p$ is an initial object in the category of meadows.

Proof. From the observations above, it appears that the initial meadows is the minimal subalgebra of the direct product of a set $G$ of zero-totalized minimal fields. It is easily seen that every prime field $G_p$ must be in $G$, otherwise there is no nontrivial homomorphism from a subalgebra of $\prod G$ into $G_p$. So if $Q \not\in G$, the initial meadow is the algebra $A$ of the previous lemma. On the other hand, if $Q \in G$, by (3) of the lemma we have a surjective homomorphism $h : A \to Q$. Then $(1, h) : A \to A \times Q$ shows that $A$ must be isomorphic to the minimal subalgebra of $\prod G$.

Corollary 2.6. Let $s, t$ be closed meadow terms. Then $Md \vdash s = t$ iff for all primes $p$, $G_p \models s = t$.

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.

We may consider meadows from the point of view of the theory of computable rings and fields as surveyed in detail in Stoltenberg-Hansen and Tucker [11]. Using results from this survey we can add the following. Let $\mathcal{R}$ be a meadow. If $\mathcal{R}$ is a computable ring then inversion as defined by $x^{-1} = \text{any } y \text{ such that } x \cdot x \cdot y = x$ and $y \cdot y \cdot x = y$ is computable. Thus, if the ring is computable, then so is the meadow; and if the ring is a field then it is computable as a zero-totalized field. Now, since every finite ring is computable, every initial meadow of finite characteristic $k > 0$ is computable. The computability of the initial meadow of characteristic 0 will follow from the Normal Form Theorem.

§3. Normal forms for initial meadows. 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

$$\sum_{i=0}^{\psi(t)-1} Z_i \cdot \phi_i(t) + G_{\psi(t)} \cdot \phi(t)$$
where \( \phi \) interprets \( t \) in the Galois field with order \( p_i \) (the \( i \)-th prime). \( \phi \) is its interpretation in the rational numbers, \( \mathbb{Z} \) and \( \mathbb{G} \), select significant models, and \( \psi(t) \) is an effective upper bound. This is Theorem 3.10. It then follows immediately, that the closed word problem for meadows is decidable.

We denote by \( \mathbb{N} \) the set of natural numbers: \( \text{Ter}_{Md} \) denotes the set of closed meadow terms.

**Definition 3.1.** 1. We define the set of numerals \( \mathbb{N}_{Md} \subseteq \text{Ter}_{Md} \) by

\[
\mathbb{N}_{Md} = \{ \overline{n} \mid n \in \mathbb{N} \}
\]

where for \( n \in \mathbb{N}, \overline{n} \) is defined inductively as follows:

(a) \( \overline{0} = 0 \).

(b) \( \overline{n + 1} = \overline{n} + 1 \).

2. We define the set of normal rational terms \( \mathbb{Q}_{Md} \subseteq \text{Ter}_{Md} \) by

\[
\mathbb{Q}_{Md} = \{ 0 \} \cup \{ \overline{n} \cdot m^{-1}, -(\overline{n} \cdot m)^{-1} \mid n, m \in \mathbb{N} \text{ and } m > 0 \text{ and } \gcd(n, m) = 1 \}.
\]

3. For \( t \in \text{Ter}_{Md} \), we denote by \( |t| \) the interpretation of \( t \) in \( \mathbb{Q} \).

Observe that \( | \cdot | \) respects addition, multiplication and subtraction. That is \( \text{Md} \vdash n + m = n + m \), \( \text{Md} \vdash n \cdot m = nm \) and if \( m \leq n \), then \( \text{Md} \vdash n - m = n - m \).

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

**Definition 3.2.** We define \( \phi : \text{Ter}_{Md} \rightarrow \mathbb{Q}_{Md} \) as follows:

\[
\phi(t) = \begin{cases} 0 & \text{if } |t| = 0. \\ \overline{n \cdot m}^{-1} & \text{if } |t| = \frac{n}{m} > 0 \text{ with } n, m \in \mathbb{N} \text{ and } \gcd(n, m) = 1. \\ -(\overline{n \cdot m})^{-1} & \text{if } |t| = \frac{n}{m} < 0 \text{ with } n, m \in \mathbb{N} \text{ and } \gcd(n, m) = 1. \end{cases}
\]

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 3.3.** 1. For \( n \in \mathbb{N} \), define \( \mathbb{G}_{n,Md} \subseteq \mathbb{N}_{Md} \) by

\[
\mathbb{G}_{n,Md} = \{ \overline{i} \mid i \leq p_n \}.
\]

2. For \( n \in \mathbb{N} \), define the evaluation \( \phi_n : \text{Ter}_{Md} \rightarrow \mathbb{G}_{n,Md} \) by: for \( t \in \text{Ter}_{Md} \), \( \phi_n(t) \) is the unique numeral \( m, 0 \leq m < p_n \), such that \( \mathbb{G}_n \models m = t \). We denote the corresponding natural number by \( |\phi_n(t)| \).

Obviously, \( \phi \) and \( \phi_n \) assign to provably equal terms syntactically identical normal rational terms and numerals, respectively. Thus we have for \( s, t \in \text{Ter}_{Md} \),

\[
\text{Md} \vdash s = t \Rightarrow \phi(s) = \phi(t) \text{ and } \phi_n(s) = \phi_n(t).
\]

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 3.4.** For \( n \in \mathbb{N} \), define \( Z_n = 1 - p_n \cdot p_n^{-1} \).

**Proposition 3.5.** For all \( n \in \mathbb{N} \) and \( t \in \text{Ter}_{Md} \),

\[
\text{Md} \vdash Z_n \cdot t = Z_n \cdot \phi_n(t).
\]
Observe that $G$ however, and in particular, in the zero-totalized field of characteristic $n$.

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 3.6.** For $n \in \mathbb{N}$, define $G_n \in \text{Ter}_{Md}$ inductively as follows:
1. $G_0 = 1$.
2. $G_{n+1} = G_n \cdot (1 - Z_n)$.

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

**Lemma 3.7.** 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. $n \leq m \Rightarrow Md \vdash G_m = G_n \cdot G_n$, and
5. if $0 < k < p_n$, then $Md \vdash G_n \cdot k \cdot k^{-1} = G_n$.

**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 3.8.** We define $\psi : \text{Ter}_{Md} \rightarrow \mathbb{N}$ inductively as follows.
1. $\psi(0) = 0 = \psi(1)$.
2. $\psi(-t) = \psi(t)$.
3. $\psi(t)^{-1} = \psi(t)$.
4. $\psi(t + t') = \max \{\psi(t), \psi(t')\}$ if $\phi(t) = 0$ or $\phi(t') = 0$,
   where $i$ is the least natural number such that $p_i > m_1$.
5. $\psi(t \cdot t') = \max \{\psi(t), \psi(t')\}$

**Proposition 3.9.** For each $t \in \text{Ter}_{Md}$ and all $n \in \mathbb{N}$, if $\psi(t) \leq n$ then $Md \vdash G_n \cdot t = G_n \cdot \phi(t)$.

**Proof.** It suffices to prove $Md \vdash G_{\psi(t)} \cdot t = G_{\psi(t)} \cdot \phi(t)$ by Lemma 3.7.4. We employ structural induction. The base cases are trivial. In the induction step the cases for inversion and multiplication follow from Lemma 3.7.3–4, 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 $Md \vdash G_{\psi(r)} \cdot r = G_{\psi(r)} \cdot \phi(r)$ and $Md \vdash G_{\psi(s)} \cdot s = G_{\psi(s)} \cdot \phi(s)$.
We therefore can expand cases follow by a similar argument taking in addition the significance of repeated removal of shared prime factors using again 3.7.

Proof. Theorem 3.10

For each $t \in \text{Ter}_{\text{Md}}$, $\text{Md} \vdash t = \sum_{i=0}^{n-1} Z_i \cdot \phi_i(t) + G_{\psi(i)} \cdot \phi(t)$.

Proof. First observe that

\[
G_n \cdot t = (Z_n + (1 - Z_n)) \cdot G_n \cdot t
\]

by Proposition 3.5

\[
= Z_n \cdot G_n \cdot t + (1 - Z_n) \cdot G_n \cdot t
\]

by Lemma 3.7.2.

We therefore can expand $t$ as follows:

\[
t = G_0 \cdot t
\]

by repeated use of $(*)$

\[
= Z_0 \cdot \phi_0(t) + \cdots + Z_{\psi(i) \cdot 1} \cdot \phi_{\psi(i) \cdot 1}(t) + G_{\psi(i)} \cdot t
\]

Corollary 3.11. For each $t \in \text{Ter}_{\text{Md}}$ and $\psi(t) \leq n \in \mathbb{N}$, $\text{Md} \vdash t = \sum_{i=0}^{n-1} Z_i \cdot \phi_i(t) + G_n \cdot \phi(t)$.

Proof. By expanding $t$ as far as necessary and Proposition 3.9.
Corollary 3.12. For all $s, t \in \text{Ter}_{\text{Md}}$,

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

Proof. Left to right is obvious. For the reverse direction apply the previous corollary.

Corollary 3.13. The closed word problem for meadows is decidable.

In Bergstra and Tucker [3] 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.


§ 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 $\prod_{p \mid k} G_p$.

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

The finite initial meadows are computable and—since the closed term problem is decidable—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.

REFERENCES


INFORMATICS INSTITUTE, UNIVERSITY OF AMSTERDAM
SCIENCE PARK 107, 1098 XG AMSTERDAM, THE NETHERLANDS
E-mail: I.Bethke@uva.nl
E-mail: P.H.Rodenburg@uva.nl