

# The Rational Numbers as an Abstract Data Type<sup>1</sup>

J A Bergstra<sup>2</sup>

University of Amsterdam,  
Informatics Institute,  
Kruislaan 403,  
1098 SJ Amsterdam,  
The Netherlands

J V Tucker<sup>3</sup>

Department of Computer Science,  
University of Wales Swansea,  
Singleton Park,  
Swansea, SA2 8PP,  
United Kingdom

## Abstract

We give an equational specification of the field operations on the rational numbers under initial algebra semantics using just total functions 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 of L Moss. We also give a though axiomatic examination of the divisibility operator, in which some interesting new axioms and models are discovered, and equational specifications of some other algebras of rationals are given, including one with the modulus function. 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?

## 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

---

<sup>1</sup>To refer to this paper cite as one of the following: Research Report PRG0504, Programming Research Group, University of Amsterdam, August 2005 or Technical Report CSR12-2005, Department of Computer Science, University of Wales Swansea, August 2005.

<sup>2</sup>Email: janb@science.uva.nl

<sup>3</sup>Email: j.v.tucker@swansea.ac.uk

is denoted by  $n$  whole units and  $m$  subunits or, in this case,  $n\frac{m}{k} = \frac{(nk+m)}{k}$  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 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 operations we call here *rational arithmetics*. The algebra  $(\mathbb{Q}|0, 1, +, -, \cdot, ^{-1})$  is usually called the *field* of rational numbers when the operations satisfy certain axioms.

In this paper we will model some rational arithmetics, including the field, as abstract data types. 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.

Since the common rational arithmetics are computable algebras, they have various equational specifications under initial and final algebra semantics, according to our general theory of algebraic specifications of computable data types (e.g. Bergstra and Tucker [2, 3, 4, 5]). Computable rational arithmetics even have equational specifications that are also complete term rewriting systems ([5]). However, these general specification theorems for computable data types involve hidden functions and are based on equationally definable enumerations of data. Recently, in Moss [17], 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 [5], but is based on a remarkable enumeration theorem for the rationals in Calkin and Wilf [6]. He also gave specifications of enrichments of rational arithmetics with a modulus operator and with a floor.

In particular, 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 [17]. The equation  $0^{-1} = 0$  occurs in several other places as well (e.g. [12]). The 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 tough axiomatic examination of

the divisibility operator, in which some interesting new axioms and models are discovered, and related results on fields and other rational arithmetics.

The structure of the paper 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, one recursive 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 paper can be read as a sequel to Bergstra and Tucker [4, 5], which contains a literature survey and complementary results. With several unfamiliar axioms about the familiar inverse operator in action, care is needed in verifying equations and other formulae.

## 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: ADJ [9], Meseguer and Goguen [14], Wirsing [30], ...

The theory of algebraic specifications is based on theories of universal algebras (e.g., Wechler [28], Meinke and Tucker [13]), computable and semicomputable algebras (Stoltenberg-Hansen and Tucker [20]), and term rewriting (Klop [16], Terese [23]).

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  $Alg(\Sigma)$  and the class of all total  $\Sigma$ -algebras satisfying all the axioms in a theory  $T$  is  $Alg(\Sigma, T)$ . 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:  $\rightarrow$  field;
1:  $\rightarrow$  field;
+: field  $\times$  field  $\rightarrow$  field;
-: field  $\rightarrow$  field;
.: 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  $CR1, \dots, CR8$

etc.

**equations  $CR$**

$$(x + y) + z = x + (y + z) \quad (1)$$

$$x + y = y + x \quad (2)$$

$$x + 0 = x \quad (3)$$

$$x + (-x) = 0 \quad (4)$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (5)$$

$$x \cdot y = y \cdot x \quad (6)$$

$$x \cdot 1 = x \quad (7)$$

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad (8)$$

**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 in involving  $^{-1}$  *without any guards*, such as  $x \neq 0$ :

**equations  $SIP$**

$$(-x)^{-1} = -(x^{-1}) \quad (9)$$

$$(x \cdot y)^{-1} = x^{-1} \cdot y^{-1} \quad (10)$$

$$(x^{-1})^{-1} = x \quad (11)$$

**end**

The set  $CR \cup SIP$  of equations and its extensions are our basic object of study. We will also need other axioms, especially about  $^{-1}$ .

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

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

and the *axiom of separation (Sep)*

$$0 \neq 1.$$

*Guarded* versions of  $SIP$  - such as,  $x \neq 0 \implies (x^{-1})^{-1} = x$  - can be proved from Gil and Sep.

Later we will add to  $CR \cup SIP$  the *restricted inverse law (Ril)*,

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

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

## 2.3 Totalised Fields and Algebras satisfying the Specifications

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

$$T_{field} = CR \cup Gil \cup Sep.$$

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

Totality means that for all totalised fields  $A \in Alg(\Sigma, T_{field})$  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

$$0_A^{-1} \cdot 0_A \neq 1.$$

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.

Now, the axiomatic theory of fields is one of the central subjects of 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 [12], p. 695):

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

In fact, 0 is a common choice for the value of  $0^{-1}$ .

Our own interest will be in the specification  $CR \cup SIP$ . Shortly, we shall show that this specification of the rationals will force the choice of  $0^{-1} = 0$ .

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

$$Q_0 = (\mathbb{Q} | 0, 1, +, -, \cdot, ^{-1})$$

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  $T_{field}$  and is a totalised field of rationals.

Similarly, and more generally, we can define totalised fields  $Q_a$  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 CR:*

- (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:

$$\begin{array}{ll}
 0 + 0 = 0 & \text{by CR3} \\
 (0 + 0) \cdot x = 0 \cdot x & \text{multiplying both sides by } x \\
 0 \cdot x + 0 \cdot x = 0 \cdot x & \text{by CR8 and CR6} \\
 (0 \cdot x + 0 \cdot x) + (-(0 \cdot x)) = 0 \cdot x + (-(0 \cdot x)) & \text{adding to both sides} \\
 0 \cdot x + (0 \cdot x + (-(0 \cdot x))) = 0 & \text{by CR1 and CR4} \\
 0 \cdot x + 0 = 0 & \text{by CR4} \\
 0 \cdot x = 0 & \text{by CR3}
 \end{array}$$

(b) We calculate:

$$\begin{array}{ll}
 (-1) \cdot x = (-1) \cdot x + (x - x) & \text{by CR3 and CR4} \\
 = ((-1) \cdot x + (x \cdot 1)) - x & \text{by CR7 and CR1} \\
 = ((-1) \cdot x + (1 \cdot x)) - x & \text{by CR6} \\
 = ((-1) + 1) \cdot x - x & \text{by CR8} \\
 = (1 + (-1)) \cdot x - x & \text{by CR2} \\
 = 0 \cdot x - x & \text{by CR4} \\
 = 0 - x & \text{by this Lemma clause (a)} \\
 = -x & \text{by CR3}
 \end{array}$$

(c) We calculate:

$$\begin{array}{ll}
 (-x) \cdot y = ((-1) \cdot x) \cdot y & \text{by this Lemma clause (b)} \\
 = (-1) \cdot (x \cdot y) & \text{by CR5} \\
 = -(x \cdot y) & \text{by this Lemma clause (b)}
 \end{array}$$

(d) We calculate:

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

(e) We calculate:

$$\begin{aligned}
(-x) + (-y) &= 0 + ((-x) + (-y)) && \text{by CR3} \\
&= (-(x + y) + (x + y)) + ((-x) + (-y)) && \text{by CR3} \\
&= -(x + y) + ((x + -x) + (y + -y)) && \text{by CR1 and CR2} \\
&= -(x + y) + (0 + 0) && \text{by CR4} \\
&= -(x + y) + 0 && \text{by CR3} \\
&= -(x + y) && \text{by CR3}
\end{aligned}$$

(f) We calculate:

$$\begin{aligned}
-(-x) &= 0 + -(-x) && \text{by CR3} \\
&= (x + (-x)) + -(-x) && \text{by CR4} \\
&= x + ((-x) + -(-x)) && \text{by CR1} \\
&= x + 0 && \text{by CR3} \\
&= x && \text{by CR3}
\end{aligned}$$

□

We know from (a) that  $0 = 0 \cdot 0^{-1}$  is valid in a commutative ring. On adding the axioms *SIP* to *CR* we force a value for  $0^{-1}$ :

**Theorem 2.2.** *The following equation is provable from  $CR \cup SIP$ :*

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

*Proof.* First observe that:

$$\begin{aligned}
0 &= 0^{-1} + -(0^{-1}) && \text{by CR4} \\
&= 0^{-1} + (-0)^{-1} && \text{by SIP1} \\
&= 0^{-1} + 0^{-1} && \text{by Lemma 2.1(d)}
\end{aligned}$$

Now we calculate:

$$\begin{aligned}
0^{-1} &= (0^{-1} + 0^{-1})^{-1} && \text{by applying } ^{-1} \\
&= (1 \cdot 0^{-1} + 1 \cdot 0^{-1})^{-1} && \text{by CR6 and CR7} \\
&= ((1 + 1) \cdot 0^{-1})^{-1} && \text{by CR8} \\
&= (1 + 1)^{-1} \cdot (0^{-1})^{-1} && \text{by SIP2} \\
&= (1 + 1)^{-1} \cdot 0 && \text{by SIP3} \\
&= 0 && \text{by Lemma 2.1(a) and CR2}
\end{aligned}$$

□

## 2.5 Equational sub-theories of fields

One might ask: What is wrong with the unguarded equation  $x \cdot x^{-1} = 1$ ? It is easy to show that it contradicts Sep, i.e.,

$$CR \cup \{x \cdot x^{-1} = 1\} \vdash 0 = 1.$$

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

**Lemma 2.3.**  $CR \cup SIP \cup Ril \vdash u \cdot x \cdot y = u \implies u \cdot x \cdot x^{-1} = u$

*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) sub-theories of  $T_{field} = CR \cup Gip \cup Sep$ . First, we need this cancellation lemma:

**Lemma 2.4.**  $T_{field} \vdash x \cdot y = 1 \wedge x \cdot z = 1 \rightarrow y = z$ .

*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  $y = x^{-1} = z$ .  $\square$

**Lemma 2.5.**  $T_{field} \cup \{0^{-1} = 0\} \vdash SIP$  and  $T_{field} \cup \{0^{-1} = 0\} \vdash Ril$

*Proof.* Consider the three axioms of SIP in turn.

1.  $(-x)^{-1} = -(x^{-1})$ . If  $x = 0$  then the equation is true trivially. Suppose  $x \neq 0$  and so  $-x \neq 0$ . We calculate:

$$\begin{aligned} 1 &= (-x) \cdot (-x)^{-1} && \text{by Gip} \\ &= (-1 \cdot x) \cdot (-x)^{-1} && \text{by Lemma 2.1 (b)} \\ &= x \cdot -1 \cdot (-x)^{-1} && \text{by CR 6} \\ &= x \cdot -(-x)^{-1} && \text{by Lemma 2.1 (b).} \end{aligned}$$

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

$$\begin{aligned} x^{-1} &= -(-x)^{-1} && \text{by Cancellation Lemma 2.4} \\ -(x^{-1}) &= -(-(-x)^{-1}) && \text{by applying } - \\ &= (-x)^{-1} && \text{by Lemma 2.1 (f).} \end{aligned}$$

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 CR

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

Thus, by cancellation,  $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$ .

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

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

By cancellation,  $(x^{-1})^{-1} = x$ .

The derivation of Ril is obvious. □

Notice that for any closed equation,  $T_{field} \vdash t = s$  implies  $T_{field} \cup \{0^{-1} = 0\} \vdash t = s$ .

### 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  $0, 1, 1+1, (1+1)+1, \dots$  by  $0, \underline{1}, \underline{2}, \underline{3}, \dots$ . Now we define a set  $I$  of closed  $\Sigma$ -equations between numerals by

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

**Theorem 3.1.** *There exists a recursive equational initial algebra specification  $(\Sigma, CR \cup SIP \cup I)$ , without hidden functions, of the totalised field  $Q_0$  of rational numbers, i.e.*

$$T(\Sigma, CR \cup SIP \cup I) \cong Q_0.$$

*Proof.* First, note that, by inspection,

$$Q_0 \models CR \cup SIP \cup I.$$

By initiality, there exists a unique  $\Sigma$ -homomorphism  $\phi: T(\Sigma, CR \cup SIP \cup I) \rightarrow Q_0$ .

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:

$$\mathbb{Q} = \{0\} \cup \left\{ \frac{n}{m} \mid n > 0, m > 0, \gcd(n, m) = 1 \right\} \cup \left\{ -\frac{n}{m} \mid n > 0, m > 0, \gcd(n, m) = 1 \right\}.$$

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

**Lemma 3.2.** *The following hold:*

$$\begin{aligned}
\phi([0]) &= 0; \\
\phi([1]) &= 1; \\
\phi([\underline{n}]) &= n \\
\phi([\underline{n}^{-1}]) &= \frac{1}{n} \\
\phi([\underline{n} \cdot \underline{m}^{-1}]) &= \frac{n}{m}, \text{ providing } \gcd(n, m) = 1. \\
\phi([\underline{-(n \cdot m^{-1})}]) &= -\frac{n}{m}, \text{ providing } \gcd(n, m) = 1.
\end{aligned}$$

*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

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

where we use  $:$  to denote division on natural numbers. □

These observations suggest the following definition and lemma. Let

$$TR = \{0\} \cup \{\underline{n \cdot m^{-1}} | n > 0, m > 0, \gcd(n, m) = 1\} \cup \{\underline{-(n \cdot m^{-1})} | n > 0, m > 0, \gcd(n, m) = 1\}.$$

**Lemma 3.3.** *The set  $TR$  is a transversal for the equivalence relation  $\equiv_{CR \cup SIP \cup I}$ , i.e., 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

$$\phi([t]) = \phi([t']).$$

Then by Lemma 3.3 we know that  $[t] = [r]$  and  $[t'] = [r']$  for unique  $r, r' \in TR$ . Thus,

$$\phi([r]) = \phi([r'])$$

But, by Lemma 3.2, we know that  $\phi([r])$  and  $\phi([r'])$  have values in the normal form of  $\frac{n}{m}$ , or  $-\frac{n}{m}$  providing  $\gcd(n, m) = 1$  etc. This happens if, and only if,  $r = r'$  and hence if, and only if,  $[t] = [t']$ .

It remains to prove the Lemma 3.3.

*Proof.* Let  $E = CR \cup SIP \cup I$ . We have to show that:

- (1) for each closed term  $t \in T(\Sigma)$  there is some  $u \in TR$  such that  $E \vdash t = u$ ; and
- (2) for any closed terms  $k, l \in TR$ , 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  $TR$ . 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  $TR$ . We take the following subcase: suppose

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

Now,

$$\begin{aligned}
(\Sigma, E) &\vdash r \cdot s = \underline{n} \cdot \underline{m}^{-1} \cdot -(\underline{k} \cdot \underline{l}^{-1}) && \text{by substitution} \\
&\vdash r \cdot s = \underline{n} \cdot \underline{m}^{-1} \cdot (-1) \cdot (\underline{k} \cdot \underline{l}^{-1}) && \text{by CR6 and CR7} \\
&\vdash r \cdot s = (-1) \cdot \underline{n} \cdot \underline{m}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1} && \text{by CR8} \\
&\vdash r \cdot s = (-1) \cdot (\underline{n} \cdot \underline{k}) \cdot (\underline{m}^{-1} \cdot \underline{l}^{-1}) && \text{by SIP2} \\
&\vdash r \cdot s = (-1) \cdot (\underline{n} \cdot \underline{k}) \cdot (\underline{m} \cdot \underline{l})^{-1} && \text{by SIP3} \\
&\vdash r \cdot s = (-1) \cdot (\underline{n.k}) \cdot (\underline{m.l})^{-1} && \text{by SIP3} \\
&\vdash r \cdot s = -(\underline{n.k}) \cdot (\underline{m.l})^{-1} && \text{by SIP3}
\end{aligned}$$

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

$$\begin{aligned}
(\Sigma, E) &\vdash r \cdot s = -(\underline{u.p}) \cdot (\underline{u.q})^{-1} && \text{by definition} \\
&\vdash r \cdot s = -(\underline{u} \cdot \underline{p}) \cdot (\underline{u} \cdot \underline{q})^{-1} && \text{by Lemma 3.4} \\
&\vdash r \cdot s = -(\underline{u} \cdot \underline{u}^{-1})(\underline{p} \cdot \underline{q}^{-1}) && \text{by CR6 and SIP2} \\
&\vdash r \cdot s = -\underline{p} \cdot \underline{q}^{-1} && \text{by equations of I}
\end{aligned}$$

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

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

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

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  $CR \cup SIP \cup I$  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 abbreviation:

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

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

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

The operator  $Z$  is a definable auxiliary function 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. We define a special equation  $L$  (for Lagrange):

$$Z(1 + x^2 + y^2 + z^2 + u^2) = 0.$$

$L$  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 3.5.** *There exists a finite equational initial algebra specification, without hidden functions, of the totalised field  $Q_0$  of rational numbers; in particular,*

$$T(\Sigma, CR \cup SIP \cup L) \cong Q_0.$$

*Proof.* First, note that, by inspection,

$$Q_0 \models CR \cup SIP \cup L.$$

We know that  $CR$  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  $Q_0 \models x \neq 0 \implies x \cdot x^{-1} = 1$  we conclude that  $L$  is valid.

By initiality, there exists a unique  $\Sigma$ -homomorphism  $\phi: T(\Sigma, CR \cup SIP \cup L) \rightarrow Q_0$ .

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 subsection 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,

$$T(\Sigma, CR \cup SIP \cup L) \models CR \cup SIP \cup I$$

By initiality, there exists a unique  $\Sigma$ -homomorphism  $\phi: T(\Sigma, CR \cup SIP \cup I) \rightarrow T(\Sigma, CR \cup SIP \cup L)$ . But by Theorem 3.1,  $T(\Sigma, CR \cup SIP \cup I) \cong Q_0$  and so there is a  $\Sigma$ -homomorphism  $\psi: Q_0 \rightarrow T(\Sigma, CR \cup SIP \cup L)$ . By Lemma, we have  $\phi$  is a  $\Sigma$ -isomorphism with  $\psi$  as its inverse and  $T(\Sigma, CR \cup SIP \cup L) \cong Q_0$ . □

## 4 A simpler specification using the modulus function

Consider the algebra  $Q_0$  of rational numbers expanded with the modulus function  $|\cdot|$  and let this be denoted

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

We will give an equational specification of this algebra. The following two sets of equations can be added to  $CR + SIP$ . The first specifies the modulus operator on the rational numbers

**equations** *MOD*

$$|0| = 0 \tag{12}$$

$$|1| = 1 \tag{13}$$

$$|-x| = |x| \tag{14}$$

$$|x \cdot y| = |x| \cdot |y| \tag{15}$$

$$|x^{-1}| = (|x|)^{-1} \tag{16}$$

$$|1 + (|x|)| = 1 + |x| \tag{17}$$

**end**

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

**equations** *Modril*

$$Z(1 + |x|) = 0 \tag{18}$$

**end**

To get used to the axioms for  $|\cdot|$  we prove a simple lemma of use later:

**Lemma 4.1.** *For each  $k \in \mathbb{N}$ ,  $CR \cup Mod \vdash |k| = \underline{k}$ .*

*Proof.* By induction on  $k$ .

*Basis,  $k = 0$ :* We calculate:

$$\begin{aligned} |0| &= |0| && \text{by definition of } \underline{0} \\ &= 0 && \text{by 19 of } Mod \\ &= \underline{0} && \text{by definition of } \underline{0} \end{aligned}$$

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

$$\begin{aligned}
\underline{k+1} &= \underline{k} + 1 && \text{by definition of } \underline{k+1} \\
&= 1 + \underline{k} && \text{by commutativity CR2} \\
&= 1 + |\underline{k}| && \text{by induction hypothesis} \\
&= |1 + \underline{k}| && \text{by 24 of Mod} \\
&= |1 + \underline{k}| && \text{by induction hypothesis} \\
&= |\underline{k+1}| && \text{by CR2 and the definition of } \underline{k+1}
\end{aligned}$$

□

**Theorem 4.2.** *The initial algebra  $T(\Sigma \cup \{|\ |\}, CR + SIP + MOD + Modril)$  is isomorphic to the algebra  $Q_{0,|\ |}$  of rational numbers.*

*Proof.* The proof follows the pattern of earlier theorems (Theorems 3.1 and 3.5). For notational convenience, let

$$E = CR \cup SIP \cup Mod \cup Modril.$$

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

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

As  $Q_{0,|\ |}$  is  $\Sigma \cup \{|\ |\}$ -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

$$\mathbb{Q} = \{0\} \cup \left\{ \frac{n}{m} \mid n > 0, m > 0, \gcd(n, m) = 1 \right\} \cup \left\{ -\frac{n}{m} \mid n > 0, m > 0, \gcd(n, m) = 1 \right\}.$$

This suggests that we should use the previous transversal

$$TR = \{0\} \cup \{ \underline{n} \cdot \underline{m}^{-1} \mid n > 0, m > 0, \gcd(n, m) = 1 \} \cup \{ -(\underline{n} \cdot \underline{m}^{-1}) \mid n > 0, m > 0, \gcd(n, m) = 1 \}.$$

as a transversal for  $T(\Sigma \cup \{|\ |\}, E)$ . 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 generalise the numeral notation for the naturals to a notation for the rationals. For each  $r \in \mathbb{Q}$ , we define

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

Thus, with this notation,  $TR = \{\underline{r} \mid r \in \mathbb{Q}\}$ .

**Lemma 4.3.** *The  $\Sigma \cup \{|\ |\}$  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).  $\square$

**Lemma 4.4.** *The set  $TR$  is a transversal for the equivalence relation  $\equiv_E$  on  $T(\Sigma \cup \{|\})$ .*

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

$$\psi([t]) = \psi([t'])$$

then, by Lemma 4.4, there exist  $\underline{r}, \underline{r}' \in TR$  such that

$$E \vdash t = \underline{r} \text{ and } E \vdash t' = \underline{r}'$$

Thus,

$$\psi([\underline{r}]) = \psi([\underline{r}'])$$

Now, by Lemma 4.3,

$$\psi([\underline{r}]) = r \text{ and } \psi([\underline{r}']) = r'$$

Thus,

$$r = r'.$$

Since  $TR$  is a transversal, this happens if, and only if, the terms

$$\underline{r} = \underline{r}'$$

and hence  $[r] = [r']$  and  $[t] = [t']$ .

It remains to prove Lemma 4.4. We note the following.

**Lemma 4.5.**  $CR \cup Mod \cup Modril \vdash I$

*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  $CR \cup Mod \cup Modril \vdash Z(\underline{n}) = 0$ .

*Basis*  $n = 1$ . We calculate:

$$\begin{aligned} Z(\underline{1}) &= Z(\underline{1} + \underline{0}) && \text{by CR3 and the definition of } \underline{0} \\ &= Z(\underline{1} + |\underline{0}|) && \text{by 19 of } Mod \\ &= 0 && \text{by Modril} \end{aligned}$$

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

$$\begin{aligned} Z(\underline{k+1}) &= Z(\underline{k} + 1) && \text{by the definition of } \underline{k+1} \\ &= Z(1 + \underline{k}) && \text{by CR2} \\ &= Z(1 + |\underline{k}|) && \text{by Lemma 4.1} \\ &= 0 && \text{by Modril} \end{aligned}$$

□

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

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

*Basis.*  $Ht(t) = 0$ . Then  $t = 0$  or  $t = 1$  and we are done.

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

Case  $t = s + s'$ . By induction,

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

for  $\underline{r}, \underline{r}' \in TR$ . Thus,

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

Now  $\underline{r} + \underline{r}'$  does not contain  $|\$  and so reduces to some element in  $TR$ .

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 Mod 19.

If  $\underline{r} = \underline{n} \cdot \underline{m}^{-1}$  then

$$\begin{aligned} t &= |\underline{n} \cdot \underline{m}^{-1}| && \text{by definition} \\ &= |\underline{n}| \cdot |\underline{m}^{-1}| && \text{by Mod 22} \\ &= |\underline{n}| \cdot |\underline{m}|^{-1} && \text{by Mod 23} \\ &= \underline{n} \cdot \underline{m}^{-1} && \text{by Lemma ??} \end{aligned}$$

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

$$\begin{aligned} t &= |-(\underline{n} \cdot \underline{m}^{-1})| && \text{by the definition} \\ &= \underline{n} \cdot \underline{m}^{-1} && \text{by Mod 21} \end{aligned}$$

□

The specification CR + SIP + MOD + Mod + Ril of the rational numbers is simpler than the specification CR + SIP + L because it does not depend on (somewhat) sophisticated number theory.

## 5 Specifications of totalised fields and other rational arithmetics

### 5.1 On the equational theory of totalised fields

It has long been known that the class of totalised fields is not a variety, i.e., 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).

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  $CR + SIP + Sep + Gil$ .*

*Proof.* Assume the contrary and suppose that there is such a set of equations  $E$  such that  $Alg(\Sigma, E) = Alg(\Sigma, CR + SIP + Sep + Gil)$ . 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,  $I(\Sigma, E) \models CR + SIP + Sep + Gil$  and this implies

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

But the prime totalised field  $Z_2$  of characteristic 2 is also a model of  $CR + SIP + Sep + Gil$ . 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  $\psi(Z(1+1)) = Z(\psi(1+1)) = Z(\psi(1)+\psi(1)) = Z(1+1)$ . 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.  $\square$

Using a similar argument one can prove that *there is no conditional equational theory  $CE$  over the signature  $\Sigma$  of fields which is equivalent to  $CR + SIP + Sep + Gil$  in first order logic.*

### 5.2 The restricted inverse law

In the presence of  $CR + SIP$ , another way of writing *Ril* is

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

which expresses that  $x \cdot x^{-1}$  equals 1 in the presence of  $x$ . Yet another reformulation of *Ril*, is as follows:

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

We will now use the equational specification  $CR+SIP+Ril$ . If one restricts attention to the closed equations over  $\Sigma$  an interesting positive result is found.

Now  $Ril$  is derivable from  $CR+SIP+Sep+Gil$  and for that reason  $CR+SIP+Ril$  is a weaker theory than  $CR+SIP+Sep+Gil$ . Of course the key point is that  $CR+SIP+Ril$  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  $CR+SIP+Ril$ :

**Lemma 5.2.** *The following equations can be proved from  $CR+SIP+Ril$*

$$Z(0) = 1 \tag{19}$$

$$Z(1) = 0 \tag{20}$$

$$Z(x) \cdot Z(x) = Z(x) \tag{21}$$

$$(Z(x))^{-1} = Z(x) \tag{22}$$

$$(1 - Z(x)) \cdot (1 - Z(x)) = 1 - Z(x) \tag{23}$$

$$(1 - Z(x))^{-1} = 1 - Z(x) \tag{24}$$

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

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

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

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

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

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

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

□

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

$$CR \cup SIP \cup Ril \vdash Z(\underline{p}) \cdot Z(\underline{q}) = 0.$$

*Proof.* Let  $a, b \in \mathbb{Z}$  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  $Z(\underline{p}) \cdot (1 - \underline{q} \cdot \underline{q}^{-1}) = 0$  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*

$$CR + SIP + ril \vdash Z(\underline{p}) \cdot t = Z(\underline{p}) \cdot \underline{n}.$$

*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

$$\begin{aligned}
Z(\underline{p}) \cdot \underline{k} &= Z(\underline{p}) \cdot \underline{n + p \cdot l} && \text{by substitution} \\
&= Z(\underline{p}) \cdot \underline{n} + Z(\underline{p}) \cdot \underline{p \cdot l} && \text{by CR} \\
&= Z(\underline{p}) \cdot \underline{n} && \text{by Ril}
\end{aligned}$$

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

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

$$\begin{aligned}
Z(\underline{p}) \cdot \underline{t} &= Z(\underline{p}) \cdot r^{-1} && \text{by substitution} \\
&= Z(\underline{p}) \cdot Z(\underline{p}) \cdot r^{-1} && \text{by 14} \\
&= Z(\underline{p}) \cdot (Z(\underline{p}))^{-1} \cdot r^{-1} && \text{by 15} \\
&= Z(\underline{p}) \cdot (Z(\underline{p}) \cdot r)^{-1} && \text{by SIP} \\
&= Z(\underline{p}) \cdot (Z(\underline{p}) \cdot \underline{n})^{-1} && \text{by induction} \\
&= Z(\underline{p}) \cdot (Z(\underline{p}))^{-1} \cdot \underline{n}^{-1} && \text{by SIP} \\
&= Z(\underline{p}) \cdot \underline{n}^{-1} && \text{by substitution Lemma 5.2} \\
&= Z(\underline{p}) \cdot \underline{m} && \text{with } m < p \text{ such that } m = n^{-1} \pmod{p}
\end{aligned}$$

That the number  $\underline{n}$  is unique follows from an inspection of the prime field of characteristic  $p$ . In that field  $Z(\underline{p})$  equals 1 while different numerals  $\underline{n}_1$  and  $\underline{n}_2$  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  $val_p^0(t)$  the value of term  $t$  in the totalised field  $K_p^0$ . The unique number  $\underline{n}$  is  $\underline{val_p^0(t)}$ . There fore we have;*

$$CR + SIP + Ril \vdash Z(\underline{p}) \cdot t = Z(\underline{p}) \cdot \underline{val_p^0(t)}.$$

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

**Theorem 5.6.** *For any closed terms  $t, t' \in T(\Sigma)$ , we have*

$$T_{field}^0 \vdash t = t' \text{ implies } CR + SIP + Ril \vdash t = t'$$

Recall that if  $T_{field} \vdash t = t'$  then  $T_{field}^0 \vdash t = t'$ .

*Proof.* The proof is rather involved with many calculations needed to establish canonical forms. The canonical forms depend on the characteristics of the totalised 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:

$$G_1 = 1, G_2 = 1 - Z(\underline{p_1}), G_{n+1} = G_n \cdot (1 - Z(\underline{p_n})).$$

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, in particular, in the totalised field of rational numbers.

**Lemma 5.7.** *For all  $n$ , we have:*

- (i)  $G_n = 1 - Z(\underline{p_1}) - \dots - Z(\underline{p_{n-1}})$ .
- (ii)  $G_n \cdot Z(\underline{p_n}) = Z(\underline{p_n})$
- (iii) if  $n \leq m$  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.*

□

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  $\underline{r} \in TR$  such that  $CR + SIP + Ril \vdash G_n \cdot t = G_n \cdot \underline{r}$ .*

*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

$$CR + SIP + Ril \vdash G_n \cdot r = G_n \cdot r' \text{ and } CR + SIP + ril \vdash G_m \cdot s = G_m \cdot s'$$

with  $r', s' \in TR$ . Now there is a case distinction on the possible forms of  $r'$  and  $s'$ .

Let  $r' \equiv \underline{k} \cdot \underline{l}^{-1}$  and  $s' \equiv \underline{u} \cdot \underline{v}^{-1}$ . Take  $i$  larger than  $m$  and  $n$  such that  $p_i$  exceeds both  $l$  and  $v$ . Now  $CR+SIP+Ril$  proves

$$\begin{aligned} G_i \cdot t &= G_i \cdot (r + s) = G_i \cdot r + G_i \cdot s \\ &= G_i \cdot \underline{k} \cdot \underline{l}^{-1} + G_i \cdot \underline{u} \cdot \underline{v}^{-1} \\ &= G_i \cdot \underline{v} \cdot \underline{v}^{-1} \cdot \underline{k} \cdot \underline{l}^{-1} + G_i \cdot \underline{l} \cdot \underline{l}^{-1} \cdot \underline{u} \cdot \underline{v}^{-1} \\ &= G_i \cdot (\underline{v} \cdot \underline{k} \cdot \underline{v}^{-1} \cdot \underline{l}^{-1} + \underline{l} \cdot \underline{u} \cdot \underline{l}^{-1} \cdot \underline{v}^{-1}) \\ &= G_i \cdot (\underline{v} \cdot \underline{k} + \underline{l} \cdot \underline{u}) \cdot (\underline{l} \cdot \underline{v})^{-1} \\ &= G_i \cdot \underline{v} \cdot \underline{k} + \underline{l} \cdot \underline{u} \cdot (\underline{l} \cdot \underline{v})^{-1} \\ &= G_i \cdot \underline{k}' \cdot (\underline{l}')^{-1}. \end{aligned}$$

If  $k'$  and  $l'$  are not relatively prime they share a prime factor  $q = p_j$ . In particular:  $k' = q \cdot k''$  and  $l' = q \cdot l''$ . Let  $h = \max i, j$  then  $CR + SIP + ril \vdash G_i \cdot t = G_i \cdot \underline{k}'' \cdot \underline{l}''$ . 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*

$$CR + SIP + Ril \vdash G_n \cdot t = G_n \cdot \underline{val}_0^0(t)$$

*Then for all  $m > n$ ,*

$$CR + SIP + Ril \vdash t = \sum_{i=1}^{m-1} Z(\underline{p}_i) \cdot \underline{val}_{p_i}^0(t) + G_m \cdot \underline{val}_0^0(t)$$

*Proof.* We begin with a lemma.

**Lemma 5.10.** *For each  $n \in \mathbb{N}$ ,*

$$CR + SIP + Ril \vdash G_n \cdot t = Z(\underline{p}_n) \cdot \underline{val}_{p_n}^0(t) + G_{n+1} \cdot t$$

*Proof.* This is a a calculation:

$$\begin{aligned}
G_n \cdot t &= (Z(\underline{p}_n) + (1 - Z(\underline{p}_n))) \cdot G_n \cdot t && \text{by CR} \\
&= Z(\underline{p}_n) \cdot G_n \cdot t + (1 - Z(\underline{p}_n)) \cdot G_n \cdot t && \text{by CR} \\
&= Z(\underline{p}_n) \cdot G_n \cdot t + G_{n+1} \cdot t && \text{by definition} \\
&= G_n \cdot Z(\underline{p}_n) \cdot t + G_{n+1} \cdot t && \text{by CR} \\
&= G_n \cdot Z(\underline{p}_n) \cdot \underline{val_{p_n}^0(t)} + G_{n+1} \cdot t && \text{by Corollary 5.5} \\
&= Z(\underline{p}_n) \cdot \underline{val_{p_n}^0(t)} + G_{n+1} \cdot t && \text{by Lemma 5.7}
\end{aligned}$$

□

Now we choose  $k \in \mathbb{N}$  such that  $CR + SIP + Ril \vdash G_k \cdot t = G_k \cdot \underline{r}$  for some  $\underline{r} \in TR$ . Then we may expand the fomula as follows:

$$\begin{aligned}
t &= G_1 \cdot t && \text{because } G_1 = 1 \text{ and CR} \\
&= Z(\underline{p}_1) \cdot \underline{val_{p_1}^0(t)} + G_2 \cdot t && \text{by Lemma 5.10} \\
&= Z(\underline{p}_1) \cdot \underline{val_{p_1}^0(t)} + Z(\underline{p}_2) \cdot \underline{val_{p_2}^0(t)} + G_3 \cdot t && \text{by Lemma 5.10} \\
&= Z(\underline{p}_1) \cdot \underline{val_{p_1}^0(t)} + \dots + Z(\underline{p}_{k-1}) \cdot \underline{val_{p_{k-1}}^0(t)} + G_k \cdot t && \text{by repeated use of Lemma 5.10} \\
&= Z(\underline{p}_1) \cdot \underline{val_{p_1}^0(t)} + \dots + Z(\underline{p}_{k-1}) \cdot \underline{val_{p_{k-1}}^0(t)} + G_k \cdot \underline{r} && \text{by choice of } k
\end{aligned}$$

This completes the proof of the Lemma 5.9

□

Finally, we can complete the proof of Theorem 5.6. Assume that

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

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

$$\begin{aligned}
CR + SIP + Ril \vdash G_n \cdot t &= G_n \cdot \underline{val_0^0(t)} \\
CR + SIP + Ril \vdash G_m \cdot s &= G_m \cdot \underline{val_0^0(s)}
\end{aligned}$$

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

$$\begin{aligned}
CR + SIP + Ril \vdash t &= \sum_{i=1}^k Z(\underline{p}_i) \cdot \underline{val_{p_i}^0(t)} + G_k \cdot \underline{val_0^0(t)} \\
CR + SIP + Ril \vdash s &= \sum_{i=1}^k Z(\underline{p}_i) \cdot \underline{val_{p_i}^0(s)} + G_k \cdot \underline{val_0^0(s)}
\end{aligned}$$

Since  $T_{field}^0 \vdash t = s$ , the values of these closed terms in all prime fields are identical, i.e., for all  $p_i$ ,  $val_{p_i}^0(t) = val_{p_i}^0(s)$  and  $val_0^0(t) = val_0^0(s)$ . Thus, the expansions on the RHS are identical and so we have

$$CR + SIP + Ril \vdash t = s$$

□

The initial algebra of CR is the integers. However, we note that

**Lemma 5.11.** *The initial algebra of  $CR + SIP + Ril$  is a computable algebra but it is not an integral domain.*

*Proof.* It is easy to check that this completeness proof for closed term equations also provides the decidability of their derivability. Let  $x = Z(2)$  and let  $y = 1 - Z(2)$ . The both are not equal to 0 because  $x \neq 0$  in the rational numbers and  $y \neq 0$  in the prime field with characteristic 0. But  $CR + SIP + ril \vdash Z(2) \cdot (1 - Z(2)) = Z(2) - Z(2) \cdot Z(2) = Z(2) - Z(2) = 0$ .  $\square$

It may be useful to have a name for models of  $CR + SIP + Ril$  as these algebras have nice properties, in spite of not being fields nor even integral domains. We have the following proposal:

**Definition 5.12.** *A model of  $CR + SIP + Ril$  is called a meadow.*

All fields are clearly meadows but not conversely (as the initial algebra is not a field). In fact, the theorem proves a normal form theorem for meadows.

## 6 Concluding remarks

### 6.1 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 totalised 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 totalised field  $Q_0$  have a finite basis, i.e., 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 [5] that there exists such a specification with hidden functions.

The following obvious problems remain unsettled at this stage to the best of our knowledge.

Equations over  $Q_0$  are called *diophantine equations*, just as the equations over the integers to which they are intimately connected. We do not know the answer to this question:

**Problem 6.4.** *Does the totalised field  $Q_0$  of rational numbers have a decidable diophantine theory, i.e., can one decide whether or not  $\exists x_1, \dots, x_n [t_1(x_1, \dots, x_n) = t_2(x_1, \dots, x_n)]$ ?*

If the diophantine theory of the totalised 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.

Further problems are these.

**Problem 6.5.** *Is the set of equational consequences of CR + SIP + Sep + Gil decidable?*

**Problem 6.6.** *Is the set of equational consequences of CR + SIP + Sep + Gil derivable from a finite subset (i.e. is it finitely based)? In particular, CR + SIP + Ril might be a complete subset (which we have not been able to refute).*

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

**Problem 6.7.** *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  $cc$  as an auxiliary function: one adds to CR + SIP:

**equations** *CompRat*

$$cc(1) = 1 \tag{25}$$

$$cc(i) = -i \tag{26}$$

$$cc(x + y) = cc(x) + cc(y) \tag{27}$$

$$cc(x \cdot y) = cc(x) \cdot cc(y) \tag{28}$$

$$cc(-x) = -cc(x) \tag{29}$$

$$cc(x^{-1}) = (cc(x))^{-1} \tag{30}$$

$$0 = Z(1 + x \cdot cc(x) + y \cdot cc(y) + z \cdot cc(z) + u \cdot cc(u)) \tag{31}$$

**end**

In the matter of term rewriting, we do not know the answer to this question.

**Problem 6.8.** *Is there a finite equational specification of the algebra  $Q_0(i, cc)$ , (without further hidden functions), which constitutes a complete term rewriting system?*

## 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 6.9.** *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 as computation, specification and verification on continuous data are all active research areas. 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 [29]. In Roggenbach, Schroder and Mossakowski [18] there is an axiomatisation designed for the algebraic specification language CASL. In [25] 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 [27], 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 [26] for the compact case and [27] for the general case). There are many notions of computable function on the real numbers: see [24].

Obviously, technically, the specification theory of rational arithmetics is 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 processes of measuring to arbitrary accuracy*, the processes being modelled by Cauchy sequences.

Our specification  $CR \cup SIP$  draws attention to division by zero. Division by zero has been studied by Setzer [19] in which he proposed the concept of *wheels*, a sophisticated modification of integral domains with infinite, undefined and division by zero  $0^{-1} = \infty$ .

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. [1].

The problem is connected to many others (e.g., the algebraic approach to numerical software for scientific simulation in Haveraaen [10, 11]) or algebras for 3D and 4D volume graphics in Chen and Tucker [7]. In fact, it is a common view that the problem of integrating discrete and continuous computation is a barrier to progress in computer science and its application.

## References

- [1] J. ADAMEK, M. HEBERT AND J. ROSICKY On abstract data types presented by multi-equations *Theoretical Computer Science* 275 (2002) 427 - 462
- [2] J A BERGSTRA AND J V TUCKER, The completeness of the algebraic specification methods for data types, *Information and Control*, 54 (1982) 186-200
- [3] J A BERGSTRA AND J V TUCKER, Initial and final algebra semantics for data type specifications: two characterisation theorems, *SIAM Journal on Computing*, 12 (1983) 366-387.
- [4] J A BERGSTRA AND J V TUCKER, Algebraic specifications of computable and semicomputable data types, *Theoretical Computer Science*, 50 (1987) 137-181.

- [5] J A BERGSTRA AND J V TUCKER, Equational specifications, complete term rewriting systems, and computable and semicomputable algebras, *Journal of ACM*, 42 (1995) 1194-1230.
- [6] N CALKIN AND H S WILF, Recounting the rationals, *American Mathematical Monthly*, 107 (2000) 360-363.
- [7] M CHEN AND J V TUCKER, Constructive volume geometry, *Computer Graphics Forum*, 19 (2000) 281-293.
- [8] E CONTEJEAN, C MARCHE AND L RABEHASAINA, Rewrite systems for natural, integral, and rational arithmetic, in *Rewriting Techniques and Applications 1997*, Springer Lecture Notes in Computer Science 1232, 98-112, Springer, Berlin,1997.
- [9] J A GOGUEN, J W THATCHER AND E G WAGNER, An initial algebra approach to the specification, correctness and implementation of abstract data types, in R.T Yeh (ed.) *Current trends in programming methodology. IV. Data structuring*, Prentice-Hall, Engelwood Cliffs, New Jersey, 1978, pp 80-149.
- [10] M HAVERAAEN, Case study on algebraic software methodologies for scientific computing, *Scientific Programming* 8 (2000) 261-273.
- [11] M HAVERAAEN, H A FRIIS AND H MUNTHE-KAAS, Computable scalar fields: A basis for PDE software, *Journal of Logic and Algebraic Programming*, 65 (2005) 36-49.
- [12] W HODGES, *Model Theory*, Cambridge University Press, Cambridge, 1993.
- [13] K MEINKE AND J V TUCKER, Universal algebra, in S. Abramsky, D. Gabbay and T Maibaum (eds.) *Handbook of Logic in Computer Science. Volume I: Mathematical Structures*, Oxford University Press, 1992, pp.189-411.
- [14] J MESEGUER AND J A GOGUEN, Initiality, induction and computability, in M Nivat and J Reynolds (eds.), *Algebraic methods in semantics*, Cambridge University Press, Cambridge, 1985, pp.459-541.
- [15] J MESEGUER, L MOSS, AND J A GOGUEN, Final algebras, cosemicomputable algebras, and degrees of unsolvability, *Theoretical Computer Science* 100 (1992) 267-302.
- [16] J W KLOP, Term rewriting systems, in S. Abramsky, D. Gabbay and T Maibaum (eds.) *Handbook of Logic in Computer Science. Volume 2: Mathematical Structures*, Oxford University Press, 1992, pp.1-116.
- [17] L MOSS, Simple equational specifications of rational arithmetic, *Discrete Mathematics and Theoretical Computer Science*, 4 (2001) 291-300.
- [18] M ROGGENBACH, L SCHRODER AND T MOSSAKOWSKI, Specifying Real Numbers in CASL, in D Bert, C Choppy, P D Mosses (eds.) *Recent Trends in Algebraic Development Techniques: 14th International Workshop, WADT '99, Chateau de Bonas, September 15-18, 1999 Selected Papers*, Springer Lecture Notes in Computer Science 1827, 146-161, Springer, Berlin, 2004.

- [19] A SETZER, Wheels, Manuscript, 8pp, 1997. Down load at: <http://www.cs.swan.ac.uk/csetzer>.
- [20] V STOLTENBERG-HANSEN AND J V TUCKER, Effective algebras, in S Abramsky, D Gabbay and T Maibaum (eds.) *Handbook of Logic in Computer Science. Volume IV: Semantic Modelling*, Oxford University Press, 1995, pp.357-526.
- [21] V STOLTENBERG-HANSEN AND J V TUCKER, Computable rings and fields, in E Griffor (ed.), *Handbook of Computability Theory*, Elsevier, 1999, pp.363-447.
- [22] V STOLTENBERG-HANSEN AND J V TUCKER, Concrete models of computation for topological algebras, *Theoretical Computer Science* 219 (1999), 347 – 378.
- [23] TERESE, *Term Rewriting Systems*, Cambridge Tracts in Theoretical Computer Science 55, Cambridge University Press, Cambridge, 2003.
- [24] J V TUCKER AND J I ZUCKER, Computable functions and semicomputable sets on many sorted algebras, in S. Abramsky, D. Gabbay and T Maibaum (eds.), *Handbook of Logic for Computer Science* volume V, Oxford University Press, 2000, 317 – 523.
- [25] J V TUCKER AND J I ZUCKER, Infinitary initial algebraic specifications for stream algebras, in W Sieg, R Somer, C Talcott (editors), *Reflections on the foundations of mathematics: Essays in honour of Solomon Feferman*, Lecture Notes in Logic, volume 15, Association for Symbolic Logic, 2002, 234-253.
- [26] J V TUCKER AND J I ZUCKER, Abstract versus concrete computation on metric partial algebras, *ACM Transactions on Computational Logic*, 5 (4) (2004) 611-668.
- [27] J V TUCKER AND J I ZUCKER, Computable total functions on metric algebras, universal algebraic specifications and dynamical systems, *Journal of Algebraic and Logic Programming*, 62 (2005) 71-108
- [28] W WECHLER, *Universal algebra for computer scientists*, EATCS Monographs in Computer Science, Springer, 1992.
- [29] A VAN WIJNGAARDEN, Numerical analysis as an independent science, *BIT* 6 (1966) 68-81.
- [30] M WIRSING, Algebraic specifications, in J van Leeuwen (ed.), *Handbook of Theoretical Computer Science. Volume B: Formal models and semantics*, North-Holland, 1990, pp 675-788.