# The Rational Numbers as an Abstract Data Type 

J. A. BERGSTRA<br>University of Amsterdam, Informatics Institute, Amsterdam, The Netherlands

AND

## J. V. TUCKER

University of Wales Swansea, Singleton Park, Swansea, United Kingdom


#### Abstract

We give an equational specification of the field operations on the rational numbers under initial algebra semantics using just total field operations and 12 equations. A consequence of this specification is that $0^{-1}=0$, an interesting equation consistent with the ring axioms and many properties of division. The existence of an equational specification of the rationals without hidden functions was an open question. We also give an axiomatic examination of the divisibility operator, from which some interesting new axioms emerge along with equational specifications of algebras of rationals, including one with the modulus function. Finally, we state some open problems, including: Does there exist an equational specification of the field operations on the rationals without hidden functions that is a complete term rewriting system?

Categories and Subject Descriptors: D.3.1 [Programming Languages]: Formal Definition and Theory; D.3.3 [Programming Languages]: Language Constructs and Features; F.1.3 [Logics and Meanings of Programs]: Specifying and Verifying and Reasoning about Programs; F.3.2 [Logics and Meanings of Programs]: Semantics of Programming Languages; F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic


General Terms: Verification, Languages
Additional Key Words and Phrases: Rational numbers, field, meadow, division-by-zero, total versus partial functions, abstract data types, algebraic specification, equations, initial algebra, computable algebras

## ACM Reference Format:

Bergstra, J. A. and Tucker, J. V. 2007. The rational numbers as an abstract data type J. ACM 54, 2, Article 7 (April 2007), 25 pages. DOI $=10.1145 / 1219092.1219095 \mathrm{http}: / /$ doi.acm.org/ 10.1145/1219092.1219095

[^0]
## 1. Introduction

Measurements are made using some kind of gauge. To calibrate a gauge, one chooses a unit and divides that unit into a number $k$ of subunits of equal size. Then a measurement is denoted by $n$ whole units and $m$ subunits or, in this case, $n \frac{m}{k}=(n k+m) / k$ subunits. Note that measurements are finite.

The set $\mathbb{Q}$ of rational numbers is a number system designed to denote measurements. Most users make computations involving measurements. Hence, the set $\mathbb{Q}$ of rational numbers is among the truly fundamental data types. The rationals are the numbers with which we make finite computations in practice. Despite the fact they have been known and used for over two millennia, they are somewhat neglected in the modern theory of data types.

On the rationals, we calculate using standard operations such as the functions $+,-, \cdot,^{-1}$. Algebras made by equipping $\mathbb{Q}$ with some selection of operations we call here rational arithmetics. The algebra $\left(\mathbb{Q} \mid 0,1,+,-, \cdot,^{-1}\right)$ is usually called the field of rational numbers when the operations satisfy certain axioms.

In this article, we will model some rational arithmetics, including the field, as abstract data types. Now, the rationals can be specified by the field axioms; indeed, they are uniquely definable up to isomorphism as the prime subfield of characteristic 0 . However, the field axioms contain a negative conditional formula for inverse, which is difficult to apply and automate in formal reasoning. Specifically, we are interested in finding equational specifications of rational arithmetics under initial algebra semantics. Such equational axiomatisations allow simple term rewriting systems for reasoning and computation. Surprisingly, after over 30 years of data type theory, questions such as "Does there exist such an equational specification without hidden functions of the field of rational numbers?" seem to be open.

According to our general theory of algebraic specifications for computable data types (e.g., Bergstra and Tucker [1982; 1983; 1987; 1995]), since the common rational arithmetics are computable algebras, they have various equational specifications under both initial and final algebra semantics. Computable rational arithmetics even have equational specifications that are also complete term rewriting systems (by Bergstra and Tucker [1995]). However, these general specification theorems for computable data types involve hidden functions and are based on equationally definable enumerations of data. Recently, in Moss [2001], algebraic specifications of the rationals were considered. Among several interesting observations, Moss showed that there exists an equational specification with just one unary hidden function. He used a special enumeration technique that reminds one of the general methods of Bergstra and Tucker [1995], but is based on a remarkable enumeration theorem for the rationals in Calkin and Wilf [2000]. He also gave specifications of rational arithmetics with a modulus operator and with a floor.

Here we prove:
THEOREM 1.1. There exists a finite equational specification under initial algebra semantics, without hidden functions, of the rational numbers with field operations that are all total.

Our axioms include the commutative ring axioms and some general rules for inverses from which it can be deduced that

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

This equation is also true of the hidden function specification in Moss [2001]. The equation $0^{-1}=0$ occurs in several other places as well, for reasons of technical convenience (e.g., Hodges [1993] and Harrison [1998]). Our proposed specification includes a special axiom that codes a representation of an infinite subset of positive rational numbers.

The pursuit of this result leads to a thorough axiomatic examination of the divisibility operator, in which some interesting new axioms and models are discovered. In particular, we introduce a class of commutative rings with interesting division properties, which we call meadows.

The structure of the article is this: In Section 2, we give the basic equations that define the rational arithmetic operations and define some of their properties. In Section 3, we give two equational specifications of the rational field without hidden functions, one recursive and infinite, and one finite. In Section 5, we give results on fields and equational subtheories of fields, and on other rational arithmetics. Finally, in Section 6, we discuss some open problems.

This article is the first of a series on equational specifications of the rational arithmetics and their extensions, see Bergstra and Tucker [2006a; 2006b] and Bergstra [2006], launched in 2005 by Bergstra and Tucker [2005]. It can be read as a sequel to Bergstra and Tucker [1987; 1995], which contains a literature survey and the complementary general results. We use only the basic ideas of initial algebra specification. However, with several unfamiliar axioms about the familiar inverse operator in action, care is needed in verifying equations and other formulae.

We thank Kees Middelburg, Yoram Hirschfeld and an anonymous referee for valuable comments on the subject.

## 2. Axioms for Rational Arithmetic

2.1. Preliminaries on Algebraic Specifications. We assume the reader is familiar with using equations and conditional equations and initial algebra semantics to specify data types. Some accounts of this are: Goguen et al. [1978], Meseguer and Goguen [1985], and Wirsing [1990].

The theory of algebraic specifications is based on theories of universal algebras (e.g., Wechler [1992] and Meinke and Tucker [1992]); computable and semicomputable algebras [Stoltenberg-Hansen and Tucker 1995]; and term rewriting [Klop 1992; Terese 2003].

We use standard notations: typically, we let $\Sigma$ be a many sorted signature and $A$ a total $\Sigma$ algebra. The class of all total $\Sigma$ algebras is $\operatorname{Alg}(\Sigma)$ and the class of all total $\Sigma$ algebras satisfying all the axioms in a theory $T$ is $\operatorname{Alg}(\Sigma, T)$. The word "algebra" will mean total algebra.
2.2. Algebraic Specifications of the Rationals. We will build our specifications in stages. The primary signature $\Sigma$ is simply that of the field of rational numbers:

```
signature \Sigma
sorts field
operations
0: -> field;
1: }->\mathrm{ field;
```

```
\(+:\) field \(\times\) field \(\rightarrow\) field;
\(-:\) field \(\rightarrow\) field;
\(\cdot:\) field \(\times\) field \(\rightarrow\) field;
\({ }^{-1}\) : field \(\rightarrow\) field
end
```

The first set of eight axioms is that of a commutative ring with 1 , which establishes the standard properties of,+- , and $\cdot$. We will refer to these axioms by $C R 1, \ldots, C R 8$.
equations $C R$

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

end

Our first set SIP of axioms for ${ }^{-1}$ contain the following, which we call the strong inverse properties. They are "strong" because they are equations involving ${ }^{-1}$ without any guards, such as $x \neq 0$ :
equations $S I P$

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

end
We will refer to these axioms by $S I P 1, \ldots, S I P 3$. The set $C R \cup S I P$ of equations and its extensions are our basic object of study. We will also need other axioms, especially about ${ }^{-1}$.

Later, we will add to $C R \cup S I P$ the restricted inverse law (Ril),

$$
x \cdot\left(x \cdot x^{-1}\right)=x
$$

which, using commutativity and associativity, expresses that $x \cdot x^{-1}$ is 1 in the presence of $x$.

Hirschfeld (Personal Communication 2006) has shown that equations SIP1 and SIP2 are derivable from SIP3 using CR $\cup$ Ril.

The standard axioms of a field simply add to $C R$ the following: the general inverse law (Gil)

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

and the axiom of separation (Sep)

$$
0 \neq 1
$$

Guarded versions of the equations of SIP—such as, $x \neq 0 \Longrightarrow\left(x^{-1}\right)^{-1}=x$-can be proved from Gil and Sep.

### 2.3. Totalized Fields and Algebras Satisfying the Specifications.

Let us consider the notion of a field in our setting. Let ( $\Sigma, T_{\text {field }}$ ) be the axiomatic specification of fields, where

$$
T_{\text {field }}=C R \cup G i l \cup S e p
$$

The class $\operatorname{Alg}\left(\Sigma, T_{\text {field }}\right)$ is the class of total algebras satisfying the axioms in $T_{\text {field }}$. For emphasis, we refer to these algebras as totalized fields.

For all totalized fields $A \in \operatorname{Alg}\left(\Sigma, T_{\text {field }}\right)$ and all $x \in A$, the inverse $x^{-1}$ is defined. In particular, $0_{A}^{-1}$ is defined. What can it be?

Now suppose $0_{A}^{-1}=a$ for some $a \in A$. Then, we must expect that

$$
0_{A}^{-1} \cdot 0_{A} \neq 1_{A} .
$$

To see this, note that $a \cdot 0_{A}=0_{A}$ for all $a$ in a ring (see Lemma 2.1(a) below). So $0_{A}^{-1} \cdot 0_{A}=0_{A}$ and $0_{A} \neq 1_{A}$ by Sep. Thus, at this stage, the actual value $0_{A}^{-1}=a$ can be anything. Choosing $0_{A}^{-1}=a$ we may speak of an $a$-totalized field and, in particular, when $a=0$ of a 0 -totalized field.

Now, the axiomatic theory of fields is one of the central topics in the model theory of first order languages: it has shaped the subject and led to its best applications. In model theory operations in signatures are invariably total. It is common to axiomatise fields using a set of $\Pi_{2}$ sentences over the ring signature thus avoiding the question of the totality of the inverse operation. However, with this ring signature, the substructures are rings and not necessarily fields. Thus, axiomatisations based on the field signature with the following axiom are also used (see, e.g., Hodges [1993, p. 695])

$$
0^{-1}=0 \wedge x \neq 0 \Longrightarrow x \cdot x^{-1}=1
$$

In fact, 0 is a common choice for the value of $0^{-1}$. In automated reasoning, for example, Harrison [1998] used $0^{-1}=0$ and observed that SIP1, SIP2 and SIP3 are valid in the 0-totalised reals.

Our own interest will be in the specification $C R \cup S I P$. Shortly, we shall show that this specification will force the choice of $0^{-1}=0$.

The main $\Sigma$-algebra we are interested in is

$$
Q_{0}=\left(\mathbb{Q} \mid 0,1,+,-, \cdot,^{-1}\right)
$$

where the inverse is total

$$
\begin{aligned}
x^{-1}=1 / x & & \text { if } x \neq 0 \\
=0 & & \text { if } x=0
\end{aligned}
$$

This total algebra satisfies the axioms of a field $T_{\text {field }}$ and is a 0 -totalized field of rationals.

Similarly, we can define the $a$-totalized field $Q_{a}$ of rationals where the inverse is made total by $0^{-1}=a$.
2.4. Properties. We will now derive some simple equational properties from the axioms.

Lemma 2.1. The following equations are provable from $C R$ :
(a) $0 \cdot x=0$.
(b) $(-1) \cdot x=-x$.
(c) $(-x) \cdot y=-(x \cdot y)$.
(d) $-0=0$.
(e) $(-x)+(-y)=-(x+y)$.
(f) $-(-x)=x$.

Proof
(a) We calculate:

| $0+0$ | $=0$ |  | by $C R 3$ |
| ---: | :--- | ---: | :--- |
| $(0+0) \cdot x$ | $=0 \cdot x$ |  | multiplying both sides by $x$ |
| $0 \cdot x+0 \cdot x$ | $=0 \cdot x$ |  | by $C R 8$ and $C R 6$ |
| $(0 \cdot x+0 \cdot x)+(-(0 \cdot x))$ | $=0 \cdot x+(-(0 \cdot x))$ |  | adding to both sides |
| $0 \cdot x+(0 \cdot x+(-(0 \cdot x)))$ | $=0$ |  | by $C R 1$ and $C R 4$ |
| $0 \cdot x+0$ | $=0$ |  | by $C R 4$ |
| $0 \cdot x$ | $=0$ |  | by $C R 3$. |

(b) We calculate:

$$
\begin{aligned}
(-1) \cdot x & =(-1) \cdot x+(x-x) & & \text { by } C R 3 \text { and } C R 4 \\
& =((-1) \cdot x+(x \cdot 1))-x & & \text { by } C R 7 \text { and } C R 1 \\
& =((-1) \cdot x+(1 \cdot x))-x & & \text { by } C R 6 \\
& =((-1)+1) \cdot x-x & & \text { by } C R 8 \\
& =(1+(-1)) \cdot x-x & & \text { by } C R 2 \\
& =0 \cdot x-x & & \text { by } C R 4 \\
& =0-x & & \text { by this Lemma cla }
\end{aligned}
$$

(c) We calculate:

$$
\begin{aligned}
(-x) \cdot y & =((-1) \cdot x) \cdot y & & \text { by this Lemma clause (b) } \\
& =(-1) \cdot(x \cdot y) & & \text { by } C R 5 \\
& =-(x \cdot y) & & \text { by this Lemma clause (b). }
\end{aligned}
$$

(d) We calculate:

$$
\begin{aligned}
-0 & =(-1) \cdot 0 & & \text { by this Lemma clause (b) } \\
& =0 & & \text { by this Lemma clause (a). }
\end{aligned}
$$

(e) We calculate:

$$
\begin{aligned}
(-x)+(-y) & =0+((-x)+(-y)) & & \text { by } C R 3 \\
& =(-(x+y)+(x+y))+((-x)+(-y)) & & \text { by } C R 3 \\
& =-(x+y)+((x+-x)+(y+-y)) & & \text { by } C R 1 \text { and } C R 2 \\
& =-(x+y)+(0+0) & & \text { by } C R 4 \\
& =-(x+y)+0 & & \text { by } C R 3 \\
& =-(x+y) & & \text { by } C R 3 .
\end{aligned}
$$

(f) We calculate:

$$
\begin{aligned}
-(-x) & =0+-(-x) & & \text { by } C R 3 \\
& =(x+(-x))+-(-x) & & \text { by } C R 4 \\
& =x+((-x)+-(-x)) & & \text { by } C R 1 \\
& =x+0 & & \text { by } C R 3 \\
& =x & & \text { by } C R 3 .
\end{aligned}
$$

We know from (a) that $0=0 \cdot 0^{-1}$ is valid in a commutative ring. On adding the axioms $S I P$ to $C R$, we force a value for $0^{-1}$ :

THEOREM 2.2. The following equation is provable from $C R \cup S I P$ :

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

Proof. First observe that:

$$
\begin{aligned}
0 & =0^{-1}+-\left(0^{-1}\right) & & \text { by } C R 4 \\
& =0^{-1}+(-0)^{-1} & & \text { by SIP1 } \\
& =0^{-1}+0^{-1} & & \text { by Lemma } 2.1(\mathrm{~d}) .
\end{aligned}
$$

Now we calculate:

$$
\begin{aligned}
0^{-1} & =\left(0^{-1}+0^{-1}\right)^{-1} & & \text { by applying }{ }^{-1} \\
& =\left(1 \cdot 0^{-1}+1 \cdot 0^{-1}\right)^{-1} & & \text { by CR6 and CR7 } \\
& =\left((1+1) \cdot 0^{-1}\right)^{-1} & & \text { by } C R 8 \\
& =(1+1)^{-1} \cdot\left(0^{-1}\right)^{-1} & & \text { by SIP2 } \\
& =(1+1)^{-1} \cdot 0 & & \text { by SIP3 } \\
& =0 & & \text { by Lemma 2.1(a) and CR2. }
\end{aligned}
$$

2.5. EQUATIONAL SubTHEORIES OF FIELDS. Given the three axioms of SIP, one might ask: What is wrong with the unguarded equation $x \cdot x^{-1}=1$ ? It is easy to show that it contradicts Sep, that is,

$$
C R \cup\left\{x \cdot x^{-1}=1\right\} \vdash 0=1
$$

So we must try other equations for inverse. The axiom Ril implies a wider context for inverse.

LEMMA 2.3. $\quad C R \cup \operatorname{SIP} \cup R i l \vdash u \cdot x \cdot y=u \Longrightarrow u \cdot x \cdot x^{-1}=u$.

Proof. We calculate:

$$
\begin{aligned}
u \cdot x \cdot x^{-1} & =(u \cdot x \cdot y) \cdot x \cdot x^{-1} & & \text { by premiss } \\
& =u \cdot y \cdot x \cdot x \cdot x^{-1} & & \text { by commutativity } \\
& =u \cdot y \cdot x & & \text { by Ril } \\
& =u & & \text { by premiss. }
\end{aligned}
$$

Let us show that the equational specifications are (almost) subtheories of $T_{\text {field }}=$ $C R \cup G i l \cup S e p$. First, we need this cancelation lemma:
LEmMA 2.4. $T_{\text {field }} \vdash x \cdot y=1 \wedge x \cdot z=1 \rightarrow y=z$.
Proof. If $x \cdot y=1$, then $x \neq 0$. Multiply both assumptions by $x^{-1}$ and we have $x^{-1} \cdot x \cdot y=x^{-1}$ and $x^{-1} \cdot x \cdot z=x^{-1}$. So, using Gil for $x \neq 0$, we have $1 \cdot y=x^{-1}$ and $1 \cdot z=x^{-1}$. By CR7, we have $y=x^{-1}=z$.

LEMMA 2.5. $T_{\text {feild }} \cup\left\{0^{-1}=0\right\} \vdash$ SIP and $T_{\text {feild }} \cup\left\{0^{-1}=0\right\} \vdash$ Ril.
Proof. Consider the three axioms of SIP in turn.
(1) $(-x)^{-1}=-\left(x^{-1}\right)$. If $x=0$, then the equation is true trivially. Suppose $x \neq 0$ and so $-x \neq 0$. We calculate:

$$
\begin{aligned}
1 & =(-x) \cdot(-x)^{-1} & & \text { by Gil } \\
& =(-1 \cdot x) \cdot(-x)^{-1} & & \text { by Lemma 2.1(b) } \\
& =x \cdot-1 \cdot(-x)^{-1} & & \text { by CR6 } \\
& =x \cdot-(-x)^{-1} & & \text { by Lemma 2.1(b). }
\end{aligned}
$$

By Gil, we also have $1=x \cdot x^{-1}$. So,

$$
\begin{aligned}
x^{-1} & =-(-x)^{-1} & & \text { by Cancellation Le } \\
-\left(x^{-1}\right) & =-\left(-(-x)^{-1}\right) & & \text { by applying }- \\
& =(-x)^{-1} & & \text { by Lemma 2.1(f). }
\end{aligned}
$$

(2) $(x \cdot y)^{-1}=x^{-1} \cdot y^{-1}$. If $x=0$ or $y=0$, then the equation is true trivially. If $x \neq 0$ and $y \neq 0$, then $x \cdot y \neq 0$. By Gil, we have

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

and by the axioms of $C R$

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

Thus, by cancellation, $(x \cdot y)^{-1}=x^{-1} \cdot y^{-1}$.
(3) $\left(x^{-1}\right)^{-1}=x$. If $x=0$, then the equation is true trivially. If $x \neq 0$, then $x^{-1} \neq 0$. By Gil, we have

$$
\left(x^{-1}\right) \cdot\left(x^{-1}\right)^{-1}=1 \text { and }\left(x^{-1}\right) \cdot x=1 .
$$

By cancellation, $\left(x^{-1}\right)^{-1}=x$.
The derivation of Ril is obvious.

Notice that for any closed equation, $T_{\text {feld }} \vdash t=s$ implies $T_{\text {field }} \cup\left\{0^{-1}=0\right\} \vdash$ $t=s$, which is trivial as $\vdash$ is monotonic.

## 3. Initial Algebra Specification

We give two algebraic specifications of the rationals, one infinite and one finite.
3.1. A Recursive Equational Specification. Let us define the numerals over $\Sigma$ by $\underline{0}=0$ and $\underline{n+1}=\underline{n}+1$. We denote $0,1,1+1,(1+1)+1, \ldots$ by $0, \underline{1}, \underline{2}, \underline{3}, \ldots$. Now we define a set $I$ of closed $\Sigma$-equations between numerals by

$$
I=\left\{\underline{n} \cdot(\underline{n})^{-1}=1 \mid n>0\right\} .
$$

Theorem 3.1. There exists a recursive equational initial algebra specification ( $\Sigma, C R \cup S I P \cup I$ ), without hidden functions, of the totalised field $Q_{0}$ of rational numbers, that is,

$$
T(\Sigma, C R \cup S I P \cup I) \cong Q_{0}
$$

Proof. Clearly, the specification $I$ is decidable. Note that, by inspection,

$$
Q_{0} \models C R \cup S I P \cup I .
$$

By initiality, there exists a unique $\Sigma$-homomorphism $\phi: T(\Sigma, C R \cup S I P \cup I)$ $\rightarrow Q_{0}$.

As $Q_{0}$ is $\Sigma$-minimal, we know that $\phi$ is surjective. Thus, to complete the proof, we must show that $\phi$ is also injective.

Consider $Q_{0}$. The domain $\mathbb{Q}$ of $Q_{0}$ can be represented as follows:

$$
\begin{aligned}
\mathbb{Q}= & \{0\} \cup\left\{\left.\frac{n}{m} \right\rvert\, n>0, m>0, \operatorname{gcd}(n, m)=1\right\} \\
& \cup\left\{\left.-\frac{n}{m} \right\rvert\, n>0, m>0, \operatorname{gcd}(n, m)=1\right\} .
\end{aligned}
$$

We use this representation to calculate the values of $\phi$ on certain equivalence classes of terms in $T(\Sigma, C R \cup S I P \cup I)$ :

Lemma 3.2. The following hold:
$\phi([0])=0$
$\phi([\underline{1})=1$
$\phi([\underline{n}])=n$
$\phi\left(\left[\underline{n}^{-1}\right]\right)=\frac{1}{n}$
$\phi\left(\left[\underline{n} \cdot \underline{m}^{-1}\right]\right)=\frac{n}{m}$, providing $\operatorname{gcd}(n, m)=1$.
$\phi\left(\left[-\left(\underline{n} \cdot \underline{m}^{-1}\right)\right]\right)=-\frac{n}{m}$, providing $\operatorname{gcd}(n, m)=1$.
Proof. Cases (i) and (ii) are obvious since $\phi$ preserves constants. Case (iii) is shown by induction on $n$. Case (iv) is shown by induction on $n$ and uses the interpretation of ${ }^{-1}$. The last two cases are based on

$$
\phi\left(\left[\underline{n} \cdot \underline{m}^{-1}\right]\right)= \begin{cases}\frac{\phi([n])}{\phi(\underline{m}]} & \text { if } \operatorname{gcd}(n, m)=1 ; \\ \frac{n: g g d n, m)}{m: g c d(n, m)} & \text { otherwise }\end{cases}
$$

where we use: to denote division on natural numbers.

These observations suggest the following definition and lemma. Let

$$
\begin{aligned}
T R= & \{\underline{0}\} \cup\left\{\underline{n} \cdot \underline{m}^{-1} \mid n>0, m>0, \operatorname{gcd}(n, m)=1\right\} \\
& \left.\cup-\left(\underline{\underline{n}} \cdot \underline{\underline{m}^{-1}}\right) \mid n>0, m>0, \operatorname{gcd}(n, m)=1\right\} .
\end{aligned}
$$

LEMMA 3.3. The set TR is a transversal for the equivalence relation $\equiv_{C R U S I P \cup I}$, that is, each equivalence class contains one and only one element of TR.

Before we prove Lemma 3.3, let us note that it is enough to prove $\phi$ is injective. For suppose

$$
\phi([t])=\phi\left(\left[t^{\prime}\right]\right) .
$$

Then, by Lemma 3.3, we know that $[t]=[r]$ and $\left[t^{\prime}\right]=\left[r^{\prime}\right]$ for unique $r, r^{\prime} \in T R$. Thus,

$$
\phi([r])=\phi\left(\left[r^{\prime}\right]\right) .
$$

But, by Lemma 3.2, we know that $\phi([r])$ and $\phi\left(\left[r^{\prime}\right]\right)$ have values in the normal form of $\frac{n}{m}$, or $-\frac{n}{m}$, provided $\operatorname{gcd}(n, m)=1$, etc. This happens if, and only if, $r=r^{\prime}$ and hence if, and only if, $[t]=\left[t^{\prime}\right]$.

It remains to prove the Lemma 3.3 as follows:
Proof. Let $E=C R \cup S I P \cup I$. We have to show that:
(1) for each closed term $t \in T(\Sigma)$ there is some $u \in T R$ such that $E \vdash t=u$;
(2) for any closed terms $k, l \in T R$, if $E \vdash k=l$ then $k \equiv l$.

The proof of (1) is by induction on the structure of term $t$ and requires a large case analysis based on the leading function symbol of $t$ in $\Sigma$ and possible normal forms for subterms in $T R$. We give one of the induction cases for illustration:

Case: Multiplication $t=r \cdot s$.
By induction, both $r$ and $s$ are provably equivalent to elements of $T R$. We take the following subcase: suppose

$$
(\Sigma, E) \vdash r=\underline{n} \cdot \underline{m}^{-1} \text { and } E \vdash s=-\left(\underline{k} \cdot \underline{l}^{-1}\right) .
$$

Now,

$$
\begin{aligned}
& (\Sigma, E) \vdash r \cdot s=\underline{n} \cdot \underline{m}^{-1} \cdot-\left(\underline{k} \cdot \underline{l}^{-1}\right) \quad \text { by substitution } \\
& \vdash r \cdot s=\underline{n} \cdot \underline{m}^{-1} \cdot(-1) \cdot\left(\underline{k} \cdot \underline{l}^{-1}\right) \quad \text { by } C R 6 \text { and } C R 7 \\
& \vdash r \cdot s=(-1) \cdot \underline{n} \cdot \underline{m}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1} \quad \text { by } C R 8 \\
& \vdash r \cdot s=(-1) \cdot(\underline{n} \cdot \underline{k}) \cdot\left(\underline{m}^{-1} \cdot \underline{l}^{-1}\right) \quad \text { by SIP2 } \\
& \vdash r \cdot s=(-1) \cdot(\underline{n} \cdot \underline{k}) \cdot(\underline{m} \cdot \underline{l})^{-1} \quad \text { by } \operatorname{SIP} 3 \\
& \vdash r \cdot s=(-1) \cdot(\underline{n . k}) \cdot(\underline{m . l})^{-1} \quad \text { by SIP3 } \\
& \vdash r \cdot s=-(\underline{n . k}) \cdot(\underline{m . l})^{-1} \quad \text { by SIP3. }
\end{aligned}
$$

Now let $u=\operatorname{gcd}(n . k, m . l)$. If $u=1$, then we are done. Suppose that $n \cdot k=u . p$ and $m . l=u . q$ and so $\operatorname{gcd}(p, q)=1$. Then we continue rewriting:

$$
\left.\begin{array}{rlrl}
(\Sigma, E) & \vdash r \cdot s & =-(\underline{u} \cdot p) \cdot(\underline{u} \cdot q)^{-1} &
\end{array}\right) \text { by definition } \quad \text { ( } \begin{aligned}
& \vdash r \cdot s=-(\underline{u} \cdot \underline{p}) \cdot(\underline{u} \cdot \underline{q})^{-1} & & \text { by Lemma } 3.4 \\
& \vdash r \cdot s=-\left(\underline{u} \cdot \underline{u}^{-1}\right)\left(\underline{p} \cdot \underline{q}^{-1}\right) & & \text { by } C R 6 \text { and SIP2 } \\
& \vdash r \cdot s=-\underline{p} \cdot \underline{q}^{-1} & & \text { by equations of } \mathrm{I} .
\end{aligned}
$$

The term $-\underline{p} \cdot \underline{q}^{-1}$ is of the required form because $\operatorname{gcd}(p, q)=1$. The following is an easy induction.

Lemma 3.4. For any $p, q \in \mathbb{N}$ we have

$$
\begin{aligned}
& (\Sigma, E) \vdash \underline{p+q}=\underline{p}+\underline{q} \\
& (\Sigma, E) \vdash \underline{p \cdot q}=\underline{p} \cdot \underline{q} \\
& (\Sigma, E) \vdash \underline{-p}=-\underline{p} .
\end{aligned}
$$

The proof of uniqueness condition (2) is easy: Suppose $k \neq l$. Then they have different interpretations in $Q_{0}$ under $\phi$. This means that they cannot be proved equal by the axioms $C R \cup S I P \cup I$ since $Q_{0}$ satisfies these axioms.

This completes the proof of Lemma 3.3 and hence the proof of Theorem 3.1.
3.2. A Finite Equational Specification. We first introduce an operation:

Definition 3.5. $Z(x)=1-x \cdot x^{-1}$.
The operator "measures" the difference between $x \cdot x^{-1}$ and 1. Clearly,

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

The operator has many useful properties. For example, the set $I$ of closed equations used in Section 3.1 can be written

$$
I=\{Z(\underline{n})=0 \mid n>0\} .
$$

The operator $Z$ is a function that is definable by a term over the field signature. It is used to simplify notations and calculations below. It does not count as a hidden function as it can be simply removed from all specifications by expanding its explicit definition.

Recall Lagrange's Theorem that every natural number can be represented as the sum of four squares (see Dickson [1952, pp. 275-303]). We define a special equation $L$ (for Lagrange):

$$
Z\left(1+x^{2}+y^{2}+z^{2}+u^{2}\right)=0 .
$$

$L$ expresses that for a large collection of numbers (in particular, those $q$ which can be written as 1 plus the sum of four squares) $q \cdot q^{-1}$ equals 1 .

Theorem 3.6. There exists a finite equational initial algebra specification, without hiddenfunctions, of the totalised field $Q_{0}$ of rational numbers; in particular,

$$
T(\Sigma, C R \cup S I P \cup L) \cong Q_{0} .
$$

Proof. First, note that, by inspection,

$$
Q_{0} \models C R \cup S I P \cup L .
$$

We know that $C R$ and SIP are valid in $Q_{0}$. To see that $L$ is valid, note that ( $1+x^{2}+$ $y^{2}+z^{2}+w^{2}$ ) is always positive and never 0 . Since $Q_{0} \models x \neq 0 \Longrightarrow x \cdot x^{-1}=1$, we conclude that $L$ is valid.

By initiality, there exists a unique $\Sigma$-homomorphism $\phi: T(\Sigma, C R \cup S I P \cup L) \rightarrow$ $Q_{0}$.

As $Q_{0}$ is $\Sigma$-minimal, we know that $\phi$ is surjective. Thus, to complete the proof, we must show that $\phi$ is also injective.

On the other hand, recalling the recursive set $I$ of numerals Section 3.1, we know that

$$
L \vdash I .
$$

This is because for each $n \in \mathbb{N}$ we can choose some $x, y, z, w$ such that $n=$ $1+x^{2}+y^{2}+z^{2}+w^{2}$. Therefore,

$$
T(\Sigma, C R \cup S I P \cup L) \models C R \cup S I P \cup I .
$$

By initiality, there exists a unique $\Sigma$-homomorphism $\phi: T(\Sigma, C R \cup S I P \cup I) \rightarrow$ $T(\Sigma, C R \cup S I P \cup L)$. But, by Theorem 3.1, $T(\Sigma, C R \cup S I P \cup I) \cong Q_{0}$ and so there is a $\Sigma$-homomorphism $\psi: Q_{0} \rightarrow T(\Sigma, C R \cup S I P \cup L)$. Thus, by minimality, we have $\phi$ is a $\Sigma$-isomorphism with $\psi$ as its inverse and $T(\Sigma, C R \cup S I P \cup L) \cong Q_{0}$.

## 4. A Simpler Specification using the Modulus Function

Consider the algebra $Q_{0}$ of rational numbers expanded with the modulus function $\|$ and let this be denoted

$$
Q_{0,| |}=\left(\mathbb{Q}\left|0,1,+,-, \cdot,^{-1},| |\right) .\right.
$$

We will give an equational specification of this algebra. The following two sets of equations can be added to $C R \cup S I P$. The first specifies the modulus operator on the rational numbers.
equations $M O D$

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

## end

The second guarantees the existence of proper inverses for sufficiently many closed terms.
equations Modril

$$
Z(1+|x|)=0
$$

end
To get used to the axioms for $\|$, we prove a simple lemma of use later:
Lemma 4.1. For each $k \in \mathbb{N}, C R \cup M O D \vdash|\underline{k}|=\underline{k}$.
Proof. By induction on $k$.
Basis, $k=0$ : We calculate:

$$
\begin{aligned}
|\underline{0}| & =|0| & & \text { by definition of } \underline{0} \\
& =0 & & \text { by } M O D 1 \\
& =\underline{0} & & \text { by definition of } \underline{0} .
\end{aligned}
$$

Induction step, $k+1$, Assume as induction hypothesis that $|\underline{k}|=\underline{k}$. We calculate:

$$
\begin{aligned}
\underline{k+1} & =\underline{k}+1 & & \text { by definition of } \underline{k+1} \\
& =1+\underline{k} & & \text { by commutativity } C R 2 \\
& =1+|\underline{k}| & & \text { by induction hypothesis } \\
& =|1+|\underline{k}|| & & \text { by MOD6 } \\
& =|1+\underline{k}| & & \text { by induction hypothesis } \\
& =|\underline{k+1}| & & \text { by } C R 2 \text { and the definition of } \underline{k+1 .}
\end{aligned}
$$

THEOREM 4.2. The initial algebra $T(\Sigma \cup\{\|\}, C R \cup S I P \cup M O D \cup$ Modril $)$ is isomorphic to the algebra $Q_{0, \|}$ of rational numbers.

Proof. The proof follows the pattern of earlier theorems (Theorems 3.1 and 3.6). For notational convenience, let

$$
E=C R \cup S I P \cup M O D \cup \text { Modril. }
$$

The equations in $E$ are valid in $Q_{0,| |}$. Thus, by initiality, there exists a unique $\Sigma \cup\{|\mid\}$-homomorphism

$$
\psi: T(\Sigma \cup\{| |\}, E) \rightarrow Q_{0,| |}
$$

As $Q_{0,| |}$ is $\Sigma \cup\{|\mid\}$-minimal, we know that $\psi$ is surjective. Thus, to complete the proof, we must show that $\psi$ is also injective.

The carrier of $Q_{0,| |}$ is the same as $Q_{0}$ and is

$$
\begin{aligned}
\mathbb{Q}= & \{0\} \cup\left\{\left.\frac{n}{m} \right\rvert\, n>0, m>0, \operatorname{gcd}(n, m)=1\right\} \\
& \cup\left\{\left.-\frac{n}{m} \right\rvert\, n>0, m>0, \operatorname{gcd}(n, m)=1\right\} .
\end{aligned}
$$

This suggests that we should use the previous transversal

$$
\begin{aligned}
T R= & \{\underline{0}\} \cup\left\{\underline{n} \cdot \underline{m}^{-1} \mid n>0, m>0, \operatorname{gcd}(n, m)=1\right\} \\
& \cup\left\{-\left(\underline{n} \cdot \underline{m}^{-1}\right) \mid n>0, m>0, \operatorname{gcd}(n, m)=1\right\} .
\end{aligned}
$$

as a transversal for $T(\Sigma \cup\{|\mid\}, E)$. Following the pattern of Theorem 3.1, we can prove new versions of the evaluation and transversal Lemmas 3.2 and 3.3.

First, we generalize the numeral notation for the naturals to a notation for the rationals. For each $r \in \mathbb{Q}$, we define

$$
\begin{aligned}
\underline{r} & =0 & & \text { if } r=0 ; \\
& =\underline{n} \cdot \underline{m}^{-1} & & \text { if } r=\frac{n}{m} \text { and } n>0, m>0, \operatorname{gcd}(n, m)=1 \\
& =-\left(\underline{n} \cdot \underline{m}^{-1}\right) & & \text { if } r=-\frac{n}{m} \text { and } n>0, m>0, \operatorname{gcd}(n, m)=1
\end{aligned}
$$

Thus, with this notation, $T R=\{\underline{r} \mid r \in \mathbb{Q}\}$.
Lemma 4.3. The $\Sigma \cup\{|\mid\}$ homomorphism $\psi$ satisfies $\psi([\underline{r}])=r$ for all $r \in \mathbb{Q}$.
Proof. This follows the same arguments as the proof of Lemma 3.2. Note clauses (i), (v) and (vi).

Lemma 4.4. The set $T R$ is a transversal for the equivalence relation $\equiv_{E}$ on $T(\Sigma \cup\{|\mid\})$.

Suppose we have proved this fact, then we can conclude the proof of the theorem as follows. If

$$
\psi([t])=\psi\left(\left[t^{\prime}\right]\right),
$$

then, by Lemma 4.4, there exist $\underline{r}, \underline{r}^{\prime} \in T R$ such that

$$
E \vdash t=\underline{r} \text { and } E \vdash t^{\prime}=\underline{r}^{\prime} .
$$

Thus,

$$
\psi([\underline{r}])=\psi\left(\left[\underline{r}^{\prime}\right]\right) .
$$

Now, by Lemma 4.3,

$$
\psi([\underline{r}])=r \text { and } \psi\left(\left[\underline{r}^{\prime}\right]\right)=r^{\prime} .
$$

Thus,

$$
r=r^{\prime} .
$$

Since $T R$ is a transveral, this happens if, and only if, the terms

$$
\underline{r}=\underline{r}^{\prime}
$$

and hence $[\underline{r}]=\left[r^{\prime}\right]$ and $[\underline{t}]=\left[\underline{t}^{\prime}\right]$.
It remains to prove Lemma 4.4. We note the following.
LEMMA 4.5. $\quad C R \cup M O D \cup$ Modril $\vdash I$
Proof. We can write the set $I$ as

$$
I=\{Z(\underline{n})=0 \mid n>0\}
$$

and so prove, by induction on $n>0$, that $C R \cup M O D \cup \operatorname{Modril} \vdash Z(\underline{n})=0$.

Basis $n=1$. We calculate:

$$
\begin{aligned}
Z(\underline{1}) & =Z(\underline{1}+\underline{0}) & & \text { by } C R 3 \text { and the definition of } \underline{0} \\
& =Z(\underline{1}+|\underline{0}|) & & \text { by MOD } 1 \\
& =0 & & \text { by Modril. }
\end{aligned}
$$

Induction Step $n=k+1$. We calculate:

$$
\begin{aligned}
Z(\underline{k+1}) & =Z(\underline{k}+1) & & \text { by the definition of } \underline{k+1} \\
& =Z(1+\underline{k}) & & \text { by } C R 2 \\
& =Z(1+|\underline{k}|) & & \text { by Lemma } 4.1 \\
& =0 & & \text { by Modril. }
\end{aligned}
$$

We can show that for every term $t \in T(\Sigma \cup\{|\mid\})$ there is an $\underline{r} \in T R$ such that $E \vdash t=\underline{r}$. Notice that by Lemma 4.5, and Lemma 3.3, we know that for all terms $t$ not containing $\|, t \in T(\Sigma), E \vdash t=\underline{r}$.

We prove the transversal lemma by induction on the height $H t(t)$ of terms $t \in$ $T(\Sigma \cup\{|\mid\})$.

Basis. $H t(t)=0$. Then $t=0$ or $t=1$ and we are done.
Induction Step, $H t(t)=k+1$. Suppose that the lemma is true for terms of height lower than $H t(t)=k$ and consider a term of height $k$. There are five cases corresponding to the operations. We consider two for illustration.

Case $t=s+s^{\prime}$. By induction,

$$
E \vdash s=\underline{r} \text { and } E \vdash s^{\prime}=\underline{r}^{\prime}
$$

for $\underline{r}, \underline{r}^{\prime} \in T R$. Thus,

$$
E \vdash s+s^{\prime}=\underline{r}+\underline{r}^{\prime} .
$$

Now $\underline{r}+\underline{r}^{\prime}$ does not contain || and so reduces to some element in $T R$.
Case $t=|s|$. This is the interesting case. By induction, $E \vdash s=\underline{r}$. There are three subcases.

If $\underline{r}=\underline{0}$, then $t=|\underline{r}|=|\underline{0}|=0$ by $M O D 1$.
If $\underline{r}=\underline{n} \cdot \underline{m}^{-1}$, then

$$
\begin{aligned}
t & =\left|\underline{n} \cdot \underline{m}^{-1}\right| & & \text { by definition } \\
& =|\underline{n}| \cdot\left|\underline{m}^{-1}\right| & & \text { by } M O D 4 \\
& =|\underline{n}| \cdot|\underline{m}|^{-1} & & \text { by } M O D 5 \\
& =\underline{n} \cdot \underline{m}^{-1} & & \text { by Lemma } 4.1 .
\end{aligned}
$$

If $\underline{r}=-\left(\underline{n} \cdot \underline{m}^{-1}\right)$, then

$$
\begin{aligned}
t & =\left|-\left(\underline{n} \cdot \underline{m}^{-1}\right)\right| & & \text { by the definition } \\
& =\underline{n} \cdot \underline{m}^{-1} & & \text { by } M O D 3 .
\end{aligned}
$$

The specification $C R \cup S I P \cup M O D \cup$ Modril of the rational numbers is simpler than the specification $C R \cup S I P \cup L$ because it does not depend on (somewhat) sophisticated number theory.

## 5. Specifications of Totalized Fields and Other Rational Arithmetics

5.1. On the Equational Theory of Totalized Fields. It has long been known that the class of totalised fields is not a variety, that is, is not definable by equations over the field signature. The argument is based on the fact that the class of totalised fields is not closed under products (compare Birkhoff's Theorem, see, e.g., Meinke and Tucker [1992]).

We can rephrase and reprove this elementary fact in the present setting as follows:
Lemma 5.1. There is no set $E$ of equations over the signature $\Sigma$ of fields that is logically equivalent with $C R \cup S I P \cup S e p \cup$ Gil.

Proof. Assume the contrary and suppose that there is such a set of equations $E$ such that $\operatorname{Alg}(\Sigma, E)=\operatorname{Alg}(\Sigma, C R \cup S I P \cup S e p \cup G i l)$. Consider the initial algebra $I(\Sigma, E)$ of $E$. Now because the $\Sigma$-algebra $Q_{0}$ of rational numbers is a model of $E$, we know that

$$
I(\Sigma, E) \models \neg(1+1=0) .
$$

To see this, note that if $1+1=0$ was valid in the initial model $I(\Sigma, E)$ in then it would be valid under every homomorphism and, in particular, would be valid in $Q_{0}$, which it is not.

Now, by assumption, $I(\Sigma, E) \models C R \cup S I P \cup S e p \cup$ Gil and this implies

$$
I(\Sigma, E) \models Z(1+1)=0 .
$$

But the prime totalized field $Z_{2}$ of characteristic 2 is also a model of $C R \cup S I P \cup$ Sep $\cup$ Gil. By initiality, here is an unique homomorphism $\phi: I(\Sigma, E) \rightarrow Z_{2}$ and, being a minimal structure, $Z_{2}$ must be a homomorphic image of $I(\Sigma, E)$. Now since $Z(x)$ is a term, $\phi Z(a)=Z(\phi(a))$ for all $a \in A$ and $\phi(Z(1+1))=Z(\phi(1+1))=$ $Z(\phi(1)+\phi(1))=Z(1+1)$. In $Z_{2}$, we have $1+1=0$, which implies $Z(1+1)=1$. Thus, the unique homomorphism $\phi$ maps $Z(1+1)=0$ in $I(\Sigma, E)$ to $Z(1+1)=1$ in $Z_{2}$, which is impossible for a homomorphism since the algebras satisfy Sep. (In fact, more generally all homomorphisms between fields must be injective.) This is a contradiction.

Using a similar argument one can prove that there is no conditional equational theory C E over the signature $\Sigma$ of fields which is equivalent to $C R \cup S I P \cup S e p \cup$ Gil in first order logic.
5.2. The Restricted Inverse Law. Recall Ril is

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

In the presence of $C R \cup S I P$, another way of writing Ril is as follows:

$$
Z(x) \cdot x=0 .
$$

We will now use the equational specification $(\Sigma, C R \cup S I P \cup R i l)$. If one restricts attention to the closed equations over $\Sigma$, an interesting positive result is found (Theorem 5.6).

Now Ril is derivable from $C R \cup S I P \cup S e p \cup G i l$ and for that reason $C R \cup S I P \cup$ Ril is a weaker theory than $C R \cup S I P \cup S e p \cup$ Gil. Of course, the key point is that $C R \cup S I P \cup R i l$ is an equational theory over $\Sigma$ in which inverses are possible.

To illustrate further the implications of Ril, here is a listing of identities that can easily be proved from $C R \cup S I P \cup R i l$ :

LEMMA 5.2. The following equations can be proved from $C R \cup S I P \cup$ Ril

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

Proof. Equations (1) and (2) are obvious in any commutative ring. The other cases are calculations; we do the remaining cases.

Consider $Z(x) \cdot Z(x)=Z(x)$.

$$
\begin{aligned}
Z(x) \cdot Z(x) & =\left(1-x \cdot x^{-1}\right) \cdot\left(1-x \cdot x^{-1}\right) \\
& =1-x \cdot x^{-1}-x \cdot x^{-1}+\left(x \cdot x^{-1}\right) \cdot\left(x \cdot x^{-1}\right) \\
& =1-x \cdot x^{-1}-x \cdot x^{-1}+\left(x \cdot x^{-1} \cdot x\right) \cdot x^{-1} \\
& =1-x \cdot x^{-1}-x \cdot x^{-1}+x \cdot x^{-1} \\
& =1-x \cdot x^{-1} \\
& =Z(x) .
\end{aligned} \quad \text { by Ril }
$$

Consider $Z(x)^{-1}=Z(x)$.

$$
\begin{aligned}
Z(x)^{-1} & =Z(x)^{-1} \cdot\left(Z(x)^{-1} \cdot Z(x)\right) & & \text { by Ril } \\
& =(Z(x) \cdot Z(x))^{-1} \cdot Z(x) & & \text { by SIP } \\
& =Z(x)^{-1} \cdot Z(x) & & \text { by above } \\
& =Z(x)^{-1} \cdot Z(x) \cdot Z(x) & & \text { by above } \\
& =Z(x) . & &
\end{aligned}
$$

Consider $(1-Z(x)) \cdot(1-Z(x))=1-Z(x)$.

$$
\begin{aligned}
(1-Z(x)) \cdot(1-Z(x)) & =1-Z(x)-Z(x)+Z(x) \cdot Z(x) & & \text { by expansion } \\
& =1-Z(x)-Z(x)+Z(x) & & \text { by above } \\
& =1-Z(x) & &
\end{aligned}
$$

Consider $(1-Z(x))^{-1}=1-Z(x)$.

$$
\begin{array}{rlrl}
(1-Z(x))^{-1} & =\left(1-\left(1-x \cdot x^{-1}\right)\right)^{-1} & & \text { by expansion } \\
& =\left(x \cdot x^{-1}\right)^{-1} & & \\
& =x^{-1} \cdot\left(x^{-1}\right)^{-1} & & \text { by } C R \\
& =x^{-1} \cdot x & & \text { by } C R \\
& =x \cdot x^{-1} & & \\
& =\left(1-\left(1-x \cdot x^{-1}\right)\right) & & \\
& =1-Z(x) . &
\end{array}
$$

Lemma 5.3. Let $p, q$ be different prime numbers. Then

$$
C R \cup S I P \cup R i l \vdash Z(\underline{p}) \cdot Z(\underline{q})=0 .
$$

Proof. Let $a, b \in \mathbb{Z}$ be such that $1=a \cdot p+b \cdot q$. There are different cases of which we will do one. Assume $a=n$ and $b=-m$ for $n, m \in \mathbb{N}$. Then $\underline{1}=\underline{n} \cdot \underline{p}-\underline{m} \cdot \underline{q}$. We calculate:

$$
\begin{aligned}
Z(\underline{p}) & =Z(\underline{p}) \cdot 1 & & \text { by multiplying } \\
& =Z(\underline{p}) \cdot(\underline{n} \cdot \underline{p}-\underline{m} \cdot \underline{q}) & & \text { by substituting } \\
& =Z(\underline{p}) \cdot \underline{n} \cdot \underline{p}-Z(\underline{p}) \cdot \underline{m} \cdot \underline{q} & & \text { by SIP } \\
& =Z(\underline{p}) \cdot \underline{p} \cdot \underline{n}-Z(\underline{p}) \cdot \underline{q} \cdot \underline{m} & & \text { by above } \\
& =0 \cdot \underline{n}-Z(\underline{p}) \cdot \underline{q} \cdot \underline{m} & & \text { by Ril } \\
& =Z(\underline{p}) \cdot \underline{q} \cdot-\underline{m} . & &
\end{aligned}
$$

By Lemma 2.3, we have $Z(\underline{p})=Z(\underline{p}) \cdot \underline{q} \cdot \underline{q}^{-1}$. Thus, $Z(\underline{p}) \cdot\left(1-\underline{q} \cdot \underline{q}^{-1}\right)=0$ and this is $Z(\underline{p}) \cdot Z(\underline{q})=0$.

Lemma 5.4. For each prime $p$ and closed term $t \in \Sigma$, there is a unique natural number $n<p$ such that

$$
C R \cup S I P \cup R i l \vdash Z(\underline{p}) \cdot t=Z(\underline{p}) \cdot \underline{n} .
$$

Proof. This is proved by an induction on the structure of $t$.
Basis. If $t \equiv \underline{k}$ then write $k=n+p \cdot l$ for natural numbers $n$ and $l$ with $n<p$. Now

$$
\begin{array}{rlrl}
Z(\underline{p}) \cdot \underline{k} & =Z(\underline{p}) \cdot n+p \cdot l \\
& =Z(\underline{p}) \cdot \underline{n}+Z(\underline{p}) \cdot \underline{p} \cdot \underline{l} & & \text { by substitution } \\
& =Z(\underline{p}) \cdot \underline{n} & & \text { by } C R \\
& & \text { by Ril. }
\end{array}
$$

Induction Step. There are four cases corresponding with $+,-, \cdot,{ }^{-1}$ of which we will do one for illustration.

Let $t \equiv r^{-1}$ then we calculate:

$$
\begin{aligned}
Z(\underline{p}) \cdot \underline{t} & =Z(\underline{p}) \cdot r^{-1} & & \text { by substitution } \\
& =Z(\underline{p}) \cdot Z(\underline{p}) \cdot r^{-1} & & \text { by Lemma } 5.2 \\
& =Z(\underline{p}) \cdot(Z(\underline{p}))^{-1} \cdot r^{-1} & & \text { by Lemma } 5.2 \\
& =Z(\underline{p}) \cdot(Z(\underline{p}) \cdot r)^{-1} & & \text { by SIP } \\
& =Z(\underline{p}) \cdot(Z(\underline{p}) \cdot \underline{n})^{-1} & & \text { by induction } \\
& =Z(\underline{p}) \cdot(Z(\underline{p}))^{-1} \cdot \underline{n}^{-1} & & \text { by } S I P \\
& =Z(\underline{p}) \cdot \underline{n}^{-1} & & \text { by Lemma } 5.2
\end{aligned}
$$

$$
=Z(\underline{p}) \cdot \underline{m} \quad \text { with } m<p \text { such that } m=n^{-1} \quad \bmod p
$$

That the number $\underline{n}$ is unique follows from an inspection of the prime field of characteristic $p$. In that field $Z(p)$ equals 1 while different numerals $n_{1}$ and $n_{2}$ with $n_{1}$ and $n_{2}$ both below $p$ have different interpretations.

By inspection, we can check the following refinement of the statement of the lemma.

Corollary 5.5. Let val $l_{p}^{0}(t)$ the value of term $t$ in the totalised field $K_{p}^{0}$. The unique number $\underline{n}$ is val ${ }_{p}^{0}(t)$. Therefore, we have

$$
C R \cup S I P \cup \operatorname{Ril} \vdash Z(\underline{p}) \cdot t=Z(\underline{p}) \cdot \underline{v a l} l_{p}^{0}(t) .
$$

The following theorem states that the equational subtheory $T_{\text {feld }}^{0}$ can prove all the closed identities that are true in all fields.

Theorem 5.6. For any closed terms $t, t^{\prime} \in T(\Sigma)$, we have

$$
T_{\text {feeld }}^{0} \vdash t=t^{\prime} \text { implies } C R \cup S I P \cup \text { Ril } \vdash t=t^{\prime}
$$

Recall that if $T_{\text {field }} \vdash t=t^{\prime}$ then $T_{\text {field }}^{0} \vdash t=t^{\prime}$.
PROOF. The proof is rather involved with many calculations needed to establish canonical forms. The canonical forms depend on the characteristics of the totalized fields.

Let $p_{n}$ represent an enumeration of the primes in increasing order, starting with $p_{0}=2$. Then, we define the following special terms:

$$
G_{1}=1, G_{2}=1-Z\left(\underline{p_{1}}\right), G_{n+1}=G_{n} \cdot\left(1-Z\left(\underline{p_{n}}\right)\right) .
$$

For each $n$, the term $G_{n}$ equals 0 in any prime field $K_{p_{n}}^{0}$ with characteristic $p_{n}$ or less. For all $n$, the term $G_{n}$ equals 1 in any field of characteristic 0 and, in particular, in the totalized field of rational numbers.

Lemma 5.7. For all $n$, we have:
(i) $G_{n}=1-Z\left(\underline{p_{1}}\right)-\cdots-Z\left(\underline{p_{n-1}}\right)$.
(ii) $G_{n} \cdot Z\left(p_{n}\right)=\bar{Z}\left(p_{n}\right)$
(iii) if $n \leq \overline{m,}$ then $G_{m} \cdot G_{n}=G_{m}$
(iv) if $k<p_{n}$, then $G_{n} \cdot \underline{k} \cdot \underline{k}^{-1}=G_{n}$.

Proof. Exercise.

Using these $G$ terms the following lemma can be stated:
Lemma 5.8. For each closed term $t$ over $\Sigma$, there is a unique term $\underline{r} \in T R$ such that $C R \cup S I P \cup R i l \vdash G_{n} \cdot t=G_{n} \cdot \underline{r}$.

Proof. The proof uses induction of the structure of terms. We give the case of addition in the induction step. Let $t \equiv r+s$ and assume that

$$
C R \cup S I P \cup \text { Ril } \vdash G_{n} \cdot r=G_{n} \cdot r^{\prime} \text { and } C R \cup S I P \cup R i l \vdash G_{m} \cdot s=G_{m} \cdot s^{\prime}
$$

with $r^{\prime}, s^{\prime} \in T R$. Now there is a case distinction on the possible forms of $r^{\prime}$ and $s^{\prime}$.
Let $r^{\prime} \equiv \underline{k} \cdot \underline{l}^{-1}$ and $s^{\prime} \equiv \underline{u} \cdot \underline{v}^{-1}$. Take $i$ larger than $m$ and $n$ such that $p_{i}$ exceeds both $l$ and $\bar{v}$. Now $C R \cup S I \bar{P} \cup$ Ril proves

$$
\begin{aligned}
G_{i} \cdot t=G_{i} \cdot(r+s) & =G_{i} \cdot r+G_{i} \cdot s \\
& =G_{i} \cdot \underline{k} \cdot \underline{l}^{-1}+G_{i} \cdot \underline{u} \cdot \underline{v}^{-1} \\
& =G_{i} \cdot \underline{v} \cdot \underline{v}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1}+G_{i} \cdot \underline{l} \cdot \underline{l}^{-1} \cdot \underline{u} \cdot \underline{v}^{-1} \\
& =G_{i} \cdot\left(\underline{v} \cdot \underline{k} \cdot \underline{v}^{-1} \cdot \underline{l}^{-1}+\underline{l} \cdot \underline{u} \cdot \underline{l}^{-1} \cdot \underline{v}^{-1}\right) \\
& =G_{i} \cdot(\underline{v} \cdot \underline{k}+\underline{l} \cdot \underline{u}) \cdot(\underline{l} \cdot \underline{v})^{-1} \\
& =G_{i} \cdot \underline{v} \cdot \underline{k}+\boldsymbol{l} \cdot \mathbf{u} \cdot(\underline{l} \cdot \underline{v})^{-1} \\
& =G_{i} \cdot \underline{k^{\prime}} \cdot\left(\underline{l}^{\prime}\right)^{-1} \cdot
\end{aligned}
$$

If $k^{\prime}$ and $l^{\prime}$ are not relatively prime, they share a prime factor $q=p_{j}$. In particular: $k^{\prime}=q \cdot k^{\prime \prime}$ and $l^{\prime}=q \cdot l^{\prime \prime}$. Let $h=\max (i, j)$ then $C R \cup S I P \cup$ Ril $\vdash G_{i^{\prime}} \cdot t=$ $G_{i^{\prime}} \cdot \underline{k^{\prime \prime}} \cdot \underline{l}^{\prime \prime}$. By repeating the removal of shared prime factors until no more exist the required representation is obtained. That the representation is unique follows from its interpretation in the prime field of characteristic 0 .

The following defines the canonical terms:
Lemma 5.9. Let $t \in T(\Sigma)$. Suppose that

$$
C R \cup S I P \cup \text { Ril } \vdash G_{n} \cdot t=G_{n} \cdot \underline{v a l_{0}^{0}(t) .}
$$

Then, for all $m>n$,

$$
C R \cup S I P \cup \text { Ril } \vdash t=\sum_{i=1}^{m-1} Z\left(\underline{p_{i}}\right) \cdot \underline{v a l}_{p_{i}}^{0}(t)+G_{m} \cdot \underline{v_{0} a l_{0}^{0}(t)} .
$$

Proof. We begin with a lemma.
Lemma 5.10. For each $n \in \mathbb{N}$,

$$
C R \cup S I P \cup \operatorname{Ril} \vdash G_{n} \cdot t=Z\left(\underline{p_{n}}\right) \cdot \underline{v a l_{p_{n}}^{0}(t)}+G_{n+1} \cdot t .
$$

Proof. This is a calculation:

$$
\begin{aligned}
G_{n} \cdot t & =\left(Z\left(\underline{p_{n}}\right)+\left(1-Z\left(\underline{p_{n}}\right)\right)\right) \cdot G_{n} \cdot t & & \text { by } C R \\
& =Z\left(\underline{p_{n}}\right) \cdot G_{n} \cdot t+\left(1-Z\left(\underline{p_{n}}\right)\right) \cdot G_{n} \cdot t & & \text { by } C R \\
& =Z\left(\underline{p_{n}}\right) \cdot G_{n} \cdot t+G_{n+1} \cdot t & & \text { by definition } \\
& =G_{n} \cdot Z\left(\underline{p_{n}}\right) \cdot t+G_{n+1} \cdot t & & \text { by } C R \\
& =G_{n} \cdot Z\left(\underline{p_{n}}\right) \cdot v a l_{p_{n}}^{0}(t)+G_{n+1} \cdot t & & \text { by Corollary } 5.5 \\
& =Z\left(\underline{p_{n}}\right) \cdot v a l_{p_{n}}^{0}(t)+G_{n+1} \cdot t & & \text { by Lemma } 5.7 .
\end{aligned}
$$

Now we choose $k \in \mathbb{N}$ such that $C R \cup S I P \cup$ Ril $\vdash G_{k} \cdot t=G_{k} \cdot \underline{r}$ for some $\underline{r} \in T R$. Then we may expand the formula as follows:

$$
\begin{aligned}
t & =G_{1} \cdot t & & \text { because } G_{1}=1 \\
& =Z\left(\underline{p_{1}}\right) \cdot \underline{v a l_{p_{1}}^{0}(t)+G_{2} \cdot t} & & \text { and } C R \\
& =Z\left(\underline{p_{1}}\right) \cdot \underline{v a l_{p_{1}}^{0}(t)}+Z\left(\underline{p_{2}}\right) \cdot \underline{v a l_{p_{2}}^{0}(t)+G_{3} \cdot t} & & \text { by Lemma } 5.10 \\
& =Z\left(\underline{p_{1}}\right) \cdot \underline{v a l_{p_{1}}^{0}(t)}+\cdots+Z\left(\underline{p_{k-1}}\right) \cdot v a l_{p_{k-1}}^{0}(t)+G_{k} \cdot t & & \text { by repeated use of } \\
& =Z\left(\underline{p_{1}}\right) \cdot v a l_{p_{1}}^{0}(t)+\cdots+Z\left(\underline{p_{k-1}}\right) \cdot \underline{v a l_{p_{k-1}}^{0}(t)+G_{k} \cdot \underline{r}} & & \text { bemma choice of } k .
\end{aligned}
$$

This completes the proof of the Lemma 5.9
Finally, we can complete the proof of Theorem 5.6. Assume that

$$
T_{\text {field }}^{0} \vdash t=s
$$

for any closed terms $t, s \in T(\Sigma)$. We choose $n, m$ such that

$$
\begin{aligned}
C R \cup S I P \cup R i l \vdash G_{n} \cdot t & =G_{n} \cdot \underline{v a l_{0}^{0}(t)} \\
C R \cup S I P \cup R i l \vdash G_{m} \cdot s & =G_{m} \cdot \underline{v a l_{0}^{0}(s)} .
\end{aligned}
$$

Take $k=\max (n, m)$. Then, by Canonical Term Lemma 5.9,

$$
\begin{aligned}
& C R \cup S I P \cup R i l \vdash t=\sum_{i=1}^{k} Z\left(\underline{p_{i}}\right) \cdot \underline{v_{l} l_{p_{i}}^{0}(t)}+G_{k} \cdot \cdot \underline{v_{l} l_{0}^{0}(t)} \\
& C R \cup S I P \cup R i l \vdash s=\sum_{i=1}^{k} Z\left(\underline{p_{i}}\right) \cdot \underline{v_{i} l_{p_{i}}^{0}(s)}+G_{k} \cdot \underline{v_{0} l_{0}^{0}(s)} .
\end{aligned}
$$

Since $T_{\text {field }}^{0} \vdash t=s$, the values of these closed terms in all prime fields are identical, that is, for all $p_{i}, v a l_{p_{i}}^{0}(t)=\operatorname{val}_{p_{i}}^{0}(s)$ and $v a l_{0}^{0}(t)=v a l_{0}^{0}(s)$. Thus, the expansions on the right-hand side are identical and so we have

$$
C R \cup S I P \cup R i l \vdash t=s .
$$

The initial algebra of $C R$ is the integers. However, we note that
Corollary 5.11. The initial algebra of $C R \cup S I P \cup$ Ril is a computable algebra but it is not an integral domain.

Proof. It is easy to check that the completeness proof for closed term equations (Theorem 5.6) also provides the decidability of their derivability. In any integral domain, we have $x \cdot y=0$ implies $x=0$ or $y=0$. Let $x=Z(2)$ and let $y=1-Z(2)$. We calculate: $C R \cup S I P \cup \vdash \mathbf{Z}(2) \cdot(1-\mathbf{Z}(2))=\mathbf{Z}(2)-\mathbf{Z}(2) \cdot \mathbf{Z}(2)=$ $Z(2)-\mathbf{Z}(2)=0$. Thus, for these choices, $x \cdot y=0$ in the initial meadow. But both $x$ and $y$ are not equal to 0 in the initial meadow because, under homomorphisms, $x \neq 0$ and $y \neq 0$ in prime fields with different characteristics 2 and 0.

The algebras that are models of $C R \cup S I P \cup$ Ril have nice properties, in spite of not being fields nor even integral domains. We have the following proposal for a name, derived from their connection with fields:

Definition 5.12. A model of $C R \cup S I P \cup$ Ril is called a meadow.
All fields are clearly meadows but not conversely (as the initial meadow is not a field). In fact, the theorem proves a normal form theorem for meadows.

## 6. Concluding Remarks

6.1. Open Problems. The rational numbers are not well understood computationally or logically, even in the case of equational logic, possibly the simplest logic. We failed to obtain answers to the following problems:

PROBLEM 6.1. Does the totalized field $Q_{0}$ of rational numbers have a decidable equational theory?

In connection with algebraic specifications, the following is related to Problem 6.1. In fact, its positive solution would, by general specification theory, solve Problem 6.1.

PROBLEM 6.2. Does the totalized field $Q_{0}$ have a finite basis, that is, an $\omega$ complete equational initial algebra specification?

The following problem is quite basic:

PROBLEM 6.3. Is there a finite equational specification of the totalised field $Q_{0}$, without hidden functions, which constitutes a complete term rewriting system?

We know from our Bergstra and Tucker [1995] that there exists such a specification with hidden functions.

Equations over $Q_{0}$ are called diophantine equations, just as equations over the integers are. We do not know the answer to this question:

PROBLEM 6.4. Does the totalized field $Q_{0}$ of rational numbers have a decidable diophantine theory, that is, can one decide whether or not $\exists x_{1}, \ldots, x_{n}\left[t_{1}\left(x_{1}, \ldots, x_{n}\right)=t_{2}\left(x_{1}, \ldots, x_{n}\right)\right]$ ?

If the diophantine theory of the totalized field of rationals is decidable (Problem 6.4), then the diophantine theory of the ring of rationals is also decidable (as it is the syntactic subtheory without division), and this latter question is a long standing open problem. Perhaps it is easier to show that Problem 6.4 is undecidable.

The specifications we have presented lead to questions, for instance:
Problem 6.5. Does the specification $C R \cup S I P$ admit Knuth-Bendix completion?

Questions proliferate as one reflects on the number of algebras based on rational numbers.

PROBLEM 6.6. Is there a finite equational specification of the algebra $Q_{0}(i)$ of complex rational numbers, without hidden functions?

It is in fact possible to provide an initial algebra specification using the complex conjugate $c c$ as an hidden function: see Bergstra and Tucker [2006a]. In the matter of term rewriting, we do not know the answer to this question:

PROBLEM 6.7. Is there a finite equational specification of the algebra $Q_{0}(i, c c)$, (without further hidden functions), which constitutes a complete term rewriting system?

Although there seems to be little work with this precise focus (e.g., Contejean et al. [1997]), a great deal is known about computable fields (see Stoltenberg-Hansen and Tucker [1999b]).
6.2. Related and Future Work. It seems to us that an important task for the theory of algebraic specifications-and for formal methods in general-is this:

PROBLEM 6.8. To create a comprehensive theory of computing, specifying and reasoning with systems based on continuous data. Ideally, the theory should integrate discrete and continuous data.

At present, this is a huge and complicated task because computation, specification and verification on continuous data are all active research areas with disparate agendas. In fact, the task is a challenge in the special case of real numbers. The existing algebraic specification literature on the reals is limited. One of the earliest attempts at an axiomatic specification of any data type was the study of computer reals in van Wijngaarden [1966]. In Roggenbach et al. [2004], there is an axiomatization designed for the algebraic specification language CASL. In Tucker and Zucker [2002], there is a specification using infinite terms.

There is some progress on the question: Can all computable functions on continuous data be algebraically specified? In Tucker and Zucker [2005], it is shown that a computably approximable function on a complete metric algebra can be specified by a form of conditional equations. In fact it is shown there is one universal set of equations that can specify all computably approximable functions. (See Tucker and Zucker [2004] for the compact case and Tucker and Zucker [2005] for the general case.) There are many notions of computable function on the real numbers: see Tucker and Zucker [2000].

Obviously, technically, the specification theory of rational arithmetics is a basic subject for these tasks. If the rational numbers are the data type for measuring in units and subunits then the real numbers can be seen as the data type for the process of measuring to arbitrary accuracy, the measuring procedures being modeled by Cauchy sequences.

Our specification $C R \cup S I P$ draws attention to division by zero. Division by zero has been studied by Setzer [1997] in which he proposed the concept of wheels, a sophisticated modification of integral domains with constants for infinity and undefined, and division by zero with $0^{-1}=\infty$. Setzer's idea has been taken up in Carlström [2004].

For algebraic specification there is a great interest in limited types of first order formulae that are "close" to equations. Of course, conditional equations are an important example since they have initial models; another example of formulae are multi-equations studied by Adamek et al. [2002].

The problem is connected to many others such as the algebraic approaches to numerical software for scientific simulation, in Haveraaen [2000] and Haveraaen et al. [2005], and to 3D and 4D volume graphics, in Chen and Tucker [2000]. In fact, it is not an uncommon view that the problem of integrating discrete and continuous computation is a barrier to progress in computer science and its application.

## REFERENCES

Adamek, J., Hebert, M., and Rosicky, J. 2002. On abstract data types presented by multiequations. Theoret. Comput. Sci. 275, 427-462.
Bergstra, J. A. 2006. Elementary algebraic specifications of the rational function field. In Logical approaches to computational barriers. Proceedings of Computability in Europe 2006, A. Beckmann et al. Eds. Lecture Notes in Computer Science, vol. 3988, Springer-Verlag, New York, 40-54.
Bergstra, J. A., AND Tucker, J. V. 1982. The completeness of the algebraic specification methods for data types. Inf. Cont. 54, 186-200.
Bergstra, J. A., AND Tucker, J. V. 1983. Initial and final algebra semantics for data type specifications: Two characterisation theorems. SIAM J. Comput. 12, 366-387.
Bergstra, J. A., AND Tucker, J. V. 1987. Algebraic specifications of computable and semicomputable data types. Theoret. Comput. Sci. 50, 137-181.
Bergstra, J. A., And Tucker, J. V. 1995. Equational specifications, complete term rewriting systems, and computable and semicomputable algebras. J. ACM 42, 1194-1230.
Bergistra, J. A., And Tucker, J. V. 2005. The rational numbers as an abstract data type. Res. Rep. PRG0504, Programming Research Group, University of Amsterdam, August 2005, or Tech. Rep. CSR122005, Department of Computer Science, University of Wales, Swansea, August 2005.
BERGSTRA, J. A., AND TUCKER, J. V. 2006a. Elementary algebraic specifications of the rational complex numbers. In Goguen Festschrift, K. Futatsugi et al., Eds. Lecture Notes in Computer Science, vol. 4060. Springer-Verlag, New York, pp. 459-475.
Bergstra, J. A., And Tucker, J. V. 2006b. Division safe calculation in totalised fields. Res. Rep. PRG 0605, Programming Research Group, University of Amsterdam, September 2006 or Tech. Rep. CSR 14-2006, Department of Computer Science, University of Wales Swansea, September 2006.
Calkin, N., AND WILF, H. S. 2000. Recounting the rationals. Amer. Math. Monthly 107, 360-363.
CARLSTRÖM, J. 2004. Wheels - On division by zero. Math. Struct. Comput. Sci. 14, 143-184.
Chen, M., AND Tucker, J. V. 2000. Constructive volume geometry. Computer Graphics Forum 19, 281-293.
Contejean, E., Marche, C., and Rabehasaina, L. 1997. Rewrite systems for natural, integral, and rational arithmetic. In Rewriting Techniques and Applications 1997. Lecture Notes in Computer Science vol. 1232. Springer-Verlag, Berlin, Germany, pp. 98-112.
DICKSON, L. E. 1952. History of the Theory of Numbers. Chelsea, New York.
Goguen, J. A., Thatcher, J. W., And Wagner, E. G. 1978. An initial algebra approach to the specification, correctness and implementation of abstract data types. In Current Trends in Programming Methodology. IV. Data Structuring R.T. Yeh, Ed., Prentice-Hall, Engelwood Cliffs, pp. 80-149.
Harrison, J. 1998. Theorem Proving with the Real Numbers, Springer-Verlag, New York.
HAVERAAEN, M. 2000. Case study on algebraic software methodologies for scientific computing. Sci. Prog. 8, 261-273.
Haveraaen, M., Friis, H. A., and Munthe-KaAs, H. 2005. Computable scalar fields: A basis for PDE software. J. Logic Alg. Prog. 65, 36-49.
Hodges, W. 1993. Model Theory. Cambridge University Press, Cambridge, UK.

Meinke, K., And Tucker, J. V. 1992. Universal algebra. In Handbook of Logic in Computer Science. Volume I: Mathematical Structures, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 189-411.
Meseguer, J., And Goguen, J. A. 1985. Initiality, induction and computability. In Algebraic Methods in Semantics. M. Nivat and J. Reynolds, Eds. Cambridge University Press, Cambridge, pp. 459-541.
Klop, J. W. 1992. Term rewriting systems. In Handbook of Logic in Computer Science. Volume 2: Mathematical Structures, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 1-116.
Moss, L. 2001. Simple equational specifications of rational arithmetic. Discr. Math. Theoret. Comput. Sci. 4, 291-300.
Roggenbach, M., Schröder, L., and Mossakowski, T. 2004. Specifying real numbers in CASL. In Recent Trends in Algebraic Development Techniques. 14th International Workshop (WADT'99) (Chateau de Bonas, Sept. 15-18, 1999), D. Bert, C. Choppy, and P. D. Mosses, Eds. Lecture Notes in Computer Science, vol. 1827. Springer-Verlag, Berlin, 146-161.
SETZER, A. 1997. Wheels. Manuscript, 8 pp. Download at: http://www.cs.swan.ac.uk/csetzer.
Stoltenberg-Hansen, V., and Tucker, J. V. 1995. Effective algebras. In Handbook of Logic in Computer Science. Volume IV: Semantic Modelling, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 357-526.
Stoltenberg-Hansen, V., and Tucker, J. V. 1999. Computable rings and fields. In Handbook of Computability Theory, E. Griffor, Ed. Elsevier, North-Holland, Amsterdam, The Netherlands, pp. 363447.

Stoltenberg-Hansen, V., and Tucker, J. V. 1999. Concrete models of computation for topological algebras. Theoret. Comput. Sci. 219, 347-378.
Terese, 2003. Term Rewriting Systems. Cambridge Tracts in Theoretical Computer Science 55, Cambridge University Press, Cambridge, UK.
TUCKER, J. V., AND ZUCKER, J. I. 2000. Computable functions and semicomputable sets on many sorted algebras. In Handbook of Logic for Computer Science. Volume V: Logic and Semantical Methods, S. Abramsky, D. Gabbay, and T. Maibaum, Eds. Oxford University Press, Oxford, UK, pp. 317-523.
TUCKER, J. V., AND ZUCKER, J. I. 2002. Infinitary initial algebraic specifications for stream algebras. In Reflections on the Foundations of Mathematics: Essays in honour of Solomon Feferman, W. Sieg, R. Somer and C. Talcott, Eds. Lecture Notes in Logic, Vol. 15, Association for Symbolic Logic, pp. 234-253.
TUCKER, J. V., AND ZUCKER, J. I. 2004. Abstract versus concrete computation on metric partial algebras. ACM Trans. Computat. Logic 5, 4, 611-668.
TUCKER, J. V., AND ZUCKER, J. I. 2005. Computable total functions on metric algebras, universal algebraic specifications and dynamical systems. J. Alg. Logic Prog. 62, 71-108.
WECHLER, W. 1992. Universal algebra for computer scientists. EATCS Monographs in Computer Science. Springer-Verlag, New York.
VAN WIJNGAARDEN, A. 1966. Numerical analysis as an independent science. BIT 6, 68-81.
WIRSING, M. 1990. Algebraic specifications. In Handbook of Theoretical Computer Science. Volume B: Formal Models and Semantics, J. van Leeuwen, Ed. North-Holland, Amsterdam, The Netherland, pp. 675-788.

RECEIVED SEPTEMBER 2005; REVISED JANUARY 2007; ACCEPTED JANUARY 2007


[^0]:    Authors' addresses: J. A. Bergstra, University of Amsterdam, Informatics Institute, Kruislaan 403, 1098 SJ Amsterdam, The Netherlands, e-mail: janb@science.uva.nl; J. V. Tucker, Department of Computer Science, University of Wales Swansea, Singleton Park, Swansea, SA2 8PP, United Kingdom, e-mail: j.v.tucker@swansea.ac.uk.
    Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or direct commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.
    © 2007 ACM 0004-5411/2007/04-ART7 \$5.00 DOI 10.1145/1219092.1219095 http://doi.acm.org/ 10.1145/1219092.1219095

