A negative result on algebraic specifications of the meadow of rational numbers

Jan A. Bergstra & Inge Bethke

January 25, 2016

Abstract

$\mathbb{Q}_0$—the involutive meadow of the rational numbers—is the zero-totalized expansion field of the rational numbers where the multiplicative inverse operation is made total by imposing $0^{-1} = 0$. In this note, we prove that $\mathbb{Q}_0$ cannot be specified by the usual axioms for meadows augmented by a finite set of axioms of the form $(1 + \cdots + 1 + x^2) \cdot (1 + \cdots + 1 + x^2)^{-1} = 1$.

1 Introduction

This note contributes to the algebraic datatype specification of $\mathbb{Q}_0$—the rational numbers equipped with a total inverse operation. Advantages and disadvantages of dividing by zero in various ways have been amply discussed in the mathematics and logic literature (see e.g. [7, 9]) and we do not wish to add to those matters here. The same holds for issues regarding the origins of various approaches to division by zero. But we believe that the observation made in [4] that $\mathbb{Q}_0$ has a finite initial algebra specification was at that time original. Here we elaborate on this theme.

In [4] it is shown that

$$\mathbb{Q}_0 \cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + L_4)$$

where $\mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + L_4)$ is the initial algebra of the theory Md of meadows given in Table 1 enriched with the axiom L_4 given in Table 2 for $n = 4$. The characterization above has been sharpened in [3] where it is shown that

$$\mathbb{Q}_0 \cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + L_2). \tag{‡}$$

In [1] it is proved that every finite specification of $\mathbb{Q}_0$ can be given in the form $\mathsf{Md} + e$—the meadow axioms enriched with a single equation. Moreover, observe that both L_4 and L_2 do not hold in the presence of the imaginary unit i. In general, every finite algebraic specification of $\mathbb{Q}_0$ contains an equation not valid in $\mathbb{C}_0$—the zero-totalized expansion field of the complex numbers. Again, this is proved in [1].

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

Table 1: The set Md of axioms for meadows

$$(1+x_1^2+\cdots+x_n^2)\cdot(1+x_1^2+\cdots+x_n^2)^{-1}=1 \quad (L_n)$$

Table 2: The axiom schema L_n

In the sequel we denote by $(\mathbb{Z}/p\mathbb{Z})_0$ the zero-totalized expansion of the finite prime field of order p. Moreover, we define for $n \in \mathbb{N}$ the numerals $\underline{n}$ by $\underline{0} := 0$ and $\underline{n+1} := \underline{n}+1$. A necessary and sufficient condition for an initial algebra specification of $\mathbb{Q}_0$ is given in the following theorem.

Theorem 1. *Let E be a set of meadow equations. Then*

$$\mathbb{Q}_0 \cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md}+E) \textit{ if and only if for all prime numbers } p,\ (\mathbb{Z}/p\mathbb{Z})_0 \not\models E.$$

Proof: Assume $\mathbb{Q}_0 \cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md}+E)$. Then $\mathsf{Md}+E \vdash \underline{p}\cdot\underline{p}^{-1} = 1$ for all prime numbers p. Hence $(\mathbb{Z}/p\mathbb{Z})_0 \not\models E$ for all primes p. For the converse, assume $(\mathbb{Z}/p\mathbb{Z})_0 \not\models E$ for all primes p. Recall that every minimal meadow is a subdirect product of minimal zero-totalized expansion fields (see e.g. [5]). The minimal zero-totalized expansion fields are the zero-totalized prime fields $(\mathbb{Z}/p\mathbb{Z})_0$ and $\mathbb{Q}_0$. In particular, the initial algebra of $\mathsf{Md}+E$ is such a subdirect product. Since every $\mathbb{Z}/p\mathbb{Z}_0$ is not a model of E, it follows that $\mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md}+E)$ must be isomorphic to $\mathbb{Q}_0$. □

An application of this theorem yielding a positive result is given below. First we recall a few facts from the theory of numbers (see e.g. [6], Ch. 3). For every odd prime p one of the two congruences $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$ hold. Given a prime p and a natural number $0 < n < p$, n is called a *quadratic residue* of p if there exists a natural number x such that $x^2 \equiv n \mod p$. If the congruence is insoluble, n is said to be a *quadratic non-residue.* Every prime p has quadratic residues since $1^2 \equiv 1 \mod p$, but for $p > 3$ there are more: e.g. if $p = 19$, the quadratic residues are 1, 4, 5, 6, 7, 9, 11, 16 and 17. In general, every odd prime p

has $\frac{p-1}{2}$ quadratic residues. If $p \equiv 1 \mod 4$ then the lists of quadratic residues and quadratic non-residues are both symmetrical in the sense that if n is a (non-)quadratic residue then $p-n$ is one. On the other hand, if $p \equiv 3 \mod 4$, then n is a quadratic residue if and only if $p-n$ is a quadratic non-residue (see e.g. the case of $p = 19$). The quadratic residues and non-residues have a simple *multiplicative property*: the product of two residues or of two non-residues is a residue.

Example. There also exist finite initial algebra specifications of $\mathbb{Q}_0$ of the form $\mathsf{Md}+e$ where e is a single variable equation. Consider the equation $f(x) \cdot f(x)^{-1} = 1$ where $f(x) = (x^2-2)(x^2-3)(x^2-6)$. Inspection shows that $f(x)$ has no rational root. Thus $\mathbb{Q}_0 \models f(x) \cdot f(x)^{-1} = 1$. On the other hand, $f(x)$ has a root modulo every prime number p:

- If $p = 2$ then $f(x)$ has a root modulo p for $x = 0$.
- If $p > 2$ we apply the multiplicative property of quadratic residues and non-residues. If (x^2-2) or (x^2-3) have a root modulo p, then $f(x)$ has a root modulo p. If neither (x^2-2) nor (x^2-3) has a root modulo p then both 2 and 3 are non-residues of p. Hence 6 is a residue of p, i.e. (x^2-6) has a root modulo p and thus $f(x)$ has a root modulo p.

It follows that $(\mathbb{Z}/p\mathbb{Z})_0 \not\models f(x) \cdot f(x)^{-1} = 1$ for every prime number p. By the above theorem we may conclude that $\mathsf{Md} + f(x) \cdot f(x)^{-1} = 1$ is an initial algebra specification of $\mathbb{Q}_0$.

In the next section we apply Theorem 1 in order to give a negative result.

2 A negative result

A general question concerning the specification of the rationals is whether there exists a logical weakest initial algebra specification. In this section we show that the weakening from L_4 to L_2 cannot be prolonged in a straightforward way.

$$\begin{aligned} (1+\underline{n}+x^2) \cdot (1+\underline{n}+x^2)^{-1} &= 1 \quad (H_n) \\ (1+\underline{n}) \cdot (1+\underline{n})^{-1} &= 1 \quad (C_n) \end{aligned}$$

Table 3: The axiom schemas H_n and C_n

Substituting 0 for x in H_n in Table 3, we obtain the axiom C_n. In [4] it is proved that $\{C_n \mid n \in \mathbb{N}\}$ together with Md specify the rational numbers. The question then arises whether $\mathbb{Q}_0$ can be specified by $\mathsf{Md} + \Gamma$ for some finite subset $\Gamma \subset \{H_n \mid n \in \mathbb{N}\}$. We give a negative answer below.

Consider the function $f : \mathbb{N} \to \mathbb{N}$ defined by

$$f(n) = \begin{cases} 0 & \text{if } n \leq 1 \text{ or } n \text{ is composite,} \\ n - max\{i \mid i \text{ is a quadratic residue of } n\} & \text{if } n \text{ is prime.} \end{cases}$$

E.g. $f(19) = 2$. In [8], a table for the values of $f(n)$ can be found for the first 10^5 natural numbers (see entry A088192). The occurring values increase very slowly: the largest value found in that table is 43.

In [10], Wright proved the following theorem (see Theorem 2.3).

Theorem 2. *Every nonempty finite subset of $\mathbb{N}^+$ is a set of quadratic residues for infinitely many primes.*

As a corollary we obtain that the function f is unbounded.

Corollary 1. *f is unbounded.*

Proof: For $n \in \mathbb{N}$ with $n > 2$ consider the set $A = \{1, 2, 3, \ldots, n\}$. By the previous theorem we can pick a prime p such that every element of A is a quadratic residue of p. In particular, 2 is a quadratic residue of p. It follows from Gauss's lemma that $p \equiv 7 \mod 8$ and hence $p \equiv 3 \mod 4$. Thus, since $1, 2, 3, \ldots, n$ are all quadratic residues, $p-1, p-2, p-3, \ldots, p-n$ are all quadratic non-residues. So $max\{i \mid i \text{ is a quadratic residue of } p\} < p - n$. Therefore $f(p) > n$. □

We now prove that for every finite $\Gamma \subset \{H_n \mid n \in \mathbb{N}\}$ there exists a prime p with $(\mathbb{Z}/p\mathbb{Z})_0 \models \Gamma$.

Proposition 1. *Let $\Gamma \subset \{H_n \mid n \in \mathbb{N}\}$ be finite. Then there exists a prime p such that $(\mathbb{Z}/p\mathbb{Z})_0 \models \Gamma$.*

Proof: Say $\Gamma = \{H_0, \ldots, H_n\}$. Pick a prime p such that $f(p) > n+1$. Suppose $(\mathbb{Z}/p\mathbb{Z})_0 \not\models H_m$ for some $0 \leq m \leq n$. We derive a contradiction as follows. By the assumption, there exists $0 \leq x < p$ with $1 + m + x^2 = 0$, i.e. $x^2 \equiv p - (m+1) \mod p$. Hence $p - (m+1)$ is a quadratic residue of p. Therefore $p - (m+1) \leq max\{i \mid i \text{ is a quadratic residue of } p\}$ and hence

$$m+1 = p-(p-(m+1)) \geq p - max\{i \mid i \text{ is a quadratic residue of } p\} = f(p) > n+1 \geq m+1. \quad \square$$

We can now show that $\mathbb{Q}_0$ cannot be specified by a finite set of H_n-axioms.

Theorem 3. *Let $\Gamma \subset \{H_n \mid n \in \mathbb{N}\}$ be finite. Then $\mathbb{Q}_0 \not\cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + \Gamma)$.*

Proof: Immediately by the preceding proposition and Theorem 1. □

Corollary 2. $\mathbb{Q}_0 \not\cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + L_1)$

Remark: Observe that $\mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + L_1)$ is a non-cancellation meadow of characteristic 0 which does not contain $\mathbb{Q}_0$ as a subalgebra since $\mathbb{Q}_0 \not\cong \mathcal{I}(\Sigma_{\mathsf{Md}}, \mathsf{Md} + L_1)$. The existence of such a structure has already been proved in [2] (see Theorem 2.1). However, the proof given there relies on the compactness theorem.

3 An open question

Open questions arise when we extend the rational numbers. E.g. consider the meadow of Gaussian rationals—denoted $\mathbb{Q}_0(i)$—obtained by adjoining the imaginary number i to the meadow of rationals. It is not difficult to see that the polynomial given in the example in Section 1 also yields an initial algebra specification of the Gaussian rationals. Since $f(x) = (x^2-2)(x^2-3)(x^2-6)$ has only real roots, there exist no complex rational ones. It follows that $\mathbb{Q}_0(i) \models f(x) \cdot f(x)^{-1} = 1$. Moreover, working in $\mathsf{Md} + \{i^2 + 1 = 0\}$ it can be shown that every closed term over $\Sigma_{\mathsf{Md}} \cup \{i\}$ is provable equal to a term of the form $l \cdot m^{-1} + p \cdot q^{-1} \cdot i$ where l, m, p, q are numerals. Hence $\mathsf{Md} + \{f(x) \cdot f(x)^{-1} = 1, i^2 + 1 = 0\}$ yields an initial algebra specification of $\mathbb{Q}_0(i)$.

Up to isomorphism, there exists only one simple extension of the rational numbers generated by a transcendental number t. We are unable to prove or disprove the existence of a finite initial algebra specification of $\mathbb{Q}_0(t)$ with t a new constant interpreted as a trancendental element.

Acknowledgement: We are indebted to Rob Tijdeman for valuable discussions including a proposal for proving Corollary 1 and the suggestion to make use of [10].

References

[1] Bergstra, J.A. and Bethke, I. (2015). *Subvarieties of the variety of meadows.* `arXiv: 1510.0402` [math.RA].

[2] Bergstra, J.A., Bethke, I. and Ponse, A. (2015). Equations for formally real meadows. *Journal of Applied Logic*, 13(2):1–23.

[3] Bergstra, J.A. and Middelburg, C.A. (2011). Inversive meadows and divisive meadows. *Journal of Applied Logic*, 9(3):203–220.

[4] Bergstra, J.A. and Tucker, J.V. (2007). The rational numbers as an abstract data type. *Journal of the ACM*, 54(2), Article 7.

[5] Bethke, I. and Rodenburg, P. (2010). The initial meadows. *Journal of Symbolic Logic*, 75(3): 888–895.

[6] Davenport, H. (1952). *The Higher Arithmetic*, Cambridge University Press.

[7] Komori, Y. (1975). Free algebras over all fields and pseudo-fields. Report 10, pp. 9 - 15, Faculty of Science, Shizuoka University, Japan.

[8] *The on-line encyclopedia of integer sequences.* `http://oeis.org`

[9] Ono, H. (1983). Equational theories and universal theories of fields. *J. Math. Soc. Japan*, 35:289–306.

[10] Wright, S. (2007). Patterns of quadratic residues and nonresidues for infinitely many primes. *Journal of Number Theory*, 123:120–132.